16(3-A), pp.302-416, 2018 **ISSN 1334-4684**

INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS

Scientific Journal

A. Nemes, G. Mester and T. Mester	302	A Soft Computing Method for Efficient Modelling of Smart Cities Noise Pollution
M. Kiss and L. Muha	313	The Cybersecurity Capability Aspects of Smart Government and Industry 4.0 Programmes
A. Szabó, E. Szűcs and T. Berek	320	Illustrating Training Opportunities Related to Manpower Facility Protection through the Example of Máv Co.
A. Albini, D. Tokody and Z. Rajnai	327	The Categorization and Information Technology Security of Automated Vehicles
P.M. Hell and P.J. Varga	333	Accurate Radiofrequency Identification Tracking in Smart City Railways by Using Drones
G. Liebmann, L. Hanka and G. Schuster	342	Probabilistic Approach and Fuzzy System Based Support of the Railway Stations' Smart Security System
D. Simonyi and T. Kovács	350	Brain-Computer Interface-Based Feasibility of Entering Customer Code on Ticket Vending Machines
G.K. Kiss Leizer	360	Possible Areas of Application of Drones in Waste Management during Rail Accidents and Disasters
J.I. Mezei and K. Lazányi	369	Are We Ready for Smart Transport? Analysis of Attitude Towards Public Transport in Budapest
P. Holicza and E. Kadëna	376	Smart and Secure? Millennials on Mobile Devices

(continued on the back cover)

Scientific Journal
INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS

INDECS, volume 16, issue 3, part A, pages 302-416, year 2018
Published 28th September 2018 in Zagreb, Croatia
Released online 30th September 2018

Office

Croatian Interdisciplinary Society
c/o Faculty of Mechanical Engineering & Naval Architecture
I. Lučića 1, HR – 10 000 Zagreb, Croatia
E-mails: editor@indecs.eu (for journal), ured@idd.hr (for publisher)

Editors

Josip Stepanić, Editor-in-Chief, University of Zagreb, Zagreb (HR)
Josip Kasač, Assistant Editor, University of Zagreb, Zagreb (HR)
Mirjana Pejić Bach, Assistant Editor, University of Zagreb, Zagreb (HR)

Advisory Board

Vjekoslav Afrić, University of Zagreb, Zagreb (HR)
Aleksa Bjeliš, University of Zagreb, Zagreb (HR)
Marek Frankowicz, Jagiellonian University, Krakow (PL)
Katalin Martinás, Eötvös Loránd University, Budapest (HU)
Gyula Mester, University of Szeged, Szeged (HU)
Dietmar Meyer, Budapest University of Technology and Economy, Budapest (HU)
Sibila Petlevski, University of Zagreb, Zagreb (HR)
Wei-bin Zhang, Ritsumeikan Asia Pacific University, Beppu (JP)

Editorial Board

Serghey A. Amelkin, Program Systems Institute, Pereslavl-Zalesskij (RU)
Željko Božić, University of Zagreb, Zagreb (HR)
Nikša Dubreta, University of Zagreb, Zagreb (HR)
Robert Fabac, University of Zagreb, Varaždin (HR)
Erik W. Johnston, Arizona State University, Phoenix (US)
Urban Kordeš, University of Ljubljana, Ljubljana (SI)
Dean Korošak, University of Maribor, Maribor (SI)
Anita Lee-Post, University of Kentucky, Lexington (US)
Olga Markič, University of Ljubljana, Ljubljana (SI)
Damir Pajić, University of Zagreb, Zagreb (HR)
Petra Rodik, University of Zagreb, Zagreb (HR)
Biserka Runje, University of Zagreb, Zagreb (HR)
Armano Srbljinović, University of Zagreb, Zagreb (HR)
Karin Šerman, University of Zagreb, Zagreb (HR)

Technical Editors

Jelena Ćosić Lesičar, University of Zagreb, Zagreb (HR)
Amalija Horvatić Novak, University of Zagreb, Zagreb (HR)

Published by *Croatian Interdisciplinary Society* (http://www.idd.hr) quarterly as printed (ISSN 1334-4684) and online (ISSN 1334-4676) edition. Printed by *Redak d.o.o.* (HR) in 50 pieces. Online edition, http://indecs.eu, contains freely available full texts of published articles.

Journal INDECS is financially supported by Croatian Ministry of Science and Education.

Content of the journal INDECS is included in the DOAJ, EBSCO, EconLit, ERIH PLUS, Ulrich's and Web of Science Core Collection.

INDECS publishes original, peer-reviewed, scientific contributions prepared as reviews, regular articles and conference papers, brief and preliminary reports and comments to published articles. Manuscripts are automatically processed with the system Comet, see details here: http://journal.sdewes.org/indecs.

The accessibility of all URLs in the texts was checked one weak before the publishing date.

TABLE OF CONTENTS

Dániel Tokody and Gyula Mester ii Editorial: Roadmap for Smart, Sustainable and Safe Cities

REGULAR ARTICLES

Attila Nemes, Gyula Mester and Tibor Mester 302 A Soft Computing Method for Efficient Modelling of Smart Cities Noise Pollution

Miklós Kiss and Lajos Muha 313 The Cybersecurity Capability Aspects of Smart Government and Industry 4.0 Programmes

Anikó Szabó, Endre Szűcs and Tamás Berek 320 Illustrating Training Opportunities Related to Manpower Facility Protection through the Example of Máv Co.

Attila Albini, Dániel Tokody and Zoltán Rajnai 327 The Categorization and Information Technology Security of Automated Vehicles

Péter Miksa Hell and Péter János Varga 333 Accurate Radiofrequency Identification Tracking in Smart City Railways by Using Drones

Gábor Liebmann, László Hanka and György Schuster 342 Probabilistic Approach and Fuzzy System Based Support of the Railway Stations' Smart Security System

Dénes Simonyi and Tibor Kovács 350 Brain-Computer Interface-Based Feasibility of Entering Customer Code on Ticket Vending Machines

Géza Károly Kiss Leizer 360 Possible Areas of Application of Drones in Waste Management during Rail Accidents and Disasters

János Imre Mezei and Kornélia Lazányi 369 Are We Ready for Smart Transport? Analysis of Attitude Towards Public Transport in Budapest

Peter Holicza and Esmeralda Kadëna 376 Smart and Secure? Millennials on Mobile Devices

Dániel Tokody, Attila Albini, László Ady, Zoltán Rajnai and Ferenc Pongrácz 384 Safety and Security through the Design of Autonomous Intelligent Vehicle Systems and Intelligent Infrastructure in the Smart City

Janos Simon and Gyula Mester 397 Critical Overview of the Cloud-Based Internet of Things Pilot Platforms for Smart Cities

Dalibor Dobrilović 408 Networking Technologies for Smart Cities: An Overview

iv Abstracts in Croatian

EDITORIAL: ROADMAP FOR SMART, SUSTAINABLE AND SAFE CITIES

Benevolo lectori salutem,

the present thematic issue of INDECS examines the driving forces behind smart, sustainable and safe city implementations. Besides the results of international and European best practice efforts, the importance of a holistic approach to cities and the issues of cities as complex systems will also be discussed.

Our further aim is to explore the relationship between various research topics (e.g., cyber physical systems, sensors, networks, smart and emerging technologies, intelligent transportation systems etc.) and sustainable safe city implementations. The urban structures and technological advances presented in this thematic issue mark the arrival of the sustainable development of communities, meaning that these intelligent and smart systems will cover all aspects of life. The essence of the pioneer "smart" concept is to develop common, synergic cooperation between different urban structures with the purpose of creating more liveable cities.

The complexity of smart cities can be well demonstrated by Cohen's wheel. Cohen names six major areas in smart city implementations. These characteristics are the following: smart economy, smart government, smart mobility, smart environment, smart living and smart people. This model illustrates clearly the complexity of the smart city as a system.

The present thematic issue also reviews some new trends in the sustainable development of communities focusing on new technologies and the use of scientific innovations, in particular, on the issues of innovations and improvements in design, development, and in the implementation of smart, sustainable and safe cities. The aim of this issue is to offer researchers an opportunity to extend their existing scientific relationships all over the world in the field of emerging key technologies in the development of smart cities including, among others, the use of drones, cyber security methods, blast protection technologies, smart materials, soft computing methods, autonomous intelligent vehicles, etc.

We sincerely hope that researchers working in various field of the development of smart, sustainable and safe cities will find common research areas in the present thematic issue, and they can co-operate in these international projects. The majority of these projects focus on smart cities that can be successfully implemented by developing sustainable communities all over the world.

Cordially,

Budapest, 25th May 2018

Guest editors:

Dipl.-Ing. Daniel Tokody

Prof. Dr. Sci. Gyula Mester

Interdisciplinary Description of Complex Systems 16(3-A), 302-312, 2018

A SOFT COMPUTING METHOD FOR EFFICIENT MODELLING OF SMART CITIES NOISE POLLUTION

Attila Nemes[1,] *, Gyula Mester[1] and Tibor Mester[2]

[1]Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

[2]Geomant-Algotech
Budapest, Hungary

DOI: 10.7906/indecs.16.3.1
Regular article

Received: 23rd January 2018.
Accepted: 31st August 2018.

ABSTRACT

Noise pollution is one of the most relevant problems in urban area. The main source of noise pollution is the number and type of motor vehicles, but other parameters depending on street configuration yield to a system hardly to be exactly modelled by classical mathematical methods. Smart cities are expected to dynamically control the urban traffic to reduce not just traffic jams, but also to ensure a comfortable noise level for inhabitants.

This article gives a design method for efficient genetic fuzzy modelling of traffic generated smart cities noise pollution based on fuzzy logic, multi objective genetic algorithm, gradient descent optimisation and singular value decomposition in the MATLAB environment. Genetic algorithms with objectives to minimise the maximum absolute identification error, the root mean square of the identification error, reduce model complexity and ensure maximal numerical robustness are applied to Zadeh type fuzzy partition membership function parameters preliminary identification, and then gradient descent method is used for their fine-tuning optimization, while the fuzzy rule consequence linear parameters are calculated by singular value decomposition method to find the least squares optimal training data fitting of the model. The training data set is built from measured data, combined with carefully selected simulation data to ensure the completeness of the model and its numerical robustness.

Detailed analysis of the method and results by computer simulation of the identification process show the validity of the proposed method.

KEY WORDS

noise pollution, mathematical modelling, fuzzy logic, singular value decomposition, genetic algorithm

CLASSIFICATION

JEL: Q53, R41

*Corresponding author, η: Mr.Attila.Nemes@gmail.com; –; –

INTRODUCTION

Noise pollution is an uncomfortable sound level obstructing the quality of life, typical to industrial road side areas with high traffic. Traffic jams and heavy traffic are highly annoying and obstructing not just because of time loss and increased engine exhaust air pollution effects, but also because of noise pollution. Intelligent, flexible traffic control is one of the popular subjects of smart city research. Solutions taking care of the life quality of resident people along roads do consider the noise levels. There are many passive construction design solutions to reduce the traffic noise starting from building protective walls, changing the road surface or planting appropriate vegetation between the road and houses [1]. The bottom line is that the traffic nose primarily depends on two hard to change factors – the street width and the house heights defining the geometry, the air volume which is subject to the third obvious factor, the noise source level itself, which is produced by the number passing vehicles. So a smart city traffic control system balancing the nose pollution has to primarily relay on balancing the number of vehicles passing by each fixed configuration street. The noise level depends not only on the number of vehicles, but also on their type. There are multiple levels of differentiations; the most basic is: cars, motorcycles and heavy vehicles [2].

This paper presents a design method for efficient genetic fuzzy modelling of the traffic generated urban noise pollution. Fuzzy systems are known to be trainable for universal nonlinear function approximations even for as complex problems as multi-rotor copter flight dynamics modelling [3]. By using Zadeh-type fuzzy partitions for the antecedent part we can guarantee the continuity of the fuzzy system output for the complete input space [4]. Genetic algorithms are known powerful tools for global nonlinear search, thus suitable for efficient preliminary identification of fuzzy membership parameters [5] and also capable of fuzzy structure optimisation [6]. We use an alternative multi-objective vector comparison in a dominance based ranking method scheme [7], since the two essential quality indicators of any function approximation – the maximum absolute error and the root mean square error – are independent properties usually competing with the model complexity, while all are to be simultaneously minimised. Once the proximity of the global optimum of membership parameters is found, we can rely on fast gradient descent methods to pinpoint the exact optimal values of membership parameters that minimise the approximation error. Using an appropriate representation of the Takagi-Sugeno-Kang type fuzzy logic system the calculation of fuzzy rule consequent linear free parameters becomes a high dimensional, but still a mere linear equation solving problem, which we can solve by a numerically robust, least square error optimal singular value decomposition method [8].

Analysing the singular values of fuzzy rule parameters we can also evaluate the quality of the used training data relative to the planned antecedent membership function fuzzy-cluster complexity, more even we can use this information to select only important samples from the training data, thus reducing its size, while maintaining the numerical quality of the solution [9]. As the (for us) available measured data is by far insufficient for creating a universal noise level model [10], we include to our training set results by other models to obtain a well-defined robust complete fuzzy system of continuous output, no worse than the current known models, an also having the potential for seamless further quality improvements by training for any further real life measured data or any new model data.

NOISE POLLUTION MODELLING

Noise pollution sound pressure systems have very complex structure and therefore it is very hard to identify. Previous efforts [1, 2] have been devoted to determining linear

representations and linear combinations of the system parameter logarithmic values in the following general form:

$$L_{AeqT} = \alpha_0 + \alpha_1 n_{eq} + \alpha_2 X\,, \tag{1}$$

where L_{AeqT} is the equivalent continuous sound level in decibel (dB), α_i denotes identification parameters, n_{eq} is the number of or the logarithm of the number of equivalent vehicles per hour, X is a function of the observer distance from the noise source or W that is either the width or the logarithm of the width of the road, advanced models also account for H, the average height or the logarithm of the height of buildings in the considered road section, which is responsible for the sheer air volume where the noise is distributed, and also the refraction surface, further on some models also include dampening and amplifying modifiers as the road surface quality, the elevation of the road, distance from junctions and other vehicle velocity factors. The equivalent number of vehicles n_{eq}, the most important factor for the noise level can be in general defined as:

$$n_{eq} = n_c + \beta_1 n_{mc} + \beta_2 n_{hv}, \tag{2}$$

where n_c is the number of passing cars, n_{mc} of motorcycles, n_{hv} of heavy vehicles, and c_i are multiplication coefficients usually β_1 is between 2 and 4, β_2 is between 8 and 16. Such linear models are often used because they are easy to implement, albeit they allow only an approximate modelling of the real urban traffic noise pollution. For more accurate results in modelling real nonlinear systems it is advised to use nonlinear models [11-13].

NOISE MEASUREMENT

The set of measurements is performed on various street roads of a typical medium-size northern Serbia town of Subotica. The suitable method for determining the noise pollution is the measurement of the effective equivalent A-weighted energy-average sound pressure level, with the following approximation:

$$L_{AeqT} = 10\log\left(\frac{1}{T}\sum_{i=1}^{T} 10^{L_i/10}\right), \tag{3}$$

where T is the observation time, the number of sound level samples to be accumulated, L_i is the A-weighted sound level in dB(A), defined in the sound level meter standards IEC 60651, IEC 60804, IEC 61672, ANSI S1.4. The number of cars, motorcycles and heavy vehicles per minute was visually monitored in person, and manually counted.

FUNCTION IDENTIFICATION BY ZADEH-TYPE FUZZY PARTITIONS

For the noise pollution model identification method we use fuzzy logic systems (FLSs) with Zadeh-formed membership functions (MFs). More exactly we use Takagi-Sugeno-Kang (TSK) type FLSs having $n=3$ inputs and 1 output. These FLSs can be expressed as:

$$f(\boldsymbol{x}) = \sum_{l=1}^{M} \omega_l(\boldsymbol{x}) \cdot y_l(\boldsymbol{x}) \,/\, \sum_{l=1}^{M} \omega_l(\boldsymbol{x}), \tag{4}$$

where M is the number of fuzzy rules, x is the vector of n input variables, y_l is a scalar function of n input variables, and y is a linear function of inputs for the first order TSKs. Thus y_l is defined by $n + 1$ parameters, respectively. The antecedent, the premise part of a fuzzy rule is defined by MFs as:

$$\omega_l(\boldsymbol{x}) = \prod_{i=1}^{n} \mu_{F_l(i)}(x_i), \tag{5}$$

where $\mu_{F_l(i)}(x_i)$ is the membership function of the i^{th} input variable in the l^{th} rule that defines the linguistic value $F_{l(i)}$. The human readable, intuitive linguistic form of the l^{th} rule from the previously described first order TSK FLS is [14]:

$$IF\ (x_1\ is\ F_{l(1)})\ AND\ (x_2\ is\ F_{l(2)})\ldots\ AND\ (x_n\ is\ F_{l(n)})\ THEN\ y_l = \sum_{j=1}^{n} c_{l(j)} \cdot x_j + c_{l(0)}. \quad (6)$$

We can use fuzzy partitions defined by Zadeh-formed MFs. For $\boldsymbol{b}$ parameters $b_1 \le b_2 \le b_3 \le b_4$ defining the MFs, which are non-linear second order polynomial, so called Z-, S-, and π-functions, named after their shape, defined respectively as:

$$\begin{aligned} mfz(x, b_1, b_2) &= \begin{cases} 1 & x \le b_1 \\ 1 - 2((x - b_1)/(b_2 - b_1))^2 & b_1 < x \le ½(b_2 + b_1) \\ 2((b_2 - x)/(b_2 - b_1))^2 & ½(b_2 + b_1) < x \le b_2 \\ 0 & x > b_2 \end{cases} \\ mfs(x, b_1, b_2) &= 1 - mfz(x, b_1, b_2) \\ mf\pi(x, b_1, b_2, b_3, b_4) &= \begin{cases} mfs(x, b_1, b_2) & x \le b_2 \\ 1 & b_2 < x \le b_3 \\ mfz(x, b_3, b_4) & x > b_3. \end{cases} \end{aligned} \quad (7)$$

For setups when more than one value x exists, such that the degree of membership of x is equal to one, the interval where the $\mu_k(x, \boldsymbol{b}) = 1$ (the interval $[b_2, b_3]$ for $mf\pi$ type μ_k) is the so-called plateau of the μ_k MF. When having for example three naturally ordered linguistic values $l \in \{\alpha, \beta, \gamma\}$ (for example α = *'low'*, β = *'medium'*, γ = *'large'*) there are hard constraints on b_i parameters to preserve the natural linguistic ordering:

$$\begin{aligned} & b_{a1} < b_{b1} < b_{c1} \\ & b_{a2} \le b_{a3} < b_{b2} \le b_{b3} < b_{c2} \le b_{c3} \\ & b_{a4} < b_{b4} < b_{c4}. \end{aligned} \quad (8)$$

When a linguistic variable can be assigned K different linguistic values, each described by a MF $\mu_k(x, \boldsymbol{b})$ such that for every input x it holds that $\sum_{k=1}^{K} \mu_k(x, \boldsymbol{b}) = 1$, the MFs are said to form a fuzzy-partition. By imposing restrictions (8) on all linguistic variables of the FLS, and assuming the rule base is complete – it covers the whole input domain – it follows that the TSK model structure (4) for a multi-input $\boldsymbol{x}$ vector simplifies to [15]:

$$f(\boldsymbol{x}) = \sum_{l=1}^{M} \omega_l(\boldsymbol{x}, \boldsymbol{b_l}) \cdot y_l(\boldsymbol{x}, \boldsymbol{c_l}) = \boldsymbol{W}(\boldsymbol{x}, \boldsymbol{b}) \cdot \boldsymbol{c}, \quad (9)$$

where $\boldsymbol{c}$ is the compound vector of all the so called linear $\boldsymbol{c_l}$ and $\boldsymbol{b}$ is the compound vector of non-linear $\boldsymbol{b_l}$ parameters (parameters defining the linear and non-linear sub-functions) of the fuzzy system and $\boldsymbol{W}$ is the appropriate compound coefficient matrix such that equation (9) holds. This way the resulting formula is simple, still guarantying uniform input coverage and continuous system output – TSK FLSs of fuzzy partitions can even be made periodic [3, 18].

MULTI-OBJECTIVE GENETIC ALGORITHMS

A genetic algorithm (GA) is constructed on bases of imitating natural biological processes and natural Darwinian evolution. GAs are widely used as a search and optimisation tool [16]. Real-life optimisation problems often have multiple objectives. The comparison of two vectors in this case is not trivial. Multiobjective optimisation can be defined as the problem of finding a vector of decision variables which satisfies constraints and optimises a vector function whose elements represent the objective functions. These functions form a mathematical description of performance criteria that are usually in conflict with each other. Hence, the term "optimise" means finding such a solution that would give the values of all the objective functions acceptable to the designer [17].

Introduced in [5] and elaborated in [18] the idea behind the definition of a new vector comparison algorithm, named quality-dominance is to extend the Pareto-dominance relation in a way that a domination decision could be also made for vectors, which are not comparable

by Pareto dominance, while a human heuristic would name a clear preference. Defining a dominance relation $\prec_q(\boldsymbol{r}, \boldsymbol{s})$ (or briefly $\boldsymbol{g} \prec_q \boldsymbol{s}$) between two vectors of n elements $\boldsymbol{r} = (r_i)$ and $\boldsymbol{s} = (s_i)$, for $i=1..n$, $n \in \mathbb{N}^+$, where each i^{th} element type has a well-defined scalar '<' (less than) strict partial order binary endorelation and also the equivalence relation '=' is defined. Defining a helper function $\#_{q<}(\boldsymbol{r}, \boldsymbol{s})$, which for vectors $\boldsymbol{r}$ and $\boldsymbol{s}$ defines two values $(g_r, l_r) = \#_{q<}(\boldsymbol{r}, \boldsymbol{s})$, where $g_r, l_r \in \mathbb{N}_0$ and g_r is equal to the cardinality of set $G_{rs}=\{ r_i \mid s_i < r_i \}$, $i=1..n$; and l_r is equal to the cardinality of set $L_{rs}=\{ r_j \mid r_j < s_j \}$, $j=1..n$. For a minimisation problem vector $\boldsymbol{r}$ **quality-dominates** vector $\boldsymbol{s}$, or briefly: $\boldsymbol{r} \prec_q \boldsymbol{s}$ if $g_r < l_r$ or in case of $g_r = l_r$ $\boldsymbol{r}$ quality-dominates vector $\boldsymbol{s}$ if $\sum_i (r_i - s_i) < \sum_j (s_j - r_j)$, where i is such that $r_i \in G_{rs}$ and j is such that $r_j \in L_{rs}$. In [5] a **measurement value** for $\prec_q(\boldsymbol{r}, \boldsymbol{s})$ is defined as

$$\mathrm{d}_{<q}(\boldsymbol{r}, \boldsymbol{s}) = \begin{cases} l_r - \mathrm{g}_r, & \text{for } \mathrm{g}_r < l_r, \\ \sum_j \frac{(s_j - r_j)}{l_r} - \sum_i \frac{(r_i - s_i)}{\mathrm{g}_r}, & \text{for } \mathrm{g}_r = l_r, \end{cases} \tag{10}$$

where i is such that $r_i \in G_{rs}$ and j is such that $r_j \in L_{rs}$.

We use the dominance measurement based ranking method [18]. At generation t the dominance measurement based rank of the i^{th} individual $\boldsymbol{r}_i^t$ in a GA population, which dominates all $\boldsymbol{s}_j^t$ individuals in the current population is the i^{th} individual current position, the individual's rank is defined as:

$rank_i(\boldsymbol{r}_i^t)$ is the sum of the dominated comparison measurements for every other $\boldsymbol{s}_j^t$ individual of generation t in correlation to the i^{th} individual.

$rank(\boldsymbol{r}_i^t) = \sum_{j=1}^{n} \boldsymbol{d}_{<*}(\boldsymbol{r}_i^t, \boldsymbol{s}_j^t)$, where '*' can stand for any comparison method (the classical Pareto vector-, the new quality vector-, or the simple weighted sum scalar-comparison) [18].

The key question for a GA is the coding of possible solutions, which will evolve through several generations. Fundamental schemata theory suggests that small alphabets are good, because they maximise the number of schema available for genetic processing, so binary coding is implemented [16]. To avoid Hamming cliffs Gray coding is used. Low probability (1 %) mutation is an important part of every GA. The chromosomes are simply the concatenated bit strings of all the parameters with fixed position for every gene, high probability (0.8) simple two point crossover will ensure low disruptiveness and high rate of inheritance during the reproductive phase. Stochastic universal sampling having minimal spread and zero bias is used for selection with a rather low (1.2) selection pressure. Continuous exploration of the search space is achieved together with consistent convergence by the combination of genetic operators in this manner [3-5, 7-9, 18].

SINGULAR VALUE DECOMPOSITION AND GRADIENT DESCENT BASED FUZZY MODELLING

We use the minimal universal representation of Zadeh partitions, by which it can be easily optimised without any constraints, the method as introduced in [3, 4] and elaborated in [18]. To represent a fuzzy partition of K membership functions we take K pieces of rational, positive or zero parameters $a_\kappa \in R_0^+, \kappa = 1, \ldots, K$ and form the b_k nonlinear parameters of the Zadeh-type MFs forming fuzzy-partitions as:

$$b_k = \sum_{j=1}^{k} a_j \,/\, \sum_{\kappa=1}^{K} a_\kappa. \tag{11}$$

For cases when an $a_\kappa = 0$ we obtain $b_k = 0$, thus the fuzzy partition structure complexity is reduced by one MF, thus the complete fuzzy system structure complexity, the number of rules are significantly reduced. In cases when there remains only a single $a_\kappa > 0$ the fuzzy system

rule degrades to a simple linear equation. Finally, in the case when all K pieces of $a_\kappa = 0$ the fuzzy partition and the whole fuzzy consequent degrades to a constant, and the fuzzy system becomes indifferent to the reduced input channel; it becomes independent of the corresponding input variable. These a_κ parameters are suitable for efficient stochastic global search as by GAs, and can be freely fine-tuned with any gradient descent-based method [3-5, 8, 18]; also the Jacobian of the FLS can be calculated with regards to a_κ for advanced nonlinear least squares data fitting methods.

The proposed fuzzy-partition representation has been used in a multi-objective genetic algorithm [5, 18]. One chromosome consists of the number of MFs for every input and the corresponding parameters as in equation (11) for every possible MF partition of each input. The population size is selected to be 50 times the number of parameters. For parameter coding we use 16 bit binary Grey-coded chromosomes. The objective functions we have used are:

- *maxE* – the maximum absolute error of the identification,
- *MSE* – the mean squared error of the identification,
- *RuleN* – the number of used fuzzy rules for the identification divided by the maximum possible number of rules for the selected design,
- *RankW* – is calculated from the matrix rank of $\boldsymbol{W}(\boldsymbol{x}, \boldsymbol{b})$ of equation (9), which is normed to the theoretically maximal possible rank of the same FLS structure.

Based on the transformation of the TSK FLS equation (9) to the $f(\boldsymbol{x}) = \boldsymbol{W}(\boldsymbol{x}, \boldsymbol{b}) \cdot \boldsymbol{c}$ format, we split the identification into two problems: First part is the nonlinear problem of finding optimal $\boldsymbol{W}(\boldsymbol{x}, \boldsymbol{b}(\boldsymbol{a_\kappa}))$ values, which are defined as a function of system input vector $\boldsymbol{x}$ and the nonlinear MF b_k parameters of equation (7). By representing b_k as a function of a_κ via equation (11) any numerical nonlinear unconstrained optimisation can be applied to a_κ parameters. The second part, when $\boldsymbol{W}(\boldsymbol{x}, \boldsymbol{b})$ is fixed (by selected optimal, or candidates for optimal $\boldsymbol{b}$ parameters) to constant values**,** of the problem is a 'simple' solution to a linear equation system, which is best solved for a given training data set of {***input, output***} sample vectors of $\{\boldsymbol{x_{training}}, \boldsymbol{f_{training}}\}$ time series in an error square optimal manner by the numerically robust, general SVD decomposition method as: $\boldsymbol{c} = \boldsymbol{V S^{-1} U^T} \cdot \boldsymbol{f_{training}}$ for the SVD decomposition of $\boldsymbol{W_{training}}(\boldsymbol{x_{training}}, \boldsymbol{a_\kappa}) = \boldsymbol{USV^T}$.

In the applied GA chromosomes are evaluated through the following eight steps.

1.) For each i of n inputs: K_i, number of MFs of the i^{th} input is decoded from the chromosome.
2.) For each K_i: corresponding $\boldsymbol{a_\kappa}$ parameters are decoded from the chromosome.
3.) All required parameters $\boldsymbol{b}$ of Zadeh-formed MFs of equation (7) that form fuzzy partitions are calculated as proposed in (11).
4.) Using training inputs $\boldsymbol{x_{training}}$, all possible training antecedents $\omega_l(\boldsymbol{x_{training}})$ are formed from are evaluated as in equation (5) to get $\boldsymbol{W_{training}}(\boldsymbol{x_{training}}, \boldsymbol{a_\kappa})$ of equation (9).
5.) $y_l(\boldsymbol{x_{training}})$, the corresponding fuzzy rule training consequent parts for all training numerical inputs are evaluated by SVD based LS method as:

$$\boldsymbol{c} = \boldsymbol{V S^{-1} U^T} \cdot \boldsymbol{f_{training}}, \tag{12}$$

by the SVD of the compound antecedent matrix of $\boldsymbol{USV^T} = \boldsymbol{W_{training}}(\boldsymbol{x_{training}}, \boldsymbol{a_\kappa})$ and $\boldsymbol{f_{training}}$ is the measured training noise level.

6.) parameters $\boldsymbol{a_\kappa}$ of step 2.) are further optimised by a gradient decent based method for no more than $\sum_{i=1}^{n} K_i$ steps, where n is the dimension of the input space and K_i is the number of used MFs. For every gradient descent iteration step 4.) and 5.) are repeated.

7.) The resultant fuzzy system $f(\boldsymbol{x})$ is evaluated by equation (9) for the test data set, which is disjunct to the training data set – separated randomly from available samples before the identification process starts – and its cardinality is 10% of the training data set.
8.) For the test data set the *maxE*, *MSE*, *RuleN/maxRuleN*, *RankW/maxRankW* of the identification is calculated, where

$$maxRuleN = \prod_{i=1}^{n} K_i, \text{ and } maxRankW = (n+1) \cdot maxRuleN.$$

To increase the efficiency of the GA after each evaluation the initial chromosome defining a fuzzy system used in step 1.) and 2.) is updated with its optimised MF parameter values resulting from step 6.).

FUZZY SYSTEMS TRAINING DATA SET QUALITY ANALYSIS AND REDUCTION

Training data set, a prerequisite for system identification is a set of measurements of system responses, outputs to be modelled – $\boldsymbol{f}_{training}$ – while the system is being driven along a pre-defined trajectory of inputs – $\boldsymbol{x}_{training}$. As this input training path must be sufficiently exiting so that all system output characteristics can be observed, it is natural that for a good quality identification we must operate with very large input-output training data sets. Evaluating models, iteratively optimising parameters along large training sets and especially performing SVD of large matrices is extremely time consuming. Thus, it is always a challenge for identification tasks to find sufficiently exciting, but not an oversized training data set. In case of modelling complex systems filtering out unnecessary samples, while still leaving all the necessary data for good quality identification is not a trivial strait forward process. In case of every identification problem, specific approaches are used when deemed necessary.

The condition number of a matrix – in our case the compound antecedent data set $\boldsymbol{USV}^T = \boldsymbol{W}_{training}$ – which defines a linear system of equations – in our case equation (9) – is called the condition number of the equation; it is the ratio of the largest and the smallest singular value – in our case for $\boldsymbol{S} = [s_{ij}]$ it is $cond(\boldsymbol{W}_{training}) = \max(s_{ii}) / \min(s_{ii})$. The higher the condition number, the more uncertain the solution is; the more chaotic, the more sensitive the solution is to small disturbances of system parameters. The natural goal for a good quality, robust linear system solution is to have as small a condition number as possible. A very well-conditioned linear system of equations has a condition number of three orders of magnitude less than the reciprocal of the numerical precision of our calculations. In case of double precision floating point digital computer calculous we can rely on a numerical precision of at least ~10^{-16}, which means that any condition number < 10^{10} will already result in a sufficient precision of up to six decimal places, but of course a < 10^3 condition number will be preferred. Rank deficiency of $\boldsymbol{W}_{training}$ is obviously out of question when the goal is to get a complete fuzzy system with no undefined rules – no undefined outputs for any input region.

For an identification error least squares (LS) optimal $\boldsymbol{c}$ vector one can use the SVD transformation property as in equation (12) $\boldsymbol{c} = \boldsymbol{VS^{-1}U^T} \cdot \boldsymbol{f}_{training.full}$ for the SVD decomposition of $\boldsymbol{W}_{training.full} = [\boldsymbol{W}(\boldsymbol{x}_{training.full}, \boldsymbol{b})] = \boldsymbol{USV^T}$, where $\boldsymbol{f}_{training.full}$ is the vector of all available training data**,** for the input training series $[\boldsymbol{x}_{training.i}]$, i = 1, .., N; where N is the number of all available training data inputs. As introduced in [9] and elaborated in [18] we apply a greedy selection algorithm to $[\boldsymbol{x}_{training.i}]$ and thus to the corresponding $\boldsymbol{f}_{training.i}$ training data set, such that we can determine an arbitrary 'quality per size' balanced, but reduced training data set $\boldsymbol{x}_{training.reduced} = [\boldsymbol{x}_{training.j}]$ and a corresponding $\boldsymbol{f}_{training.reduced}$ for FLS based function identifications. The objective of the

greedy search is to select input-output training data pairs ($[\boldsymbol{x}_{training.j}], \boldsymbol{f}_{training.j}$), such that they maximise the condition number decrease of the $\boldsymbol{W}_{training.reduced} = [\boldsymbol{W}(\boldsymbol{x}_{training.j}, \boldsymbol{b})]$ of the FLS antecedent matrix [18].

Considering the proof of the universal fuzzy approximation theorem, for a general case we cannot boundlessly 'generalise' our fuzzy model, we cannot reduce the number of MFs – and by this the required rank of $\boldsymbol{W}$ – to an arbitrary low level, since by this we lose the universal function approximation quality of our FLS. On the other hand if we go for a too complex fuzzy structure, however large the measured training data set we capture, there is a point after which there will be no independent samples (rows of $\boldsymbol{W}$ will not be linearly independent), the training path is called 'insufficiently exciting', the training data is not fit for defining a complete TSK FLS based on fuzzy partition antecedents, the matrix rank of $\boldsymbol{W}$ of equation (9) will not be complete, it will be $rank(\boldsymbol{W}) < (n + 1) \cdot \prod_{i=1}^{n} K_i$, where n is the dimension of the input space and K_i is the number of used MFs. Consequences of such an identification attempt is popularly called identification 'overfitting', where the model can only precisely match the training data, while it performs poorly on disjunct test data sets, which did not take part in the identification process.

The approach taken in this paper is to extend the real measured training data set of 120 samples (Figure 1.) with a carefully reduced set of 800 simulation values based on equations (1) and (2) of [1, 2]. The same approach can be taken for any further new measurement data or any further new reliable models, which we want to merge in, thus to re-train our model for a higher precision or even to include new input regions.

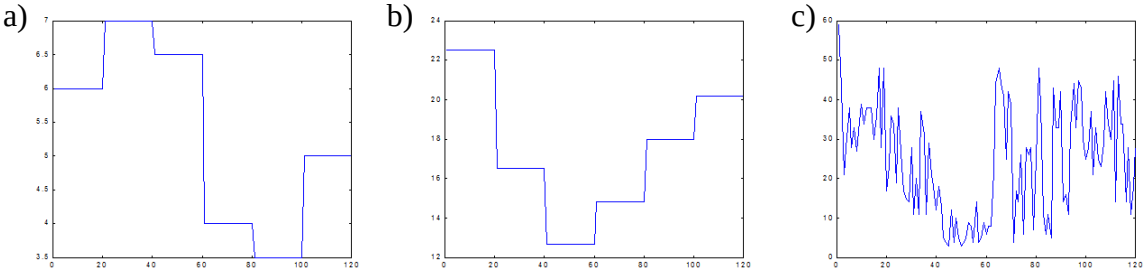

Figure 1. Training data set – measured system inputs of a) average building heights (m), b) average Street width (m) and c) number of equivalent vehicles per second.

IDENTIFICATION RESULTS

The GA process convergence is presented along the identification error objective changes through 50 generations of evolution in Figure 2.

The selected non-dominated identification solution has 48 rules defined for [4, 3, 4] MFs corresponding to inputs [n_{eq}, W, H]. The $\boldsymbol{a}_{\boldsymbol{\kappa}}$ parameters are [291, 25068, 43316; 30436, 29813, 0; 29442, 26577, 56388]. The corresponding $\boldsymbol{b}$ parameters are [0, 0.0042, 0.3693, 1; 0, 0.5052, 1; 0, 0.2619, 0.4984, 1]. The fuzzy partitions are graphically presented in Figure 3.

The training data had been extended to result in system output as presented on Figure 4., which also presents the overlapping output of a selected non-dominated solution and separately the corresponding training data identification error.

The expected system output, the system identification output, and the identification error along randomly selected test samples, which did not take part in the training process, are presented in Figure 5.

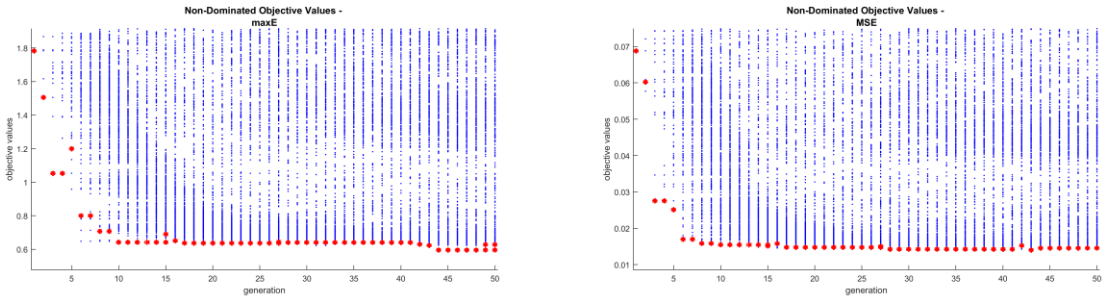

Figure 2. GA convergence a) maximal absolute error evolution, b) mean square error evolution.

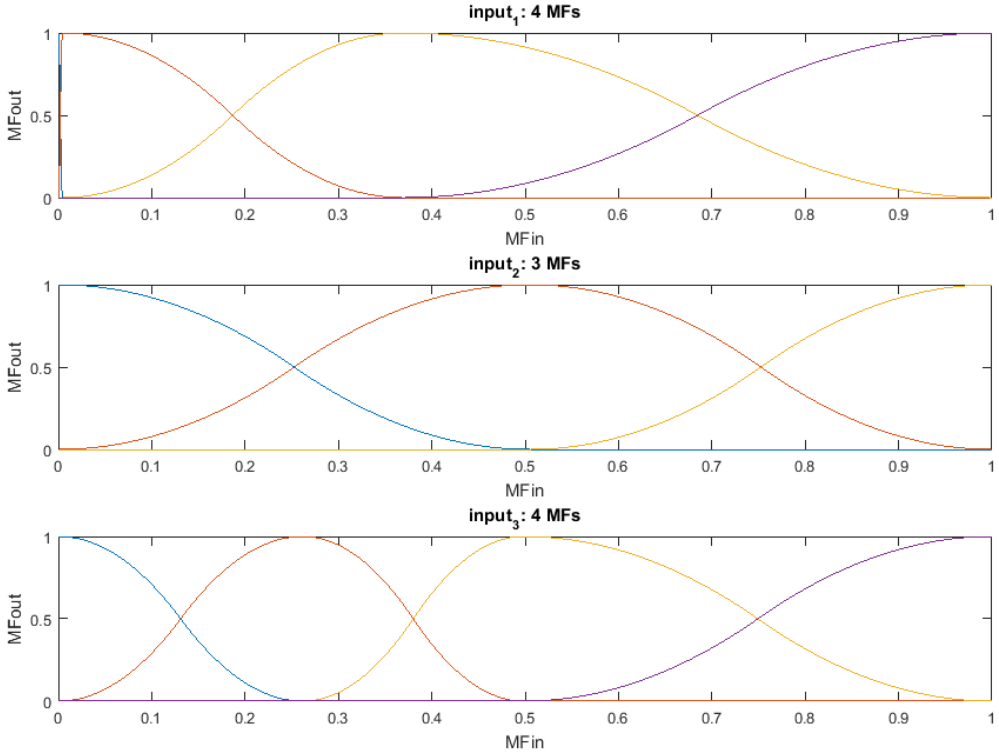

Figure 3. Zadeh type fuzzy partitions for the premise part of inputs [n_{eq}, W, H].

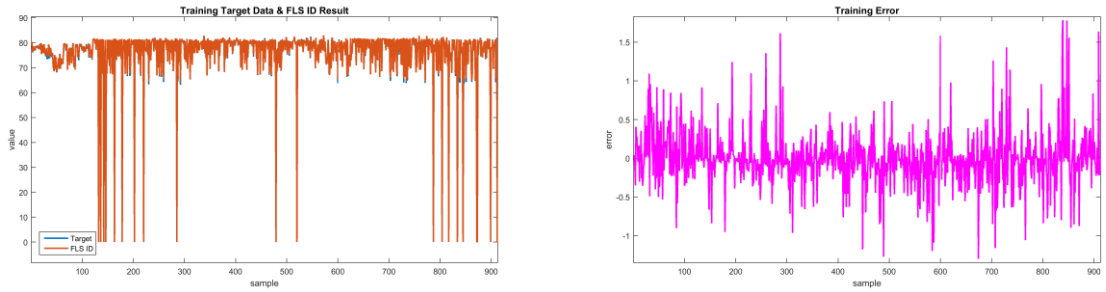

Figure 4. Training data set outputs a) desired and identified output (dBA), b) training error (dBA).

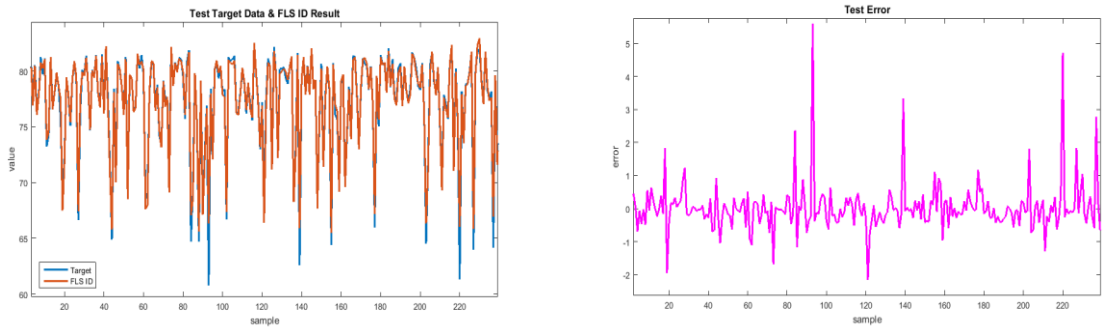

Figure 5. System identification test results: expected and identified output, dBA (left), identification error, dBA (right).

CONCLUSIONS

The presented identification method is capable of sufficiently precise modelling of real measured systems (which data has noise and measurement error) and approximating simulated system (no noise, no measurement error) models to an extreme precision. The definition of fuzzy partitions provides a guarantee that the resulting FLS uniformly covers the complete defined input space, more even the FLS structure guaranties its output is continuous for the complete input space. By extending the measured training data set with simulated values, we have ensured that our model output is nowhere significantly worse than a selected mathematical model, while it precisely approximates the measured data of the real system for all inputs that are in the appropriate range of the provided measured training data set. By extending the training data set and repeating the identification process our model is easily fine-tuned to match further real data.

This robust noise pollution model can be used for making traffic control decisions where the induced noise levels have to be confined. The controlled street configuration must be defined by the street width and average building height, the control input is the equivalent car number and the system model output is the resulting noise level.

REFERENCES

[1] Gulliver, J. et al.: *Development of an open-source road traffic noise model for exposure assessment*.
Environmental Modelling and Software **74**, 183-193, 2015,
http://dx.doi.org/10.1016/j.envsoft.2014.12.022,

[2] Vincenzo, B.; Crocco, F. and Mongelli, D.W.E.: *A mathematical model for traffic noise prediction in an urban area.*
In: Mastorakis, N., et al., eds.: *Recent Advances in Mechanics. Proceedings of the ... 4th WSEAS International Conference on Urban Planning and Transportation*. WSEAS Press, Corfu, pp.405-410, 2011,

[3] Nemes, A.: *Continuous Periodic Fuzzy Logic Systems and Smooth Trajectory Planning for Multi-Rotor Dynamic Modeling*.
Acta Polytechnica Hungarica **13**(6), 215-234, 2016,

[4] Nemes, A.: *Function Identification by Unconstrained Tuning of Zadeh-type Fuzzy Partitions.*
2nd International Symposium of Hungarian Researchers on Computational Intelligence. Budapest, 2001,

[5] Nemes, A.: *System Identification Based on Multi-Objective Optimisation and Unconstrained Tuning of Zadeh-type Fuzzy Partitions.*
2nd IEEE International Symposium on Intelligent Systems and Informatics, Subotica, 2003,

[6] Mester, G.; Pletl, S.; Nemes, A. and Mester, T.: *Structure optimization of fuzzy control systems by multi-population genetic algorithm*.
6th European Congress on Intelligent Techniques and Soft Computing. EUFIT'98, 1, pp.450-456, 1998,

[7] Nemes, A.: *New Genetic Algorithms for Multi-objective Optimisation.*
1st International Symposium of Hungarian Researchers on Computational Intelligence, Budapest, 2000,

[8] Nemes, A. and Mester, G.: *Unconstrained Evolutionary and Gradient Descent-Based Tuning of Fuzzy partitions for UAV Dynamic Modeling*.
FME Transactions **45**(1), 1-8, 2017,
http://dx.doi.org/10.5937/fmet1701001N,

[9] Nemes, A. and Lantos, B.: *Training Data Reduction for Optimisation of Fuzzy Logic Systems for Dynamic Modelling of Robot Manipulators by Genetic Algorithms*.
IEEE Instrumentation and Measurement Technology Conference, IMTC 2001, Budapest, 2001,

[10] Mester, G.; Nemes, A.; Pletl, S. and Mester, T.: *Soft Computimg metoda za optimalno modeliranje buke.*
5th Symposium on Computer Sciences and Information Technologies, YUINFO '99, Kopaonik, pp.1-5, 1999,

[11] Rodic, A.; Mester, G. and Stojkovic, I.: *Qualitative Evaluation of Flight Controller Performances for Autonomous Quadrotors.*
In: Pap, E., ed.: *Intelligent Systems: Models and Applications*. Topics in Intelligent Engineering and Informatics 3. Springer-Verlag, Berlin & Heidelberg, pp.115-134, 2013,
http://dx.doi.org/10.1007/978-3-642-33959-2_7,

[12] Mester, G.; Pletl, S.; Pajor, G. and Rudas, I.: *Adaptive Control of Robot Manipulators with Fuzzy Supervisor Using Genetic Algorithms.*
In: Kaynak, O., ed.: International Conference on Recent Advances in Mechatronics, ICRAM'95. 2, Istanbul, pp.661-666, 1995,

[13] Mester, G.; Pletl, S.; Pajor, G. and Jeges, Z.: *Flexible Planetary Gear Drives in Robotics.*
1992 International Conference on Industrial Electronics, Control, Instrumentation and Automation – Robotics, CIM and Automation, Emerging Technologies, IEEE IECON '92, 2, pp.646-649, San Diego, 1992,
http://dx.doi.org/10.1109/IECON.1992.254556,

[14] Wang, L.: *Adaptive Fuzzy Systems and Control: Design and Stability Analysis.*
Prentice Hall, Englewood Cliffs, 1994,

[15] Hellendoorn, H. and Driankov D., eds.: *Fuzzy Model Identification, Selected approaches.*
Springer-Verlag, Berlin & Heidelberg, 1997,

[16] Goldberg, D.E.: *Genetic Algorithms in Search, Optimization and Machine Learning.*
Addison-Wesley Longman Publishing Co. Inc., Boston, 1989,

[17] Osyczka, A.: *Multicriteria optimisation for engineering design.*
In: Gero, J.S., ed.: Design Optimisation. Academic Press, pp.193-227, 1985,

[18] Nemes, A.: *Tools for Efficient Soft Computing Modelling and Feasible Optimal Control of Complex Dynamic Systems.* Ph.D. Thesis.
Óbuda Univesity, Budapest, 2017.

Interdisciplinary Description of Complex Systems 16(3-A), 313-319, 2018

THE CYBERSECURITY CAPABILITY ASPECTS OF SMART GOVERNMENT AND INDUSTRY 4.0 PROGRAMMES

Miklós Kiss* and Lajos Muha

Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.16.3.2
Regular article

Received: 14th February 2018.
Accepted: 31st August 2018.

ABSTRACT

To operate smart cities it is necessary to have proper governance, industry and services ecosystems that can be built upon. The smarter the elements of the system are, the more complex IT infrastructure will be; and these will directly or indirectly have an impact on each other. Last year signified how vulnerable these industry and service systems are in the government and corporate sectors. Significant cyber-attacks such as Wannacry or NotPetya can influence the operations of an organization to a degree that might pose a challenge to governments of cities, countries or even a continent. These campaigns targeted industrial and supply chains. How was survival possible? What competencies were needed to operate our industry in such a harmful environment? In this study we will highlight which competencies are needed for Smart City and Industry 4.0 to successfully implement major projects that benefit the development of smart cities.

KEY WORDS

competencies, IT governance, industry 4.0, smart city, program management

CLASSIFICATION

ACM: K.4, K.6
JEL: A10, C10

*Corresponding author, η: kismkls@gmail.com; –;
H–1428 Budapest, Pf.:31, Hungary

INTRODUCTION – INFORMATION FLOW THAT MAKES YOU SMART

It is not easy to accurately define what a Smart City or Industry 4.0 is, as these are continuously transforming and forming. At the same time, we can find some fixed points with an evolved consensus. The most basic criteria is probably that in respect of both ecosystems sensors and information flow between separate elements occur which enable aligned and closely coherent operation and development of complex systems [1].

The concept of Smart Cities includes and integrates both information and communication technologies and numerous other physical technologies, such as the Internet of Things (IoT), that made possible the optimization and high efficiency of services and city operations [2]. In the field of industry, similar processes are underway at companies, when automation (Industry 1.0) was followed by mass production (Industry 2.0), then computerization (Industry 3.0), and today by organizing actual objects and sensors into networks we have reached Industry 4.0 [3]. IoT, cyber-physical systems and artificial intelligence promoting data interpretation and utilization appear here as well [4].

Several internationally acknowledged companies recognized these aspects of information technology and combined them with their own core competences. Cisco and IBM possess programs, projects and methodologies to promote the integration and connection of these technologies in the modern industrial and urban environments [5, 6].

However, to analyze the issue, it is not enough to apply the technocrat approach alone. One has to take into consideration the complex approach in which the other elements of the ecosystem are also included: people, government, economy, environment, mobility and viability [7, 8], Consequently, when speaking about Smart Cities and Industry 4.0, we need to refer not only to the technology, but we should think about the utilized systems (citizens, enterprises), implementation of missions, operational and strategic governance [9]. It is important to mention that beyond international good practices, domestic regulation was also created: Government Decree 56/2017. (III. 20.) on the modification of certain government decrees related to the definition of *Smart City* and *Smart City methodology*, which among others, highlights the requirements of connection with innovation and strategy [10]. Hungarian Lechner Knowledge Center promotes the improvement of Smart Cities on domestic level [11].

So, we can see that when we want to study smart systems, we also need to bear in mind other elements of the ecosystem (government, enterprises, and organizational abilities). To be able to operate Smart Cities and advanced industrial conformations in the long term, we need to be able to implement these innovations (programs, projects) and make them sustainably operational afterwards.

The issue of cybersecurity is a very important factor in terms of the complex information infrastructure. The higher the complexity of an ecosystems' information network the more vulnerable these systems will be. Therefore, from the moment of planning of these innovations, one has to deal with the projects' cybersecurity matters as well [12]. Availability, confidentiality and integrity are fundaments in which all circumstances have to be secured to sustain stable conditions [13]. The so-called Big Data, originated from sensors and other sources, also represents a major challenge for designers of smart ecosystems [14]. So, in this research, we try to find those organisational competences and features that promote the secure innovation and operation of cities and industrial facilities.

In the following section, we will highlight the cybersecurity challenges of Smart City operators by demonstrating an example case. The third section will introduce competences that may achieve long-term development and projects of a 4th generation enterprise or developed government.

MODERN WAY OF EXTORTION THAT MAY EVEN DISABLE CITIES

In 2016 an interesting incident kept the world and especially the citizens of San Francisco awake. The city's public transportation system was disabled by a ransomware for a long time; a HDDCryptor variant made the data stored on the public transport companies' computers unaccessable [15]. In 2017, another challenge was put to companies utilizing information technology. These two incidents of large-scale impacted both company and government information technology systems.

The WannaCry ransomware campaign occuring in May 2017, spread so fast that the protection utmostly utilised defensive system (SIEM, IPS), operation approach (backup, obsolete systems, ITIL) and human skills (awareness). The reportedly state-sponsored campaign highlighted that an attack of this kind is a potential risk to Smart Cities and industrial facilities connected to a network [16, 17]. The NotPetya campaign following WannaCry pointed out how a targeted campaign can be managed, against government targets. Although there was some collateral damage, the main impact was to a country's information technology infrastructure [18, 19].

These events illustrate the importance of allocating project and operational competences to enterprises investing now in Industry 4.0 innovations. Cities establishing their own Smart City infrastructure also require project and operational competences. What are these competences? This research on organisational competences impacting the success of IT (safety) projects and programmes is trying to determine the answer to this question.

SECURITY CAPABILITY ASPECTS OF SMART PROJECTS

The aforementioned cases highlight that to operate smart ecosystems it is indispensable to have IT systems that enable interconnection and operation of complex systems. For Smart Cities and Industry 4.0 however, beyond technological components competences are required that promote safe operations. Planning and implementation of innovations/projects with respect to IT security is also required. The research mentioned further in the text aims to define these competences, in other words, what are the variables that characterize the enterprise and civil service sector. How do these two segments relate and which components of the main variables have the most significant impact on the complete ecosystem? One further benefit of the research is that we can have a screenshot of the actual situation in relation to both the governmental players and industrial players concerned in the supply chain.

STUDY ON THE FACTORS IMPACTING THE SUCCESS OF SMART CITY PROJECTS

Organization maturity: questions in this group were framed based on the COBIT maturity model, therefore the relation of variables also reflects the sequence (from management to process improvement) [20]. This section of the research points out that the usual maturity level of organizations is typically between maturity level 2 and 3 (this is supported by the lower variance of the responses to these two questions: 0,78 and 0,97). There is stratification between governance and industrial units around maturity level 3 (2,44 and 3,10). This indicates that governance processes are on one hand documented, but there are no real measurements and feedback on the other hand. Generally speaking, maturity of civil service organisations lags behind enterprises. This confirms the need to emphasise competences in Smart City projects.

Logical controls of the organisation: Answers to the questions in this competence group shows there is no significant difference between enterprises and governments. However, it is

clear that enterprises implement more security planning and to risk analysisat project planning which will be required in complex Smart City governance as well [21, 22].

Development demand of organisations: Effort for the qualification of employees is similarly present in both government and enterprise organisations (governments do not reach enterprise levels though). This indicates that besides the operation of complex Industry 4.0 and Smart Cities, resources have to be allocated not only to the qualification of co-workers, but to raise awareness of all stakeholders, especially of the general population (see cybersecurity challenges of technologies mentioned earlier) [23].

Strategy: The greatest difference has been registered in the frequency of regular reviews of the created strategies. While in the field civil service this correction is done every 2-3 years in average (due to reasons traced back to political cycles), private organizations review strategies annually. This implicates the need for restructuring todays' civil service systems of cities of the future (the integration of results of the rapid technological development should be integrated into legislation as quickly as possible) [24].

Efficiency of projects: Investigation of this variable resulted that project management techniques (e.g agile innovation or Scrum methodology) necessary in a dynamically developing city can not really be implemented into todays' civil service. Results are centered around the mean of 3, based on which, at Smart Cities a lot of attention has to be paid to fulfill the social requirements at the highest possible level [25].

The research aimed to prove if variables of the four competence groups have any impact on the *project success*, and to find the significant variables. One single variable was created for the "project group" which contains the characteristics of the five separate variables belonging to four groups. This requirement can be fulfilled by the so-called dimension reduction, that is, by generating a principal component. By generating the principal component, the $n > 5p$ rule is fulfilled, Bartlett's test returns a significant value, KMO value is 0,788, which suggests good suitability. Communality values over 0,5 indicate that the explanatory power of the variables used in the final model is still adequate. In the final model, the principal component explains 57 % of the variance of the other variables which only just confirms the model's validity. With the regression analysis performed with the only variable explaining project success generated this way, we managed to identify the variable components with the highest impact on the dependent variable. Multiple regression analysis was performed by competence groups in each case with the exclusion of non-significant variables (backward elimination method).

Maturity: regression model is $-1{,}851 + 0{,}263 \cdot \textit{documentedness} + 0{,}358 \cdot \textit{innovation}$, zero-order collerations of the coefficient table contains the relationship between the independent variable and dependent variable, which shows a weaker than average result (0,394 and 0,492), the models' explanatory power is still adequate: $R^2 = 0{,}302$. In this case, maturity levels of 3 and 5 (documentedness of processes and routine of innovation) have significant impact on the project success, while the regression model did not indicate significant connection in terms of maturity levels 1, 2 and 4. Apparently, it is important to identify and regularly review the processes of these complex smart ecosystems.

Control: $-2{,}612 + 0{,}196 \cdot \textit{security planning} + 0{,}215 \cdot \textit{daily practice} + 0{,}360 \cdot \textit{incident management}$, zero-order correlations indicate average relationship with the independent variable (0,502, 0,458 and 0,587), the model's explanatory power is average: $R^2 = 0{,}471$. Clearly, consideration of security aspects, complying with well-defined rules and well-defined incident management practices have impact on success. Therefore, cyber security incidents will be manageable both for governance and industry.

Development: –2,002 + 0,245·*employee qualification* + 0,376·*structure change*, zero-order data indicate average correlation here also with the project success variable (0,498 and 0,579), the model's explanatory power is still adequate: $R^2 = 0,390$. Education of co-workers and structure changes aligned with the project have significant impact on the project success of future cities and industrial units. This indicates that government organisations regularly running projects should consider developing a more flexible structure supporting management, and should not disregard competence training of employees and of the population.

Strategy: –1,645 + 0,221·*strategy depth* + 0,378·*strategy review frequency*, based on zero-order data, strategy depth has weak correlation (0,358), while review frequency has medium connection (0,471) with the dependent variable. The model's explanatory power is just acceptable: $R^2 = 0,283$. Depth of strategies (organisation, IT, IT security) and update regularity of these have impact on the success of delivered projects. Therefore, leaders of those cities and enterprises that do not attend to strategy planning and regular update, will eventually be at a disadvantage compared to organisations that disseminate strategies of appropriate depth and quality.

SUGGESTIONS AND AFTERWORD

Summarizing the identified variables by competence groups (maturity, control, development and strategy) – 5 per group, 3 in the development group – was an important step to get to know the current situation of the civil service and enterprises, which also helps us understand requirements of the Smart Cities and next-generation industry. The comparative investigation pointed out that government organizations lag behind the market players. Enterprises' maturity – especially on level 3 and 4 – is considerable, which is reflected by the effective performance of daily functions and in the quality of performed tasks. Fine-tuned action plans based on measurements enable quick interference so that Smart City and Industry 4.0 innovations can be utilized at the highest possible degree:

- considering the result of the research, that industry organizations have a higher maturity level, their involvement and the best possible utilization of synergies is necessary (see examples from IBM and Cisco),
- security planning should be delivered at the planning phase of complex projects/programs; it is not enough to attach the adequate controls to the programs defining the future retrospectively, as in this case there will be an increasing gap between the real risks and application of regulations,
- it is important to base information security on real incident management procedures (with respect to increasing risks due to new technologies) where the full incident lifecycle is followed.

New technologies mean new risks as well. This research, revealing relevant competences is an assistance for managing these risks of the key projects of future cities and industries.

REFERENCES

[1] Hamblen, M.: *Just what IS a smart city?* https://www.computerworld.com/article/2986403/internet-of-things/just-what-is-a-smart-city.html, accessed 12th February 2018,

[2] Cohen, B.: *The 3 Generations Of Smart Cities.* https://www.fastcompany.com/3047795/the-3-generations-of-smart-cities, accessed 12th February 2018,

[3] –: *Production, organized in networks, or what is "Industry 4.0". In Hungarian.* http://lignomat.hu/HiREK/Halozatba_szervezett_gyartas_avagy_mi_az_az_Ipar_40.html, accessed 12th February 2018,

[4] –: *Industrial Automation.*
https://www.lanner-america.com/knowledgebase/industry-4-0, accessed 12th February 2018,
[5] IBM*: IBM builds a smarter planet.*
https://www.ibm.com/smarterplanet/us/en, accessed 12th February 2018,
[6] Cisco: *Cities and Communities*.
https://www.cisco.com/c/en/us/solutions/industries/smart-connected-communities.html, accessed 12th February 2018,
[7] Szendrei, Zs.: *Smart City, the city of the future.*
http://www.urb.bme.hu/segedlet/varos1/eloadasok_2014/07B_SMART%20CITY_SZENDREI%20ZSOLT_kivonat.pdf, accessed 12th February 2018,
[8] Giffinger, R.: *Smart cities Ranking of European medium-sized cities. Vienna: Center of Regional Science*.
http://www.smart-cities.eu/download/smart_cities_final_report.pdf, pp.10-12, accessed 12th February 2018,
[9] Lados, M.: *Smart cities treatise (IBM).*
Hungarian Academy of Sciences, Institute for Regional Studies, West Hungarian Research Department **16**, 2011,
[10] *Government Decree 56/2017. (III. 20.) on the modification of certain government decrees related to the definition of "Smart City" and Smart City methodology.*
[11] –: *Smart City.*
http://okosvaros.lechnerkozpont.hu/hu, accessed 12th February 2018,
[12] Lados, M.: *Smart Cities – Smart people.*
XVI Actual issues of urban traffic,
http://www.ktenet.hu/download.php?edid=1123, accessed 12th February 2018,
[13] Gordon, A.: *CISSP Training Series.*
CRC Press, New York, 2015,
[14] Nyikes, Z. and Rajnai, Z.: *The BIG DATA Application to the Hungarian National Digital Infrastructure.*
Professional Muster: Academic-professional magazine of the Military National Security Service. Special issue, 74-85, 2015,
[15] Gibbs, S.: *Ransomware attack on San Francisco public transit gives everyone a free ride.*
https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware, accessed 12th February 2018,
[16] *WannaCry: Are you safe?*
https://www.kaspersky.com/blog/wannacry-ransomware/16518, accessed 12th February 2018,
[17] Gallacher, L. and Morris, H.: *ITIL Foundation Exam Study Guide.*
John Wiley & Sons, London, 2012,
[18] Rothwell, J.; Titcomb, J. and McGoogan, C.: *Petya cyber attack: Ransomware spreads across Europe with firms in Ukraine, Britain and Spain shut down.*
http://www.telegraph.co.uk/news/2017/06/27/ukraine-hit-massive-cyber-attack1, accessed 13th February 2018,
[19] Landry, J.; Izraeli, N.; Shamir, U.; Fenton, C. and Liba, I.: *Dissecting notPetya, SentinelOne whitepaper 2017.*
https://go.sentinelone.com/rs/327-MNM-087/images/Dissecting%20NotPetya%20-%20WP.pdf?aliId=21202168, accessed 12th February 2018,
[20] IT Governance Institute*: COBIT 4.1.*
IT Governance Institute, Rolling Meadows, 2007,
[21] –: *Act L of 2013 on the electronic information security of state and local government and organizations.*
[22] –: *Minister of Interior Decree on the requirements for technical security, secure information technology devices and products, and security class and level classification defined in the Act L of 2013 on the electronic information security of state and local government and organizations*. 41/2015. (VII. 15.)

[23] Gallacher, L. and Morris, H.: *ITIL Foundation Exam Study Guide*.
John Wiley & Sons, London, 2012,
[24] Kápolnai, A.: *E-business strategy for enterprise senior management*.
Aula, Budapest, 2002,
[25] Szabó, L.: *Project management.*
Pearson Education, Harlow, 2012.

Interdisciplinary Description of Complex Systems 16(3-A), 320-326, 2018

ILLUSTRATING TRAINING OPPORTUNITIES RELATED TO MANPOWER FACILITY PROTECTION THROUGH THE EXAMPLE OF MÁV CO.

Anikó Szabó[1,] *, Endre Szűcs[1] and Tamás Berek[2]

[1]Óbuda University, Doctoral School on Safety and Security Sciences, Budapest, Hungary

[2]National University of Public Service
Budapest, Hungary

DOI: 10.7906/indecs.16.3.3
Regular article

Received: 2nd February 2018.
Accepted: 31st August 2018.

ABSTRACT

Smart towns plan several progressive practical innovations with the aim of ensuring the convenience of its inhabitants and that of commuters or visitors. These innovations aim at not only ensuring convenience but also at increasing the living standards based on sustainable results with the help of smart tools and logical methods. The foundation of smart towns is to ensure the security of its inhabitants. Hence, it is a vital task to maintain the operation under normal conditions of critical infrastructure. According to the Act 1997. year CLIX. critical infrastructure is also related to the railway activity of MÁV-group. The Act concerns armed security sentry, conservationist and agrarian sentry. Hence safeguarding activity is performed by both security guards and armed security guards at MÁV groups. Their duties do not only consist of preventive security tasks but also defence in certain unique cases in accordance with the regulations of their field of work. In order for them to perform their duties properly it is vital that an extensive, regular and practice-oriented training of security guards to happen. This publication aims at illustrating the current training opportunities applied in the field of safeguarding that ensure the functioning of the MÁV group. Also, some potential improvements of training opportunities are shed a light on. We outline the internal training opportunities security professionals – employed by MÁV Co. – can participate at. Besides that, we illustrate the possibilities of employee retraining and courses professionals employed by MÁV Co. are offered in order for them to become well-trained professionals that can fit the complex system of the concept of a smart town.

KEY WORDS

smart town, smart people, critical infrastructure, railway, safeguarding, security guard, training

CLASSIFICATION

JEL: I28, O25, R41

*Corresponding author, η: aniko.szabo.bdi@gmail.com; –;
OE-BDI office, Nepszinhaz str. 8, 1081 Budapest, Hungary

INTRODUCTION

On supervising the professional know-how of security guards several occasions made me aware of the possible risks their incomplete scope of learning of practical knowledge may bear. Despite having the necessary qualifications, in most cases they lack either in-depth knowledge, understanding implications or being skilled in practice. It results in the security guard being insecure in situations requiring action. Consequently, they made fundamentally wrong decisions in more than one case. Repeated tactics of private security measurement trainings are supposed to help these, where legal, service object-specific knowledge is periodically revised, as well as first-aid knowledge and self-defence practice.

Presumably, security guard trainings are part of a detailed, well-structured and complex training system in case of a company of nationwide employment with over 1000 employees that offers services nationwide, and has a significant client traffic related to its objects. The Hungarian Railway (MÁV Co.) fully met all these criteria as maintains and operates a vital infrastructure that is highly important regarding the functioning of the state- from the national safety viewpoint. In order to achieve a proper functioning, safeguarding activity is performed by both security guards and armed security guards. Their professional education of high standards is a basic necessity that adds to the circle of highly skilled, broad-minded employees of smart towns.

As for the cargo freight of MÁV group, the component of freight of dangerous goods above all requires a high-level preparation of security guards. Freight of dangerous goods qualify as dangerous activity. Hence, its security is determined by the legal regulations and their observance to a great extent. This factor affects the choice of freight method and organizing the security protection of the cargo [1].

The current study is the first part of a trilogy, which aims at describing the internal educational system in the field of safeguarding to which interviews with MÁV Co. Security Directorate General served as a source. It sheds a light on the need for a constant, detailed practice oriented training in this professional field.

THE DEVELOPMENT OF THE MÁV GROUP CONCERNING SAFEGUARDING

The Hungarian State Railways was founded in 1869 that can be considered as the legal predecessor of Hungarian Railway (MÁV Co.) that eventually got deprivatised in 1945. The MÁV Co. was converted into a public limited liability company in 1993 that eventually became a private limited company in 2005. The freight transport division left under the name of MÁV Cargo Freight Transport Ltd. in 2006 and continued functioning as an affiliated firm. Having been privatized in 2008 it was renamed as Rail Cargo Hungária Ltd. in 2010. Similarly, the passenger transport division also left MÁV Co. in 2006 and continued functioning as MÁV-START Co. in 2006 [2-4].

In case of MÁV Co. the industrial police activity was called into being in order to ensure the protection of the assets of the company, its edifies with special attention to operational areas, train stations and freight. A change was made in the structure of industrial police activity in 1993, when MÁV Co. began the employment of armed safety guards in accordance with the decree nr. 39/1976. (X.30.). In the beginning, their task was freight accompaniment that was extended to safeguarding train stations later on. (As of 2006 armed security guards were safeguarding the freight and cars of MÁV Cargo, as these tasks did not cease after it became an affiliated firm.) Security and safeguarding activity were provided by own workforce within the framework of industrial police until 1996. Up to that moment industrial guards performed

facility protection that worked both as security guards and as armed security officers. In 1996 The MÁV Vasútőr Vagyonvédelmi és Szolgáltató Ltd. was established with the aim of ensuring that security and safeguarding activity – that previously had been provided within the framework of industrial police – could be provided by a company owned by MÁV Co. from 1997. From that moment on security guards provided the service instead of industrial security employees. Armed security guards also got employed by MÁV Vasútőr Ltd.. Later, MÁV Vasútőr Ltd. and two other MÁV owned companies, (namely: MÁV Ingatlankezelő Ltd., MÁV Vagyonkezelő Ltd.), merged into MÁV-KERT Co. that was founded in 2003. After that, MÁV-KERT Ltd. was renamed as MÁV Létesítményüzemeltető and Vasútőr Ltd. The latter company ceased to exist in 2015 and MÁV Co. took over its scope of activities. Thus, property security guards and armed security officers became employees of MÁV once again. From 2017 on up to present MÁV Co. orders service from companies winning in public procurement procedures in order for them to perform functions as security guards. Armed security guards provide their service as employees of MÁV [2].

SAFEGUARDING ACTIVITY OF MÁV CO.

The aim of the MÁV-group is to provide service of the highest standard possible to support the passenger and freight transport in order for Security Directorate General to protect the facilities, appliances and intellectual goods. The safeguarding field is responsible for organising, supervising and controlling both safeguarding and manpower guarding, as well as the synchronised operation of security technology equipment and last, but not least it coordinates the investments belonging to their scope of duties [5].

The guarding tasks have been grouped with respect to objects, premises and values to be protected. Several positions are available in order to take care of these duties in case of an order from the MÁV-group. Various forms of service are available, such as object protection, onsite patrolling, reception service or train station patrolling. The latter can appear either in form of operational area patrol, patrolling in private areas open for public circulation or even mobile patrol by train or own vehicle. Beside these, there might be armed security guards, surveillance officer, cargo security guards, security guard assuring passenger transport and event security guards [3].

DESCRIBING THE SAFEGUARDING TRAINING SYSTEM OF MÁV CO.

At MÁV Co. the staff getting involved with property security or safeguarding are required to have a certain level of qualification to be able to fulfil the given positions. In addition to that, pursuing constant professional development, staff is required to periodically participate in company-offered training sessions relevant to their position. The training sessions might either be compulsory or eligible. Defence and security experts are offered property security and safeguarding training, as well as armed security guards, security guards by their external employer. Similarly, employees of MÁV Co. as well as external employee entering the premises of MÁV Co. are offered similar education, which this publication does not aim at describing [6, 7].

The documents and professional store of learning enlisted form part of the training: Direction for Training Order, Safeguarding Order, Local Manual for Security Guard, Labour Safety and Fire Protection, Rail Professional Knowledge, Traffic- and Rail Technology Knowledge, Theoretic and Technical Knowledge of Tools for Confident Use, Ethical codex. The essence of the above listed materials is described in different depth regarding the given position. The store of learning at the trainings are offered by professional instructors of the given field, such as guarding security knowledge is taught by the expert of defence of MÁV, or on issues related to freight transport information is delivered by a competent expert of MÁV. Along

with that, different lecturers are invited to enrich the knowledge of the participants, such as from the national police staff.

PROPERTY SECURITY PROFESSIONAL DIRECTION AND SUPERVISION

Executives in the fields of property security and safeguarding, together with the safety and security experts working in this field are required to have obtained professional qualification in order to be able to take the position, such as: security and security engineer degree. Typically, intermediate level qualification is sufficient to be able to fulfil an operative position. These positions are available mainly at the Területi Vasútbiztonság.

In case the potential candidate for a position possesses only partial knowledge MÁV Baross Gábor Training Centre ensures that the candidate obtain the necessary training. Employees working in the field are to obtain such a qualification concerning expert-level property security course. These specialised trainings are either provided by external official instructor or internal vocational trainer for participants of adult education. In this moment, the training centre is responsible for ensuring and organising professional training for the employees of MÁV Co. Its main aim is to provide professional training, retraining for the employees and to deepen their knowledge in order to have professionals with the necessary know-how [8].

Above that, employees in the field have the opportunity to participate in trainings of own choice within the framework of a one-year training. However, these optional trainings, even ones remotely related to their field, are to be approved by the proper management. This training method highly supports the broad perspective, decreasing human risk and the efficiency of the functioning of the adjoining fields as the areas of defence and security is revealed in diverse and overlapping activities [9, 10].

TRAINING OF ARMED SECURITY GUARDS

In the periods when security guards were either employed directly by MÁV Co. or indirectly belonged to MÁV Vasútőr Ltd. there was an opportunity to retrain them internally and eventually employ them as security guards.

Currently, at MÁV Co. those candidates for armed security guard positions are preferred to possess some kind of a former qualification – beside health and psychological aptitude – despite it not being a basic requirement. Although security guard activity is regulated by completely different acts, many parallels can be drawn in their scope of duties. Thus, formerly obtained qualification is thought to provide a basis for professional overview that results in an easier understanding of professional knowledge and acquiring practical information concerning this job [11].

Having applied successfully, candidates take part in a month-long collective internal training. Having completed the training they have the opportunity to spend time shadowing a more experienced workmate during which they can acquire the practical information.

The training ends with taking an exam consisting of both a theoretical and a practical part in which authorities get involved. At the theoretical exam legal and professional knowledge is to be given an account of, whereas in case of the practical exam weapons knowledge and self-defence knowledge are to be tested. As for legal knowledge, the candidate is required to be adept in related directions of constitutional, state administration and criminal law and criminal action law beside being enlightened in applying the specification of law of armed security sentry. Professional knowledge offers security guards a broad scope of learning such as code of conduct, elements of risk, first aid and even forensic science principles. As for testing self-defence, the board of examiners checks whether the examinee is familiar with the basic elements, averting attacks or the procedure of forcing by corporeal power. The weapons

knowledge exam is entitled to measure competence of using and handling arms, as well as having successfully acquired the knowledge of handling, storage and maintenance of device used in the process of forcing. Having successfully passed the exam, the employee is entitled to work as an armed security guard. Naturally, in case of an unsuccessful exam, there is the opportunity of a retake [12, 13].

The theoretical knowledge and skills acquired in practice is periodically checked by the board of examiners. The board of examiners consist of the organisation that operates sentry-duty and of representatives of central police forces supervising sentry-duty. Shooting skills is to be tested annually in form of shooting. The board of examiners checks theoretical knowledge biannually, health aptitude is revised every three years, while psychological aptitude is tested every four years.

TRAINING OF SECURITY GUARDS

Prior to security guard trainings professional knowledge to be acquired was provided at plant security, as well as professional preparation of employees of the field. After the property security law got into existence, security guard trainings were launched, hence former in-company processes discontinued. Thus, only candidates were able to get employed in such a position who had already possessed a security guard id card and fulfilled the employment requirements of MÁV Co. such as the psychological and health aptitude.

The MÁV Co. provided training periodically for security guards (formerly called security agents) or also occasional trainings for its employees as of the MÁV Co. plant security period. The basis of these trainings is a central Direction for Training that is obligatory in case of each MÁV Co. employee. In addition to that basis, professional knowledge and practical know-how were added. A Vasútőr Ltd. provided recurring training for security guards biannually. This store of learning involved acts and inside regulations that is still core material of the training syllabus of present companies with regard to the period and contents. One of the pillars of education is property security regulations of MÁV Co. that is provided in the framework agreement contract. Companies offering property security services are given the information concerning property security in the framework agreement contract in order for them to apply it in professional knowledge acquisition. Training is provided by vocational trainers ordered from MÁV Co. or by an educator employed by an external company having command of the necessary knowledge. This person is responsible for teaching labour safety and fire protection knowledge. On top of that, there is need for MÁV Co. professionals to deliver special knowledge that is related to the danger of operational areas or describing individual solutions applied in property security, as well as their adept applications, such as special car types, railroad structures, edifices, locks or car tracking systems. The accident surveyor gives a lecture on behalf of MÁV Co. providing further information on dangerous goods, traffic with regard to providing property security services in a depth necessary for a proper functioning.

Delivering this knowledge is accomplished in course of a four-day course, in 6-8 hour daily sessions. The number of participants vary between 10-20 depending on working hours. The safety guard is to sign the educational record to testify understanding and having acquired the knowledge delivered [2].

CONCLUSIONS

In this study we have shown the development of safeguarding of MÁV-group in parallel to its organizational transformation, as well as its current professional direction. Also, we described the requirements of training and functioning of safeguarding trainings in case of both security and armed security guards. All in all, it can be concluded that MÁV Co. bears a similarity to

state companies with respect to the training system of security guards, the parameters of which were mentioned in the introduction. The training material, repetition and records of training sessions show similarity, among others. It was worth selecting MÁV Co. as an example for this study as its structural system as for safeguarding and training system has a logical setup, which includes elaborate and widespread store of learning. A highly positive traits is that it has an actively used quality checking system, which is itemized as for employees, work, or procedures. At the same time, it can be said that the professionals at MÁV only check the existence of the educational records, at this point verification of knowledge is absent. Experts at MÁV Co. are unable to directly verify the depth and quality of their training. On top of that, there is no way for them to examine whether the security guard has acquired the knowledge and is capable of reacting to a certain situation skilfully. This shortcoming is not a unique phenomenon but can be considered a general problem nationally.

E-learning material, which would be available for each employee at a time, could complement the current system or could serve as a substitute to the current system on the whole. E-learning is an existing training method in the diverse and extensive educational system of MÁV Co. to provide trainings for employees. In order to be more efficient, it would be worth considering how it could be extended to external employees. Besides, Tactics of Private Security Measurement videos, thought-provoking case studies and easily understandable legislative explanations could be incorporated in the electronic material. In the end, a test could be done to verify the extent security guards' level of knowledge has risen [14, 15].

This learning method could also be applied in case of handover of duty. For instance, in case of each handover of duty the security guard could read a short summary of the topics the 2-3 question test is about. Using the answers given, time for preparation, time spent for giving an answer, the program could calculate which field would need to be further practiced in case of each security guard. Also, the program could serve as a point of reference along what guidelines to develop the learning material. The training schedule could be shaped up-to-date, with constant feedback according to the needs. Also, emphasis on topics could be shifted based on necessities. All this in order for an intelligent application to support the safeguarding activity of MÁV Co. in the complex system of smart towns. This intelligent application is capable of adjusting to the security guards' needs and level of knowledge and is able to react on these elements besides maintaining a focus on executives' needs [16, 17].

ACKNOWLEDGEMENT

The research on which the publication is based has been carried out within the framework of the project entitled "The Development of Integrated Intelligent Railway Information and Safety System" (Application number: GINOP-2.2.1-15-2017-00098).

REFERENCES

[1] Berek, L. and Solymosi, J.: *Safety of Transport of Hazardous Materials.* Bolyai Szemle **24**(2), 46-62, 2015,

[2] Staffer at MÁV Zrt.: *Interview*. Security Directorate General, Date of the interview: 2nd October 2017,

[3] –: *MÁV-groups homepage.* https://www.mavcsoport.hu/mav-csoport/bemutatkozas, accessed 2nd November 2017,

[4] Mezei, I.: T*he Hungarian Railway is 125 years old.* MÁV Zrt., Budapest, 1993,

[5] *A MÁV Zrt. Operative and Organisational Manual Volume I. General data and regulations*. https://www.mavcsoport.hu/sites/default/files/upload/page/mszsz170101.pdf, accessed 2nd February 2018,

[6] Bodrácska, Gy. and Berek T.: *The role of the preventive provisions in the complex security system during the building trade projects*.
Hadmérnök **5**(1), 17-23, 2010,
[7] Bodrácska, Gy. and Berek, T.: *Manpower defence in the building sector of safeguarding*.
Hadmérnök **5**(4), 38-49, 2010,
[8] –: *MÁV Service-provider Center Co. Baross Gábor Center of Education*.
http://www.bgok.hu/index.php, accessed 2nd November 2017,
[9] Beke, É. and Kovács, T.: *Principles and objectives of the safety and security science in the United States' educational system*.
Hadmérnök **12**(4), 207-215, 2017,
[10] Vasvári, Gy.: *Security organising methodology – Information Security Management System Organisation Methodology*.
Vasware Consulting, Budapest, 2011,
[11] Krauzer E.: *Tactics for Private Security Measurement for Security guards and Armed Security guards*.
PRO-SEC Publishing Company, Budapest, 2012,
[12] –:*Decree of Ministry of Internal Affairs on the professional and exam requirements of qualifications belonging to the sector of Minister of Internal Affairs, as well as countermanding ministerial decree on certain, professional and exam requirements.*
20/2013. (V. 28.)
[13] –:*Decree of Ministry of Internal Affairs on issuing Operational and Duty Manual of armed security sentry*.
27/1998. (VI. 10.)
[14] Dai, N.H.P.; Van Thinh, D. and Rajnai, Z.: *Learning attitude in XXI century*.
2016 IEEE 14th International Symposium on Applied Machine Intelligence and Informatics (SAMI). IEEE, Herlany, pp.115-119, 2016,
http://dx.doi.org/10.1109/SAMI.2016.7422992,
[15] Tokody, D., Holicza, P. and Schuster, G.: *The smart mobility aspects of intelligent railway*.
2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics. Timisoara, pp.323-326, 2016,
http://dx.doi.org/10.1109/SACI.2016.7507394,
[16] Némediné, K.K.; Káposzta, J. and Péli, L.: *Analysis of the Applicability of Smart Initiatives in Hungary.*
Studia Mundi – Economica **4**(4), 29-37, 2017,
[17] Forgó, S.; Hauser, Z. and Kis-Tóth, L.: *Learning without the boundaries of space and time*.
Iskolakultúra **8**(12), 123-139, 2004.

Interdisciplinary Description of Complex Systems 16(3-A), 327-332, 2018

THE CATEGORIZATION AND INFORMATION TECHNOLOGY SECURITY OF AUTOMATED VEHICLES

Attila Albini*, Dániel Tokody and Zoltán Rajnai

Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.16.3.4
Regular article

Received: 23rd March 2018.
Accepted: 31st August 2018.

ABSTRACT

In addition to mechanical changes automation plays an increasingly important role in the evolution of vehicles. The development of autonomous automobiles is the driving force behind the evolution of the information technology (IT) infrastructure in vehicles. Self-reliance requires more and more automation. Enhanced level of automation requires increased operational reliability. This will also resulting an increased level of safety in the cyberspace of vehicles. Endangering cyberspace can also come from a threat of natural and human origin. IT security is the protection against threats of natural origin. It includes protection against natural and technological impacts. For these reasons, it is important to increase IT security in the IT infrastructure of vehicles. This article examines IT security increasing system building technologies from the aspect of the overall IT infrastructure of vehicles. These technologies enable faster processing, increased availability and greater flexibility. The study requires the creation of a new vehicle automation categorization. Technologies are examined according to these new categories and the functional layers of the general IT infrastructure.

KEY WORDS

IT infrastructure, IT security, increase, technology, vehicle

CLASSIFICATION

ACM: C.0, K.6.5
JEL: O39, R41

*Corresponding author, η: attila.albini@gmail.com; +3630 526 7757;
OE-BDI office, Nepszinhaz str. 8, 1081 Budapest, Hungary

INTRODUCTION

For a long time, technological progress was a top priority in vehicle development. Shortly afterwards solutions appeared that affected the integrity of the consignment. This becomes more important for the transport of special items, living things, humans and dangerous materials. The following viewpoints were to enhance the comfort and driving experience. Later the environmental impact of vehicles became detectable. As a further problem, the amount of raw materials used to produce fuel is finite. Alternative solutions for fuel, engines and power transmission have appeared to maintain the environment and technology. The electronics and ICT (info-communication technology) help the development of sustainable technologies [1, 2]. However the human factor is the biggest risk in the safety of vehicles. This risk is equally visible in the design, manufacturing, maintenance, driving of the vehicle and in the organization of the traffic. Sustainability requires the risks be treated. Automation reduces the human factor [2, 3]. The use of electronic and information technologies is the basis of automation. The use of ICT makes the question of cyber security important. IT security contains the protection of cyberspace against natural impacts and technological failures [4, 5].

This article explores IT security enhancing technologies from the aspect of IT infrastructure according to the vehicle automation and the automation of traffic organization. The analysis of IT security enhancing technologies follow the logic of the solutions used in the construction of ICT clouds. These technologies enable faster processing, increased availability and greater flexibility. The examination reveals that it is worth introducing wider categorization of vehicles and traffic management systems. Therefore, the study also proposes a new categorization. The IT security increasing technologies are analyzed according to these new categories and the IT infrastructure layers.

TECHNOLOGIES THAT INCREASE INFORMATION TECHNOLOGY SECURITY

The need for increasing IT security has gradually emerged in the development of information technology. This primarily means independent operation from natural and technological impacts. Secondly it means that the management of resources is flexible. The cloud systems have developed along a similar criteria system. Thus, analysis of building technologies used in clouds can help in the examination.

The first major problem of IT systems was to shorten the processing response time. The answer was the grid technology. Later on to increase the availability became the main consideration. The solution is the cluster technology. Virtualization is the answer to the problem of flexible resource grouping. System protection against major impacts has led to the emergence of the disaster-tolerant solutions based on the split technology [4].

The purpose of grid technology is to shorten processing time. Performing tasks is autocratic. Multiple processing points perform a particular task at a time. Each processing point only performs a subtask that assigned by the controller component. If a processing point error occurs, the subtask is redistributed to another processing point. There is no need for fast communication between the components. Heterogeneous devices can be included in the system [4].

Cluster technology aims to increase availability. Performing tasks is based on a democratic principle. There are several processing points but one task is performed by only one processing point. If a processing point error occurs, another processing point takes over its role. The change of role is very fast and is based on a joint decision of the processing points. This mechanism only works with fast communication. This technology requires homogeneous processing points [4].

The primary purpose of virtualization is to ensure regrouping of resources. To achieve this possibility the resources of the virtualized structure layer are covered and are presented only in the required quantity and quality to the upper layer. This will ensure that the system resources are distributed flexibly. The goal of split technology is replicating consistent system states to long distance. This will allow the system to restart in a remote place in case of a critical impact [4].

Cloud systems could be created by using these technologies. These technologies serve to increase IT security. So the IT security of IT infrastructures should be considered in accordance to the principles of these technologies.

GENERAL INFORMATION TECHNOLOGY INFRASTRUCTURE

The modeling of the general IT infrastructure should be built on philosophical basis for the sake of uniform analysis. The proposed aspects are the structural and functional division of the infrastructure. Infrastructure layers can be identified on the basis of structural layers, which is consistent with human abstraction levels. Functional divisions can be defined by identifying the equivalence with the abstract categories of human thinking [6].

Structural layers can be considered as the vertical segments of the system. The bottom layer is the fundamental layer. It contains the energy resource management. This layer corresponds to the natural energy environment of man. The second layer is the hardware layer, which generates the physical IT resources. This layer is analogous to man's material environment. Next layer is the virtual layer. This generates the logical IT resources and corresponds to human modeling. The operation layer is the implementation of the main features. This layer corresponds to the operating layer of the model. The management layer is the top layer, which provides the operation of the system in time [6].

Horizontal division may be the functional division. These are information paradigm elements based on abstract categories. These should be supplemented with components that express change. Elements of the horizontal structure include storage, transformation, transmission, statogenesis (non-organizational changes) and morphogenesis (organizational changes) [6].

AUTOMATION LEVELS OF VEHICLES

Classification of vehicle automation is currently based on the automation of the vehicle's driving function [3]. Because of the impact of IT security technologies, it is important to take into account all related components of the system and their problems. Therefore the categorization used so far is not enough. To identify new categories the abstract categories can help: thing, property, relation. In the aspect of vehicles these are the technical functions of the vehicle, the storage function of the vehicle and the movement of the vehicle. An expanded interpretation of the relation category requires the inclusion of the aspect of transport organizing. It corresponds to the control of the transporting. An example sentence for checking: “the vehicles took the consignments to the destination within the planned time”. In the criteria system of examination *the vehicle* is equivalent with the technical compliance, *consignment* is equivalent with the storage, *took* with the move, *destination* and *in time* with the time management and routing. Problems associated with the aspects are: storage, maintenance, driving, routing. The levels to be found for each problem can be the following:

- category S (storage) – (i) objects, (ii) living things and special objects, (iii) humans, (iv) hazardous material,
- category M (maintenance) – (i) traditional maintenance, that neither detects errors nor periodic maintenance automated. (ii) controlled maintenance, where proactive monitoring is performed but repair management and periodic maintenance are not automated,

(iii) with the exception of periodic maintenance the vehicle manages the errors automatically, (iv) fully automated, where the vehicle manages errors and periodic maintenance automatically,

- category D (driving) – (i) traditional driving. (ii) controlled driving, in which case a supervisor can take over the driving. (iii) fully automatic driving. (iv) convoy driving, where vehicles close to each other synchronize their movements,
- category R (routing) – (i) conventional static routing, (ii) dynamic on-line routing, (iii) dynamic routing with centralized control, (iv) dynamic central and community routing at the same time.

The new classification of automated vehicles can be defined by the SMDR categorization system. For example, the SMDR-3232 marking means that the vehicle delivers humans, has controlled maintenance, automated driving and dynamic routing. Table 1 shows the categorization.

Table 1. New categorization of automated vehicles.

Categories	**Category S**	**Category M**	**Category D**	**Category R**
Abstract category	Property	Thing	Relation	Control
Aspect of vehicle	Storage in vehicle	Technical operation	Moving the vehicle	Traffic control
Problem	**Storage**	**Maintenance**	**Driving**	**Routing**
Level 1	Objects	Traditional maintenance	Traditional driving	Static routing
Level 2	Creatures, special objects	Controlled maintenance	Controlled driving	Dynamic routing
Level 3	Humans	Periodic maintenance	Automatic driving	Central routing
Level 4	Hazardous material	Automatic maintenance	Convoy driving	Community routing

TECHNOLOGIES IN INFORMATION TECHNOLOGY INFRASTRUCTURE

IT security increasing technologies in the IT infrastructure of vehicles should be examined by the layers and the new categories.

It is worth minimizing the risk of all threats in the energy layer from S2, M3, D3, R3 levels. At least in vibration, water intrusion and thermal protection. In the power supply at least the cluster technology principle should be applied.

With regard to hardware devices the local processing should be ensured above M2 and D2 levels. Not self-contained sensor and actuator units should be used, but gridded processing units. This reduces the amount of data being transferred. In addition the big data effect occurs later in the central unit. This solution also allows for the redundant storage of data. This principle is in line with the principles of increasing the technical security of IoT devices [2]. For the internal communication of the vehicle on D3 and R3 levels the cluster principle should be used. For the external communication on D4 and R4 levels the gridded cluster principle should be used.

When processing data it is worth introducing virtualized service management. From a logical point of view it is necessary to separate the handling of the physical parameters and the parameters of the logic functions required for the operation of the vehicle. The relationships

and dependencies of these two layers must be determined. This follows the principle of virtualized grid-cluster. Usage of this technology is recommended above the M2 and D2 levels. In addition it must be ensured that a given parameter can be defined in at least two different ways to ensure the redundant calculating.

The functions of the vehicle must be implemented in the operational layer. Artificial intelligence items should be used to make decisions because they can contain heuristic elements [7] and provide a quick method [8-10]. In category S it is necessary to allow the use of split technology for convenience and possible legal compliance. This will allow storing convenience functions and the law specific parameters in a vehicle-independent location. It makes the initial parameterization of the vehicles simple [5].

From R3 level, it is strongly recommended to use all that technologies in traffic management centers which help increase availability, ensure system integrity and data consistency. It is also recommended to use full scale management and disaster tolerant solutions.

CONCLUSIONS

The development of the ICT systems is becoming increasingly important in the development of vehicles. The level of automation is growing steadily [1-2]. Sustainability also requires increased security. Increasing security also requires increased security of IT infrastructure. This is a part of IT security [5]. In the case of vehicles, this primarily means safety against natural impacts and technological failures. Furthermore it means shorter processing time and more flexibility. The requirements of the IT cloud systems are similar. So the principle of inquiry is the same as principle of examining IT cloud building technologies [4-5].

The current definition of automation levels does not match the scope of the examination [3], so a new and more extensive automation categorization has been created. New categories are defined on the basis of abstract categories of human thinking and supplemented with statogenesis. These correspond to storage (S), maintenance (M), driving (D) and routing (R) problems. This was the basis for SMDR categorization. Each subcategory has four levels, depending on the degree of automation.

IT security increasing technologies in the IT infrastructure of vehicles have been examined in the layers of infrastructure [6] and the new categories. Proposals have been made to apply the principles of cloud building technologies and to use artificial intelligence [7-10]. It was found that the technologies used to enhance the features of vehicle systems functions is the same as the technologies used to increase the technical security of IoT devices [2]. Further expectation is that systems of traffic management centers created in the future should be like IT clouds.

ACKNOWLEDGEMENTS

The research presented in this article was carried out as part of the EFOP-3.6.2-16-2017-00016 project in the framework of the New Széchenyi Plan. The completion of this project is funded by the European Union and co-financed by the European Social Fund.

REFERENCES

[1] Mester, G.; Pletl, S.; Pajor, G. and Jeges, Z.: *Flexible Planetary Gear Drives in Robotics*. Proceedings of the 1992 International Conference on Industrial Electronics, Control, Instrumentation and Automation. San Diego, pp.646-649, 1992, http://dx.doi.org/10.1109/IECON.1992.254556,

[2] Wolz, U.: *The required technologies for Automotive towards 2020*. The 20th Asia and South Pacific Design Automation Conference. IEEE, Chiba, p.1, 2015, http://dx.doi.org/10.1109/ASPDAC.2015.7058916,

[3] SAE International: *Automated Driving – Levels of driving automation are defined in new SAE International standard J3016*.
https://cdn.oemoffhighway.com/files/base/acbm/ooh/document/2016/03/automated_driving.pdf, accessed 20th March 2018,

[4] Albini, A. and Rajnai, Z.: *Felhőelméleti fenntarthatóság adaptálása humán rendszerekre – Adapting cloud computing sustainability to human systems*. In Hungarian.
Lépések a fenntarthatóság felé **22**(3), 17-19., 2017,

[5] Kovács, Z.: *Cloud Security in Terms of the Law Enforcement Agencies*.
Hadmérnök **7**(1), 144-156, 2012,

[6] Albini, A.; Tokody, D. and Papp, J.: *IT Infrastruktúra Informatikai Biztonsági Aspektusai – IT Security Aspects of IT Infrastructure*. In Hungarian.
Bánki Reports **1**(1), 11-16, 2018,

[7] Rotar, C. and Iantovics, L.B.: *Directed Evolution – A New Metaheuristic For Optimization*.
Journal of Artificial Intelligence and Soft Computing Research 7(3), 183-200, 2017,
http://dx.doi.org/10.1515/jaiscr-2017-0013,

[8] Rodic, A.; Mester, G. and Stojković, I.: *Qualitative Evaluation of Flight Controller Performances for Autonomous Quadrotors*.
In: Pap, E., ed.: Intelligent Systems: Models and Applications. Topics in Intelligent Engineering and Informatics **3**. Springer Verlag, Berlin & Heidelberg, pp.115-134, 2013,
http://dx.doi.org/10.1007/978-3-642-33959-2_7,

[9] Brassai, S.T.; Iantovics, L.B. and Enachescu, C.: *Optimization of Robotic Mobile Agent Navigation*.
Studies in Informatics and Control **21**(4), 403-412, 2012,
http://dx.doi.org/10.24846/v21i4y201206,

[10] Mester, G. and Rodic, A.: *Sensor-Based Intelligent Mobile Robot Navigation in Unknown Environments*.
International Journal of Electrical and Computer Engineering Systems **1**(2), 1-8, 2010.

Interdisciplinary Description of Complex Systems 16(3-A), 333-341, 2018

ACCURATE RADIOFREQUENCY IDENTIFICATION TRACKING IN SMART CITY RAILWAYS BY USING DRONES

Péter Miksa Hell* and Péter János Varga

Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.16.3.5
Regular article

Received: 8th May 2018.
Accepted: 31st August 2018.

ABSTRACT

Smart traffic is one of the key pillars of a smart city infrastructure. In the near future, more and more automated shipping systems are going to be used, eliminating the human factor as a possible source of error. In other words, safe operation of automated systems is one of the most important tasks. The direct supply of smart cities and their industrial facilities is best served by road and rail freight and passenger transport. The spreading of laws and automated systems reduces the number of accidents, but it does not completely eliminate it. With regard to the railway disasters that have occurred in recent years, we have observed that the time between the accident and the start of the rescuing process and repair is one of the most important factors for a successful operation. The localization of railway accidents is often difficult or time-consuming due to field conditions. This time can be greatly reduced by a drastic system that helps the work of disaster relief agencies and conscripts. Trolleys and tankers are nowadays equipped with an RFID (Radio Frequency Identification) transponder to keep track of shipment movement. In this article we investigate what kind of assistance could a drone equipped with RFID reader and navigation infrastructure provide in case of a traffic accident or a disaster situation, with particular regard to the dangerous goods transported on a fixed track. The goal is to develop the application of a modern and innovative technology that can make a smart city more secure.

KEY WORDS

drone, RFID, railway, communication, disaster situation, dangerous goods

CLASSIFICATION

JEL: L63, L92

*Corresponding authors, η: hell.peter@kvk.uni-obuda.hu, –;
Óbuda University, Tavaszmező u. 15-17., H – 1084 Budapest

INTRODUCTION

Railway accidents are still happening today. Their number has declined in recent years, but according to statistics, it is still high. Figure 1 shows the number of the evolution of European accidents between 2010 and 2016 [1]. When it comes to disasters, one of the most important factors is to obtain the information that necessary to start a professional rescue.

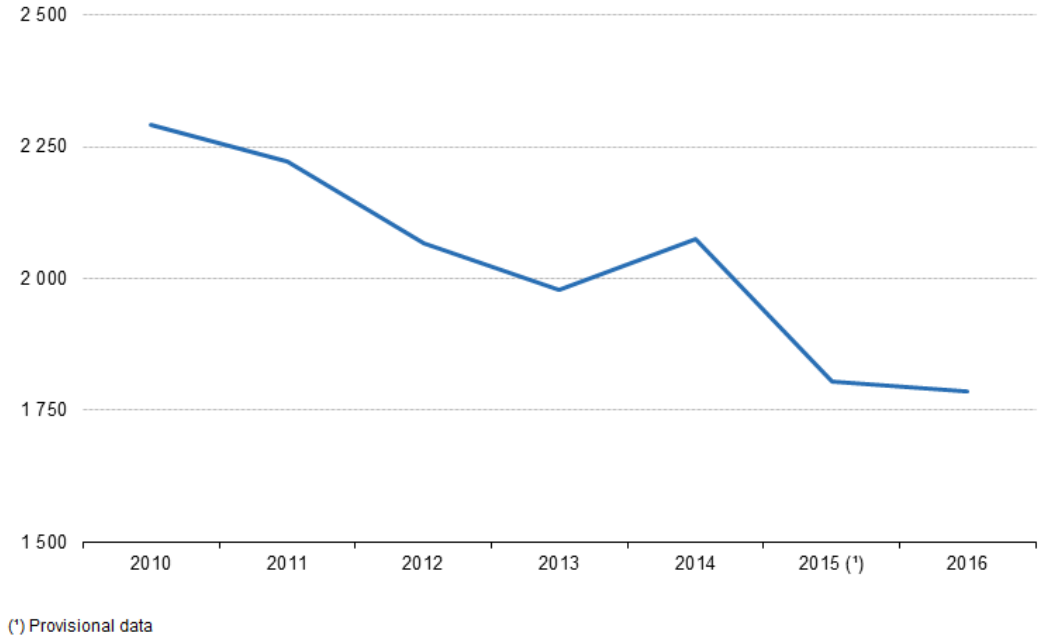

Figure 1. Number of rail accidents in the EU, 2010-2016 [1].

Smart development aims to provide an integrated solution to the problems of urban life, but it also brings a number of new problems along, which should also be addressed. The creation of smart cities attracts the infrastructure development of its industrial facilities. The use of new technologies not only offers opportunities but also raises security issues. Therefore, all options should be taken into account in the design, installation and operation of such systems. The latest digital technologies should be applied to existing, but well-functioning systems.

The aim of the research is to create a drone system that would reduce the time of the exploration of accidents. The spread of drones for different target tasks is emerging. The smart city concept provides an opportunity to create an infrastructure that can use such tools in special, even life-saving cases. Researching this area can help the use of drones in disaster recovery.

Theoretical and practical implementation of the research is underway. This includes assessing the possibilities of using target drones in a disaster situation and the possibility of using the prepared drone. Practical test measurements are ongoing with experts in disaster prevention.

PRESENTING AND DEFINING THE TERMS USED IN THE RESEARCH

The following terms and concepts are of fundamental importance to understand this topic.

- Hazardous Substance: Any solid, liquid or gaseous substance of which the manufacturing, handling, storage, transport usage can produce infectious, poisonous, irritating, flammable, explosive, corrosive or harmful substances, or other harmful substances such as steam, mist, or radioactive radiation, and may thus endanger the health of those who come into contact with it or damage property. The transport of dangerous substances and hazardous

waste is governed by international conventions (Basel Convention): RID for Rail transport; ARD for road transport and AND for waterway.

- RID – Regulation on International Carriage of Dangerous Goods: The European Convention on the International Carriage of Dangerous Goods by Rail. It is co-ordinated with ADR and UN-numbers (UN-ID) in the Act LXXX of 2011.
- ADR – *Accord Dangreuses Route*: European Agreement on the International Carriage of Dangerous Goods by Road. It was established in 1957 in Geneva. Hungary joined ADR in 1979.
- ADN – The European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways: The European Agreement on the International Carriage of Dangerous Goods by Inland Waterways was established in 1941. European states consider this to be the guiding principle for inland waterway navigation.
- UN numbers: An internationally recognized identification number issued by the United Nations (UN) Expert Committee for the identification of certain chemicals or groups of compounds. On hazardous material vehicles, the hazardous orange board plays a role in alerting other road users to the danger of dangerous goods being transported, and on disaster response units to provide essential information during an accident or an emergency. That is why the correct marking of the vehicle is a very important aspect. Irregular vehicle marking may have unforeseeable consequences. The hazard number is also known as the Kemler number. The orange warning sign is divided into two parts. The upper part contains the danger number and the lower part contains the material number.
- UAV – Unmanned Aerial Vehicle or drone: Remote controlled (RC) aircraft. The nowadays fashionable ‘drone’ expression has been given to this device after its beelike buzzing voice. Drones were initially military targets, but they became involved in civilian development with the advancement of technology. Regarding the purpose of their civil use, the main areas are hobby, film production, parcel delivery, scientific research, law enforcement, and military duties.
- RFID – Radio Frequency Identification: Technology used for automatic identification and data transmission, the core of which is to store and transmit data using RFID tags or transponders and a reader. The reader and the label do not have to physically contact each other. The reading distance depends on the tag and the reader, and can vary from a few centimeters to several tens of meters. The RFID tag can be fixed, glued or embedded in the object to be identified. This can be an object, component, creature, or a system to be identified.

An example of an alloy of systems is a railroad or rail network within the transport sector. Installed sensor systems may already be able to optimize the current traffic situation without human intervention or send feedback to the central supervisor. But such a complex infrastructure can only be an element of smart cities, smart industrial facilities, where, besides the ease and order of living, security also plays a major role. Railway accidents can occur not only in cities, where it is easy to carry out rescue processes, but also in the open, difficult to reach track between municipalities. The RID by Rail stipulates the UN numbers (United Nations numbers) labeling for transport and storage of cargo containing dangerous goods [2]. If these *labels* are visible, and not damaged, then the goods are easily identifiable. However, in the event of an accident, the labels could become damaged or end up in non-visible, inaccessible places due to vehicle and cargo damage. Identifying the leakage of hazardous materials from damaged packaging and tankers is a much more complicated task from then on. Identification of unidentified hazardous chemical substances is currently carried out with special instruments but in many cases they cannot be transported to the site with a drone due to the physical parameters (mass, geometrical extension) of these instruments [3]. The most

important factors in the event of such accidents are time, rapid analysis and rescue. Therefore, the implementation of a different method for the identification of damaged goods and cargo can be of great help in the future. In Europe, there is currently no uniform tracking system for trains. The tracking is mostly limited to locomotives, not to rail wagons. Therefore, in the case of such accidents, it is difficult to pre-assign important backup-enhancing such as the exact type of accident and its spatial extent. It is difficult to determine the type and quantity of the damaged materials that are released from packing units. The method of study does not analyze the chemical and physical properties, but reads the RFID chip information placed in the cargo that contains cargo-specific data [4]. In this research, we investigate how a radio frequency RFID reader system mounted on a drone and the infrastructure for identification can provide assistance in an accident or a disaster.

DRONES USED IN DISASTER RELIEF

Drones (UAVs) were originally designed to be unmanned vehicles for military use. The development of civil aircraft has been accelerating in the last decade and its scope has also widened. Its management and orientation capabilities have grown dramatically thanks to the rapid change in microelectronics, while the performance of the devices has also increased, enabling them to be deployed in newer areas. The use of drones for security and disaster recovery must be distinguished from hobby use, as its advantages are unquestionable [5].

In Europe, disaster prevention agencies possess a number of specialized drones. Among others, they play a major role in flood protection, such as helping to determine the extent of the flooded area, the location of possible critical points and the availability of escape routes. They also play a useful role in the fire brigade, for example in the case of forest fire, the size of the fire can be quickly assessed. The typical equipment for these devices includes a high resolution camera, a thermal camera, or an air component sensor, a gas sensor, and a radiation meter [6, 7].

During the research, we examined several devices currently in retail [8]. Most small-sized (less than 5 kg of self-weight) drones are not capable of performing special tasks. Because of their stability due to their take-off mass, they cannot transmit other measuring instruments or sensors beyond the base camera. In most cases, the implementation of disaster protection tasks is carried out in non-ideal visibility and weather conditions, so only high-end drones with high performance, more stability, higher payloads, higher take-off weights of up to 8 to 10 kg and more reliable navigation are convenient. Drones capable of doing such tasks are usually small series mass devices or individually assembled devices, which are much higher in price than a hobby drone, but still are of a magnitude more favorable than a helicopter carrying out similar tasks. Not to mention the operating, maintenance costs and the education of people handling them [9].

RFID TECHNOLOGY

The RFID contactless system for identifying information is one of the most dynamically developing communication technologies today. We use such systems for access control systems, bankcard payment (Paypass), or toll payment systems for lorries. The procedure uses radio signal transmission for data exchange. When identifying hazardous goods, the basic idea is that the object to be identified contains a transponder element capable of storing information of the goods so that they can be identified [10].

The RFID active transponder, shown in Figure 2, is a mechanically strong, robust, weather-resistant and corrosive, highly refractory unit. It also ensures the operation of wagons. For more reliable identification, transponders can be placed on several sides (side, bottom, top) of rail tankers. This will increase read access.

It is possible to place a microcontroller on the side of the railway wagon, tanker, or container, or on the cargo to store the data needed for the identification of the transported material. It should also contain the antenna required for the radio link. The other unit of the RFID system is a reader mounted on the drone as shown in Figure 2. The readings would be transmitted via a radio channel to the evaluating experts [11].

The reading distance between RFID readers and transponders depends on the type of system. The current readout of active transponders and high gain antennas is currently a few tens of meters, but this distance increases with the development of technology, which further increases the efficiency of the system.

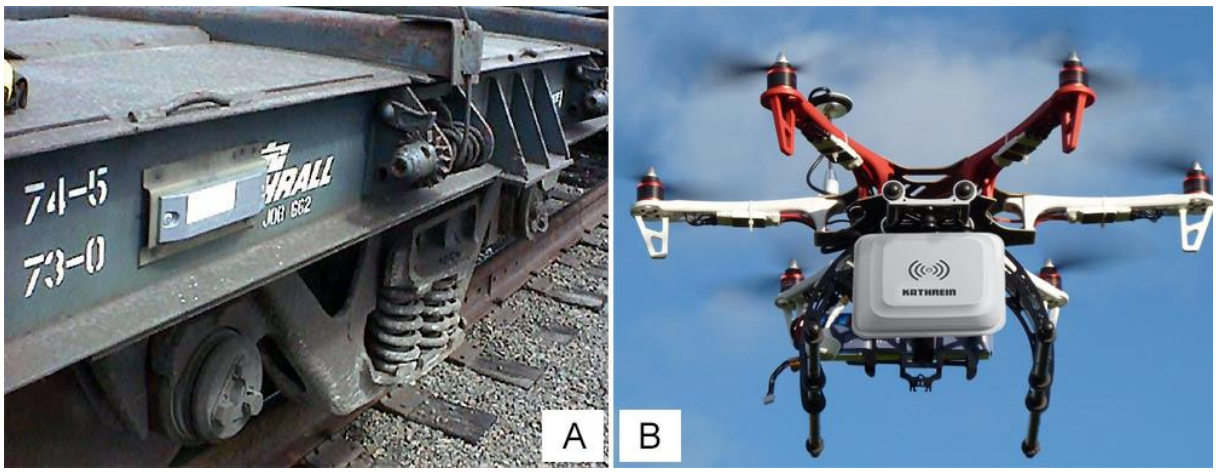

Figure 2. A railcar mounted with an RFID transponder (left) [12] and a drone mounted with an RFID reader (right).

In the event of an accident, the vehicle often suffers a serious damage or the visibility may be inadequate, so the UN numbers on the cargo and other data may not be visually legible. RFID identification allows one to read vehicle and cargo data from a safe distance. The data would be sent to the rescue control bodies by the drone, who may begin to devise the backup strategy with the necessary information, and prepare protective equipment, and neutralizing and disinfecting devices [13]. The basic structure of the RFID system is shown in Figure 3.

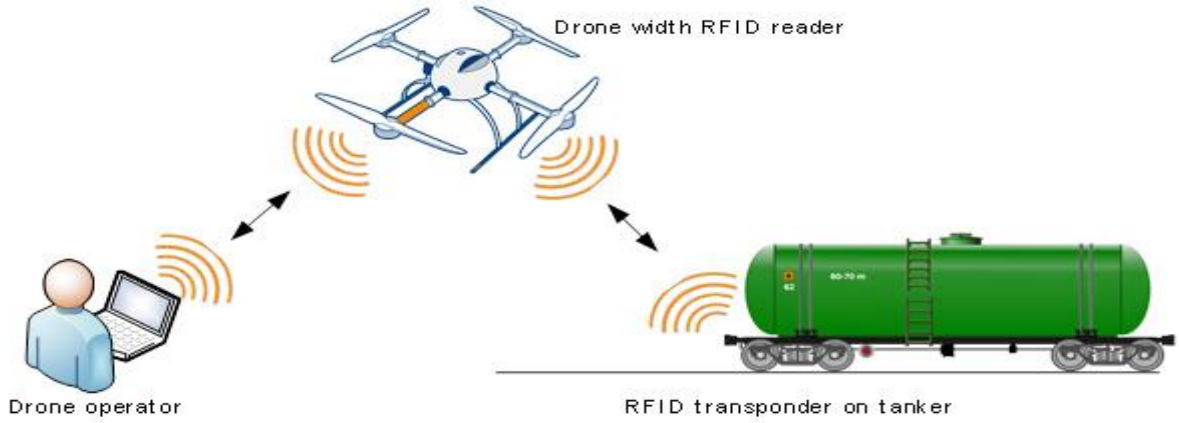

Figure 3. Theoretical structure of a RFID reader system mounted on a drone.

CHOOSING THE RIGHT DRONE FOR THE TASK

Safe operation of a drone is influenced by many factors. These include:

- the geometry of the drone, its own mass, its maximum take-off mass,
- remote control (communication) type and range,
- power supply required for operation, flight time,
- weather and environmental conditions.

The geometrical size of the drone and the take-off mass are related to stability. An aircraft specially designed for a disaster protection tasks is from 8 kg to 10 kg. It is easy to transport, manageable and is safe and stable in a wind speed of up to 50 km/h, with a 65 km/h wind gust. The communication distance between the drone and its pilot can be several kilometers without causing any technical problems, but according to the law there has to be a direct view of the flying device. Regarding the usability of the system, two parameters are determinative: the transportable mass and the sufficient power for the desired distance. The ground must be securely covered by the drone back and forth, and on-site tasks must be carried out, which means additional running time. To do a quick job, the RFID reader antenna on the deck must be able to read from 8 m to 10 m away from the transponder [14]. Determining the reading distance depends on one hand on the compliance of the safe object approach distance and the speed of the drone and the response time of the reader transponder. The reading (object approach) distance can be calculated from the jamming and spreading of the train cars involved in the accident. It is from about 8 m to 10 m in length, compared to the size of a wagon. Larger reading distance requires a larger geometric size and weight antenna system, which also requires higher power consumption. The average reading distance of RFID systems ranges from a few centimeters to some ten centimeters. Larger reading distance is only available from a few manufacturers. Figure 4 shows the comparison of important parameters – with regards to the reading process – of Kathrein RFID readers. The geometric size of reading antennas is within the applicable size limit. Horizontal and vertical opening angles are on average 50°, which in practice means that if a drone equipped with an RFID reader is at a previously defined safe 8-10 m distance away from a transponder-mounted wagon, the scan (sweeping) range is about 10 m radius area. The read-only requirements are met by all three readers, but only the WIRA 7070 is suitable for the weight limit and the power consumption of the antennas.

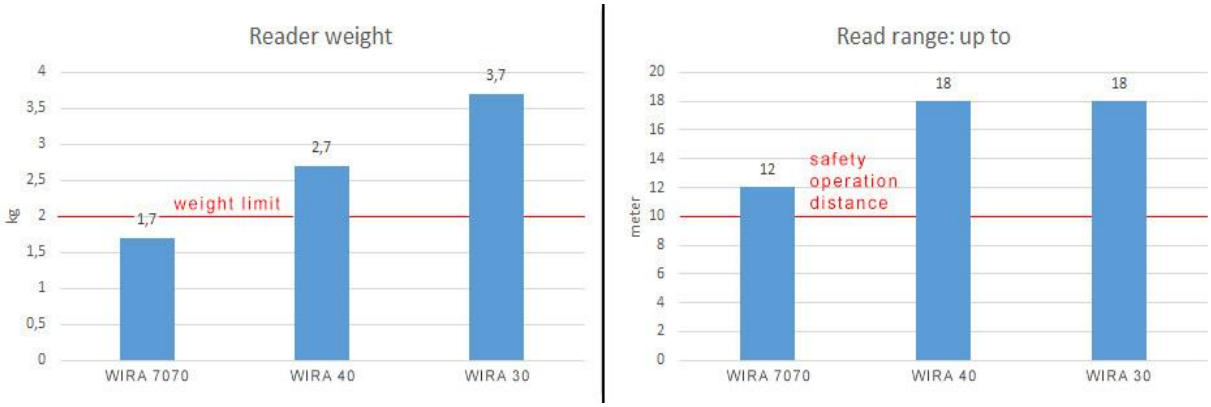

Figure 4. Parameter limits for selecting the RFID reader [15] (authors' edit of https://www.kathrein-solutions.com/datasheets).

The category of drones to perform the task was determined based on the previously described technical requirements and parameters. Henceforth we chose XYRIS 6 type hexacopter manufactured by VespaDrones for the planned test measurements [16]. The basic self-weight of the drone (frame structure, control and navigation equipment, FPV camera, motors, etc.) is 6 kg [17]. The maximum safe take-off mass defined by the manufacturer is 9,5 kg, therefore the deck-mounted RFID reader and accessories (controller, communication unit) should not

exceed 3,5 kg. The manufacturer's recommended maximum flight speed is 50 km/h. Based on the test flights and calculations, the flight time was 25 minutes with an average speed of 30 km/h without load. This time was reduced drastically to 15 minutes once the device was loaded with 3 kg of measuring equipment, thus considerably reducing the flying distance. Figure 5 shows the flight values of the drone without load and under load.

Based on the measurement and computational results, a drone built with test-measuring RFID readers is suitable for carrying out the task. By increasing the reading distance or scanning speed, the workflow can be accelerated, but based on test measurements, the incorrect readout rate of the transponders also increases. Also, the number of missed transponders increases due to the reader-transponder response time.

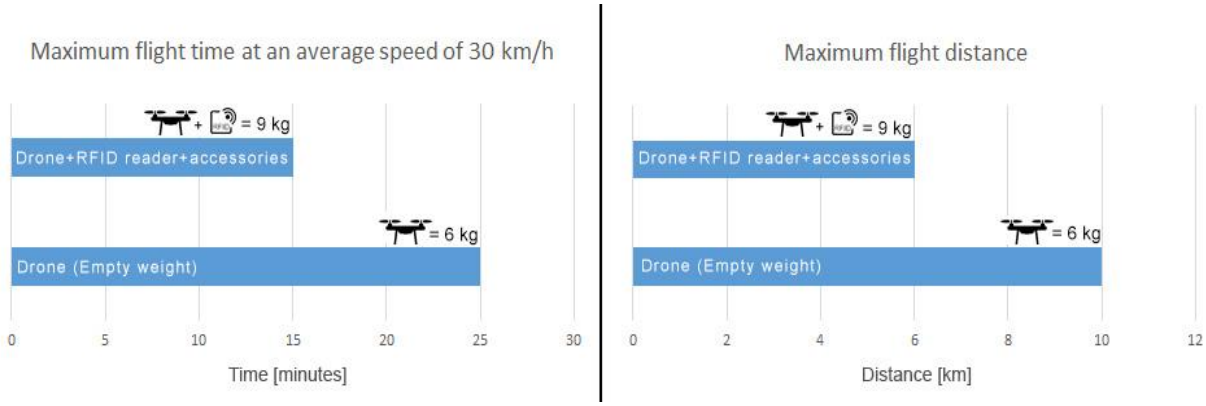

Figure 5. Driving distance with the RFID system (left) and without it (right).

CONCLUSION

Drones have so far had an unquestionable role in disaster relief. Safe operation for a smart city is a must for secure infrastructure, so drone-mounted RFID technology can be of extraordinary significance. If we take into account, based on the current measurements and calculations, that the drone has to perform tasks at the destination site, it can be established that, in addition to the present technical construction, the distance between the drone and the drone pilot cannot be greater than 2-3 km. This distance is not great, if the site is hard to approach by walking or by taking a public road than it can be reached up to a quarter hour earlier with the drone, significantly affecting the rescue result. Test measurements show that the system works at the principle level. Flight parameters of the drone and RFID technology, such as distance or operating time can be increased. The drone-mounted RFID system still requires further improvements, but it can provide undeniable help in quickly identifying hazardous substances. By applying this technology, measures can be taken sooner, with fewer human resources involved.

Conclusions and questions that emerged in the process of calculations and measurements raise new promises and suggestions for further research. But it is undeniable that the RFID system seems to be a good solution and can realize the research ideas. During further work, more drones and RFID systems have to be designed and tested to make the system as effective as possible in the work of disaster protection organizations.

ACKNOWLEDGEMENT

The research on which the publication is based has been carried out within the framework of the project entitled "The Development of Integrated Intelligent Railway Information and Safety System" (Application number: GINOP-2.2.1-15-2017-00098).

REFERENCES

[1] Eurostat: *Rail accident fatalities in the EU*.
http://ec.europa.eu/eurostat/statistics-explained/index.php/Rail_accident_fatalities_in_the_EU, accessed 5th May, 2018,

[2] OTIF: *Convention concerning International Carriage by Rail (COTIF) Appendix C – egulations concerning the International Carriage of Dangerous Goods by Rail (RID).*
https://otif.org/fileadmin/new/2-Activities/2D-Dangerous-Goods/RID_2017_E.pdf, accessed 5th May, 2018,

[3] Šolc, M. and Hovanec, M.: *The Importance of Dangerous Goods Transport by Rail*.
Naše More **62**(3), 181-186, 2015,
http://dx.doi.org/10.17818/NM/2015/SI17,

[4] Kiss Leizer, G.K. and Berek, L.: *The Safety Technology Questions of Wastes Arising in the Course of Catastrophes in the Continental Traffic*.
Műszaki Tudományos Közlemények **5**, 2016

[5] Asghar, K.M.; Safi, E.A.; Khan, U.I. and Alvi, A.B.: *Drones for Good in Smart Cities: A Review*.
https://www.researchgate.net/publication/316846331_Drones_for_Good_in_Smart_CitiesA_Review, accessed 5th May, 2018,

[6] Restás, Á.: *The system and possibilities of training uav pilots for disaster management tasks*.
Bolyai Szemle **24**(3), 157-174, 2013,

[7] Restás, Á. and Dudás, Z.: *Human aspects and special features of uav use supporting disaster mangement*.
Repüléstudomány közlemények **25**(1), 23-45, 2013,

[8] Hell, P.: *Drone protection systems in fesility management*.
Hadmérnök **12**(3), 37-47, 2017,

[9] Rodic, A.; Mester, Gy. and Stojković, I.: *Qualitative Evaluation of Flight Controller Performances for Autonomous Quadrotors*.
In: Pap, E., ed.: Intelligent Systems: Models and Applications. TIEI 3. Springer Verlag, Berlin & Heidelberg, pp.115-134, 2013,
http://dx.doi.org/10.1007/978-3-642-33959-2_7,

[10] Moran, O.; Gilmore R.; Ordóñez-Hurtado, R. and Shorten, R.: *Hybrid Urban Navigation for Smart Cities*.
https://arxiv.org/pdf/1705.01516.pdf, accessed 5th May, 2018,

[11] Kiss Leizer, G.K. and Tokody, D.: *Radiofrequency Identification by using Drones in Railway Accidents and Disaster Situations*.
Interdisciplinary Description of Complex Systems **15**(2), 114-132, 2017,
http://dx.doi.org/10.7906/indecs.15.2.1,

[12] Transcore: *Rail and Intermodal Automatic Equipment Identification*.
https://www.railway-technology.com/contractors/signal/transcore, accessed 5th May, 2018,

[13] Transcore: *RFID and Rail: Advanced Tracking Technology*.
https://www.railway-technology.com/contractors/signal/transcore, accessed 5th May, 2018,

[14] He, W.; He, Y. and Tentzeris, M.M.: *Modeling, design and experimentation of a UHF RFID tag antenna embedded in railway tickets*.
2015 IEEE International Symposium on Antennas and Propagation & USNC/URSI National Radio Science Meeting. IEEE, Vancouver, 2015,
http://dx.doi.org/10.1109/APS.2015.7305097,

[15] KATHREIN Solutions GmbH: *RFID Readers, antennas.*
https://www.kathrein-solutions.com/products/hardware/rfid-antennas, accessed 5th May, 2018,

[16] Vespadrones: *Drone datashit: XYRIS 6 type hexacopter datashit.*
http://vespadrones.com, accessed 5th May, 2018,

[17] Menouar, H.; Guvenc, I. and Akkaya, K.: *UAV-Enabled Intelligent ransportation Systems for the Smart City: Applications and Challenges*.
IEEE Communications Magazine **53**(3), 2017,
http://dx.doi.org/10.1109/MCOM.2017.1600238CM.

Interdisciplinary Description of Complex Systems 16(3-A) 342-349, 2018

PROBABILISTIC APPROACH AND FUZZY SYSTEM BASED SUPPORT OF THE RAILWAY STATIONS' SMART SECURITY SYSTEM

Gábor Liebmann*, László Hanka and György Schuster

Óbuda University, Doctoral School of Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.16.3.6
Regular article

Received: 5th February 2018.
Accepted: 31st August 2018.

ABSTRACT

One of the keystones of the smart city is the transportation. The railway is the crucial part in the main public- and also the goods-transportation today, and the significance will be constantly growing. Nowadays the increase in threats and decrease in the sense of security generates a high need for designing smart and multi-level integrated security systems on the railway stations. The security risk of these territories has risen in the last years, because the public transportation plays an important role in the lives of nowadays people and will grow in the future. That means a rise in incidences of robbery, vandalism and even terrorism. The integration of the conventional systems gives more possibility and reliability for the facility management and the end-users to prevent the aforementioned incidences. The power of the complex (human-electrical-mechanical) system can be usable if in the central monitoring station only qualified and well trained operators work. Because of the difficulty of the multi-level integrated security systems, without suitable and well-trained users and operators the efficiency of the security decrease. Furthermore, the efficiency of the complex system can be lower than the unintegrated conventional realizations, so that's why it is needed to integrate special smart functions.

Managing the smart complex security systems on the aforementioned railway stations are difficult due the human factor and the large number of connections and internal processes. However, the recently created and improved probabilistic approach- and fuzzy system can be a useful mathematical solution for the aforementioned cases. These methods can be used in the full scaled security system, if first – like the Fuzzy logic – an expert level analysis gives enough information about the crucial parts of the system. With them comes the possibility to give and get data from the determined system, and continuously recalculate the factors and – in some cases – it can also be done online. It helps to generate and send prompt information to the facility management, and with it can maximize the fully functional operational efficiency and reduce the hazards.

This article gives a useful guideline for the facility management of the smart cities' railway stations. It declares the main connections with theirs hazards to find the key elements and the in-, and outbound parameters of the smart complex security system. The generated knowledge base will contain also more additional information about the efficiency and the improvement of the system, too.

KEY WORDS

smart security on railway stations, complex security system, fault tree analysis, probabilistic approach

CLASSIFICATION

JEL: C60, O30

*Corresponding author, η: liebmann.gabor@gmail.com; +36 20 825 9954;
8th Népszínház utca, Budapest, H-1081, Hungary

INTRODUCTION

Nowadays the *smart city* is one of the most mentioned expression what can be found everywhere, but the real extent is un-, or poorly-defined. Everybody has only a feeling of it. One can find the broad, data-driven and the citizen-focused definitions depending on which sector is in the focus. There definitions rarely include liveability and sustainability [1].

The transportation is one of the keystones of the nowadays cities, where the railway is the crucial part in the main public and also the long distance goods transportation, and the significance will be constantly growing. The new smart cities also need these service, but with optimized function on a minimized territory is an essential condition, what concentrates the quantity of the travellers and the value of the goods, too. The security risk of these territories has risen in the last years, because the public transportation plays an important role in the lives of nowadays people and will grow in the future. That means a rise in incidences of robbery, vandalism and even terrorism, so to prevent these actions it is needed to design, and operate a *complex* security system on these areas. In this case the meaning of the *complex* expression is a hard connected human-, electrical (multi-level integrated security system), and mechanical protection. The integration of the conventional systems gives more possibility and reliability for the facility management and the end-users to prevent the aforementioned incidences. The power of the complex (human-electrical-mechanical) system can be usable if in the central monitoring station only qualified and well trained operators work. Because of the difficulty of the multi-level integrated security systems, without suitable and well-trained users and operators the efficiency of the security decrease. Furthermore, the efficiency of the complex system can be lower than the unintegrated conventional realizations, so that is why it is needed to integrate special smart functions.

Managing the smart complex security systems because of the aforementioned reasons is difficult due to the human factor and the large number of connections and internal processes. In this article we show and test more mathematical functions and methods that can be usable in the full scaled security system of the Facility Management.

THE RAILWAY STATION'S ENVIRONMENTAL RISK

The stations comprise diverse outdoor and indoor facilities, many of them work 7/24. On the railway stations there is a crucial need to guard passengers, employees, goods, infrastructure, and assets against possible threats. These facilities in particular have become at least as vulnerable as airports. They must therefore meet very demanding criteria with regard to security, safety, communications, and building automation – also to uphold their reputation as providers of safe, well-organized services that travellers and freight forwarders can rely on [2].

The aforementioned enviromental risk generates security challanges of the complex system, such as preventing and responding vandalism, robberies, sabotage and terrorism. When the security challenges are succesfully met, it gives employees and passangers confidence in the safety of train stations [3].

DETERMINING AN OPERATIONAL MODEL OF THE STATION'S COMPLEX SECURITY SYSTEM

The designing-, installating-, and finalizing-term of the security system is only the begining, since the facility management has to operate it constantly 7/24. It cannot be done without specialized and expert employees at the economy and at the security part, too. To prevent the mailfunctions and get the highest efficiency of the system it is needed to generate a special pointer what can show the momentary state of the complex security system.

For the pointer generation the first step is to determine the inputs, the variables, the outputs and the functions of the security system on the station with their inner connections. With the aforementioned elements the operation diagram of the station's global security system is shown in Figure 1. The model is designed for the inner connections of the global security system. The arrows represent the connection and the direction, the bulk of the area represents the importance of the subsystem.

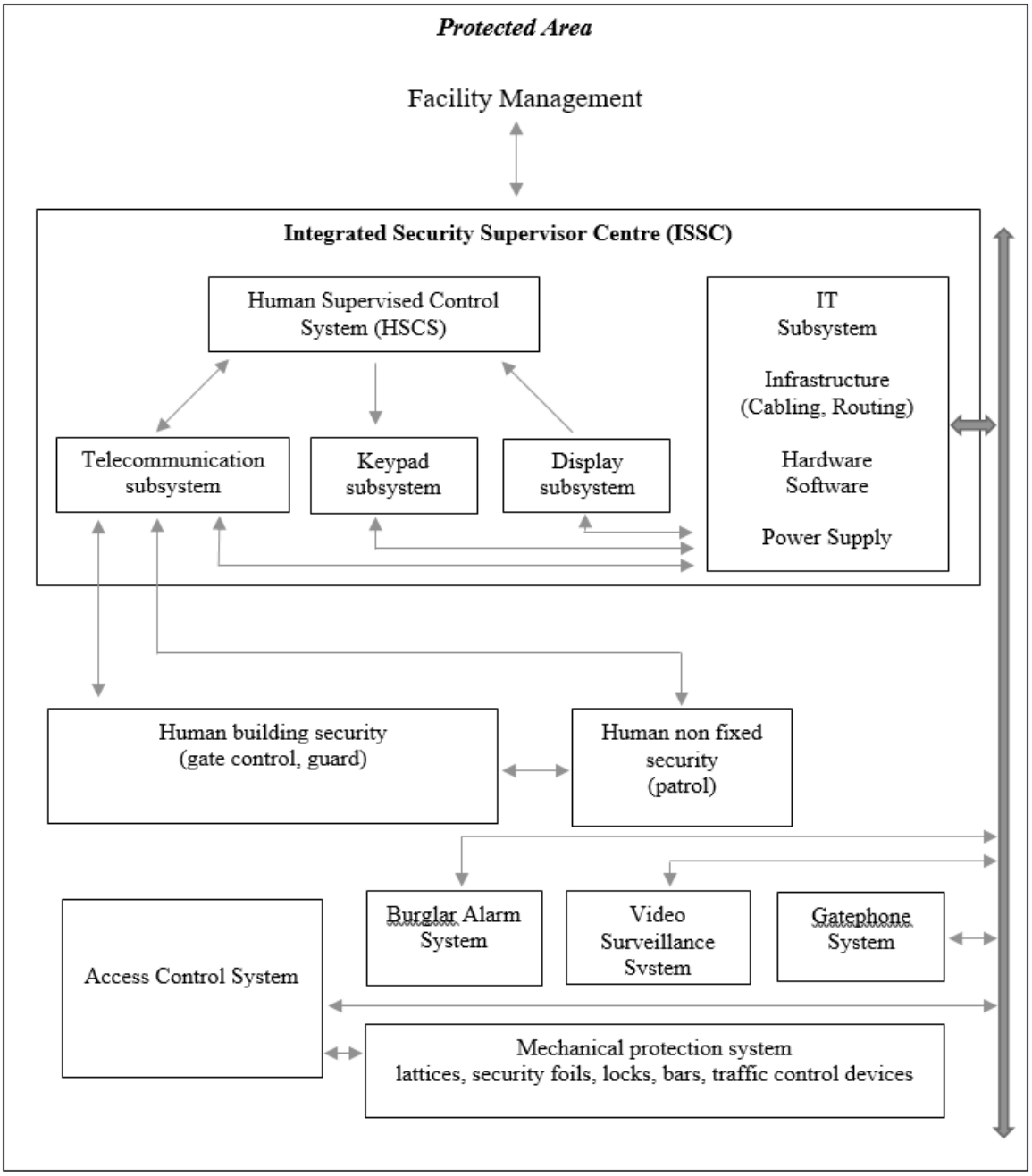

Figure 1. The model of the complex security system on a railway station.

Wthin a station, five independent security parts can be found: the mechanical protection, the access control system, the electrical protection system, the human security system and the integrated security supervisor centre (ISSC). In the system architecture an undetermined protection subsystem the Information Technology area can be found. It is not part of the protection but it has connected to all protection subsystems and it is also connected to the outer area, that means it is one of the most significante part of the complex protection system. The following security subsystems will determine the efficiency of the complex system.

The mechanical protection subsystem

To prevent the unauthorized entrance to a secured area it is needed to install special mechanical elements lattices, security foils to the windows and doors, bars and traffic control devices to the vehicle entrances, and locks for all places where higher risk is possible. These devices are the background of the complex protection.

The access control subsystem

The access control system is the bridge between the mechanical and the electrical protection system. It is neither mechanical, nor electrical part, but both. The main function is preventing the unauthorized entrance to the restricted area, but it also generates alarm signals to the ISSC. It is not only for controlling the traffic but it also stores all information with time-stamps in non-volatile memory at the controlled area and also send them into the supervisor system.

The electrical protection subsystem

The electrical protection subsystem contains the video surveillance, the burglar alarm, the gate-phone systems. These systems are working together and some inputs and outputs of the access control is integrated here through the ISSC, too. It means a burglar alarm signal can occur a video event, so the connected camera will display on the alarm monitor and also can generate an access control event where all connected electric locks are disabled, only the security guards are allowed to pass through these gates.

The *human* security guard and patrol subsystem

The *human* security of the complex system is the most important sector, because without any physical force there can't be an efficient security system. There are two independent part of it, the first part is for the building security, they stand on a pre-defined place (eg. on the passenger and the industrial entrances of the railway stations) of the area and check the traffic and operate the mechanical-, the electrical-, and the access control-systems. The other part of the human security is the patrol. They are well trained guards divided into small teams. They patrol the area, to prevent the hazards of unattended baggage, unauthorized entrance. Theirs official uniform and the physical demonstrative presence gives the opportunity of the secure feeling in the area what can reduce the hazards possibility. In an unexpected event the ISSC can send these teams immediately and directly to the risk to prevent or to solve problems. For the efficient managing of this system we need a hierarchical structure with well-defined information and command routes.

The integrated security supervisor centre's subsystem

The ISSC is for the efficient operation of the protection, what collects all information connected to the protection in the inner and outer area and converts them into the same protocol. With the converted and pre-analysed signals can coordinate with the subsystems.

It can be seen that the subsystems can work together without ISSC, but in this case because of the low level integration the efficiency of them is poor. To prevent any security hazard or bomb attack, it needs an efficient multilevel (low and high) integrated protection system with well-educated and well-trained operators, patrols and security guards. Without the suited trainings it can occur that the efficiency of the complex system is lower than the separated and low level integrated systems, in a disaster because of the latent of the secure feeling the response can be slow or wrong.

PROBABILITY TREE AND FAULT TREE ANALYSIS

To determine all functions with the risk factors in the smart complex security systems on the aforementioned railway stations are very difficult due to the human factor and the large

number of connections and internal processes. However, the recently created and improved probabilistic approach with fuzzy system expert analysis is a useful mathematical solution for the aforementioned cases. These methods can be used in the full scaled security system, if first – like the Fuzzy logic – an expert level analysis gives enough information about the crucial parts of the system. With them comes the possibility to give and get data from the determined system, and continuously recalculate the factors and – in some cases – it can be done On-Line, too. The best method for modelling the aforementioned multi-level integrated system is the fault tree diagram. It is used to conduct fault tree analysis (or FTA).

The FTA is a technique for reliability and safety analysis. The Bell Telephone Laboratories developed the concept in 1962 for the US Air Force for use with the Minuteman system. It was later adopted and extensively applied by the Boeing Company. The fault tree analysis is a symbolic *analytical logic technique* found in operations research and in system reliability. The FTA helps determine the cause of failure or test the reliability of a system by stepping through a series of events logically. The benefits of fault trees is that a fault tree creates a visual record of a system that shows the logical relationships between events and causes lead to that failure. The modularising of the FTA gives the opportunity to reduce the number of inputs and define them in blocks. The modularising has to be done before the analysis takes place [4]. It helps in computerising the FTA and helps also the facility management quickly understand the results of the analysis and pinpoint weaknesses in the design and identify errors. A fault tree diagram will help prioritize issues to fix what occur the failure. In many ways, the fault tree diagram creates the foundation for any further analysis and evaluation. For example, when changes or upgrades are made to the system, you already have a set of steps to evaluate for possible effects and changes. You can use a fault tree diagram to help you design quality tests and maintenance procedures. It is a good pointer that can show the state of the whole complex system.

TESTING THE COMPLEX SYSTEM'S FTA FOR EFFICIENCY METHOD

We made a complex system model of the railway station to test our efficiency computing method. We designed an event buffer on the test complex protection system, what have recorded all important events for a month, after it we have analysed all the events, with that data we could make three different groups that can be used for templates. We hope that these templates will give a fast method of the average efficiency measurement about the system. In the test month we recorded the following events in the event buffer: external buildings false alarms (infra beam detectors outside) occurred 10 times, external buildings false alarms (inside) 5 times, false fire alarms 5 times, stolen mobiles (office area) 3 times, while stolen official stamp and other devices and/or purse (no recorded data) occured 3 times. There was no recorded data for stolen purse, drug usage signs and for poisonous chemical stolen from a technical area.

The first event group contained data that is not directly connected to the complex system (events coming from outside only for redundant recording). The early recognition of these events will be important to reduce the mathematical analysing speed in the future, so they will not go through the FTA analyse method. They will not be dropped, because these items can be used for "no need for FTA analysing" template. These items were in our test system e.g. the false fire events, because these events also came into the *human* protection system but only for redundant recording.

The second event group contained data that is directly connected to the complex system and the occurrence was only one or maximum two times, so these data cannot be used for templates in the future but can significantly modify the efficiency of it (e.g. stolen chemicals, drug usage signs, etc.).

The third event group contained data that is directly connected to the complex system and the occurrence was more than two times, so these data can be used for templates in the future (e.g. external building false alarms inside and outside).

We generated blocks from the complex system elements to reduce the FTA diagrams size, without generating false information in the system, because the aforementioned – fuzzy logic style – expert level analysis gives enough information about the crucial parts of the system.

We could define the fault probability average rate for each subsystem's device of the test system, because of more than 10 years' operational experience in these mechanical and electrical protection systems and more than 4 years' operational experience in these *human* systems.

We made all FTA diagrams for the aforementioned second and third event groups. We made the fault analysis and counted all probability of them, we followed step by step and we got that the probability of fault is between 0,26 and 0,39 the efficiency of the system is between 0,61 and 0,74.

In our test system the following event occurred: From the technical area of the protected station a poisonous chemical was stolen. In that area there are access control system, but this room was not protected, there was a video-surveillance system, but in that room there weren't cameras, the nearest cameras were on the corridor and showed common view about the traffic. On the corridor an access control system can be found, and there was patrol, and at the building's entrance a security checkpoint, too.

The FTA diagram of the event can be seen in Figure 2. The core event can occur by only the Mechanical Protection System Fault – the doors lock fault, or the employee did not use it – but for the post analysing the other subsystems proper protection efficiency is needed. This is one side why we have used it for the FTA all the three other subsystems, and in the future with the FTA refining will give the possibility for the facility management to generate additional suggestions about the system's improvement. The defined access control subsystem fault probabilities were the following: Reader 0,03, Control Panel 0,01 and Electric Lock 0,05. The Access Control Fault probability can be calculated by the following formula:

$$P_T = 1 - \prod_{i=1}^{n}(1 - P_i) = 1 - [(1 - P_1)\,(1 - P_2)\,\ldots\,(1 - P_i)] \qquad (1)$$

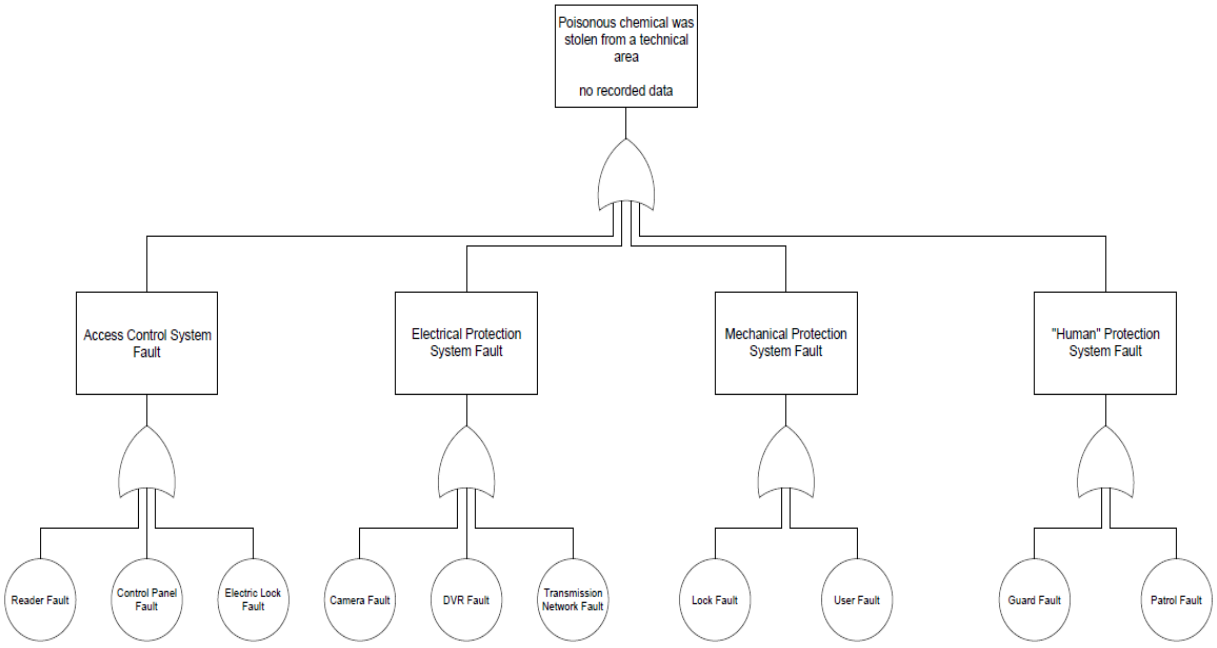

Figure 2. An example event FTA diagram.

The calculated probability of this subsystem was $P_T = 0{,}083$.

The defined electrical protection subsystem fault probabilities were the following: camera 0,1, DVR 0,05 and transmission network 0,05. The counted probability of this subsystem was $P_T = 0{,}18775$.

The defined mechanical protection subsystem fault probability were the following: lock 0,01, and user 0,1. The calculated probability of this subsystem was $P_T = 0{,}109$.

The defined *human* protection subsystem fault probability were as follows: guard 0,02 and patrol 0,01. The coalculated fault probability of this subsystem was $P_T = 0{,}0298$.

The accumulated fault probability indicator number was in this event $P_T = 0{,}356139$, so the efficiency indicator was $1 - P_T = 0{,}64386$.

The analysis showed that the stolen events fault probability rate was the same in the tested complex system, because of the connected subsystems and was not related to the fact that the owner left it unattended or not.

More than 50 events can be recorded in this period and most of them can be used as a template because of the frequently occurrence.

In our test system an unneeded patrol usage event occurred 10 times. More building area have been protected by a burglar alarm system after working hours. This building has in-, and outside area with different sensors. In Figure **Error! Reference source not found.** can be seen the unneeded patrol usage *frequent* event's FTA diagram. In this situation the core event can occur only by the Electrical Protection System Fault (an opened window/door, a false PIR signal, a control panel hazard, or a *noise* in the communication circuit), but there is another subsystem what can occur as an unneeded operation, the Ctral Supervision System Fault. The defined electrical protection system fault probabilities were the following:

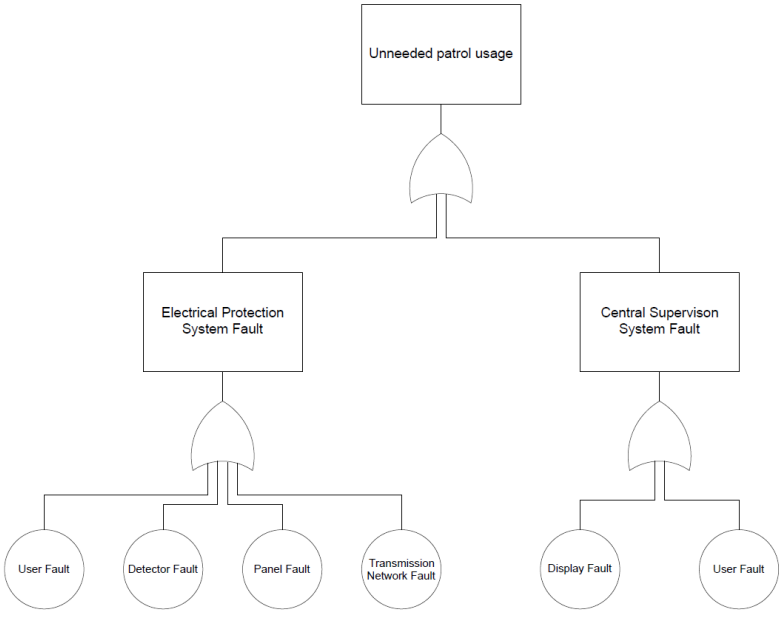

Figure 3. A frequent example event.

user 0,05, detector 0,15, control panel 0,03 and transmission 0,01. The Electric Protection System Fault probability can be calculated wth expression (1). The calculated probability of this subsystem was $P_T = 0{,}220561$.

The defined central supervision system fault probabilities were the following: display 0,05 and user 0,1 so the calculated probability of this subsystem was $P_T = 0{,}145$.

The accumulated fault probability indicator number was in this event P_T = 0,33358, while the efficiency indicator number was $1 - P_T$ = 0,66642.

In the test system the FTA showed that in this kind of fault group the probability rates are the same and independent of the fault's place, so they could be used as a template in future.

With the aforementioned FTA diagrams we could declare the weighted global indicator number of the complex system, what was P_T = 0,3483 and the global weighted average efficiency number was $1 - P_T$ = 0,6516.

SUMMARY AND CONCLUSION

The mentioned theoretical, logical and mathematical methods can give a useful information about the complex system's efficiency.

This article gives a useful guideline for the facility management of the smart cities' railway stations. It declares the main connections with their hazards to find the key elements and the inbound and outbound parameters of the smart complex security system. The pre-generated knowledge base and FTA templates gives the opportunity to get a main view of the global system's efficiency. If a special self-learning software algorithm will be used at the analysis and with a special maintenance and repairing contract, what contains also a system improvement agreement, it gives the possibility that the efficiency of the full scaled complex system will be continuously in the optimal state.

The facility management always gets on-line information about the state of the system with the needs of the improvement and also the cost, that means the management gets all important information for the proper budget planning for years and gets the ability to reduce the security risk of the smart cities' stations.

ACKNOWLEDGEMENT

The research on which the publication is based has been carried out within the framework of the project entitled "The Development of Integrated Intelligent Railway Information and Safety System" (application number: GINOP-2.2.1-15-2017-00098).

REFERENCES

[1] Ramaprasad, A.; Sánchez-Ortiz, A. and Syn, T.: *A Unified Definition of a Smart City*. Springer International Publishing AG, Cham, 2017,

[2] Bosch Security Systems: *Train station Solutions for Ensuring Security and Safety from Bosch Security Systems*. Bosch Security Systems, 2012,

[3] Ruffolo, F. and Cinquino, A.: *Smart security systems for the rail industry*. Alstom Industry, Montreal, 2006,

[4] Sinnamon, R.M. and Andrews, J.D.: *Fault Tree Analysis and Binary Decision Diagrams*. Proceedings of 1996 Annual Reliability and Maintainability Symposium. IEEE, Las Vegas, 1996, http://dx.doi.org/10.1109/RAMS.1996.500665,

[5] Systems and Reliability Research Office of Nuclear Regulatory Research: *Fault Tree Handbook.* U.S. Nuclear Regulatory Commission, Washington, 1981.

Interdisciplinary Description of Complex Systems 16(3), 350-359, 2018

BRAIN-COMPUTER INTERFACE-BASED FEASIBILITY OF ENTERING CUSTOMER CODE ON TICKET VENDING MACHINES

Dénes Simonyi* and Tibor Kovács

Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.16.3.7
Regular article

Received: 11th May 2018.
Accepted: 31st August 2018.

ABSTRACT

The availability of EEG-based Brain-Computer Interface (BCI) devices, which are also available in everyday applications, has widened the application environment. Many manufacturers have marketed their own mobile device, which will become virtually accessible to everyone in the near future, opening up new perspectives in the modern world of human-machine interaction. One of its potential areas is to broaden the communication capabilities of people with physical disabilities, providing them with data inputs that they had previously not been able to. Such a feature is a keyboardless text input. In Hungary, in case of online shopping, the receipt of a train ticket through the MÁV ticket sales machines is also possible to be received by entering the customer code by typing numbers on a touch screen. However, due to disability, physical injury or other reasons, there are cases where the user is unable to use hands, therefore this possibility is virtually impossible to access for them. This omission may, in our opinion, be eliminated by alternative identification methods. The purpose of this research is to assess the feasibility of entering characters using EEG based BCI techniques on those machines. The research consists of two parts. In the first part, the technical parameters of railway ticket vending machines were surveyed to determine whether or not they provide an opportunity to connect external devices and provide backgrounds for software communication with BCI. The second part of the research is a questionnaire research. We visited institutions that care for people with reduced mobility and asked them to fill out our questionnaire with their patients to assess the need for a possible BCI tool on rail ticket vending machines. We have also prepared a second questionnaire to measure the attitude of healthy individuals to the use of this device.

KEY WORDS

brain-computer interface, biometric identification, ticket vending machines, rail transport

CLASSIFICATION

ACM: 10010583.10010786.10010808
JEL: L84

*Corresponding author, η: denes.simonyi@gmail.com; +381 601661675;
Narodnog fronta 15, Feketić/Bácsfeketehegy, Serbia

INTRODUCTION

The concept of a smart city means something different for everyone. There is one meaning for an architect, another for a doctor, something else for an entrepreneur. But in the same way, it means something to a child, a different thing to an adult, a healthy person, and a sick person. If you search the web, you will find countless different definitions. Like many decades ago, when the notion of smart cities was only utopian in the public consciousness, today everyone is trying to describe his own point of view in some way. Everyone agrees that, in the case of smart cities, all forms of transport have an infinite amount of potential to exploit. Public transport, including rail transport, plays a key role, as it is one of the most economical and environmentally friendly forms of transport for everyone. Of course, this efficiency can be further enhanced with the introduction of new services and the further development of the existing ones.

This research is concerned with the expansion and possible facilitation of an essential component of rail passenger transport, the purchase of electronic train tickets. It is trying to find out whether technical and social judgment can be implemented in the near future on rail ticket vending machines by entering the customer code using Brain Computer Interface (BCI). This technique would not only be a new option in the ticketing process on vending machines, but it could also provide assistance to people with reduced mobility who are unable to use them due to their illness or disability.

BRAIN COMPUTER INTERFACE

The Brain Computer Interface is a computer communication device that provides a direct, non-muscular communication channel between an individual and the computer. To achieve communication, brainwaves are required. This can be achieved without inserting electrodes (MEG, PET, fMRI and optical imaging) and electrodes (EEG), which can be invasive and non-invasive. At the moment, EEG is the only technology that has short time constraints and can be implemented with relatively simple and inexpensive equipment. The use of currently available techniques only provides some indirect way of text input (selective attention, motor imagery) [1-8].

Three key factors have been taken into account when designing research goals:

1.) It is important that the ticket vending machines are constituting a compact unit, they are not equipped with external USB ports. In these vendors, communication between the BCI device and the machine must be realized through existing external ports. The two most popular BCI devices currently available are Bluetooth or USB port support, but Bluetooth connectivity can also be achieved via USB dongle [9-13].
2.) Society generally does not react with immediate acceptance to technological innovations, following Rogers' innovation curve [14]. How much time is needed for the majority to accept a new innovation product depends on a number of circumstances [15].
3.) Based on the data of the Hungarian census of 2011, the number of physically disabled persons in Hungary is 232 206. This is 2,34 % of the total Hungarian population, and almost half of all the disabled, that is 47 %. 39,87 % of people with disabilities have said that their disability is disturbing in traffic [16].

During the research we examined the following three questions:

1.) Are today's available ticket vending machines able to connect a BCI device to them?
2.) Is such a technical innovation acceptable to users?
3.) Does such a device make it easier for handicapped or disabled people to buy tickets for rail travel?

RESEARCH METHODS

The technical data of railway ticket vending machines was obtained from the data sheets provided by 3 different vending machines. In the second part of the research, we investigated the second and third research domains by anonymous online questionnaire research. We have treated the responses of physically disabled people separately.

RESEARCH RESULTS

It is true that the Neurosky EEG helmet realizes Bluetooth communication [17], but it does not necessarily require a built-in Bluetooth adapter, even with a Bluetooth dongle that can be connected via a USB port. Based on this, the minimum connection condition is the USB port. Emotiv's products supports Bluetooth and USB communication [18].

For the application of a BCI device that can be used on railway ticket vending machines without an external USB port, it is needed to find a solution for communicating with the available input ports. Both manual and automatic bank card readers, with which MÁV's vending machines are also equipped [15], support the ISO7816 standard [19-22]. This means they can read IC cards. The solution requires the creation of a device that creates a connection between the BCI device and the card reader. The ticket machine must also have a software that can read data received from the card reader and transmit it to the software written on the BCI. To do this, the correct data transfer rate must be ensured. Emotiv headset sampling rate is 2 048 bit/second [18], Neurosky headset is 6 144 bit/second [17]. Between the reader and the card the initial speed is 9 600 bit/second [23]. This is sufficient to transfer signals from the device.

Another important aspect was which operation system the BCI software is running on. There are officially available text input softwares, and two of them, BCI2000 and OpenVibe are the most common [24-26]. However, as this area is not fully explored yet, it is constantly under development and research. In addition, firms distributing headsets also provide their products with the so-called SDK (Software Development Kit) for such programming languages that can be used to write application programs on multiple operating systems. Microsoft Windows is supported for each of the devices studied [12, 17, 18].

Three of the examined railway ticket dispensers and their important parameters for research are presented in Table 1. Table 1 shows that all machines have a USB port and operate on a Linux or Windows operation system. This is in line with our expectations and we can conclude from this point that the use of the BCI tool can be used to enter the customer code on the train ticket vending machines.

We tried to get information about MÁV's rail ticket vending machines, but we only found out that they were based on industrial PC. Based on videos found on YouTube, among which there are some showing that the automated operating system sends an error message to the user, the operation system running on them is Microsoft Windows.

Table 1. Railway ticket vending machines and their parameters [13, 26, 27].

Manufacturer	Type	Operation System	Number of USB ports	Built-in Bluetooth
LKS	42" touch screen ticket vending machine with ticket dispenser, ticket printer	Windows 7 or XP operation system, O.S. not included	6	N/A
Elektronet	TVM 0012	Microsoft Windows	8	N/A
Breeze Innovations	Breeze ECC – A SMC/ ATVM Client	Linux	6	N/A

Summarizing the results, we can conclude that the available train ticket vending machines support the BCI tools when the software is installed.

CAN SUCH TECHNICAL INNOVATIONS BE ACCEPTABLE TO USERS?

We tried to answer the question using an anonymous questionnaire survey online, intended to be a preliminary survey, and it can be used for a detailed, comprehensive research later on.

As we have already mentioned when formulating the goals, the wide differentiation of innovation depends on a number of parameters, along the Rogers curve, happening in stages: cognition, interest, evaluation, testing, and acceptance.

The participants in the process, based on the dynamics of innovation, are divided into five groups according to Rogers [14]:

1.) innovators 2,5 %,
2.) early adopters 13,5 %,
3.) early majority 34 %,
4.) late majority 34 %,
5.) laggards 16 %.

The Rogers curve is shown in Figure 1.

With the questions in the questionnaire, we wanted to find out the general information about what they think influences the group of individuals they belong to: gender, education, work, computer skills, internet habits, electronic ticket buying, if they are aware that railway ticket vending machines exist in Hungary.

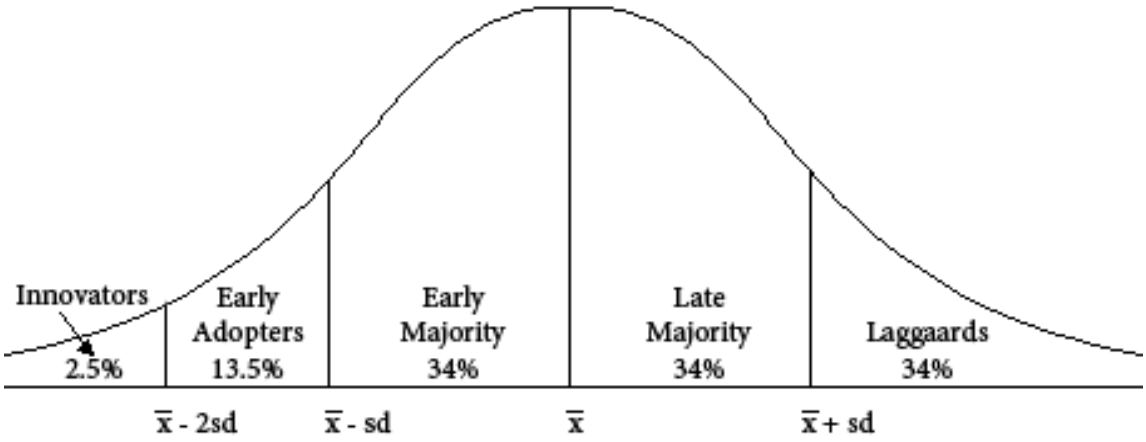

Figure 1. Innovation adoption curve [27].

In addition, we have been looking for the extent to which they show interest in the use of the ticketing automats with the BCI tool, and how often they would use it.

The questionnaire was filled out by a total of 166 persons, of whom 74 were physically disabled or disadvantaged, and 92 were physically not disabled/disadvantaged.

Since our intention was to pay special attention to the responses of physically disabled/disadvantaged respondents, and the ratio did not either correspond to the distribution of population in Hungary, the analysis was carried out separately for the two groups. Therefore, the results of the non-disabled/disadvantaged group and the results of the physically disabled/disadvantaged group will be presented separately.

The gender distribution of non-disabled/disadvantaged groups is 31 women and 61 men, Table 2.

Table 2. Gender distribution of physically not disabled / disadvantaged respondents.

Age	Male	Female	∑
18-24	25	5	30
25-34	20	8	28
35-44	11	9	20
45-54	3	6	9
55-64	1	2	3
above 64	1	1	2
∑	**61**	**31**	**92**

Table 3. Gender distribution of physically disabled / disadvantaged respondents.

Age	Male	Female	∑
18-24	2	4	6
25-34	4	5	9
35-44	3	4	7
45-54	6	9	15
55-64	7	16	23
above 64	6	8	14
∑	**28**	**46**	**74**

Filling out the questionnaire was voluntary, via a web interface, which meant that we could not influence gender. It appears from the tables that the majority of men (66,30 %) are in the non-disabled/disadvantaged group, while in the disabled / disadvantaged group women are, in similar proportions (62,16 %).

In the non-disabled/disadvantaged group, the majority of respondents are under the age of 45 (84,78 %), while the majority of applicants in the disabled / disadvantaged group belong to the age group above 44 (70,27 %).

The questionnaire contained two questions which we used to divide the respondents into three groups. In the first group, following Rogers' division, there were the innovators, early adopters and early majority, the second group was the late majority, while the third group was the laggards and those who are not willing to accept the technology at the moment.

The first group represents those individuals who would use the device on a regular basis to respond to them and would clearly buy it if it was to match the price of a mid-range keyboard.

In the second group, we classified those individuals who would try the device and buy it, or may be uncertain whether they would buy the device if its price would match the price of a mid-range keyboard. In the third group, we grouped individuals who would not try and would not use the device either.

All three groups were based on two replies, the aim of which was to filter out the respondents who gave conflicting answers. After the discontinuation of the controversial questionnaires, we received a total of 61 evaluable questionnaires from the non-disabled / disadvantaged group and 46 questionnaires from the disabled / disadvantaged group.

The gender ratio corresponds to the aggregate ratio in all divisions, so we did not make a separate statement for this.

The aggregate percentage distribution of results is shown in Table 4.

Analyzing the results, it can be stated that 55,74 % of the non-disabled / disadvantaged respondents are in the first group. This is only 5,74 % higher than the rate set by Rogers. In the case of disabled/disadvantaged, it is 43,48 %, which is only 6,52 % lower than that of Rogers.

In the second group, which includes the late majority by Rogers, the proportion of non-disabled/disadvantaged respondents is 11,05 % lower than that of Rogers and 7,3 % higher in the disabled/disadvantaged group. It is a group of two sub-groups and, if we examine it, the difference on one side in both cases is almost exactly reflected in the difference on the other side. In the case of non-disabled/disadvantaged persons it is –5,31 % and 0,78 % for the disabled/disadvantaged group.

The third group is the group of laggards. The proportion of non-disabled/disadvantaged respondents in this group is 21,31 %. The difference of –5,31 % in the second group appears visibly here, as they are also borderline categories. The proportion of disabled/disadvantaged respondents is only 0,78 % different from Rogers, which is a negligible difference.

With this in mind, we have looked at the responses that determine the limitations and we have come to the conclusion that the aforementioned deviations result from these, and that by replicating the research on a larger population, these responses have to be defined in more details and additional opportunities for respondents.

PARAMETERS DEFINING THE GROUPS

As the next step, we determined the factors that are most characteristic of each group. The results were determined according to Table 4. Defining factors within the group were those with the highest number of responses in the given group.

RESULTS OF NON-DISABLED/DISADVANTAGED RESPONDENTS

The first group is characterized by 18-44 year-olds with a high school education at least, and their job also requires at least high school education. They have at least basic IT knowledge, place of living is not a factor. In this group, there are individuals who are familiar with, used, and also do not use the E-ticket service and rail ticket vending machines.

The second group is characterized by 45-54 year-olds, there are no one without profession and none are post-graduates, and their occupation is characterized by being machine builders, operators and drivers as well as agriculture and forestry occupations. They have mid-level IT skills. Following the first group, this group has the majority of people living in the capital city. One third of the regular users of ticketing machines are in this group.

The third group contains the majority of people over the age of 54. This group includes non-educated people with primary education, non-skilled workforce and most of the people who do not have the proper IT background knowledge to use the computer on their own. The same number of people lives in county capitals as in the first group, and one third of them uses rail ticket vending machines.

The resulting curve is shown in Figure 2.

RESULTS OF DISABLED/DISADVANTAGED RESPONDENTS

The first group includes 25-44 year-olds and those above 54, college, university and postgraduate qualifications, and most of the people requiring higher education. There is the same number of non-qualified workplaces in this group as in the second (40%). The group is characterized by medium-level IT skills and IT knowledge. This group contains the majority of people living in Budapest, in other cities and in the villages. This group has the most individuals who have not used it yet, have used it or regularly use the E-ticket service. In this group there are the most individuals who know the existence of railway ticket vending machines but have not used them yet.

Table 4. Percentage distribution of the factors investigated by groups.

Factors examined	Non-disabled/disadvantaged			Disabled / disadvantaged		
Group	1	2	3	1	2	3
Total	**55,74%**	**22,95%**	**21,31%**	**43,48%**	**41,30%**	**15,22%**
Age group						
18-24 years	59,09%	31,82%	9,09%	20,00%	80,00%	0,00%
25-34 years	62,50%	18,75%	18,75%	57,14%	42,86%	0,00%
35-44 years	66,67%	8,33%	25,00%	50,00%	50,00%	0,00%
45-54 years	33,33%	50,00%	16,67%	25,00%	62,50%	12,50%
55-64 years	33,33%	0,00%	66,67%	41,67%	33,33%	25,00%
under 64 years	0,00%	0,00%	100,00%	60,00%	10,00%	30,00%
Highest education level						
Without graduation	0,00%	0,00%	100,00%	0,00%	100,00%	0,00%
Primary school	0,00%	33,33%	66,67%	33,33%	66,67%	0,00%
High school / Grammar school	58,62%	24,14%	17,24%	30,00%	45,00%	25,00%
College, university	57,69%	23,08%	19,23%	58,82%	29,41%	11,76%
Post-gradual (Masters/PhD)	100,00%	0,00%	0,00%	100,00%	0,00%	0,00%
Occupation						
Other jobs, with tertiary or secondary degree	61,11%	27,78%	11,11%	63,64%	27,27%	9,09%
Jobs with individual use of tertiary degree	46,67%	20,00%	33,33%	62,50%	25,00%	12,50%
Leaders in fields of economy, management, interest representation g	0,00%	0,00%	0,00%	33,33%	66,67%	0,00%
Machine operators, assemblers, and drivers	0,00%	100,00%	0,00%	33,33%	66,67%	0,00%
Jobs in industry and architecture	60,00%	20,00%	20,00%	0,00%	0,00%	0,00%
Office and business (customer relationship) professions	80,00%	0,00%	20,00%	33,33%	50,00%	16,67%
Trade and service occupations	77,78%	11,11%	11,11%	22,22%	44,44%	33,33%
Occupations in agriculture and forestry	50,00%	50,00%	0,00%	0,00%	0,00%	0,00%
Jobs not requiring any professional skills	0,00%	25,00%	75,00%	40,00%	40,00%	20,00%
Jobs at armed services	0,00%	0,00%	0,00%	0,00%	100,00%	0,00%
IT knowledge						
No proper knowledge for individual IT usage	33,33%	0,00%	66,67%	33,33%	33,33%	33,33%
Basic	50,00%	16,67%	33,33%	31,25%	43,75%	25,00%
Intermediate	36,84%	31,58%	31,58%	43,75%	43,75%	12,50%
Advanced	73,68%	21,05%	5,26%	33,33%	66,67%	0,00%
IT professional	64,29%	21,43%	14,29%	100,00%	0,00%	0,00%
Place of living						
Budapest	55,56%	44,44%	0,00%	50,00%	35,71%	14,29%
County capital city	40,00%	20,00%	40,00%	18,18%	63,64%	18,18%
City	56,00%	24,00%	20,00%	42,86%	35,71%	21,43%
Municipality / village	59,09%	13,64%	27,27%	71,43%	28,57%	0,00%
Are you aware of the MAV's E-ticket service?						
Yes, but I haven't used it yet.	53,33%	26,67%	20,00%	22,22%	66,67%	11,11%
Yes, I have used it.	54,55%	36,36%	9,09%	66,67%	22,22%	11,11%
Yes, I use it regularly.	50,00%	16,67%	33,33%	100,00%	0,00%	0,00%
No, I am not.	58,62%	17,24%	24,14%	50,00%	27,78%	22,22%
Do you know that certain train stations have ticket vending machines?						
Yes, but I haven't used the yet.	48,00%	28,00%	24,00%	64,00%	20,00%	16,00%
Yes, I have used a machine like that.	62,50%	25,00%	12,50%	37,50%	62,50%	0,00%
Yes, I regularly use them.	33,33%	33,33%	33,33%	0,00%	0,00%	0,00%
No, I don't.	64,71%	11,76%	23,53%	7,69%	69,23%	23,08%

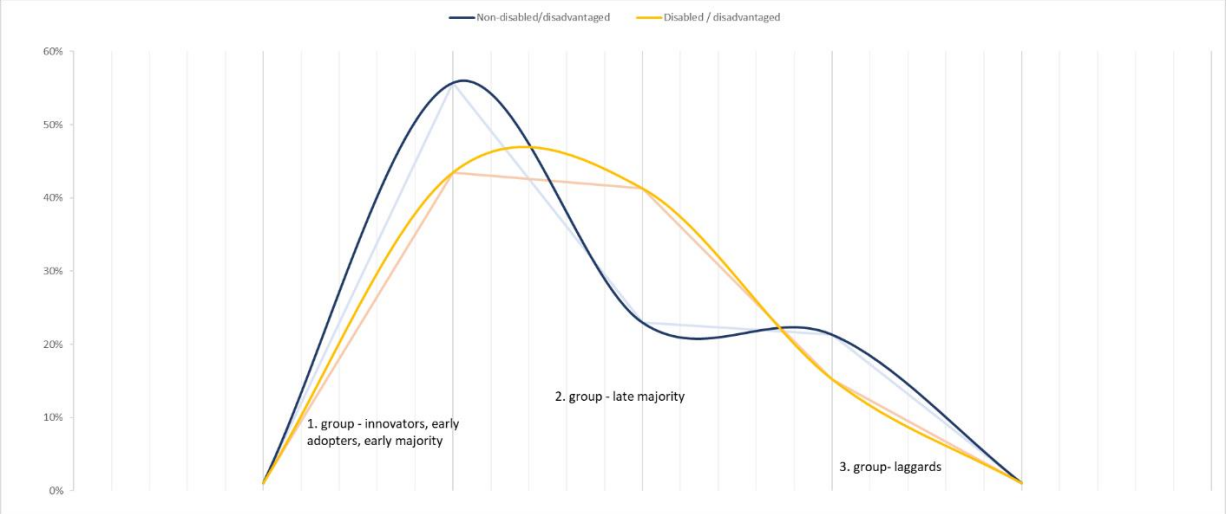

Figure 2. Distribution according to the groups.

The second group is between 18-24 and 35-54 years of age, having high school, grammar school or lower education. The most typical occupations of the group are: economists, administrative workers, interest representation leaders, legislators, operators, assemblers, drivers, office and business (customer relationship) professions, trade and service occupations and armed services. It is characterized by basic, intermediate and advanced IT skills. This group contains most individuals living in county capital cities. In this group, there are the most people who know about the E-ticket service, but have not used it, have used it, as well as those who have not used a train ticket vending machine yet.

The third group is characterized by a low percentage in all areas. Its members are older than 45, and no factor is representative in this group.

WOULD SUCH A DEVICE MAKE IT EASIER FOR DISADVANTAGED PERSONS/PEOPLE WITH DISABILITIES TO PURCHASE RAIL TICKETS?

In this issue only the responses of people with reduced mobility/disabilities have been analysed.

There was only one person who did not use the Internet. 27,03 % lives in Budapest, 25,68 % in county capitals, 32,43 % in towns and 14,86 % in municipalities or villages. 88,33 % spends several hours a day on the Internet. 45,95 % of them says that rail ticket purchases are made easier by E-ticket service, 9,46 % says there is no difference between them and traditional ticket purchases and only 1,35 % thinks it makes it more difficult. Regardless of the place of residence, the majority, who believes that E-ticket services make purchases easier, prevails everywhere. 14,86 % does not agree that rail ticket vending machines make it easier for them to buy tickets. 82,43 % of them agrees, the remaining 2,70 % did not give a sensible answer (they cannot use or do not use ticket vending machines).

The answer to the question if they had the opportunity to use a tool to enter the code into the ticket vending machine without typing, would they try/use it, is that 14,86 % would not try it, 52,70 % would try it, but not use it regularly, 32,43 % would use it regularly.

The same device would be bought by 58,11 % if it existed and would not cost more than a mid-size keyboard (of which 22,97 % would purchase it unconditionally). 29,73 % does not need it, 9,46 % thinks it is expensive and would not buy it. The remaining 2,70 % is uncertain, they cannot imagine using it.

By reviewing the responses, we can conclude that the responding disabled/disadvantaged population is open to using such a tool and sees potential. The answer to this question is yes, according to those surveyed; such a device would facilitate the purchase of rail tickets for people with mobility impairment.

ACKNOWLEDGEMENT

The research on which the publication is based has been carried out within the framework of the project entitled "The Development of Integrated Intelligent Railway Information and Safety System" (application number: GINOP-2.2.1-15-2017-00098).

REFERENCES

[1] Graimann, B.; Allison, B. and Pfurtscheller, G.: *Brain-Computer Interfaces: A gentle introduction.*
In: Graimann, B.; Pfurtscheller, G. and Allison, B., eds.: *Brain-computer interfaces*. The Frontiers collection. Springer, Berlin & Heidelberg, pp.1-27, 2010,
http://dx.doi.org/10.1007/978-3-642-02091-9,

[2] –: *Computer Interfaces.*
Wiley Encyclopedia of Electrical and Electronics Engineering. John Wiley & Sons, p.44, 2015,

[3] Lesenfants, D., et al: *An independent SSVEP-based brain-computer interface in locked-in syndrome.*
Journal of Neural Engineering **11**(3), 035002, 2014,
http://dx.doi.org/10.1088/1741-2560/11/3/035002,

[4] Valbuena, D. and Gräser, A.: *Mental Strategies to Operate a Motor-imagery-based Brain-computer Interface*.
In: Axel, G., ed.: *Methods and Applications in Automation*. Shaker Verlag, Aachen, pp.66-74, 2008,

[5] Ryan, D.B.,, et al: *Predictive spelling with a P300-based brain-computer interface: Increasing the rate of communication.*
International Journal of Human-Computer Interaction **27**(1), 69-84, 2012,
http://dx.doi.org/10.1080/10447318.2011.535754,

[6] Wolpaw, J.R., et al: *Brain-computer interfaces for communication and control.*
Clinical Neurophysiology **113**, 767-779, 2002,

[7] Pastor, M.A., et al: *Human Cerebral Activation during Steady-State Visual-Evoked Responses.*
Journal of Neuroscience **23**(37), 11621-11627, 2003,
http://dx.doi.org/10.1523/JNEUROSCI.23-37-11621.2003,

[8] Amiri, S.; Rabbi, A.; Azinfar, L. and Fazel-Rezai, R.: *A Review of P300, SSVEP, and Hybrid P300/SSVEP Brain- Computer Interface Systems.*
In: Fazel-Rezai, R., ed.: *Brain-Computer Interface Systems*. IntechOpen, pp.195-213, 2013,
http://dx.doi.org/10.5772/56135,

[9] Emotiv: *Comparison chart.*
https://www.emotiv.com/comparison, accessed 10th March 2018,

[10] Maskeliunas, R.; Damasevicius, R.; Martisius, I. and Vasiljevas, M.: *Consumer-grade EEG devices: are they usable for control tasks?*
PeerJ – the Journal of Life and Environmental Sciences 4:e1746, 2016,
http://dx.doi.org/10.7717/peerj.1746,

[11] Neurosky: *EEG Hardware Platforms*.
http://neurosky.com/biosensors/eeg-sensor/biosensors, accessed 5th May 2018,

[12] OpenBCI: *Cyton Daisy Biosensing Boards (16-Channels)*.
https://shop.openbci.com/collections/frontpage/products/cyton-daisy-biosensing-boards-16-channel?variant=38959256526, accessed 5th May 2018,

[13] OpenVibe: *Software for Brain Computer Interfaces and Rail Time Neurosciences.*
http://openvibe.inria.fr, accessed 5th May 2018,

[14] Rogers, E.: *Diffusion of Innovations*. 3rd edition.
The Free Press, New York, 1983,
[15] Orova, L. and Komáromi, A.: *Új termék elfogadásának determinisztikus és sztochasztikus modelljei.* In Hungarian.
Acta Agraria Kaposváriensis **10**(1), 103-111, 2006,
[16] KSH: *A fogyatékossággal élők helyzete és szociális ellátásuk*. In Hungarian.
http://www.ksh.hu/docs/hun/xftp/idoszaki/nepsz2011/nepsz_17_2011.pdf, accessed 5th May 2018,
[17] Neurosky: *EEG Biosensors*.
http://neurosky.com/biosensors/eeg-sensor/biosensors, accessed 5th May 2018,
[18] Emotiv: *Comparison chart – Technical Specifications.*
https://www.emotiv.com/comparison, accessed 10th May 2018,
[19] Mingtetech: *Manual cardreader MT180.*
http://www.mingtetech.com/e/PRODUCTS/Card_Readers/ManualCardReaders/p9.html, accessed 10th May 2018,
[20] Mingtetech: *Manual cardreader MT318-4.0.*
http://www.mingtetech.com/en/PRODUCTS/Card_Readers/MotorizedCardReaders/p17.html, accessed 10th May 2018,
[21] Creator (China) tech.: *CRT-288-C ATM Dip Card Reader.*
http://www.china-creator.com/card-reader/manual-card-reader/crt-288-c-atm-dip-card-reader.html, accessed 10th May 2018,
[22] Creator (China) tech.: *CRT-310 Motorized Card Reader.*
http://www.china-creator.com/card-reader/motor-card-reader/crt-310-004-motorized-ic-rfid-card-reader.html, accessed 10th May 2018,
[23] STMicroelectronnics: *AN2646 Application note*.
http://www.st.com/content/ccc/resource/technical/document/application_note/ef/6b/bd/09/7a/5b/49/b9/CD00174533.pdf/files/CD00174533.pdf/jcr:content/translations/en.CD00174533.pdf, accessed 10th May 2018,
[24] Lotte, F.; Bougrain, L. and Clerc, M.: *Electroencephalography (EEG)-Based Brain--Computer Interfaces.*
In: Webster, J.G., ed.: *Wiley Encyclopedia of electrical and Electronnics Engineering*. Wiley & Sons, 2015,
http://dx.doi.org/10.1002/047134608X.W8278,
[25] g-tec: *intendiX – User-Ready Brain-Computer Interface Applications*.
http://www.gtec.at/Products/Complete-Solutions/intendiX-Specs-Features, accessed 10th May 2018,
[26] Elektronet: *Ticket Vending Machine (TVM 0012).*
http://elektronet.com.tr/en/solutions-and-services/smart-city-solutions/ticket-vending-machine-tvm, accessed 10th May 2018,
[27] Breeze Innovations: *Breeze Embedded Computing Client*.
http://www.breezeinnovations.com/products/automatic-ticket-vending-machines, accessed 10th May 2018.

Interdisciplinary Description of Complex Systems 16(3-A), 360-368, 2018

POSSIBLE AREAS OF APPLICATION OF DRONES IN WASTE MANAGEMENT DURING RAIL ACCIDENTS AND DISASTERS

Géza Károly Kiss Leizer*

Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.16.3.8
Regular article

Received: 18th March 2018.
Accepted: 31st August 2018.

ABSTRACT

In this article the most modern versions of unmanned aerial vehicles (drones) will be presented from the aspect of safer identification of dangerous effluent materials during rail accidents and catastrophes. These technologies are crucial to minimize the pollution of dangerous waste generated during accidents or catastrophes. Doing this, exploration of further opportunities of waste management – satisfying the conditions of the highest level of environmental safety – is necessary, as well as to find new methods to handle waste in time securely and professionally. Exploration of unprecedented solutions during rail- and road accidents or catastrophes is also reasonable. Relevancy of application of drones is particular as long as the approachability of the affected area is difficult or impossible. During the neutralization of explosive, hazardous or toxic materials the risk of life could be eliminated using drones equipped with the most modern technologies.

KEYWORDS

drones, environmental safety, dangerous wastes, minimizing damages, rail accidents

CLASSIFICATION

ACM: 10010485, 10010606
APA: 4070, 4090
JEL: H12, Q53

*Corresponding author, η: kissleizer@t-online.hu; +36 30 222 8062;
*Budapest, Széchenyi I. u. 9., H – 1184, Hungary

INTRODUCTION

In order to permanently reduct wastes into the economical and social turnovers, it is necessary to reveal factors affecting engineering safety, to determine the elements of engineering safety in waste management, furthermore, the employability of these solutions.

Engineering safety is a totality of technical and technological methods and procedures, which aims to secure the existence or the functioning of somebody or something [1].

During waste management this goal could be achieved by the appliance and utilization of engineering sciences. Doing this, every single element could be an influential factor, which holds the shaping, installation, maintenance or the creation of conditions of the engineering safety.

From all of these, the most important element is the human factor. This could be manifested during vehicular catastrophes and accidents coming from malpractice or negligence, causing serious damages.

It is very important to highlight and emphasize the role of hydrocarbons polluting the soil and aquatic life. These materials are mostly emerging in the wake of disasters and they often not burn out. We also have to mention other types of special industrial or delivered liquids. By this time, polluted area must be cleaned from these liquids and materials, which have been transformed into dangerous waste [2].

SECURITY OF RAIL TRANSPORTS

Transportation is probably as old as humanity, but the level and importance of this activity has never been so determinate as today.

The most decisive way of forwarding is the rail transport. Air conveyance is fast but expensive. Waterage and railway transport is too bound, depending on the riverbed several factors or the quality of the railroad. Rail transport is the most secure solution, because the track of the cargo could be supervised or optimized rapidly [3].

The cargo must be secured, because the cargo itself could be endangered, or it may pose a threat to the environment. In light of this, protection and defense is the key to keep the cargo safe. Guarding is a permanent counteraction responding to a presumed threat on the cargo. The guard so an insurance one attaching to a hypothetical, supposed activity, the protection it began though, a related averting task ensued with an event concerned. It can be expected that large amount of waste is generated during rail disasters. Decontamination and disposal of such waste – polluting soil or water – is an urgent objective, as well as the elimination of the pollution and the rehabilitation of the affected area.

RFID IDENTIFICATION OF WASTES COMING FROM ACCIDENTS AND DISASTERS

In case of waste management, our personal behavior and the rules of traffic must be extended in order to manage an accident or a catastrophe, to reduce the effects of hazardous materials and to hold polluting effects. These steps and know-how would be similar to the well known first aid exam, obligatory for all drivers. One of the possible solution to treat a damaged tanker is the appliance of the Vetter-pillows. These pillows are easy to deploy even by laymen [4].

Radio Frequency Identification (RFID) provides reading of the information carrier chip of the vehicle from safe distance by radio waves during disasters and accidents. This method also works at great speed of the vehicle.

During catastrophes and accidents the vehicle often suffers so severe damage that UN numbers and other information of the cargo become unreadable. The information carrier unit is also vulnerable; in this case, reading is also impossible. A rapidly employed drone would be capable to read a properly installed chip, in order to rapidly identify dangerous goods. Following this, obtained information must be transmitted to the units participating in recovery actions. Possessing the necessary information, these units could prepare the appropriate tools of decontamination, protective clothing, etc. Shaping of the strategy of neutralization is also possible before taking actions at the location of the disaster.

Significance of this combined method is extraordinary, if the location of the disaster or accident is out of the way or impossible to approach. In case of poisoning, contamination or explosion the RFID system could help to save those who involved in the rescue process. The recommended procedure may significantly decreases pollution of hazardous wastes, because effluent, non-burning hazardous materials become hazardous waste by touching the ground. The affected area of the rail and the environment also become contaminated, because of time factor and the fast spreading of the pollution. We would like to highlight that groundwater could be also polluted when hydrocarbons diffuse into the soil [5].

WITH DRONES AGAINST WASTE

The drone is a small, propeller driven unmanned aerial vehicle, available for multiple useful tasks. Drones' applicability could be demonstrated by their employment in American metropolises, where illegal waste dumping world was reduced, following the appearance of these aerial vehicles. This problem is also cardinal, where illegal waste dumping is a common phenomenon along the railways, inhabited regions, parking places and green areas.

Over the recent years, many research groups are working in order to exploit the potential advantages of quadrotor rotorcrafts as UMAVs of future. This article is addressed to problems of controller performances evaluation and analysis. The main benefits of this research concern with achievement of a controller architecture that should enable quadrotor high dynamic performances, robustness to external perturbations as well as satisfactory trajectory tracking precision [6].

Autonomous quad-rotor helicopters increasingly attract the attention of potential researchers. A wide area of robotics research is dedicated to aerial platforms. The quad-rotor architecture has low dimensions, good manoeuvrability, simple mechanics and payload capability. The electrically powered four-rotor quadrotor helicopter architecture has been chosen for this research [7].

A basic principle can be that whenever a traditional aircraft can prove to be useful, drone can be a benefit, too. Obviously, not all traditional aircraft uses can be substituted, but the author believes that the rate of potential applications of drone is on the rise due to technological development. Based on experience, the spread of drone is expected to reduce the costs of aerial applications, so by following the previous train of thought, we can conclude that drone could also be used in cases where traditional aerial reconnaissance was not previously considered owing to its high costs although its effectiveness was never doubted [8].

Application of drones could be more useful at the prevention of rail accidents and catastrophes. On the other hand, appliance of UAS/UAV is more suitable in practice to identify dangerous rail cargo.

Stating the eruption in the center of the disaster's time scale any activity, so logically also all UAS applications supporting disaster management can be thematically separated like it. Before the eruption as a pre-disaster activity UAS application can support the prevention or

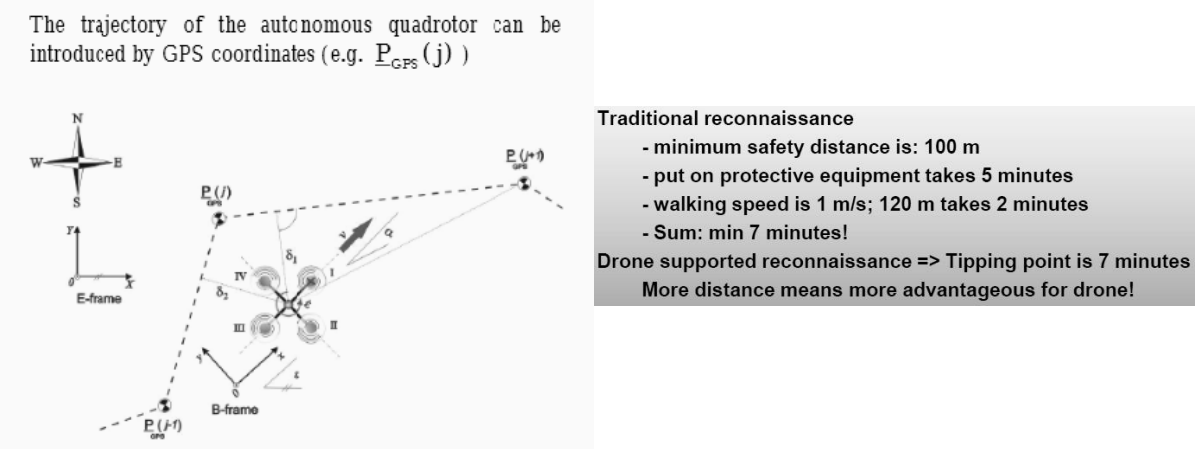

Figure 1. Drones is related to the transport of dangerous merchandises accidents the opportunities of a happening application [9].

be able to supply the early detection. In case of man-made disasters like a chemical accident during illegal transport, the UAS railway observation belongs to prevention, following a toxic smoke spreading belongs to early detection, while avoiding the escalated forest fire by UAS flight patrol can belong to both prevention and early detection [10].

The popularity of drones constantly increases among hobby aviators and companies as well. More and more areas are going to use of these devices for different purposes. At the CES 2015 in Las Vegas, only 4 manufacturers were presents, while this year, 27 appeared. The market potentials are clearly shown by the fact that, more than 100 000 units were sold in 2013 in the USA, while in 2015, more than a million units were sold, thereby creating a 1,7 billion dollar industry. The drones of sales will exceed 3,7 millions. The sales forecasts for drones 2013 between 2017 are shown in Figure 2 [11].

OPTIONS OF APPLICATION OF DRONES

There are many way to scale different disasters. Disasters can be scaled from limited to escalated, by the effected area or population, from the eruption to slowly spreading by the time it develops, or in many other ways depending on the condition we take into account. This article uses namely some disasters such as floods, earthquakes, nuclear accidents and forest fires, however demonstratively expresses that topic is so huge, all presented work is just touching the surface [12].

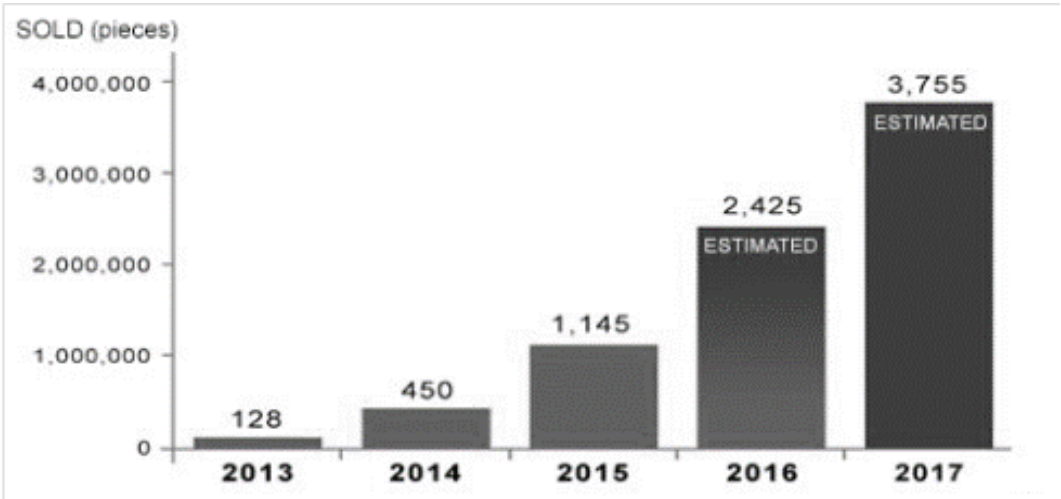

Figure 2. Progress in the sale of drones between 2013 and 2017 in America [13].

The main advantage of rapid mapping systems based on drones is to acquire swiftly sensory data on the disaster area where ones can hardly access. For this reason, there have been many studies on the application of dron systems to the disaster management.

It is difficult to access information about the transportation of dangerous goods, and, in case of an accident, it is necessary to conduct a collective analysis of data stored in different systems in order to be able to carefully assess the situation. Consequently, it would be necessary to ensure the accurate tracking of vehicles transporting dangerous goods in railway transport, too. There is no uniform monitoring and tracking system for railway vehicles in Europe. In Hungary, tracking is restricted to the locomotives of railway companies. Nevertheless, there are international examples for the unique identification of railway wagons. The railway systems of the United States have a strong tradition in this field.

In the United States 1,7 million types of hazardous substances are transported by railway each year. Dow Chemical has already started to use the RFID system, in order to help to identify railway wagons carrying hazardous chemicals. 26 000 railway wagons in North America transports about 650 types of TIH (toxic inhalation hazard) chemicals [14].

Along the railways of American metropolises illegal waste disposal was decreased, owing to the engagement of drones. Illegal waste disposal is also a serious problem in Hungary, especially in Budapest, because homeless people – permanently living at the railway areas – accumulate lots of waste. In smart cities, this kind of waste is unhealthful.

The complexity of these opportunities is very large. In light of this, I list only the most interesting ones, in connection with rail traffic. UAVs, having been initially designed for military use have found their way into the civilian arena. While the developed world uses UAVs for various applications; the developing countries benefit tremendously. This is due to their general lack of resources, remote rural locations and prevalence of various kinds of catastrophes. UAVs provide an effective, fast and less expensive solution to save more lives and the environment in developing countries. Although there are still challenges in the use of drones, they are outweighed by benefits [15].

The safety-technology purposes of drones should be distinguished from the use for hobby purposes, as they have unquestionable benefits in such application. Similarly to this topic, drones have already been used in Hungary during a flood event. Their use helped to determine the extension of the flooded area, the situation of possible critical points and the accessibility of escape routes. In case of chemical accidents, a gas detector could be mounted on the drone, which can measure the concentration of the gas escaped into the air, this way ensuring that faster and more precise measures could be taken to protect the inhabitants. There have been examples for such application in disaster management, which means that these devices are able to perform such tasks.

Our experiment was carried out in a railway environment to examine the operating of the RFID reader near a large mass of metal. On the first occasion, measurements were performed without a drone, holding the reader in hand in different positions. During the research, the commercially available drones will be equipped with the following elements: a high-resolution camera, a thermal camera, a communication module, an RFID reader and an air composition sensor. We are planning to use the drones during the transportation of hazardous substances for the identification of wastes in case of an accident or disaster. Their use in such an incident can have significant benefits in comparison with the present practice.

Former experiments proved that only high-end drones are capable of carrying a load of 1-2,2 kg by air. Such aerial vehicles of higher capacity (for example: 13 kg) are also available commercially, so these can be used to carry the implemented devices during the experiment.

According to our plans, the extra accessories of the drone will not weigh more than 4-5 kg including the batteries which ensure the long flying time. Our measurements show that the drone will be able to perform the identification of hazardous substances from a distance up to 80 m depending on the circumstances found at the site of the accident.

RADIOFREQUENCY IDENTIFICATION AND COMMUNICATION

RFID technology is one form of the Automatic Identification Systems. Its basic idea is that the object for identification is equipped with an element (transponder or tag) which is capable of data storage. The microcontroller and the antenna together is called RFID *transponder*, RFID *tag* or RFID hard tag. The information necessary for identification and other data are stored in the memory of the microcontroller.

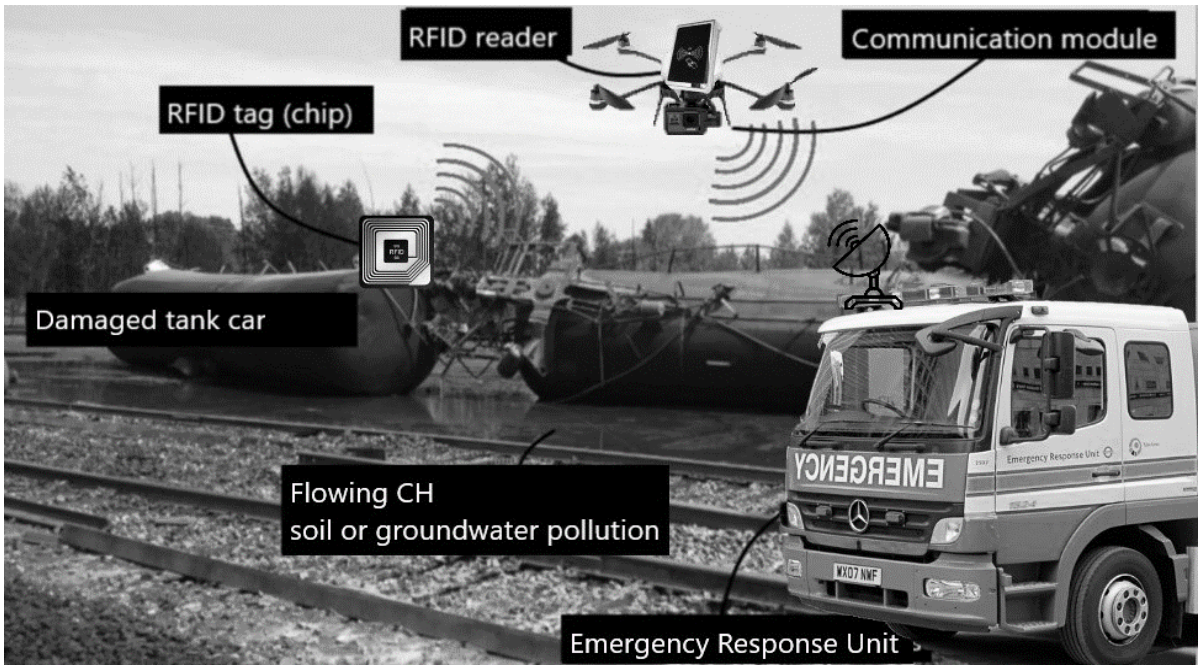

Figure 3. Conceptual draft by the author.

1 litre of gas oil can pollute 1 million litres of water. Therefore, in case of the release of 60 000 litres of gas oil, 60 billion litres of water could become unfit to drink.

This, besides causing significant harm to the environment, would have serious effect on public and personal safety, and the remediation process would impose an immense financial burden on society, as it could last for decades. As the above examples show, in the event of such accidents, the transportation infrastructure can also be seriously damaged [16].

During rail accidents and catastrophes, hydrocarbon pollution is very likely, as shown in the pictures above. Railways are mostly running close to natural waters, as a result, identification of the type and extension of pollution is possible rapidly, using the presented methods. The RFID system, mounted on the vehicle, stores the data required to idetify the transported material(s). In normal or havaria-mode the carry-on device or the drone itself is able to read the data stored in the RFID-part. Another part of the system is the communication module placed on the drone. This module is responsible for maintaining the contact between the reading device and the operator. Apart from the reading process, guidance of the drone is implemented via another communication channel. In most cases, navigation happens by GPS coordinates automatically.

The radio module is a small device, it consists only the most essential basic elements: an Atmell (ARDUINO) microcontroller and a radio IC. The radio IC devices are able to operate

on 433 MHz frequency band. The radio module requires low energy only. The 433 MHz frequency band is an ISM band, which is free to use in Hungary with strict adherence to the rules regarding the performance of the broadcast. These modules' transmission power is 100 mW, therefore it seems to be a good choice for this purpose. When selecting the drone itself, you should pay attention to the fact that most drones use the 433 MHz frequency band to forward telemetry data, so interference may occur, if our device operates in the same band.

The module is factory-equipped with an antenna, allowing to operate from 300-400 meters. A larger antenna would provide a wider action radius, for example, a Yagi antenna (the Yagi is easy to prepare in this band and it has a comfortable size). With such a range it can provide 55 kb/s data transfer rate. Data transfer should be chosen to FSK. Completion of the system requires two modules, one of them includes the programmable microcontroller. This component calibrates the radio IC's to the required frequency, sets data transfer speed and error codes. Therefore the microcontroller reads the data of the RFID through the interface, then forwards information to the radio IC in order to emit it. This signal would be received by the device of the operator, indicating the requested information automatically. Thereby we receive the crucial information from the RFID-part of the vehicle. Moreover we should take into consideration that these frequency bands are free, available to other users also. Drones also use the 433 MHz band mostly, so interference may occur. Ideal frequency should be chosen carefully. The system should be planned, constructed, tested and measured in detail.

LOCAL RECONNAISSANCE WITH THE NEWEST TECHNICAL DEVICES IN WASTE MANAGEMENT DURING RAIL ACCIDENTS

Nowadays a lot of drones are used for several purposes all over the world. As a result, wide scale civil use preceded legal regulation of the utilization of these devices, but the analysis of the related problems, furthermore, the lessons learned are also necessary to develop safe and regulated use of airspace by these vehicles worldwide. In Hungary, the next step may be taken towards the introduction of the recommended RFID-DRONE-VIRTUAL REALITY system after the establishment of the relevant legal regulation, in order to apply these solutions during the identification and disposal of hazardous wastes and items, furthermore, in case of rail accidents and disasters.

FINDINGS

How to make life on Earth safer, sustainable and disaster-free? The less energy you have to use, the less waste you have to produce! We must strive towards closed production and consumption cycles, so economic processes need to function in a circular way. Simplified natural laws must be interpreted quantitatively, and this requires serious engineering knowledge to be brought back to these laws, incorporating the parameters that will allow us to create brilliant engineering and technical security solutions, to remedy the problems of our age.

Currently, recycling (circular economy) is still managing the increasing accumulation of waste, with many years of delay, as a result, we need more sophisticated computing solutions, the use of quantum computers in order to process billions of parameters of our industrial life, to make it more bearable and livable.

Based on our proposed solution, i.e. Radio Frequency Identification by drones would make transport vehicles' identification much more, easier during railway accidents and catastrophes, thereby decreasing possibility of waste generation. Mini-drones may approach locations of accidents and catastrophes very fast in difficult circumstances, too. Transport regulation and railway area-management should be analyzed and examined from the aspect of waste-management also, in order to take adequate arrangements. In case of emergency or catastrophe the most effective methods are needed to prevent dangerous materials from diffusion safely.

High security RFID reading, identification of dangerous goods, fast forwarding of information would be an inestimable help for the people taking part in actions of recovery. Another important aspect is the life-saving, the transmission of information for the environmental and other emergency units, in order to start decontamination and restoration of the area.

ACKNOWLEDGEMENT

The research on which the publication is based has been carried out within the framework of the project entitled "The Development of Integrated Intelligent Railway Information and Safety System" (application number: GINOP-2.2.1-15-2017-00098).

REFERENCES

[1] Berek, L.: *Security.*
National Civil Service University, Budapest, 2014,

[2] Kiss Leizer, G.K. and Pokorádi, L.: *Waste Management Issues in Air Transport.*
Aeronautics Publications **27**(2), 17-25, 2015,

[3] Berek, L. and Solymosi, J.: *Security of Consignment of Hazardous Substances*.
Bolyai Review **24**(2), 46-62, 2015,

[4] Kiss Leizer, G.K. and Maros D.: *Handling of hazardous and disaster-generated waste in rail transport.*
Transportation Science Review **65**(3), 58-65, 2017,

[5] Kiss Leizer, G.K. and Berek, L.: *The Safety Technology Questions of Wastes Arising in the Course of Catastrophes in the Continental Traffic.*
Proceedings of the XXI-th International Scientific Conference of Young Engineers. Transylvanian Museum Association (EME), Cluj-Napoca, 2016,

[6] Rodic, A.; Mester, G. and Stojković, I.: *Qualitative Evaluation of Flight Controller Performances for Autonomous Quadrotors*.
In: Pap, E., ed.: *Intelligent Systems: Models and Applications*. Topics in Intelligent Engineering and Informatics **3**, pp.115-134, 2013,
http://dx.doi.org/10.1007/978-3-642-33959-2_7,

[7] Nemes, A. and Mester, Gy.: *Unconstrained Evolutionary and Gradient Descent-Based Tuning of Fuzzy Partitions for UAV Dynamic Modelling*.
FME Transactions **45**(1), 1-8, 2017,
http://dx.doi.org/10.5937/fmet1701001N,

[8] Restas, Á.: *Drone Applications for Preventing and Responding HAZMAT Disaster*.
World Journal of Engineering and Technology **4**(3), 9, 2016,
http://dx.doi.org/10.4236/wjet.2016.43C010,

[9] Restás, Á.: *Drone Supported Interventions at Dangerous Goods Transportation's Accident.*
International Conference on Transportation in Russia: Problems and perspectives. Russian Academy of Sciences, Saint Petersburg, 2016,

[10] Restás, Á.: *Disaster Management Supported by Unmanned Aerial Systems (UAS) Focusing Especially on Natural Disasters.*
Zeszyty Naukowe SGSP **61**(1), 25-34, 2017,

[11] Hell, P.; Mezei, M. and Varga, P.J.: *Drone communications analysis*.
IEEE 15th International Symposium on Applied Machine Intelligence and Informatics. IEEE, Herl'any, 2017,

[12] Restás, Á.: *Drone Applications for Supporting Disaster Management.*
World Journal of Engineering and Technology **3**(3C), 60553, 2015,
http://dx.doi.org/10.4236/wjet.2015.33C047,

[13] Kiss Leizer, G.K. and Tokody, D.: *Radiofrequency Identification by using Drones in Railway Accidents and Disaster Situations*.
Interdisciplinary Description of Complex Systems **15**(2), 114-132, 2017,
http://dx.doi.org/10.7906/indecs.15.2.1,

[14] Finkenzeller, K.: *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and near-Field Communication.* 3rd edition. John Wiley and Sons, 2010, http://dx.doi.org/10.1002/9780470665121,

[15] Papp, J.; Tokodi, D. and Schuster, Gy.: *Award-winning intelligent train control system.* Innorail Magazin **1**(4). 46-49, 2014,

[16] Tokody, D.; Schuster, Gy. and Holicza, P.: *Development of the Infocommunication System for the Intelligent Rail Transport System of Dangerous Goods in Hungary*. International conference on Applied Internet and Information Technologies. Faculty of Information and Communication Technologies, Bitola, 2016.

Interdisciplinary Description of Complex Systems 16(3-A), 369-375, 2018

ARE WE READY FOR SMART TRANSPORT? ANALYSIS OF ATTITUDE TOWARDS PUBLIC TRANSPORT IN BUDAPEST

János Imre Mezei[1,*] and Kornélia Lazányi[2]

[1]Óbuda University, Doctoral School of Safety Science
Budapest, Hungary

[2]Óbuda University, Keleti Károly Faculty of Economics
Budapest, Hungary

DOI: 10.7906/indecs.16.3.9
Regular article

Received: 7th May 2018.
Accepted: 31st August 2018.

ABSTRACT

In every case of serious development that concerns the majority of society, it is vital to analyze the current social opinion on the particular service and to analyze the possible effects, that the elements of the system being developed, could have. This is no different, when it comes to smart cities, more specifically smart traffic systems, even if these developments are to serve the improvement of people's living conditions. It is essential to determine what the decisive factors are for the man of today in choosing a mode of transport; which attributes influence that decision; what sort of opinion that individual has about different urban modes and whether he/she is ready to utilise smart means of transport. Furthermore,it is inevitable to explore, what would make people choose *smart* solutions (e.g. autonomous vehicles). Current article is to showcase the responses to the above questions of people living in the Hungarian capital, Budapest. The article begins with an overview of the international literature on smart cities and their transport system. Afterwards, the results of a research sponsored by the Hungarian Ministry of Human Capacities are presented, followed by the conclusions based on the results obtained.

KEY WORDS

smart transport, public transport, readiness, self-driving vehicle

CLASSIFICATION

JEL: L62, L92, O18, R00, R42

*Corresponding author, η: mezei.janos.imre@gmail.com; –;
Doctoral School of Safety and Security Sciences of Obuda University, H – 1428 Budapest, Pf.:31

INTRODUCTION

By 2050, over 70 % of the world's population is estimated to live in cities [1]. Municipalities are facing challenges unsolvable by present solutions, such as increasing the level of services – and through them the quality of life of the inhabitants - and at the same time improving the environmental quality [2]. For this reason the concept of smart cities is gaining ground very fast, since it promises to solve severe problems of urbanisation, such as traffic, pollution, waste management or resource efficiency. Mobility is one of the most relevant topics regarding smart urban solutions. According to the ENEA [3] already significant measures have been taken in this regard, improving fleet management and logistics processes of goods and public passenger transport facilities. Smart Mobility is fundamentally influenced and induced by modern info communication technologies used in both backward and forward applications, to support the optimisation of traffic instabilities and to provide more sustainable solutions [4].

THEORETICAL OVERVIEW

SMART CITIES

Most of the time the term smart city is defined through ICT used and its terminology [5]. It is regarded as a complex system of data, information and knowledge shared within and in-between the interconnected networks of citizens and organisations. In this aspect smart transport solutions are part of the digitalised infrastructure and are there to connect entities and to provide accessibility [6]. Nonetheless smart mobility is much more than that and is expected to infuse all territories of the smart city concept, influencing the life of all stakeholders with its competitive, green, sustainable and self-governing features [7, 8]. Bencardino summarised these expectations in six categories [9]:

- reduce traffic congestion,
- improve transfer speed,
- reduce transfer costs,
- reduce pollution,
- reduce noise pollution,
- increase safety.

However, ICT cannot provide solutions to people, unless people are eager to utilise the features provided by the smart solutions. Smart cities necessitate smart citizens who are curious and innovative and are willing to make use of the smart facilities. As Giffinger [10] defined it, the presence of "self-decisive, independent and aware citizens" is inevitable. Smart people are the clue of a smart transport system. Maturity to accept their own limitation in transfer freedom and to embrace shared or public solutions is a prerequisite that necessitates trust from the citizens [11]. ICT can only have significant impact on the quality of life of people in cities, if it does not require big investment on behalf of the citizens. Here it has to be noted that not only financial matters are taken into consideration, but the development of the necessary technological literacy and deliberate involvement may also be regarded as investment [12]. Hence, the aim of this article is to analyse the Smart Mobility readiness of people and to investigate the role of trust, and its building blocks in the creation of awareness about smart traffic solutions in the public transport and the value created through them. Faqih [13] proved that the perceived usefulness, trustworthiness and ease-of-use to have a direct impact on citizen behaviour. Trust also seems to play a decisive role in the adoption of new solutions, especially those heavily infused with ICT [14, 15]. Trust is important, since

citizens need to accept a certain extent of autonomy of vehicles and transport systems andconcede at least a part of their own control. Nonetheless primary research on the readiness and the trust issues regarding smart mobility are only limited and mainly focus on (semi-) autonomous cars [15-17]. Promoters of smart cities and smart facilities can only estimate the readiness of citizens for the future solutions. However, these estimations are important, since trusting behaviour can only be generated when sufficient amount of information is provided, and when the target group is deemed to be able to aggregate them into knowledge, and through the acceptance of change into wisdom [18].

RESEARCH

SAMPLE

We have assembled a standardized questionnaire, consisting of 15 + 4 demographic issues, in order to research general opinion on the public transport system of Budapest and on the acceptance of various autonomous vehicles. The choosing of the sample was random, using the snowball method, and ultimately 457 individuals filled out the questionnaire. Out of those 457 filled out, 450 were evaluated. In spite of this, the sample is not considered to be representative, since it lacks the size and the composition to be applicable to the base population, however it is adequate to observe fundamental correlations. The average age of participants is 24,29 years. The distribution of residence of the participants is 7,33 % village or municipality, 17,55 % small town, 10,66 % large town and 64,44 % capital, and all of them are involved in the public transport of the capital.

INCLINATION TO TRAVEL WITH VARIOUS AUTONOMOUS VEHICLES

To study the differences between groups, we were searching among independent sample t-tests to find the right methodology. Since there are different numbers of elements, considering the groups, we applied the Welch d-test as our test method. it, we examined, whether averages of the given variables deviated significantly. Only those results were presented, with which the Welch d-test proved a 95 % significance level of realization. During the tests, we were looking for answers on how an individual currently assesses a mode of transport, which in the future would be autonomous.

People who are willing to travel by autonomous tram and people who are not

First examined group consists of people willing to travel by autonomous trams and the people who are not, Table 1. A significant difference was detectable in two cases between the groups. The first was the opinion on the capital city tram system from a security point of view. In this case, those who are accepting of autonomous vehicles gave an average of 0,49 points more, than those who reject autonomous trams. The second aspect was the passenger-friendliness of trams, on which the acceptors gave an average of 0,37 points higher value. It can be inferred from this that acceptors feel that tram transport is safer.

People who are willing to travel by autonomous subway and people who are not

In case of the acceptance of autonomous subways, the four metro lines in Budapest were separeately studied, as they meet completely different technical standards. With metro line 1, significant deviations were found in 7 out of 8 attributes, between the acceptors and the rejecters, Figure 1. In each case, the acceptors gave a higher rating to the given attribute. The most prominent difference can be observed in security, where the acceptors rate the current state of metro line 1 on average 1,2 points higher, than the rejecters.

Table 1. Differences between people accepting and rejecting autonomous trams, concerning the current tram system. Independent Samples Test (autonomous trams).

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	*t*	d*f*	Sig. 2-tailed	Mean difference	Std. error difference	95% Confidence Interval of the Difference	
									Lower	Upper
Safety of Tram transport	Equal variances assumed	0,968	0,326	2,655	448	0,008	0,4902	0,1846	0,1273	0,8530
	Equal variances not assumed			2,605	206,386	0,010	0,4902	0,1882	0,1192	0,8612
Passenger Friendship of Tram transport	Equal variances assumed	0,113	0,736	2,179	448	0,030	0,3687	0,1692	0,0362	0,7012
	Equal variances not assumed			2,187	215,394	0,030	0,3687	0,1686	0,0364	0,7010

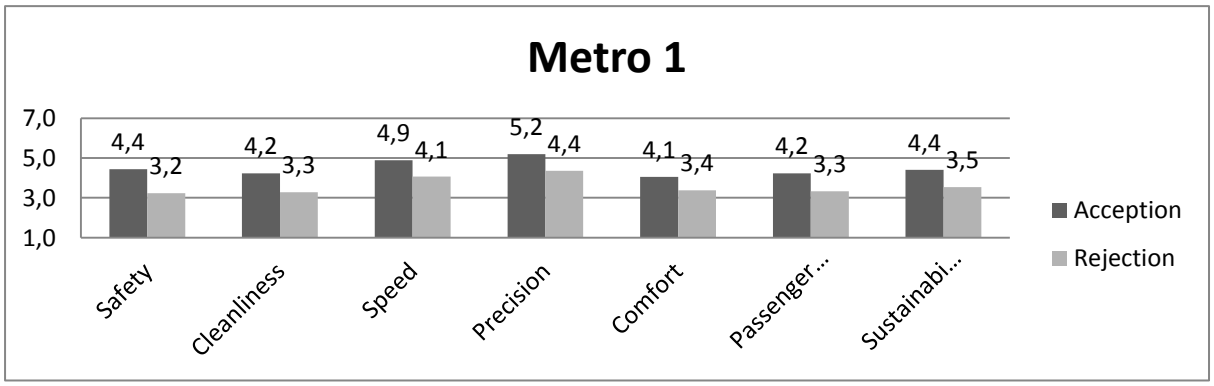

Figure 1. Differences between people accepting and rejecting autonomous subway, concerning the current metro line 1.

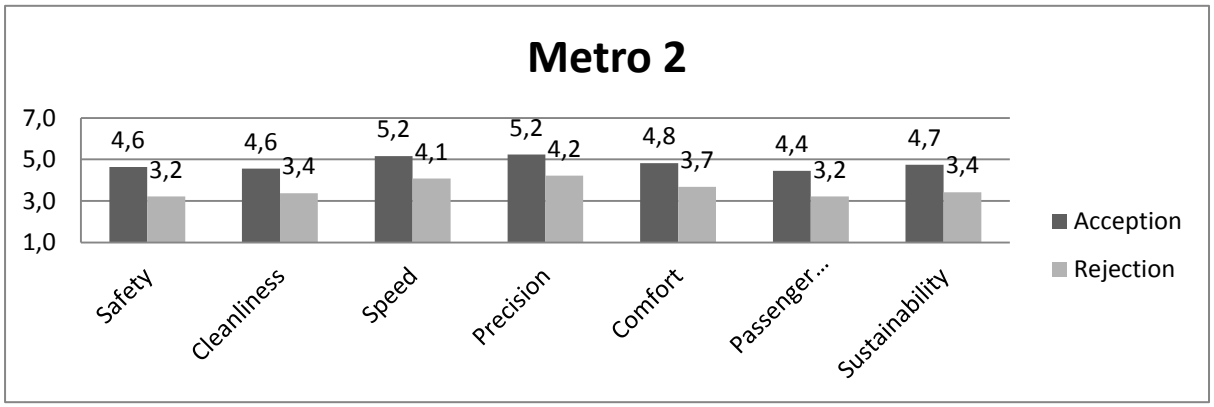

Figure 2. Differences between people accepting and rejecting autonomous subway, concerning the current metro line 2.

While observing the opinion on metro line 2, Figure 2, the same 7 attributes showed notable differences, as with metro line 1. However, it is also apparent, that between each rating, there

was at least 1 whole point in difference. From this we can deduce that the acceptors and the rejecters have a much sharper distinction, concerning metro line 2 travel. It is important to note, that with regard to the Grade of Automatization, metro line 2 qualifies for level 3, in which case it can almost be called autonomous, since the driver is mostly just a supervisor, and in charge of opening and closing the doors, but between two stations, the subway operates autonomously.

In case of metro line 3, notable differences were seen in 6 attributes, Figure 3. These were significantly less prominent, than with the other metro lines (no cases showed a difference of more than 1 point). It is important to point out, that the opinion on metro line 3 is by far the worst out of the 4 metro lines. Neither groups evaluated its security and cleanliness to the cumulated average of 3 points, from which it can clearly be concluded, that passengers are not satisfied with the quality of services, provided by metro line 3. Both the track and the subway cars have recently begun to be renovated. Prior to the start of the renovation, shutdowns were frequent in this line, which can partly be a contributing factor to the obtained results; furthermore during the reconstruction, the metro line has to be partially closed in several phases. Partly we attribute the results to these reasons.

Metro line 4 is the latest subway line in Budapest and completely autonomous. It is observable that all 8 attributes show significant differences, Figure 4. The most notable deviation was in the case of safety, where the average difference between acceptors and rejecters was 1.6 points. This clearly shows, that the people rejecting autonomous subways, mainly have a safety concern about traveling on a driverless vehicle, or are not trustung in these constructions as a whole. Overall, it is obvious, that metro line 4 had the best opinion among respondents.

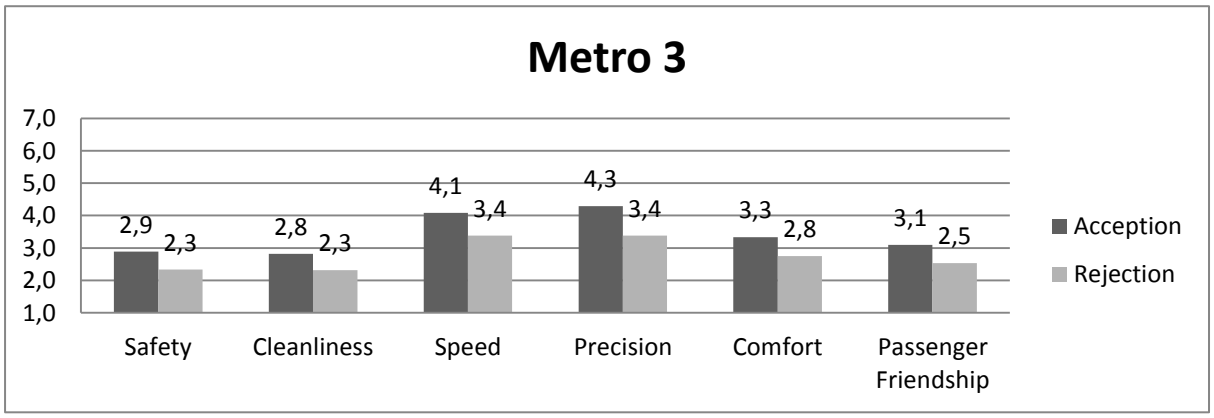

Figure 3. Differences between people accepting and rejecting autonomous subway, concerning the current metro line 3.

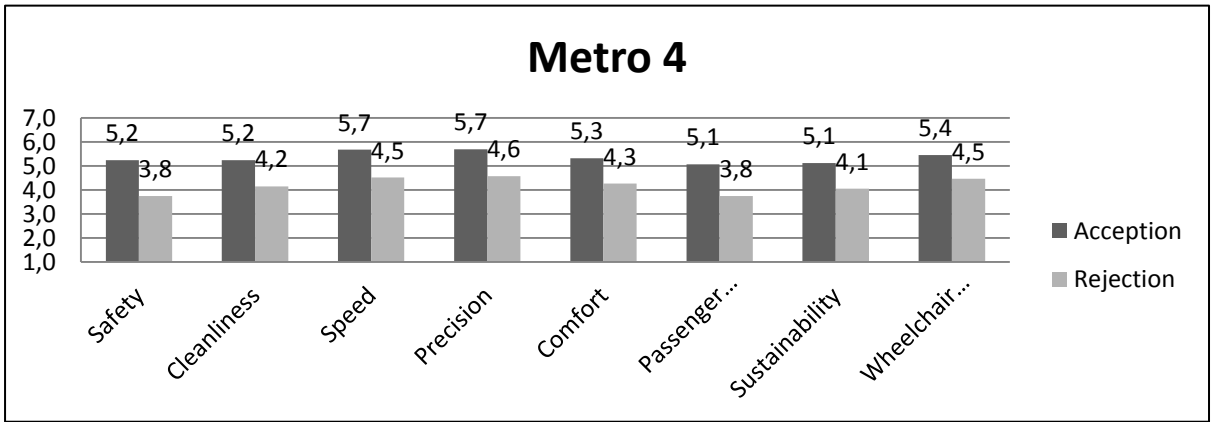

Figure 4. Differences between people accepting and rejecting autonomous subway, concerning the current metro line 4.

CONCLUSION

It can be stated that the spread of various *smart* developments and solutions will increase in urban infrastructure every year. According to this trend, the same applies to public transport. Seeing the obtained results, it can be concluded, that current opinions on tram and metro lines in Budapest are mixed, but overall these modes of transport show the highest amount of acceptance to convert into autonomous vehicles, according to the answers (70 % acceptance rate with trams and 86 % with subways). Based on the results currently obtained, it is absolutely necessary to carry out the research at a deeper level, in order to find out the cause and effect relationships about what makes a person accept autonomous vehicles in one mode of transport and rejects them in another.

ACKNOWLEDGEMENTS

Kornélia Lazányi acknowledges the support of New National Excellency Program of the Hungarian Ministry of Human Capacities.

János Imre Mezei acknowledges the support of the project "The Development of Integrated Intelligent Railway Information and Safety System" (application number: GINOP-2.2.1-15-2017-00098).

REFERENCES

[1] Dameri, R.P.: *Comparing smart and digital city: initiatives and strategies in Amsterdam and Genoa. Are they digital and/or smart?*
In: Dameri, R.P. and Rosenthal-Sabroux, C., eds.: *Smart City*. Springer, Cham, pp.45-88, 2014, http://dx.doi.org/10.1007/978-3-319-06160-3_3,

[2] Hall, P.: *Creative cities and economic development.*
Urban Studies **37**(4), 639-649, 2000, http://dx.doi.org/10.1080/00420980050003946,

[3] Valenti, G. and Mitrovich, S.: *Tecnologie ITS per i Sistemi di Trasporto*. In Italian.
http://old.enea.it/produzione_scientifica/pdf_brief/Valenti_ITStrasporti.pdf, accessed 5th May, 2018,

[4] Benevolo, C. and Dameri, R.P.: *La smart city come strumento di green development. Il caso di Genova Smart City*.
Impresa Progetto **3**, 1-36, 2013,

[5] Dameri, R.P. and Cocchia, A.: *Smart city and digital city: twenty years of terminology evolution.*
In: ItAIS 2013, X Conference of the Italian Chapter of AIS. Milano, 2013,

[6] Caragliu, A.; del Bo, C. and Nijkamp, P.: *Smart cities in Europe*.
Journal of Urban Technology **18**(2), 65-82, 2011, http://dx.doi.org/10.1080/10630732.2011.601117,

[7] Nam, T. and Pardo, T.A.: *Smart city as urban innovation: focusing on management, policy, and context*.
In: *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance*. ACM, Tallinn, 2011,

[8] Arena, M., et al.: Smart *mobility for sustainability.*
In: *AEIT Annual Conference 2013: Innovation and Scientific and Technical Culture for Development*. AEIT, 2013,

[9] Bencardino, M. and Greco, I.: *Smart Communities. Social Innovation at the Service of the Smart Cities.*
TeMA – Journal of Land Use, Mobility and Environment **INPUT 2014**, 39-51, 2014, http://dx.doi.org/10.6092/1970-9870/2533,

[10] Giffinger, R., et al.: *Smart Cities: Ranking of European Medium-Sized Cities*.
Centre of Regional Science. Vienna University of Technology, Vienna, 2007,

[11] Cisco, W.P.: *Smart City Readiness: Understand the issues to accelerate the journey.* https://www.cisco.com/c/dam/m/en_in/innovation/smartcities/assets/white-paper-c11-732985.pdf, accessed 5th May, 2018,

[12] Amoroso, E.G. *From the enterprise perimeter to a mobility-enabled secure cloud*. IEEE Security & Privacy **11**(1), 23-31, 2013, http://dx.doi.org/10.1109/MSP.2013.8,

[13] Faqih, K.: *Integrating perceived risk and trust with technology acceptance model: An empirical assessment of customers' acceptance of online shopping in Jordan.* International Conference on Research and Innovation in Information Systems (ICRIIS). IEEE, Kuala Lumpur, 2011, http://dx.doi.org/10.1109/ICRIIS.2011.6125686,

[14] Lazányi K. and Hajdu B.: *Trust in human-robot interactions.* 2017 IEEE 14th International Scientific Conference on Informatics Proceedings. IEEE Hungary Section, Košice, 2017, http://dx.doi.org/10.1109/INFORMATICS.2017.8327249,

[15] Lazányi K.: *Stressed Out by the Information and Communication Technologies of the 21st Century.* Science Journal of Business and Management **4**(1), 10-14, 2016,

[16] Schoettle, B. and Sivak, M.: *A survey of public opinion about autonomous and self-driving vehicles in the US, the UK, and Australia.* UMTRI-2014-21. University of Michigan Transportation Research Institute, Ann Arbor, 2014,

[17] Lazányi, K. and Maráczi, G.*: Dispositional trust – Do we trust autonomous cars?* IEEE 15th International Symposium on Intelligent Systems and Informatics. IEEE, New York, pp.000135–000140, 2017, http://dx.doi.org/10.1109/SISY.2017.8080540,

[18] Hussein, A.; Garcia, F.; Armingol, J. and Olaverri-Monreal, C.: *P2V and V2P Communication for Pedestrian Warning on the basis of Autonomous Vehicles.* In: Rossetti, R, et al., eds.: *Proceedings of the 19th International Conference on Intelligent Transportation Systems*. IEEE, Rio de Janeiro, pp.2034-2039, 2016, http://dx.doi.org/10.1109/ITSC.2016.7795885.

Interdisciplinary Description of Complex Systems 16(3-A), 376-383, 2018

SMART AND SECURE? MILLENNIALS ON MOBILE DEVICES

Peter Holicza* and Esmeralda Kadëna

Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.16.3.10
Regular article

Received: 17th April 2018.
Accepted: 31st August 2018.

ABSTRACT

Millennials, members of the Generation Y are constantly connected to their social circles online, they are the founders of the social media movement. These young consumers count as the largest segment of smartphone owners in most regions of the world. In fact, smartphones have become one of the most important possessions of this highly technology savvy generation. However, the advanced and widespread use of mobile devices often does not meet with the required security consciousness. People who have grown up with internet, are more likely to share personal and sensitive corporate information online by using the same device for both work and private applications, accessing free Wi-Fi networks or borrowing other devices without the appropriate protection. This work examines the crucial smartphone security risks that users face with the new technology. It aims to investigate how their practices and behaviours can pose security risks on their smartphones usage. Security practices and awareness can be improved by increasing users' knowledge. To accomplish this, education on technology is needed.

KEY WORDS

mobile device, Millennials, Generation Y, online behaviour, security

CLASSIFICATION

JEL: L63, L86, L96

*Corresponding author, η: holicza.peter@rh.uni-obuda.hu; –;
Doctoral School of Safety and Security Sciences of Obuda University, H – 1428 Budapest, Pf.:31, Hungary

INTRODUCTION: UNDERSTANDING THE MAIN USER PROFILE

It is evident that we as a society enter the digital age, physical presence and personal relations are getting less and less important. The differences in opinions between generations regarding beliefs, political views, or values, are referred to as 'generation gap'. As the whole world is facing new challenges, in terms of changes in classical roles and established norms, which result in traditional practices being less effective and often inapplicable; it is inevitable that certain adaptations in educational system, marketing, media, security and other fields related to Generation Y are necessary. The Millennials, Digital Natives, the 'we want it now' – many names have been used to describe this young generation, who are characterized as technology savvy, dexterous, open to new things and able to work in team [1]. It is evident how these characteristics make this generation more critical about technical issues and impatient; and the skill of creating *instant*, but effective solutions is being more and more appreciated and desirable in all life spheres. The values and characteristics of the Y generation have been widely researched, explained and grouped [2]. In addition, researchers mapped the psychological phenomenon that is associated with this generation, the most important of which are detailed in the following list:

- **Speed:** These young people were born in an era of technological development, and the usage of information technology novelties comes naturally to them. The information resources are today much easier to reach and the search is less time consuming, instead of going to the library, one can just "Google it" and find as much relevant information within seconds, while their predecessors did not have this luxury and would not be able to gather that amount of data through their whole lifetime. The social media enables them to be informed in real-time about the latest trends, daily events and lives of their peers and opens a platform in which they can communicate and exchange information in their private and social lives.
- **Decline of personal relationships:** It is evident that online communities transformed personal relationships. Most everyday life activities are simplified and more instant, which makes the actual human contact less important. Instead of writing a letter and waiting for it to reach the recipient, or even making a call, it is enough to just send a few words and emojis on Messenger. Planning and making arrangements is also simplified as we are now able to simply log into a website or an App and check who shared their location with us- we can know who is where and with whom. Living our lives online means sharing a lot of personal information and we are often expected to do so in order of keeping up with the contemporary world, otherwise one who decides to keep their personal life offline might become non-existent to others as the live interaction loses its value.
- **Freedom and adventure:** This generation is multilingual and the internet provided such opportunities, allowing them to roam the world virtually and made it easier to do so even in reality, as the formerly known barriers are gone [3]. The advanced technology enabled us to be online everywhere nowadays and it made it possible to travel freely to almost every corner of the world, and even working from the most exotic places, that is to be what is referred to as *digital nomads* [4].
- **Uniqueness and individualism:** They try to define themselves through their appearance and to stand out from the crowd. It is easy to shape their virtual personality and image in any way that they want and present themselves to the world in a way they are comfortable with. This freedom of *choosing* the whole life, as one present to the online community, requires the increase of consciousness. Digital technology has the ability of transforming identities [5]. These platforms are well organized and enable users to control what they want others to see, which leads to only the best moments being uploaded and shown.

According to some research, it might cause significant self-esteem problems as the audience (followers) compare only these moments to their life. On the other hand, the positive or negative feedbacks on the posts raise or decrease social self-esteem and well-being of the uploaders [6].

- **Simplicity, Simplification:** They prefer the simple, fast and more concise information, which explains the spread of image sharing web pages, apps and platforms (Instagram, Flickr, Tumblr, and Snapchat) where the text content is minimal. Members of the Y generation are reading less and less and the number of people struggling with reading comprehension is growing – if a text does not fit the mobile display, it seems to be too long to read.
- **FoMO:** This completely new phenomenon, which is the FoMO (fear of missing out) defined as the anxiety that someone feels when others are engaged in a rewarding, cheerful activity, while he/she is away [7]. It has a relevant impact on the psychological state of young people and on the quality of their lives by generating a lot of negative feelings and making individuals compete on a regular basis through social media. Because of the strong impact, it is not surprising that several marketing campaigns are based on this fear, and using the following words, expressions: *do not miss it*, *join us* etc. and require young people to constantly be online in order of feeling like a part of a community and in track of the latest trends.

MILLENNIALS' DIGITAL BEHAVIOUR

The above-mentioned conditions count as driving force of Millennials, therefore the advanced technology plays a very important role in their daily life. According to Vocalink study, smartphone is the most preferred smart device of European Millennials [8]. Mobile devices are the gateway of personal and/or business data, both local and those delivered in the cloud. During the use of such devices, millennials lead tracks and not only with regard to themselves but also to their contacts. The owner of smartphone is considered as the partial administrator of his device because some implemented security policies and relative technological mechanisms limit his actions. But alone technology cannot address security solutions [9]. That is why there is a need to analyse human based aspects, by understanding users and creating then more effective security measures as well as supporting good security practices through engagement and collaboration [9, 10].

Boshmaf et al. analysed the users' need for protection and privacy in smartphones usage. They outlined the types of data that users want to protect and investigated users' behaviour in the protection of such of data and the results showed that users want to protect their data on smartphone but they find doing so not convenient [11]. Onwubiko and Owens showed that employer's consent with security policies and guidelines in many companies is taken for granted. Instead of this they prefer a formalistic security approach [12].

Researchers are focused on examining whether users' protective behaviours are influenced by their technical knowledge and awareness of security threats [13, 14]. Wash et al. found that users' security perceptions can be grouped according to their demographic groups and technological knowledge [13]. Their observations showed that people with lower educational levels tend to make simpler security decisions [14]. Larose et al., state that peoples' security practices are affected the most by their motivation to protect themselves against security risks [15]. Many authors showed that smartphone users' privacy concerns have focused on location tracking and sharing [16, 17]. The problems of data protection against physical risks and possibility to improve weak authentication were presented by Muslokhlove. To increase the confidence of user and safety of mobile devices, upgrading the lock screen system in support of authentication and user's accessibility and providing suitable security might be a good

solution [18]. Ghosh et al. worked on user data, privacy and protection regarding semantic reasoning and user context modelling. The users' and smartphones' privacy under this framework are protected using embedded semantic policies based on the user' privacy and settings [19]. To execute the privacy policies on smartphone and to protect the data on an enterprise, Kodeswaran et al. showed a framework designed for Android platform policies [20]. The authors defined their privacy policies of acceptable information flow on mobile devices. The flow of information depends on the object involved in conforming Inter-Process Communication and its data.

USER BASED SECURITY RISKS

Mobile device users can be considered as the most effective tool that attackers have in compromising security. These devices can be victims of theft, data leakage and damage and as a result represent a significant information security risk to a Millennial. Below we present possible ways how attackers can gain access to mobile devices due to practices and users behaviours.

The malicious software (malware) industry is growing in terms of technology and structure. Malware causes breakdown of the device by entering at specific information and the damaged data/information of users becomes unusable [21]. These illegal softwares installed not directly by the user are used for all attacks that came from the outside taking advantage of the vulnerabilities in the device/system. The current platforms ask users to make the decision about accessing features such as location. These permission-granting approaches mean too much obstacles for the users. Very often most of them are ignored or not understood by users [22] and permission prompts are disruptive to the user's experience, teaching users to ignore and click through them [23]. As a consequence, users unintentionally grant applications too many permissions and become vulnerable to applications that use the permissions in malicious or questionable ways (i.e. secretly sending SMS messages or leaking location information).

Trojan or spyware, aims to seize the management and the information of the device [24]. Keyloggers are the most widely used form and are transmitted under the cover of a file that the user can unintendedly activate. The entire device in the background is under control of spywares and not noticed by the user. Worms are another type of malwares, a kind of virus, designed to spread through the network [24]. Transmitting forms (user interaction is needed) by SMS, MMS and activated by clicking on a file or opening a plug-in sent by e-mail, i.e. social engineering. Virus can penetrate into documents, send them elsewhere, distort their contents or make them unusable and make the hardware elements slow down [24]. Infected programs can be installed in other devices as well, followed by data loss, data leakage and even disruption of the conversation (for more, see *Zombie* virus) [25].

Information can also be collected and sent to someone else without permission through adware (used for advertising and promotional purposes) or cookies (supposed to offer better service to users) [24]. For iOS, the biggest threat in 2016 came from applications with very aggressive adware while Google Play saw a number of applications infected by malware [26]. Malwares are also created by some profit-oriented *teams*, like the Trojan "botnet Trojan-SMS.AndroidOS.-Opfake.a", which enabled the spread of the malware software "Backdoor.AndroidOS.Obad.a", which sends a spam containing the malware to its victim list [27]. If the mobile's operating system (OS) is out of date, it can also lead to vulnerability. Usually users don't pay attention to messages to update their mobile OS. Another issue is related to downloading from third party applications. Deficient API management is responsible for many malicious code infections. Controlled APIs have specific higher privileges to system update, file destruction, and information fetching. If attackers gain the APIs control, they could easily initiate attacks and use the privileges of the APIs [28, 29].

Other attacks (Social Engineering) [30] against users can be effective without using malicious software. *Phishing* (Password + Fishing), directs the user to a false (imitation) website in order to steal private information (credentials, credit card information, user name or password) [31]. Secure Sockets Layer (SSL)/Transport Layer Security (TLS) encryption is a protocol that assures users and provides data security when implemented correctly. Today it is used in many applications such as internet banking. If the code is left uncontrolled, the settings can be changed unwillingly and the information which was supposed to be safe and transmitted can be stolen through the communication path [32].

All smartphones have camera and touchscreen which can also lead to potential attacks. Users go to third party applications and if the source application is a problem, users are at risk of installing malicious programs. As a result, they can steal personal information or gain root access to their device [33, 34].

Considering the case of stolen or lost device, everyone can easily gain access to it if the screen is not locked, and encryption is an essential measure when it comes to security. With data like bank card information, passwords, sensitive data (messages, photos, videos, etc.), encrypting the data on smartphone keeps most personal information secure. A good defence practice against hackers can be the use of a strong password (a long one, mixed chars numbers and letters: owners' method) [35]. The longer the password, the stronger the encryption key.

CONCLUSION

The Millennials' digital habits have a lot of risk factors, such as the *internet at any price* mentality: internet access from any kind of free Wi-Fi networks, the lack of security measures and general unconsciousness about potential online threats.

Malicious softwares, Trojan or spyware, viruses, outdated operating systems, downloading from *third-party app*, unlocked touchscreen were identified. Hackers can easily manipulate this generation through Social Engineering tricks. Millennials rarely consider privacy and security of their smartphones, however, the increasing amount of sensitive data pose security challenges to users. In order to prevent data and information leakage is very important to increase the security awareness of people. Technology alone cannot address and solve security problems as they are not just a matter of technological factors, but human factor is involved as well. More attention should be paid to human behaviour, general attitude and misconceptions with regards to smartphone security. There is a need for education on technology in order of creating more effective security measures.

ACKNOWLEDGEMENT

Present article has been supported through the New National Excellence Program of the Ministry of Human Capacities of Hungary.

REFERENCES

[1] Jami, L.J.: *Who are Millennials? And what they want from libraries, bookstores and librarians.*
World Class Learning and Literacy through School Libraries. International Association of School Librarianship, Berkeley, 2008,

[2] Noble, S.M.; Haytko, D.L. and Phillips, J.: *What drives college-age Generation Y consumers?*
Journal of Business Research **62**(6), 617-628, 2009,
http://dx.doi.org/10.1016/j.jbusres.2008.01.020,

[3] Lazányi, K.: *What is the Role of Higher Educational Institutions in Managing their Students' Competencies?*
Science Journal of Business and Management **3**(1-1), 46-52, 2015,
http://dx.doi.org/10.11648/j.sjbm.s.2015030101.18,

[4] Prensky, M.: *Digital Natives, Digital Immigrants Part 1.*
On the Horizon **9**(5), 1-6, 2001,
http://dx.doi.org/10.1108/10748120110424816,

[5] Perillo, S.: *Reaching Generation Y: To be or not to be relevant.*
Australian Anglican Schools Network, Melbourne, 2007,

[6] Bolton, R.N., et al.: *Understanding Generation Y and their use of social media: a review and research agenda.*
Journal of Service Management **24**(3), 245-267, 2013,
http://dx.doi.org/10.1108/09564231311326987,

[7] Przybylski, A.K.; Murayama, K.; DeHaan, C.R.; and Gladwell, V.: *Motivational, emotional, and behavioral correlates of fear of missing out.*
Computers in Human Behavior **29**(4), 1841-1848, 2013,
http://dx.doi.org/10.1016/j.chb.2013.02.014,

[8] Vocalink*: The Millennials Influence – Europe*.
https://www.ipsos.com/sites/default/files/2017-05/vocalink-the-millennial-influence-europe.pdf, accessed 20th March 2018,

[9] Furnell, S. and Clarke, N.: *Power to the people? The evolving recognition.*
Computers and Security **31**(8), 983-988, 2012,
http://dx.doi.org/10.1016/j.cose.2012.08.004,

[10] Colwill, C.: *Human factors in information security: The insider threat who can you trust these days?*
Information Security Technical Report **14**(4), 186-196, 2009,
http://dx.doi.org/10.1016/j.istr.2010.04.004,

[11] Muslukhov, I.; Boshmaf, Y.; Kuo, C.; Lester, J. and Beznosov, K.: *Understanding Users' Requirements for Data Protection in Smartphones*.
In: Kementsietsidis, A. and Vaz Salles, M.A., eds.: *Proceedings of the 2012 IEEE 28th International Conference on Data Engineering Workshops*. IEEE, Arlington, pp.228-235, 2012,
http://dx.doi.org/10.1109/ICDEW.2012.83,

[12] Onwubiko, C. and Owens, T.J., eds.: *Situational Awareness in Computer Network Defence: Principles, Methods and Applications.*
IGI Global, Hershey, 2012,
http://dx.doi.org/10.4018/978-1-4666-0104-8,

[13] Wash, R. and Rader, E.: *Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users*.
In: Faith Cranor, L.; Biddle, R. and Consolvo, S., eds.: *Proceedings of the Eleventh Symposium On Usable Privacy and Security SOUPS 2015*. USENIX Association, Ottawa, pp.309-325, 2015,

[14] Aytes, K. and Conolly, T.: *A Research Model for Investigating Human Behavior Related to Computer Security*.
In: Americas Conference on Information Systems 2003 Proceedings. Association for Information Systems, No. 260, 2003,

[15] Larose, R.; Rifon, N. and Lee, D.:*Keeping our network safe: a model of online protection behaviour.*
Behaviour and Information Technology **27**(5), 445-454, 2008,
http://dx.doi.org/10.1080/01449290600879344,

[16] Kelley, P.G.; Benisch, M.; Cranor, L.F and Sadeh, N.: *When are users comfortable sharing locations with advertisers?*
In: Tan, D.; Fitzpatrick, G.; Gutwin, C.; Begole, B. and Kellogg, W.A., eds.: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Vancouver, pp.2449-2452, 2011,
http://dx.doi.org/10.1145/1978942.1979299,

[17] Consolvo, S., et al.: *Location Disclosure to Social Relations: Why, When, & What People Want to Share.*
In: Kellogg, W.; Zhai, S.; van der Veer, G. and Gale, C., eds.: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Portland, pp.81-90, 2005, http://dx.doi.org/10.1145/1054972.1054985,

[18] Muslukhov, I.: *Survey: Data Protection in Smartphones Against Physical Threats*.
Term project paper on Mobile Security and Privacy. University of British Columbia, Canada, 2012,

[19] Ghosh, D.; Joshi, A.; Finin, T. and Jagtap, P.: *Privacy Control in Smart Phones Using Semantically Rich Reasoning and Context Modeling.*
In: Dietrich S., et al., eds.: *Proceedings of the 2012 IEEE Symposium on Security and Privacy Workshops*. IEEE, San Francisco, pp.82-85, 2012, http://dx.doi.org/10.1109/SPW.2012.27,

[20] Kodeswaran, P., et al.: *Securing Enterprise Data on Smartphones Using Run Time Information Flow Control*.
In: Aberer, K.; Joshi, A. and Mukherjea, S., eds.: *Proceedings of the 2012 IEEE 13th International Conference on Mobile Data Management*. IEEE, Bengaluru, pp.300-305, 2012, http://dx.doi.org/10.1109/MDM.2012.50,

[21] Porter Felt, A.; Finifter, M.; Chin, E.; Hanna, S. and Wagner, D.: *A survey of mobile malware in the wild.*
In: Jiang, X.; Bhattacharya, A.; Dasgupta, P and Enck, W., eds.: Proceedings of the 1st ACM *Workshop on Security and Privacy in Smartphones and Mobile Devices*. ACM, Chicago, pp.3-14, 2011, http://dx.doi.org/10.1145/2046614.2046618,

[22] Porter Felt, A., et al.; *Android Permissions: User Attention, Comprehension, and Behavior*.
In: Faith Cranor, L., ed.: *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, Washington, No.3, 2012, http://dx.doi.org/10.1145/2335356.2335360,

[23] Motiee, S.; Hawkey, K. and Beznosov, K.: *Do Windows users follow the principle of least privilege? Investigating user account control practices*.
In: Faith Cranor, L., ed.: *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, Redmond, No.1, 2010, http://dx.doi.org/10.1145/1837110.1837112,

[24] Bidgoli, H.: *Volume III: Threats, Vulnerabilities, Prevention, Detection and Management.*
Handbook of Information Security. John Wiley & Sons, New Jersey, 2006,

[25] Gao, C. and Liu, J.: *Modeling and restraining mobile virus propagation.*
IEEE Transactions on Mobile Computing **12**(3), 529-541, 2013, http://dx.doi.org/10.1109/TMC.2012.29,

[26] McAfee: *Mobile Threat Report 2016*.
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2016.pdf, accessed 20th March 2018,

[27] Unuchek, R. and Chebyshev, V.: *Mobile Malware Evolution: 2013.*
https://securelist.com/mobile-malware-evolution-2013/58335, accessed 20th March 2018,

[28] Prodanovic, R. and Simic, D.: *Survey of Wireless Security.*
Journal of Computing and Information Technology **15**(3), 237-255, 2007, http://dx.doi.org/10.2498/cit.1000877,

[29] Kataria, A.; Anjali, T. and Venkat, R.: *Quantifying Smartphone Vulnerabilities.*
In: Dutta, M.K.; Rai, J.K. and Padey, S., eds.: *Proceedings of the 2014 International Conference on Signal Processing and Integrated Networks*. IEEE, Noida, pp.645-649, 2014, http://dx.doi.org/10.1109/SPIN.2014.6777033,

[30] Symantec: *2016 Internet Security Threat Report.*
https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf, accessed 20th March 2018,

[31] Anderson, R.J.: *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2nd ed.
Wiley Publishing Inc., Indiana, 2008,

[32] Hubbard, J.; Weimer, K. and Chen, Y.: *Study of SSL Proxy attacks on Android and iOS mobile applications.*
In: *Proceedings of the 2014 IEEE 11th Consumer Communications and Networking Conference*. IEEE, Las Vegas, 2014,
http://dx.doi.org/10.1109/CCNC.2014.6866553,

[33] Pore, A. and Bartere, M.: *A Review on Camera Based Attacks*.
International Journal of Computer Science and Technology **6**(1-1), 88-92, 2015,

[34] Bartere, M. and Pore, A.: *Preventions and Features of Camera Based Attacks on Smart Phones*.
International Journal of Emerging Trends and Technology in Computer Science **4**(4), 9-12, 2015,

[35] Keszthelyi, A. and Kadëna, E.: *Misunderstanding how Passwords Work*.
Volume of Management, Enterprise and Benchmarking in the 21st century III. Óbuda University, Keleti Faculty of Business and Management, Budapest, 2016.

Interdisciplinary Description of Complex Systems 16(3-A), 384-396, 2018

SAFETY AND SECURITY THROUGH THE DESIGN OF AUTONOMOUS INTELLIGENT VEHICLE SYSTEMS AND INTELLIGENT INFRASTRUCTURE IN THE SMART CITY

Dániel Tokody[1,] *, Attila Albini[1], László Ady[2], Zoltán Rajnai[1] and Ferenc Pongrácz[3]

[1]Óbuda University, Doctoral School of Safety and Security Sciences
Budapest, Hungary

[2]Óbuda University, Kandó Kálmán Faculty of Electrical Engineering, NextTechnologies Ltd.
Budapest, Hungary

[3]IBM Hungary Ltd.
Budapest, Hungary

DOI: 10.7906/indecs.16.3.11
Regular article

Received: 21st March 2018.
Accepted: 31st August 2018.

ABSTRACT

Our article is discussing the methodical basics of planning smart mobility. Smart mobility is one the main elements of a smart system. According to the methodology presented in our article, transportation in a smart city can be developed in a safe form, focusing on two main elements: safety and security planning of smart mobility. Intelligent (transportation) infrastructures and autonomous intelligent vehicles will be integrated in a common system in order to achieve the digital transformation of the transportation system. The aim of this research is to examine questions raised in relation to the control and communication of autonomous vehicles and vehicle systems. The development of autonomous intelligent vehicles and vehicle systems is based on the further development of the cooperating intelligent transportation systems to achieve smart mobility. The research aims to find such methods and procedures which help the safety planning of increasingly complex cyber-physical systems and system elements used in autonomous intelligent vehicles and transport systems, in view of aspects of safety and operational risks.

KEY WORDS

digitalisation of transportation, autonomous intelligent vehicle, smart city, intelligent infrastructures

CLASSIFICATION

APA: 4090, 4100
JEL: R41

*Corresponding author, η: daniel_tokody@ieee.org; –;
Doctoral School of Safety and Security Sciences of Obuda University, H – 1428 Budapest, Pf.:31, Hungary

INTRODUCTION

The aim of the present research is to examine the questions raised in connection with the control and communication of autonomous vehicles and vehicle systems, the building process of autonomous intelligent vehicles and vehicle systems, the further development of cooperative intelligent transport systems and the implementation of smart mobility. Its goal is to elaborate the methods and procedures to support the safety planning of cyber-physical systems and system elements with an increasing level of complexity in the autonomous intelligent vehicles and vehicle systems, by considering such factors as operational safety, the risks of keeping in operation and cyber security. In the processing of large amount of data generated throughout the operation of intelligent infrastructures and autonomous intelligent vehicles, a key role will be given to the information created by transforming the data collected by various sensor networks. Serious predictions and important conclusions about the communication-based and networking cooperative structure of the past can be made based on such information, including with real-time or future operation of the transport system. Therefore, processing big data (data mining, data science) will provide such information which can be used to ensure safety, operation of the transport system and achieve any business objectives related to transportation.

SYSTEM ENGINEERING FOR SMART MOBILITY

Smart mobility innovation programmes can be characterized by the use of key enabling technologies, which leads to the digitalization of transportation. In order to achieve smart mobility, a holistic approach is needed in system planning, which presupposes the synergy of the interdependent systems related to the transport system (energy sector, urban subsystems, etc.) These Key Enabling Technologies are connected by the information and communication technologies, which have an important role in the digitalisation of transportation. The digital transformation of transportation can be achieved through four basic processes: automation, digital data, digital user interface and the systems interconnectivity.

Some Key Enabling Technologies of smart mobility:

- Automation – sensor and controller network, automotive sensor fusion system [1], adaptive speed control [2], on-board vehicle self-diagnostic sensor [3], Inertial Navigation Systems [4].
- Digital data – cloud technology and Big Data [5], data fusion system [1], information distribution – driver information system [3], automotive vehicle data management [6].
- Digital user interface (driver, operator, vehicles) – driver-vehicles interaction [7], task optimization [8], maintenance [9].
- Interconnectivity – vehicle fleet management systems [10], peer to peer networking [11], knowledge accumulation [12] and Artificial Intelligence [13, 14], self-configurable vehicle clusters [15].

Based on these Key Enabling Technologies, autonomous vehicles can be considered as one of the main elements of smart mobility (see Fig. 1). The level of vehicle automation has been defined by the Society of Automotive Engineers in the document entitled “Levels of motor vehicle automation adapted from SAE Standard J3016”. LoA5 (Level 5 of Automation, the full automation of autonomous vehicles) expects the development of a transport infrastructure which is completely different from traditional infrastructures. Therefore, the other main element of smart mobility is, the intelligent (transport) infrastructure, which will be needed for the usage of autonomous vehicles. For both elements, the safe communication among the components of the system will play a key role in the operation.

Figure 1 shows an example of an autonomous intelligent vehicle's interaction/communication with physical and cyber infrastructures. Today such vehicles also contribute to the totality of a cyber-physical system. Automation - the development of cooperative transport systems and smart mobility - involve the digitalization of the automotive industry. Large-scale automation also aims to reduce the risk of human errors in the process of transportation. However, this development has a price: the effects from using cyber-physical systems must be examined during the development of autonomous intelligent vehicle systems. With the cybernetization of the industry or with the application of machines that are capable of learning, the concept and issues of safety need to be examined from a broader perspective.

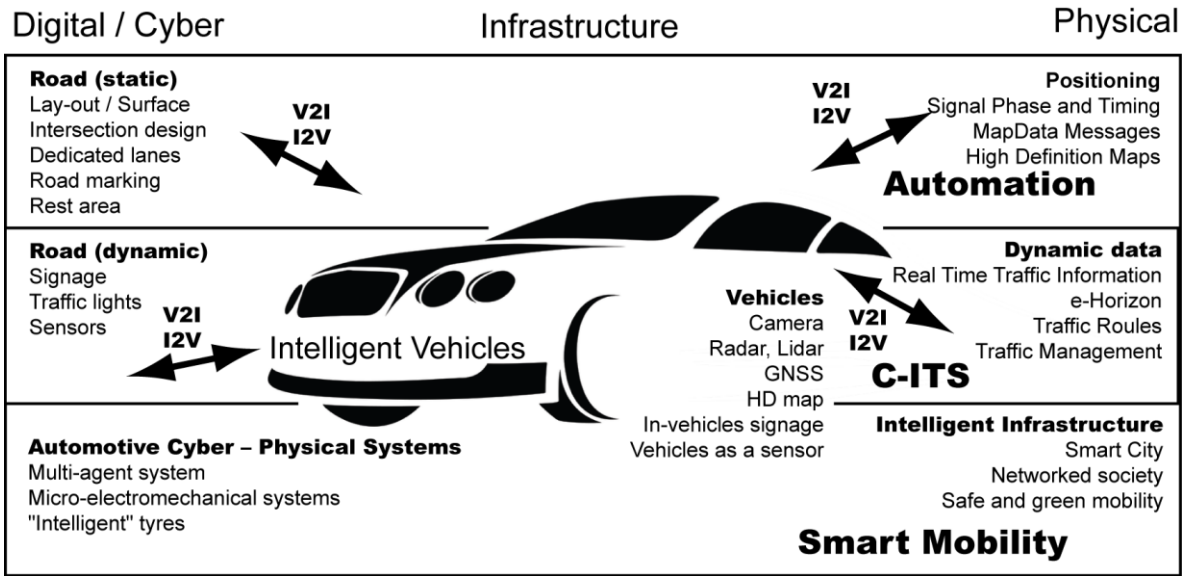

Figure 1. Strategy model of Cyber-Physical Vehicle Systems and Infrastructure (edited from [16]).

The strategy model of cyber-physical vehicle systems and infrastructures represents a plan or model, which aims to improve the safety and security of the transportation process. From the beginning stage of transportation system transformation through the way towards the implementation of cooperative intelligent transportation and smart mobility, smart vehicles will share the road with traditional vehicles – a situation which may last for a long time. In order to achieve smart mobility, besides the concept of vehicle development, research needs to be done during the planning of intelligent transportation systems about the infrastructure of transportation (fast roads, charging lanes, transport hubs, overpasses, etc.). Interactions between intelligent transportation infrastructures and autonomous vehicles need to be planned as well. Vehicle development can involve a number of fields (e.g. vehicular ad hoc network) which may become an infrastructural issue later. The same services and applications required to remain compatible during the long process of the transportation system development, even in the simplest data representation. Therefore, issues with long-term compatibility must receive special attention at the planning of the mobility system.

According to a tentative definition "Intelligent Transport Systems (ITS) are advanced applications which, without embodying intelligence as such, aim to provide innovative services relating to different modes of transport and traffic management and enable various users to be better informed and make safer, more coordinated and *smarter* use of transport networks." This definition, however, has become outdated even on a European level. This obviousness can be well illustrated by the relationship between ITS and C-ITS systems: "Vehicles are getting safer, cleaner, and more intelligent. Various sensors and assistant systems enable vehicles to monitor their environment. By means of information exchange among vehicles, as well as between vehicles and the roadside infrastructure, vehicles

transform from autonomous systems into cooperative systems. Inter-vehicle communication is a cornerstone of intelligent transportation systems (ITS), commonly referred to as cooperative ITS (C-ITS) or car-2-X communication."

During the planning phrase the strategy that says planning phase that "the focus can no longer be on the infrastructure layer alone (for instance roads and vehicles). Digital technologies also build on a data layer which contains both static data such as digital maps or traffic regulations and dynamic data such as real-time traffic information. These data are then used to develop a layer of innovative services and applications, which are made available over a layer of networks" [17] must be considered as well. This will allow the development of real cooperative intelligent transport systems in Europe with interconnected and automated mobility. C-ITS will provide an interoperable solution at a European level. Due to its insular structure, it cannot be tested in its full functionality; therefore the planning of cooperation is of primary importance. "An integrated transport system relies on the interoperability of its components. That means that systems need to be able to interact with each other, across borders and transport modes, at all levels: infrastructure, data, services, applications and networks." [17]. This interaction can be ensured through communication. "The coordinated and rapid deployment of cooperative, connected and automated vehicles will make an important contribution to improving road safety, increasing the efficiency of road transport, and ensuring the competitiveness of EU industry." [17]. C-ITS does not only refer to road transport. This fact is important to consider at the planning phase, as the development of a smart mobility system will depend on the implementation of the C-ITS.

The sector of transportation is a major energy consumer and emission source. At the planning of the energy efficiency of a smart mobility system, it is not enough to think about the use of renewable energy. It is much more important to provide a plan for cooperation to ensure the operability of the system. For example, congestions or unnecessary waiting times should be reduced in the system. Therefore, it should be possible to ensure the cooperation between the infrastructure and the various vehicles. The energy efficiency of the transportation sector may also depend on the throughput of the system, the fuel consumption and transport capacity of the vehicles, etc. For example, in the course of organizing transportation, various European systems and smart services are available to help the planning of optimal usability, the rationalization of energy consumption in the smart mobility system. In road transportation it is essential to ensure the full coverage of mobile communication, but the infrastructure itself will not become smart only by fulfilling this requirement. In order to develop an intelligent transport system it is not enough to simply introduce WIFI, LED or electric cars, but it is necessary to ensure the overall transformation of the transport infrastructure by the system-level integration of such new technologies as the use of intelligent materials, wireless sensor networks, energy harvesting, etc. The essence of planning an intelligent transport infrastructure lies within its people-oriented approach, which aims to provide maximum services for people by maintaining safety, convenience and sustainability on the long term. One way to achieve this is to make vehicles and infrastructures intelligent. In an intelligent system communication has a prominent role. As its operation is based on communication, the data processing centre of traditional transport monitoring systems needs to be further developed to create a C-ITS. Most probably it is a cloud-base approach which will be applied in intelligent transport systems instead of a centralized monitoring solution. A good example for this is the hybrid smart vehicular ad hoc network.

SERVICES OF SMART MOBILITY

The real contents of smart services have not yet been clearly identified in common practice. The main goal of smart services is to put a user into such a psychological state which helps to

accept changes and adopt novelty ideas naturally with regard to various technological innovations. One aspect of the planning of self-driving cars is to provide a comfortable, cosy, relaxing and entertaining experience during the travel. Individual ideas, however, do not make a smart solution without cooperation; therefore it is necessary to make plans for the cooperation of these services. In this sense an " 'ITS service' means the provision of an ITS application through a well-defined organisational and operational framework with the aim of contributing to user safety, efficiency, comfort and/or to facilitate or support transport and travel" [18].

One of the basic requirements of a smart mobility system which must be considered at the planning phase is that through the optimal use of traffic and travelling data it should enable the users of the intelligent infrastructure to plan their routes automatically in accordance with the basic principles of ITS services. In case of the C-ITS services related to passenger and goods traffic, uninterrupted services should be ensured at the crossing of borders in Europe. Thus, the primary goal is to provide real-time traffic information and multimodal travel information services across the EU. It is also important to develop such C-ITS applications which are related to road safety or other protective and preventive measures, e.g. applications which give a warning in case of poor visibility or at the presence of any objects, people or animals on the road. By creating the necessary vehicle-vehicle, vehicle-transport infrastructure and transport infrastructure-vehicle connections to enable safe data and information exchange, these goals can be achieved through automation, based on the data collected by the sensors of autonomous intelligent vehicles.

With regard to intelligent transport infrastructures and their related services, various elements could be identified during the planning phase: smart road, smart parking places, smart energy supply points, which may have an important role on the level of services in the development of a smart mobility system. The main criteria of a smart road that is should fit into the existing infrastructure and it should support both individual and community transport. Intelligent infrastructure creates safety and in case of a danger, it ensures prompt counter-measures. The provision of information and booking services regarding safe and protected parking places is also part of the development of smart mobility systems. In case of parking or rest areas, intelligent street lighting, surveillance and security camera systems allow further automation in operation.

Concerning the development of parking or accommodation booking systems, further research needs to be done in tourism and in user experience. On-road accommodation may be offered for those people who travel across several countries. However, those who travel to specific destinations will not opt for roadside motels if they can find accommodation with a higher service level nearby. On the level of services, it must be examined how such real-time information about local opportunities can be sent to passengers during the time of travelling. The provision of online real-time data/information on regional transfer points and empty or free parking places raises similar questions. Occupancy forecasts may not only be made on the basis of the information about free places or by other data of the booking system, but by the self-diagnoses of vehicles, through which it can be predicted which vehicle will need to stop (at the beginning stage, at the presence of a driver, he can be alerted in advance). This stopover may be calculated from the state of charge of the vehicle's battery, or it is possible to alert to any necessary servicing. The vehicle may book a parking place automatically, if it knows what parameters it has.

In the absence of self-driving cars, or in the transitional period, an application could be introduced to check the drivers' alertness and their capability to drive, and to warn them or, as an embedded solution, to stop the vehicle for an imposed rest. In case of the use of self-driving cars, the use of roadside rest areas will become less relevant. In a fully automated

system, there is no need to wait for a driver to regain his alertness, while in a hybrid transport system, where self-driving and traditional vehicles are both present, this is still necessary to ensure. In order to enhance the services of rest areas it is important to examine user demands with regard to eating and other physical needs.

In a smart mobility system a number of services can be offered to support the use of alternative fuels. In the case of e-mobility, a major task is to connect and integrate the vehicles into the electric energy system, and a wide range of smart solutions could be developed for this purpose. Until the use of electric transport becomes everyday practice, it is important to provide prompt and adequate information for the users about the application of these new technologies. There are various IT-based solutions to provide such services. Sustainable transportation may not only be approached from the point of energy efficiency. For example, automated waste collection in parking and rest areas should also be resolved. In the future, the automated collection of dropped litter or the remote monitoring of the fullness of waste bins and their automated emptying may be realized by the use of mobile robots integrated into the smart mobility system, among other elements of the infrastructure maintenance service.

THE CONCEPT OF SAFETY AND SECURITY IN AUTONOMOUS INTELLIGENT CYBER-PHYSICAL VEHICLE SYSTEMS

In order to reduce the complexity and increase the flexibility of electric cabling in motor vehicles a bus system has been implemented. With a growing scope of functionalities, the number and variety of bus systems have increased. The buses of safety functions have been separated from the networks ensuring convenience functions. Nevertheless, experience has shown that a significant proportion of motor vehicles in traffic can be affected by the vulnerability of networks from the point of cyber security. Convenience functions are not always given adequate protection and some functions are implemented without any protection at all. These security gaps can be used to access certain security functions, to disrupt their operation or take over their control even without a direct physical connection. Therefore, at the planning of autonomous intelligent vehicles, the main elements of the smart mobility system, these cyber security issues must also be considered.

SAFETY OF AUTONOMOUS INTELLIGENT CYBER-PHYSICAL VEHICLE SYSTEMS

With regard to autonomous intelligent vehicles, safety means that a given vehicle must be kept in such a condition which ensures the highest level of protection of human lives. “Safety describes the effort to prevent mistakes in the core functions of a vehicle or, in a worst case, to protect the occupants and other persons involved from harm. Components such as brakes, steering, airbags, and the crumple zone of a car, but also electronic assistants such as ESP or ABS are critical to safety” [19]. Land vehicles are important elements of intelligent transport systems. At the planning or checking of the safety of autonomous intelligent land vehicles, the following aspects defined by SAE International are considered: functional safety, active safety (e.g. Advanced Driver Assistance System), safety and reliability (e.g. electronics and electrical systems; hardware and software verification and validation [20]), safety and human factors.

Figure 2 shows an example of the cyber-physical systems related to the road safety of autonomous intelligent vehicles together with the systems related to the vehicle’s environment. As it is well illustrated by this example, the information, warning, control, intervention, severity reduction or rescue systems, which actively or passively ensure the road safety of vehicles, should all be considered from the aspect of cyber security.

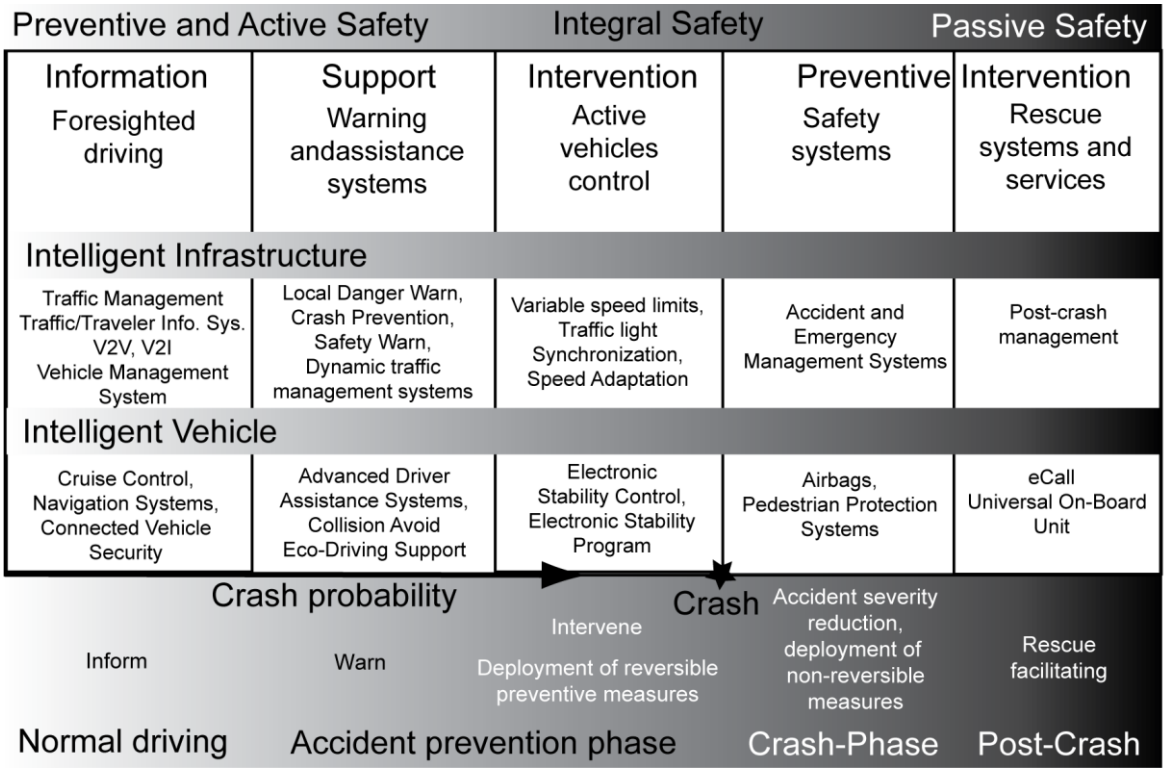

Figure 2. Safety phases of the Autonomous Intelligent Cyber-Physical Vehicle Systems (edited from [16, 21]).

"Safety integrity refers to the likelihood of a safety related system satisfactorily performing the required safety functions under all the stated conditions, within a stated period of time: without any unsafe failures. The Safety Integrity Level (SIL) assigned to a system determines the development, planning, manufacturing and operating methods that should be applied." [22]. According to certain classifications, three areas of safety can be distinguished: functional safety, technical safety and contextual safety (EN 50126-2:2017). In case of safety critical systems in the auto-industry, the values of ASIL (Automotive Safety Integrity Level) are used throughout the lifecycle of vehicles.

SECURITY OF AUTONOMOUS INTELLIGENT CYBER-PHYSICAL VEHICLE SYSTEMS

Security means the provisions made to ensure the protection of property against theft. One example for this is the way the money stored in ATMs is protected, or the use of passwords or data security in information technology. Therefore, at the checking and planning of autonomous intelligent land vehicles from the point of security the primary aim is to build a cyber safe system. With regard to the vehicles, vehicle systems and intelligent infrastucture within the intelligent transport system, other aspects of security have also been identified in the present research. "Security, on the other hand, means the security of software systems against malfunctions and external attacks. Software in cars has various roles: engine control, external communications, but also car safety and security." [19]. In the transport system, the digits '1201012356' for example, can be used as some data. If such data, however, represent the communication ID of a vehicle in the ad hoc network of vehicles, it will also represent some information within the system. According to Muha, in the taxonomy of information security, the circle of elements to be protected include the persons, the physical environment of the system, the infrastructure necessary for operation, the hardware and software products, communication devices and networks, data carriers and regulations [23].

Information security focuses on the confidentiality, integrity and availability of information. In addition, cyber security means the protection of infocommunication systems. As it can be seen in Figure 3, cyber security includes everything and everyone that can access the applications of the vehicle industry through the cyber space.

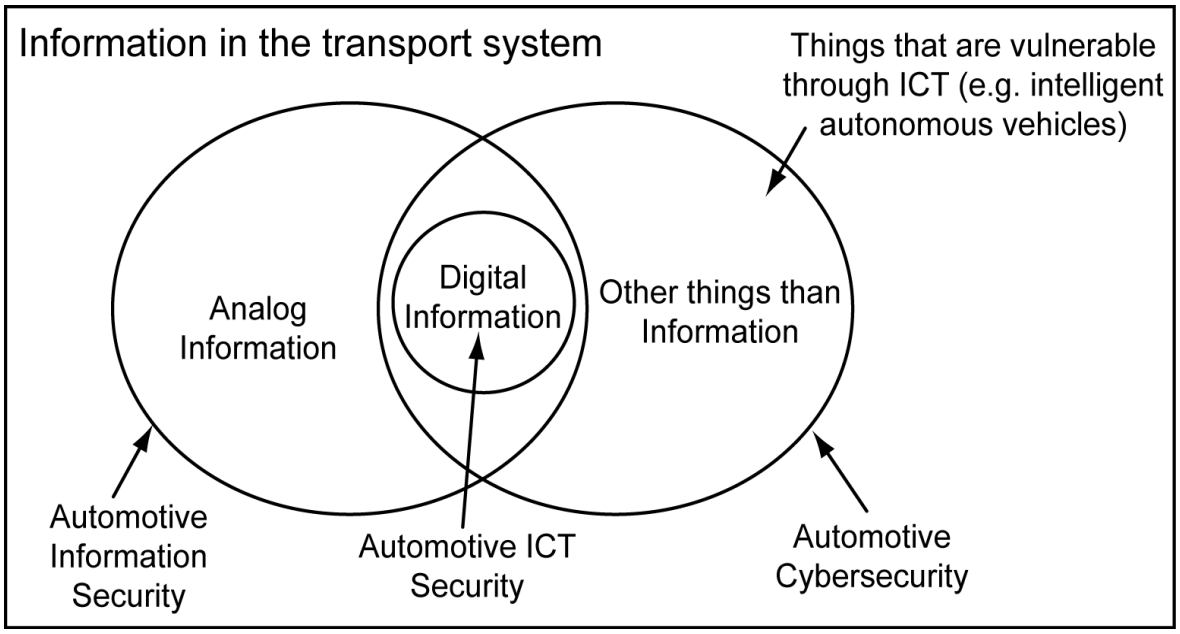

Figure 3. Venn diagram of the difference between Automotive Cyber security and Automotive Information Security [24] (authors' edit).

SAFETY AND SECURITY THROUGH ITERATIVE DESIGN – VEHICLES CYBERSECURITY SYSTEMS ENGINEERING, RISK-ORIENTED DEVELOPMENT

Figure 4 shows the iterative development process of smart mobility ecosystems. The safety and security-related development of the two basic elements of smart mobility must follow this process. The process of safety and security development is also represented in Figure 5.

The automotive connected world poses threats to product safety and performance, data integrity and access, privacy and interoperability. The ISO 26262 standard on the functional safety of the electronic systems of road vehicles already provides rules and planning guidelines, while Edition 2 specifies the requirements of cyber security procedures for interfaces. Nevertheless, this field still needs an overall automotive-specific cyber security standard. The relevant cyber security ISO standard is at the proposal stage, while the SAE standard is currently being developed, but the first edition of the recommended practice J3061TM was already issued in January 2016. Of course, other standards also affect automotive developments in the cyber security engineering process, including some general IT security standards (ISO 27001, ISO 15408) or specific security standards for V2X communications (IEEE 1609.2, ETSI TR 102 638 V1.1.1).

As this field is still in its infancy, automotive cyber security engineering processes are yet to be developed in accordance with the related standards and best practices (SEA – Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061). Cyber security engineering processes must comply with the existing systems of functional security and quality processes, and the adequately qualified personnel should be able to perform these security. The IEC 62443 standard defines four security levels, including qualitative indicators, competences and effort levels for a successful attack against the system.

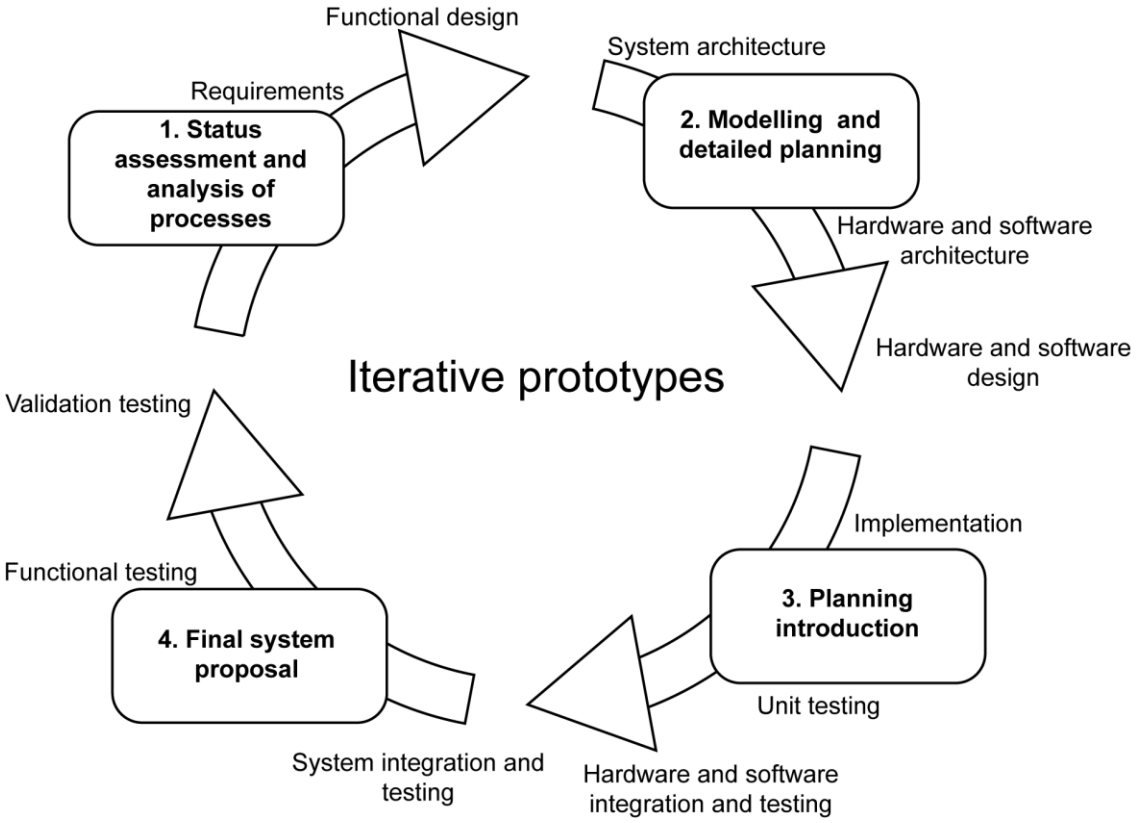

Figure 4. The development process of the iterative prototypes of smart mobility ecosystems [16] (authors' edit).

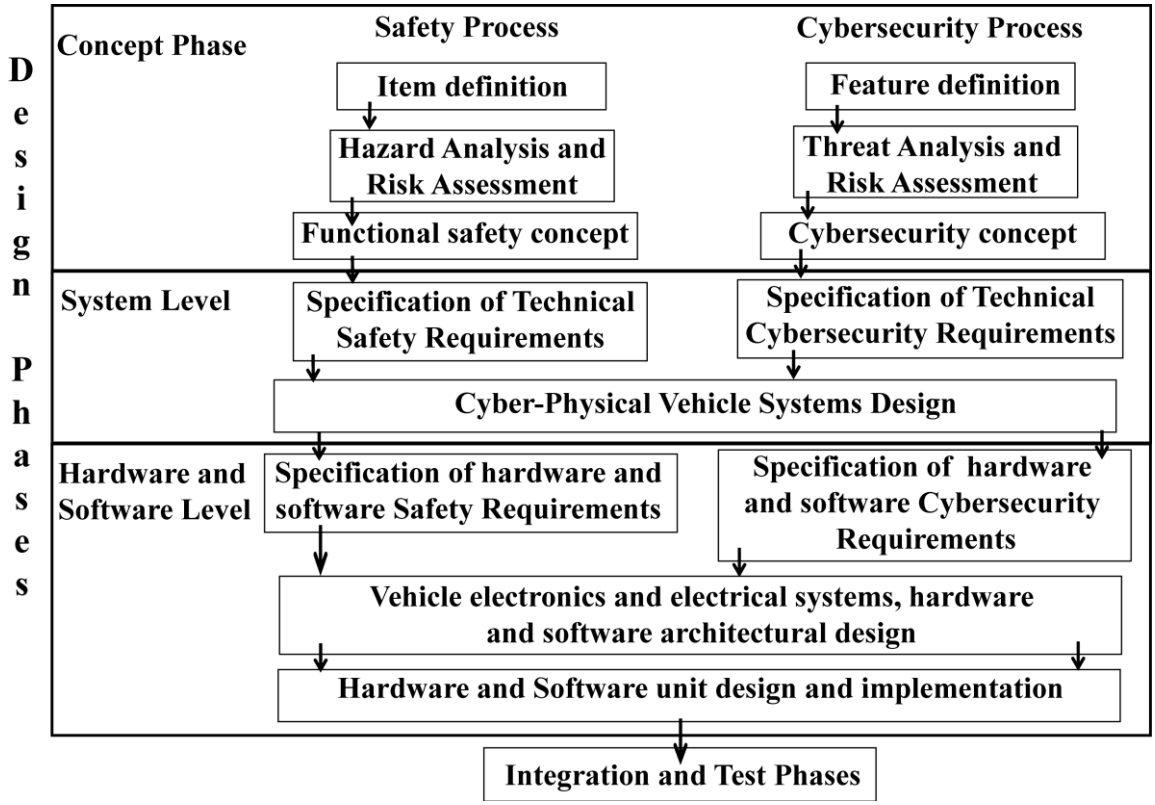

Figure 5. Safety and security through the design of autonomous intelligent vehicle systems and intelligent infrastructure [25, 26] (authors' edit).

In the course of the development process, functional safety as well as cyber security, hazard analysis and risk assessment as well as threat analysis and risk assessment, safety concepts and requirements as well as security concepts and requirements, system design as well as defence-in-depth system planning must all be conducted as shown in Figure 5. Cyber security should not simply be an additional element of the development process, but it should make an integral part of the planning phase, from the conceptual stage, through the manufacturing, operation and servicing to the decommissioning of the system. This is what the overall lifecycle management of cyber security means and it is realized in the course of the cyber security engineering process [22]. The automotive cyber security integrity level of the developed electrical, electronic and programmable electronic safety-related systems can be defined with the relevant ACSIL (Automotive Cyber Security Integrity Level) values.

CONCLUSIONS

According to Cohen, one of the main elements of the smart city is smart mobility[27]. The present article discussed the design process of this new mobility system. As the research pointed out, the two main elements of smart mobility are autonomous intelligent vehicles and vehicles systems, and intelligent transport infrastructures. The development of smart mobility has become necessary with the demand for creating cooperative intelligent transport systems. These endeavours aim to increase productivity (transport capacity, comfort), to reduce the number of accidents or the emission of harmful materials in city transport. Smart city transport can be conceived as an advanced ITS system. The marketing of smart city mobility focuses on the provision of additional services which are not available in traditional systems. The present article has shown a number of smart mobility solutions. The use of autonomous intelligent vehicles is becoming increasingly widespread (robots [28], drones [29] and self-driving cars [30]) due to their overall benefits on the society [31]. Today's advanced robot systems [32], such as self-driving cars, are capable of platooning or reaching a selected destination autonomously. Besides vehicle-to-vehicle communication, V2X (Vehicle-to-everything) communication must also be ensured to create a smart city. The functional and operational safety of vehicles has long been researched, but besides the physical infrastructure and the physical systems of the vehicles, cyber-physical complex systems are playing an increasingly important role. The cyber-security approach of automotive developments is a new but fast developing field. The present article described the aspects of the safety and cyber security-related planning of electrical, electronic and programmable electronic safety-related systems in the development of smart mobility [33].

ACKNOWLEDGEMENT

The research presented in this article was carried out as part of the project in the framework of the New Széchenyi Plan, No. EFOP-3.6.2-16-2017-00016. The completion of this project is funded by the European Union and co-financed by the European Social Fund.

REFERENCES

[1] Steinbaeck, J.; Steger, C.; Holweg, G. and Druml, N.: *Next generation radar sensors in automotive sensor fusion systems.*
2017 Sensor Data Fusion: Trends, Solutions, Applications. IEEE, Bonn, pp.1-6, 2017, http://dx.doi.org/10.1109/SDF.2017.8126389,

[2] Liubakka, M.K.; Rhode, D.S.; Winkelman, J.R. and Kokotovic, P.V.: *Adaptive automotive speed control*.
IEEE Transactions on Automatic Control **38**(7), 1011-1020, 1993, http://dx.doi.org/10.1109/9.231457,

[3] Park, S.H. and Lee, S.Y.: *Development of On-board Diagnosis via CAN for a HVI (Human Vehicle Interface) Technology*.
2012 IEEE 10th International Symposium on Parallel and Distributed Processing with Applications, 10-13 July, 2012. IEEE, Leganes, 2012,
http://dx.doi.org/10.1109/ISPA.2012.125,

[4] Stepanic, J.; Mester, G. and Kasac, J.: *Synthetic Inertial Navigation Systems: Case Study of Determining Direction.*
Proceedings of the 57th ETRAN Conference, Society for Electronics, Telecommunications, Computers, Automatic Control and Nuclear Engineering. Zlatibor, pp.RO2.7.1-RO2.7.3, 2012,

[5] Albini, A. and Rajnai, Z.: *General Architecture of Cloud.*
Procedia Manufacturing **22**, 485-490, 2018,

[6] Chaxel, F.; Bajic, E. and Richard, J.: *Automotive vehicle data management based on holon-product paradigm*.
Systems, Man, and Cybernetics. IEEE SMC, Tokyo, 2002,
http://dx.doi.org/10.1109/ICSMC.1999.816591,

[7] Walch, M., et al.: *From Car-Driver-Handovers to Cooperative Interfaces: Visions for Driver-Vehicle Interaction in Automated Driving.*
In: Meixner, G. and Müller, C., eds.: *Automotive User Interfaces: Creating Interactive Experiences in the Car*. Springer International Publishing, 2017,

[8] Waschl, H.; Kolmanovsky, I.; Steinbuch, M. and del Re, L., eds.: *Optimization and Optimal Control in Automotive Systems.*
Springer International Publishing, 2014,
http://dx.doi.org/10.1007/978-3-319-05371-4,

[9] Sarker, A.; Qiu, C. and Shen, H.: *Quick and Autonomous Platoon Maintenance in Vehicle Dynamics for Distributed Vehicle Platoon Networks.*
2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI). IEEE, Pittsburgh, 2017,

[10] Oraibi, I.; Otero, C.E. and Olasupo, T.O.: *Empirical path loss model for vehicle-to-vehicle IoT device communication in fleet management.*
16th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net). IEEE, Budva, 2017,
http://dx.doi.org/10.1109/MedHocNet.2017.8001659,

[11] Chisalita, L. and Shahmehri, N.: *A peer-to-peer approach to vehicular communication for the support of traffic safety applications.*
The IEEE 5th International Conference on Intelligent Transportation Systems. IEEE, Singapore, 2003,
http://dx.doi.org/10.1109/ITSC.2002.1041239,

[12] Krodel, M. and Kuhnert, K.D.: *Towards a learning autonomous driver system.*
26th Annual Conference of the IEEE Industrial Electronics Society. IECON 2000. 2000 IEEE International Conference on Industrial Electronics, Control and Instrumentation. 21st Century Technologies. IEEE, Nagoya, 2002,
http://dx.doi.org/10.1109/IECON.2000.973125,

[13] Iantovics, L.B., et al.: *Review of Recent Trends in Measuring the Computing Systems Intelligence.*
Broad Research in Artificial Intelligence and Neuroscience **9**(2), 77-94, 2018,

[14] Iantovics, L.B.; Emmert-Streib, F. and Arik, S.: *MetrIntMeas a novel metric for measuring the intelligence of a swarm of cooperating agents.*
Cognitive Systems Research **45**, 17-29, 2017,
http://dx.doi.org/10.1016/j.cogsys.2017.04.006,

[15] Özkul, M. and Çapuni, I.: *An autonomous driving framework with self-configurable vehicle clusters.*
2014 International Conference on Connected Vehicles and Expo. IEEE, Vienna, 2015,
http://dx.doi.org/10.1109/ICCVE.2014.7297590,

[16] European Commission: *C-ITS Platform Phase 2.*
https://ec.europa.eu/transport/sites/transport/files/2017-09-c-its-platform-final-report.pdf, accessed 8th March 2018,

[17] European Commission: *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, conn.*
https://ec.europa.eu/energy/sites/ener/files/documents/1_en_act_part1_v5.pdf, accessed 8th March 2018,

[18] European Parlament: *Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport*.
Official Journal of the European Union, 1-13, 2010,

[19] Deloitte GmbH: *Automotive Software Quality What do OEM's have to consider for the future?*
https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Risk-Risk-Advisory-Automotive-Software-Quality-EN-s.pdf, accessed 8th March 2018,

[20] Schuster, G.; Tokody, D. and Mezei, I.J.: *Software Reliability of Complex Systems Focus for Intelligent Vehicles*.
In: Jármai, K. and Bolló, B., eds.: *Lecture Notes in Mechanical Engineering – Vehicle and Automotive Engineering*. Springer, Heidelberg & Miskolc, 2017,
http://dx.doi.org/10.1007/978-3-319-51189-4_28,

[21] Safety Forum: *Final Report and Recommendations of the Intelligent Infrastructure Working Group.*
http://www.apcap.pt/downloads/Intelligent_Infrastructure_Report_v1_0_20101012.pdf, accessed 8th March 2018,

[22] Abonyi, J. and Fülep, T.: *Safety critical systems*.
http://moodle.autolab.uni-pannon.hu/Mecha_tananyag/biztonsagkritikus_rendszerek/ch03.html, accessed 8th March 2018,

[23] Muha, L.: *System Theory for Information Security*.
Bolyai Szlemle **17**(4), 137-156, 2004,

[24] Ciso platform: *Understanding difference between Cyber Security and Information Security.*
http://www.cisoplatform.com/profiles/blogs/understanding-difference-between-cyber-security-information, accessed 8th March 2018,

[25] Ardila, J.P.C. and Gallina, B.: *Towards Efficiently Checking Compliance Against Automotive Security and Safety Standards.*
2017 IEEE International Symposium on Software Reliability Engineering Workshops. IEEE, Toulouse, 2017,
http://dx.doi.org/10.1109/ISSREW.2017.33,

[26] Schmittner, C.; Ma, Z.; Reyes, C.; Dillinger, O. and Puschner, P.: *Using SAE J3061 for automotive security requirement engineering*.
In: Skavhaug, A.; Guiochet, J.; Schoitsch, E. and Bitsch, F., eds.: *Computer Safety, Reliability, and Security*. Lecture Notes in Computer Science. Springer, Cham, 2016,
http://dx.doi.org/10.1007/978-3-319-45480-1_13,

[27] Tokody, D. and Schuster, G.: *Driving Forces Behind Smart City Implementations – The Next Smart Revolution*.
Journal of Emerging Research and Solutions in ICT **1**(2), 1-16, 2016,

[28] Mester, G. and Aleksandar, R.*: Sensor-Based Intelligent Mobile Robot Navigation in Unknown Environments.*
International Journal of Electrical and Computer Engineering Systems **1**(2), 1-8, 2010,

[29] Rodić, A.; Mester, G. and Stojković, I.: *Qualitative Evaluation of Flight Controller Performances for Autonomous Quadrotors.*
In: Pap, E., ed.: *Intelligent Systems: Models and Applications*. Topics in Intelligent Engineering and Informatics 3. Springer-Verlag, Berlin & Heidelberg, pp.115-134, 2013,

[30] Mester, G.: *Autonomous self-driving robot cars*.
https://www.researchgate.net/publication/324089063_Autonom_onvezeto_robot_autok, accessed 8th March 2018,

[31] Stepanić, J.; Sabol, G. and Žebec, M. S.: *Describing social systems using social free energy and social entropy.*
Kybernetes **34**(6), 857-868, 2005,

[32] Mester, G.: *Obstacle – Slope avoidance and velocity control of wheeled mobile robots using fuzzy reasoning*.
2009 International Conference on Intelligent Engineering Systems. IEEE, Barbados, 2009,
http://dx.doi.org/10.1109/INES.2009.4924770,

[33] Tokody, D.; Mezei, I. J. and Schuster, G.: *An overview of autonomous intelligent vehicle systems.*
In: Jármai, K. and Bolló, B., eds.: *Lecture Notes in Mechanical Engineering – Vehicle and Automotive Engineering*. Springer, Heidelberg & Miskolc, 2017,
http://dx.doi.org/10.1007/978-3-319-51189-4_27.

Interdisciplinary Description of Complex Systems 16(3-A), 397-407, 2018

CRITICAL OVERVIEW OF THE CLOUD-BASED INTERNET OF THINGS PILOT PLATFORMS FOR SMART CITIES

Janos Simon[1,] * and Gyula Mester[2]

[1]University of Szeged, Faculty of Engineering
Szeged, Hungary

[2]Óbuda University, Doctoral School of Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.16.3.12
Regular article

Received: 9th March 2018.
Accepted: 31st August 2018.

ABSTRACT

The Internet of Things (IoT) has started to appear everywhere in many shapes and forms. But security is one of the crucial topics that could trip up the growth of the IoT. Following security principles used in enterprise computing can help clear that issue. Already there are more connected devices than people on the planet, according to leading researchers in this area. By 2020, there will be 50 billion connected devices, outnumbering people by more than 6 to 1. Most of these devices will be controllable over the Internet, and they will increasingly be responsible for collecting and transmitting sensitive data. Today consumers might own an app that collects information on their exercise routine. In a few years, those same people might have an Internet-enabled medical device that continually delivers data to their doctor. In the wrong hands, data from home management systems could be used to assess user's whereabouts. Likewise, businesses could be vulnerable when they connect things like HVAC, irrigation, or commercial appliances.

KEY WORDS

IoT, smart cities, smart grid, cloud platform

CLASSIFICATION

ACM: D.1.1.
JEL: L64

*Corresponding author, η: simon@mk.u-szeged.hu; +36 62 546-509;
6724 Szeged, Moszkvai krt. 9., Hungary

INTRODUCTION

The introduction of steam engines, industrialization and computers have arrived in West Balkan with a delay, as an echo of the major changes in the world. The previous three industrial revolutions have established their winners – Great Britain, the United States, and Japan – countries that have dominated the world economy in the decades since the changes occurred. Serbia, burdened with its history, geopolitical context, loss of population, low level of education, finances, was not among those winners. The fourth industrial revolution, or digitization, as it is often called, refers to the application of various technologies that enable the fusion of the real and digital world [1, 2].

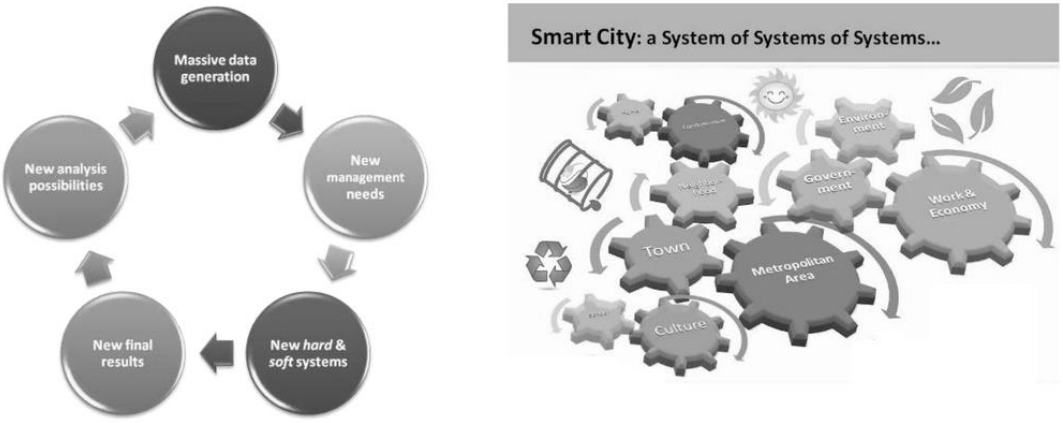

Figure 1. Smart city approach.

Digitization is not only reflected in programming, using an online form, instead of going to the counter or by connecting different databases. IT, artificial intelligence, robotics, Internet stuff, 3D printing, nanotechnology are just some of today's mature technologies that have the potential to change the world from which we live [3]. One of the sectors of great significance for West Balkan, traditionally perceived as a branch with a low potential for digitization, is agriculture. However, digitization can bring enormous positive changes in that area. Worldwide, agriculture faces a huge challenge: in order to feed humanity, 2050 will have to produce almost two times more food than it is today. Unused agricultural land is almost no longer available, and existing agro-technical measures cannot provide the necessary growth. West Balkan is facing economic non-sustainability of agricultural production, which particularly affects small producers. Digitization is the only solution today enough to respond to these challenges. It is only the first step in the exciting life of a single data and a basic prerequisite for new technologies as great data to provide their real contribution [4]. Different sensors that produce data placed on plants and animals, into land, to droplets, robots or satellites, allow us to see complex processes in agriculture. For example, to understand why even the best producers in West Balkan today in some parts of their plots have a yield difference of several times, even though they apply all agro-technical measures - and that we change it. Or to recommend what sort of sowing on which plot so that without any additional cash investments simultaneously increase the yield and reduce the risk to farmers. Or that we do not provide up to date data to support the banking and insurance sectors so that their products become available to farmers. Serbian Institute BioSens is recognized today as one of the leading scientific institutions in the world dealing with agriculture 4.0. The digital agriculture of West Balkan has already come to life through the AgroSens platform, which in just a couple of months of existence has gathered over 5 000 users who can access various

data related to their production plot without any compensation and with the help of satellite images to monitor progress and identify problems, even via mobile phones . However, the digitization of agriculture, or any other economic branch, is not a task that can be solved by only one institution [5, 6]. The domestic IT sector is solid and has already proved ready to contribute to this process. The transition from, today, the prevailing, outsourcing model of IT companies to the development of their own products can ensure that significant added value remains in West Balkan [7].

SMART CITIES

Today 3,5 billion people live in cities, which makes up about 50 % of the world's population. Estimates are that by 2040 there will be an additional 2-2,5 billion people living in cities, which will make up about 70 % of the world's population. This implies further pressure on land, water, air, raw materials and increases demands for food, water and energy, for education and medical care, employment and care for older people and people with disabilities [8, 9]. Those who live in cities use 75 % of non-renewable natural resources and participate in the production of three-quarters of the world's pollution. As a possible solution we mention the so-called *smart city*. There are more definitions to the *smart city*. One could be: A city that, through information and communication technology (ICT), unifies and coordinates the work of all city services in order to improve their work and better connectivity between city and citizens administration.

A somewhat shorter definition of the *smart city* is that it is a city that effectively integrates physical, digital and human systems in order to build an environment that will contribute to improving the lives of citizens [10, 11]. The third definition of *smart city* is that it is a city that uses ICT technology and, with the application of technological innovations, contributes to more efficient and rational use of resources, which means energy savings and reduction of negative environmental impacts.

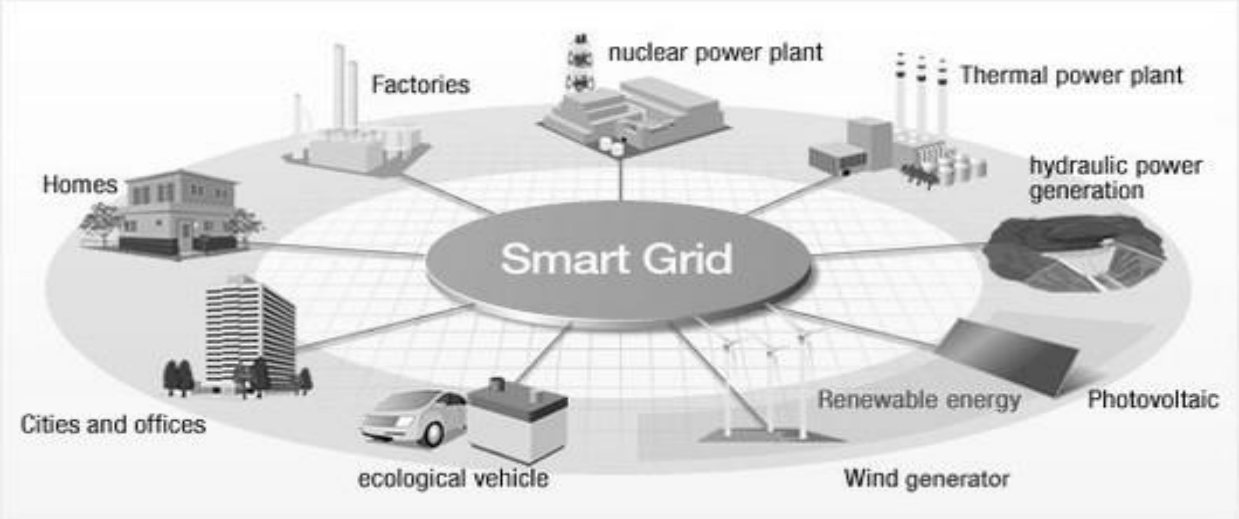

Figure 2. Smart grid.

SMART HOUSE

In the formation of the *smart city*, *smart house* is of great importance. The most important measure in this direction is rational energy consumption. It is implemented through the introduction of renewable energy sources (RES) and better thermal insulation of buildings. With the emergence of new building materials, the cost of building insulation has dropped significantly and the heat energy savings go up to 30 %. The introduction of RES is realized

by placing solar thermal collectors for obtaining hot water and installing solar photovoltaic collectors for electricity generation. Another form of savings is a heat pump with a dual function – cooling and heating [12, 13]. Where the building is exposed to stronger airflow, in combination with the above measures, energy efficiency can be achieved within the limits of 80-100 %. Special attention is focused on waste management. The goal is to reduce the amount of waste. One of the measures is: do not discard appliances and appliances before their service life expires. Already at the level of the *smart house*, the waste is sorted into bags. The obligation of the household is to place those bags in containers or to deliver them to collection centers in the city. City offices collect that waste from the container and relate it to further processing, i.e. they are recycled, burned or used for the production of biogas. *Smart House* also includes installations for remote and automatic control, which ensures the security and fire protection of the building.

HOW THE CITY BECOMES *SMART*

It is expected that *smart cities* will become very attractive for high-skilled labor and thus will be incentives for numerous activities [14]. The factors that determine the *friendly urban environment* include: urban planning, development, energy, cleanliness, supply, communications and traffic, health care, education, cultural activities. Urban planning includes the consideration of the city's development flows in the next 10-15 years. Energy consumption involves the use of natural resources (application of RES, sun, wind, geothermal energy and bio-gas). Electricity heating should be replaced by steam heating, and in the future, introduce remote cooling as an alternative to individual air conditioners. The benefit is double: aesthetic and higher energy savings [15, 16]. Ecology of *smart city* means expanding and creating new green areas and setting up solar collectors in places where it is possible. Also, wastewater treatment with the possibility of returning to watercourses, from where they would be used for irrigation.

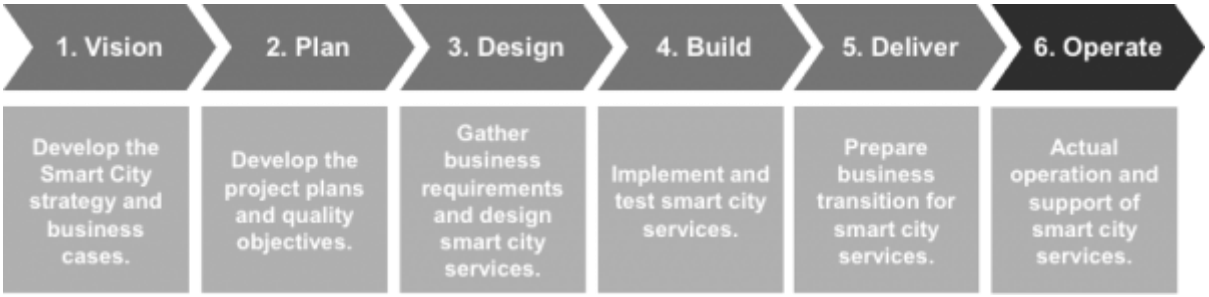

Figure 3. How the city becomes *smart*.

Waste is increasingly becoming a raw material and, in parallel, an increasing problem of large cities with dumps spreading to all sides. The goal is to reduce the amount of waste in cities as much as possible and to process as much as possible. Waste remediation measures are known, but investments are needed for the construction of waste recycling plants, combustion and conversion of waste into gas for electricity generation. By processing in recycling, combustion and biogas plants, the need for landfills is significantly reduced. PVC, LDPE, PP, PS, electronic waste, etc. are recycled [17]. For example, when bottles are being recycled, the benefit is double: it is 60 % less energy consumption than that required for the production of new bottles and less waste. Otherwise, waste management involves a program of measures that begins with the classification of household waste and ends up in the form of a new product or fuel for power plants. In the *smart city* there must be good night lighting of streets and squares. Then, clean and straight hiking trails with a width of at least 2 m without parked vehicles, clean and flat pavements free of animal and other waste, central computer system with control of traffic lights at pedestrian crossings and intersections.

SMART CITIES IN THE WORLD

There are ten cities on the list of *smart cities*, while there are five more for *waiting*. In the first place is Vienna and then followed by: Toronto, Paris, New York, London, Tokyo, Berlin, Copenhagen, Hong Kong and Barcelona. The list includes Amsterdam, Stockholm, Melbourne, Vancouver, Santa Cruz and Singapore [18]. By all criteria, Vienna is in the first place: all wastewater is brought to the main purification plant where it is purified to 95 %. They purified the treated water in the Danube. Water consumption in Vienna is quite high and amounts to 130 l per person per month. The renovated drainage channel and the construction of the embankment Vienna is well protected from floods.

INSTITUTION FOR STUDYING *SMART CITIES*

More than half of the urban areas are under greenery. An artificial island of 21 km long was built, which is used for rest and recreation [19]. The share of public transport is 35 %, the share of cyclists and pedestrians is 31 % and private vehicles 34 %. There is a tendency of further reduction in private transport to 25 % and an increase in public transport from the current 35 % to 40 % by 2020. Vienna has 29 tram and 150 bus routes. About 1000 km of cycling tracks were built. For the next decade, the possibility of remote cooling is considered. The effect of remote cooling is an energy saving of up to 80 % in relation to the already installed individual air conditioners. Some hospitals and business facilities have already been connected to a network of extreme cooling [20]0. The *Virtual City Office* works continuously and helps citizens to carry out numerous administrative tasks. Facilities for sorting, recycling of plastic waste and combustion in order to obtain electricity and biogas from organic waste were built (about 220 000 tonns annualy). The so-produced biogas is connected to the city gas network. Street lighting in Vienna involves about 150 000 pillars with over 227 000 luminaries, predominantly *ice* technology that saves electricity. The prescribed width of the sidewalk is 1,5-2 m. The cleanliness of the city is maintained by numerous cleaning teams, bunkers are placed for street waste disposal and prescribe high penalties for non-compliance with animal waste. On the other side of the world, in Toronto, they use gas as fuel for garbage trucks. In Paris, they are developing a bicycle rental program for 250 stations. A similar program is being prepared for smaller electric cars. In New York, they develop fire prevention systems. In London, the formation of the group is in the Imperial College for the study of *smart cities*. Databases related to transport and job management will be set up at the same site. In Tokyo, the buildings will be built that will combine the operation of solar panels, energy storage batteries and energy efficient appliances.

The city government of Copenhagen should reduce CO_2 emissions to zero by 2025. About 40 % of local people use bicycles as a means of transport. Hong Kong is the leader in the use of smart cards, which millions of citizens cover the cost of public transportation, shopping and car parking. Barcelona was the first to introduce solar thermal collectors for hot sanitary water, and now it is working on a project for the introduction of electric vehicles and the construction of filling stations for electric vehicles [21]. In Stockholm, it seeks to reduce the amount of greenhouse effect gases by lowering energy consumption for heating apartments enhanced by isolation of apartments, urban traffic control and the development of electronic communications in order to reduce the use of paper. A number of apartments have installed *smart meters* with the aim of reducing energy consumption. Control of city street lighting and traffic lights is under way in order to provide drivers with information on congestion in certain directions of movement. And in Santa Cruz, California, they introduced measures to reduce crime by, on the basis of historical data, sent police patrols in certain places in a high-risk city.

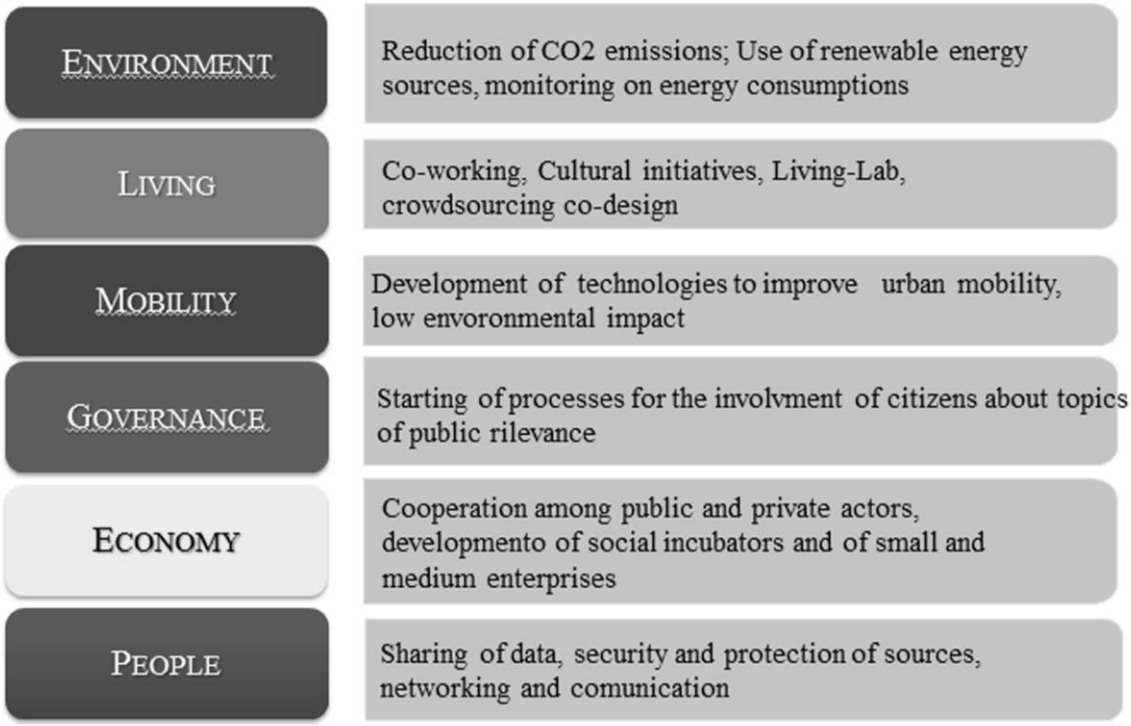

Figure 4. Smart city definition (EU).

THE DEVELOPMENT OF A SMART CITY

The development of a smart city is often associated with the realization of the following elements: smart economy, smart population, smart management, smart traffic, smart environment and smart life [22]. Some examples of the implementation of IoT applications in smart cities include: system control of traffic, smart vehicle parking solutions, air pollution level detection, download of information related to smog and carbon dioxide levels, etc. Areas of application of intelligent solutions in smart cities can be categorized into multiple domains:

- administration,
- health,
- smart buildings,
- education,
- public safety,
- traffic,
- participation programs,
- energy,
- environment.

Observed from the aspect of communication, management and data processing, the multi-layered IoT architecture of smart cities consists of:

- measurement and Reading Layer (Sensing),
- network layer for access to IoT infrastructure (Network-Centric IoT),
- cloud-Oriented Component of IoT Infrastructure (Cloud-Centric IoT) and
- application layer of IoT infrastructure (Data-Centric IoT).

The development of IoT infrastructure in smart cities includes: development platforms, accessing technologies, data warehouses, data analytics services and data security services. There are a number of platforms that are used to build IoT solutions. Among the most famous

cloud platforms are: IBM Bluemix, Microsoft Azure, Amazon Web services, HP Helion, Oracle Cloud and others. The trend of increasing population in cities is causing many problems in the social and organizational sphere, which greatly burdens the management of city structures, leads to a lack of resources, makes traffic difficult, threatens the environment and causes health problems for the population. IoT solutions can contribute to their resolution [23]. The basic idea of implementing the IoT is to provide a smart infrastructure for areas such as traffic, electricity, water supply, housing construction and public services [24, 25].

PLATFORMS FOR THE DEVELOPMENT OF THE *SMART CITY* ELEMENTS

The IoT platform is a software and hardware environment for the efficient development of the IoT system. The management of the IoT platform is complex and includes processes such as: Resource Discovery, Resource Monitoring, Platform Reconfiguration [26, 27]. On the server side, the components that are responsible for providing the platform management functionality are: Resource Directory, IoT Resources Manager, Application Configuration Configuration Configuration Manager, Configuration Testing Sub-System Configuration, Crowdsourcing Manager. IoT nodes differ in roles in the platform, so there are the following types: Infrastructure nodes, Experimental IoT nodes, Service nodes, Participating nodes are handheld devices.

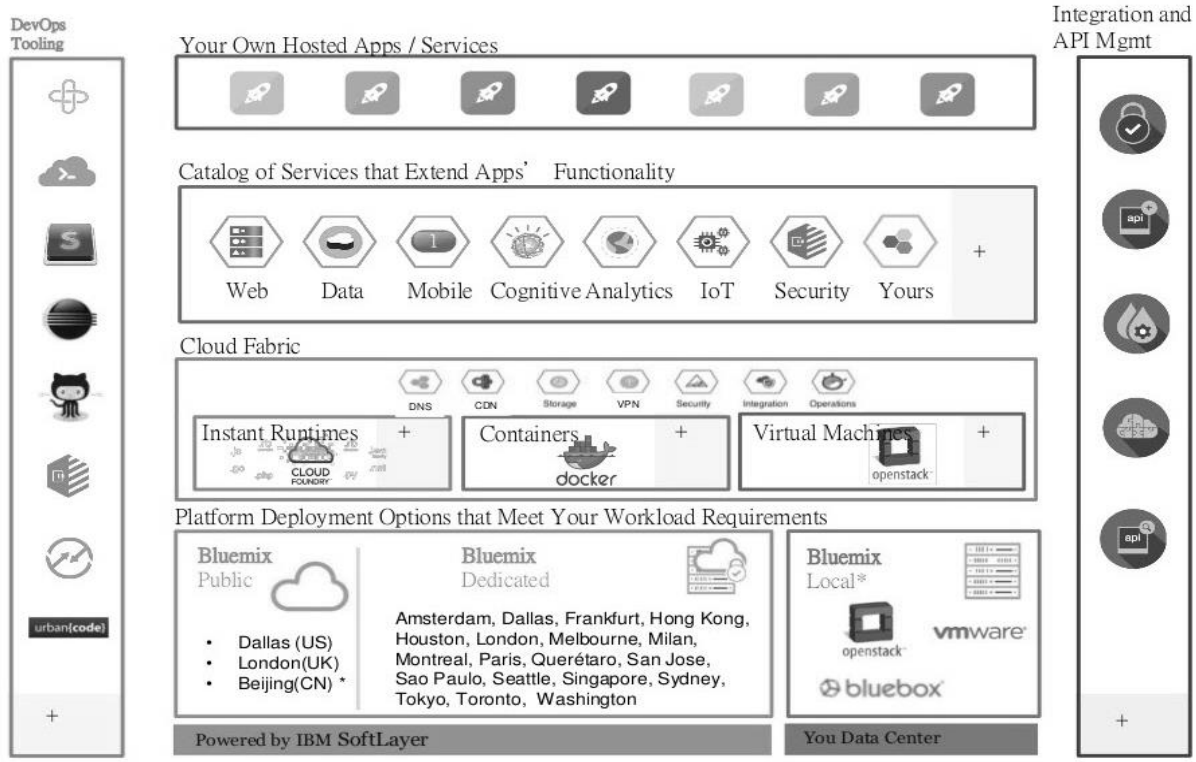

Figure 5. IBM Cloud Bluemix – Innovation platform.

When developing the *smart city* Platform, it is necessary to consider the necessary functional elements, such as:

- devices that have functions of collecting data and executing pre-defined actions and monitoring and control,
- communication components that allow connection of devices within IoT platform,
- services within the IoT platform that should enable device monitoring, device management, reporting of collected data, and discovery of devices online,

- manage the functions of the IoT platform, such as configuring, monitoring platform performance, and more,
- a security component that relates to the realization of functionality, authentication, authorization, integrity protection and data privacy,
- the application component that refers to providing the capabilities of users can monitor and use the functions of the IoT platform and manage them.

The components for the development of the Internet platform of intelligent devices are:

1.) hardware

- sensors (eg. for measuring temperature, humidity, pressure),
- actuators (eg. for lighting control, air conditioning),
- microcomputers (eg. Raspberry Pi),
- microcontrollers (eg. Arduino) and
- network infrastructure (routers, switches, cables, etc.).

2.) software

- development environments (eg. Eclipse, Arduino IDE, etc.),
- operating systems customized for devices (eg. Raspbian) and
- software for a specific smart environment.

Intelligent devices can be connected to Personal Area Network, PAN, Local Area Network, LAN, Metropolitan Area Network, WAN (Wide Area Network), and sensor networks [28-30]. Mobile technologies that have contributed to the development and application of the Internet of intelligent devices are mobile and mobile Internet, Bluetooth, RFID, WiMAX, Global Positioning System (GPS), Near Field Communication (NFC), ZigBee and others. Cloud computing and Vig data infrastructure can be used to build a quality IoT infrastructure. Cloud computing is a paradigm of delivering computer resources as a service. IoT services can also be delivered via clouds [31-33]. Regarding the integration of IoT with cloud, the following requirements must be met:

- cloud services should facilitate the communication of hardware and software in the IoT ecosystem,
- cloud protocol support is needed, such as Websocket, REST, MQTT, CoAP,
- support is needed for secure remote software updates on devices,
- web and mobile applications should allow data display, data processing, and remote device management,
- areas of application of the Internet of intelligent devices.

Internet intelligent devices can be applied to:

- personal and business purposes – automation of houses, buildings, apartments and offices,
- urban environment – automation of cities and its head parts such as roads, parking lots, lighting, surveillance systems and emergency response systems,
- education – automation of faculties, classrooms and libraries,
- healthcare – automation of hospitals, health centers, monitoring of patients and athletes, use of wearable devices,
- logistics – automation of transport, monitoring of delivery of goods and remote diagnostics of the condition of transport vehicles,
- industries – automation of factories, warehouses and warehouses, monitoring of machines and tools,
- environment – monitoring of weather conditions, pollution of air, noise, fire and floods,
- energy systems – smart electricity networks and renewable energy systems,

- retail – automation of inventory management and smart payments,
- farms – automation of irrigation systems and control of greenhouses,
- robotics – smart robots.

CONCLUSION

The concept of smart, sustainable cities is based on a simple paradigm of sustainable development, which presupposes an informatically bound metropolis that collects, analyzes, shares and displays information in a way that suits their consumer – a citizen, a member of a city administration, a policeman, a fireman, a healthcare worker or a teacher in one of the city gymnasiums. Directly on the story of the use of energy and water, the section on responsible attitude towards the environment is added. Whatever business is dealing with today, the basic maxim that ensures its future is sustainability. By 2025, the buildings will use more energy than any other class of consumers. In the United States, the share of buildings in the use of energy is high 72 %, while 40 % of the raw materials that are produced eventually end up in buildings. In the process of environmental protection, energy management, waste management and reduction of emissions of harmful gases are the core activities. A significant increase in care in these areas has been recognized in Europe and the USA. IBM is talking about an increase of more than 50 % when it comes to investing in reducing emissions, while waste and energy management is *progressing* every year with an advantage of more than 60 % compared to the previous one. Both Intel and IBM suggest that sustainability begins in the family. The ways in which individuals flow to water, electricity, and other limited resources greatly affect the social context that shapes our lives. It is precisely in this module that the importance of education is greatest, because it guarantees the availability of critical information on the importance of preserving energy resources from the earliest days of development.

REFERENCES

[1] Rodić, A.; Mester, G. and Stojković, I.: *Qualitative Evaluation of Flight Controller Performances for Autonomous Quadrotors*.
In: Pap, E., ed.: *Intelligent Systems: Models and Applications*. Topics in Intelligent Engineering and Informatics 3. Springer-Verlag, Berlin & Heidelberg, pp.115-134, 2013,
http://dx.doi.org/10.1007/978-3-642-33959-2_7,

[2] IBM: *IBM Cloud.*
http://www.ibm.com/bluemix, accessed 8th March 2018,

[3] Khan, R.; Khan, S.U.; Zaheer, R. and Khan, S.: *Future internet: the internet of things architecture, possible applications and key challenges*.
In: Rashid, H., et al., eds.: *Proceedings 10th International Conference on Frontiers of Information Technology*. IEEE, Islamabad, pp.257-260, 2013,
http://dx.doi.org/10.1109/FIT.2012.53,

[4] Erdem, A.S. and Göçen, E.: *Development of a decision support system for supplier evaluation and order allocation.*
Expert Systems and Applications **39**(5), 4927-4937, 2012,
http://dx.doi.org/10.1016/j.eswa.2011.10.024,

[5] Habibi, R.: *Perencanaan sistem smart academic dengan smart classroom dan teknologi internet of things pada stmik bina patria.*
Jurnal Transformasi **13**(1), 38-46, 2017,

[6] Gogou, E., et al.: *Cold chain database development and application as a tool for the cold chain management and food quality evaluation.*
International Journal of Refrigeration **52**,109-121, 2015,
http://dx.doi.org/10.1016/j.ijrefrig.2015.01.019,

[7] Mehta, V.: *A Novel Approach to Realize Internet of Intelligent Things*.
In: Aggarwal, V.B.; Bhatnagar, V.; Mishra, D.K., eds.: *Big Data Analytics*. Springer, Singapore, 2018,

[8] Khari, M., et al.: *Internet of Things: Proposed security aspects for digitizing the world*
3rd International Conference on Computing for Sustainable Global Development. IEEE, New Delhi, 2016,

[9] Terdik, Gy. and Gál, Z.: *Advances and practice in Internet of Things.*
In: Baranyi, P., et al., eds.: *Proceedings of the IEEE 4th International Conference on Cognitive Infocommunications*. IEEE, Budapest, pp.435 440, 2013,
http://dx.doi.org/10.1109/CogInfoCom.2013.6719286,

[10] Mester, G. and Aleksandar, R.*: Sensor-Based Intelligent Mobile Robot Navigation in Unknown Environments.*
International Journal of Electrical and Computer Engineering Systems **1**(2), 1-8, 2010,

[11] Mester, G.; Pletl, Sz.; Pajor, G. and Jeges, Z.: *Flexible Planetary Gear Drives in Robotics.* International Conference on Industrial Electronics, Control, Instrumentation and Automation. IEEE, San Diego, 1990,
http://dx.doi.org/10.1109/IECON.1992.254556,

[12] Hu, S.J.: *Evolving Paradigms of Manufacturing: From Mass Production to Mass Customization and Personalization.*
Procedia CIRP **7**, 3-8, 2013,
http://dx.doi.org/10.1016/j.procir.2013.05.002,

[13] Faruque, M.A.M. and Vatanparvar, K.: *Energy management-as-a-service over fog computing platform.*
IEEE Internet of Things **3**(2), 161-169, 2016,
http://dx.doi.org/10.1109/JIOT.2015.2471260,

[14] Alvarado, U., et al.: *Energy harvesting technologies for low-power electronics.*
Transactions on Emerging Telecommunications Technologies **23**(8), 728-741, 2012,
http://dx.doi.org/10.1002/ett.2529,

[15] Martinović, G. and Simon, J.: *Greenhouse Microclimatic Environment Controlled by a Mobile Measuring Station.*
NJAS – Wageningen Journal of Life Sciences **70-71**, 61-70, 2014,
http://dx.doi.org/10.1016/j.njas.2014.05.007,

[16] Matthews, J.; McIntosh, R. and Mullineux, G.: *Contrasting Opportunities for Mass Customization in Food Manufacture and Food Process.*
In: Fogliatto, F.S. and da Silveira, G.J.C., eds.: *Mass customization: Engineering and managing global operations*. Springer, London, pp.353-374, 2011,

[17] Nukala, R., et al.: *An IoT based approach towards Global Food Safety and Security.*
The 14th IT&T Conference. National College of Ireland, Dublin, 2015,

[18] Chirila, S.; Lemnaru, C. and Dinsoreanu, M.: *Semantic-based IoT device discovery and recommendation mechanism.*
In: Potolea, R., et al., eds.: 2016 IEEE 12th International Conference on Intelligent Computer Communication and Processing. IEEE, pp.111-116. 2016,
http://dx.doi.org/10.1109/ICCP.2016.7737131,

[19] Simon, J.: *Multicriteria fuzzy control system for microclimatic environment based on autonomous mobile measuring station.* PhD Thesis.
Faculty of Electrical Engineering on J.J. Strossmayer University in Osijek, Osijek, 2014,

[20] Soukoulis, C., et al.: *Industrial yogurt manufacture: monitoring of fermentation process and improvement of final product quality.*
Journal of Dairy Science **90**(6), 2641-2654, 2007,
http://dx.doi.org/10.3168/jds.2006-802,

[21] Xiaorong, Z., et al.: *The design of the internet of things solution for food supply chain.*
5th International Conference on Education, Management, Information and Medicine. Shenyang. China, 2015,
http://dx.doi.org/10.2991/emim-15.2015.61,

[22] Bruneo, D., et al.: *Stack4Things as a fog computing platform for Smart City applications.* IEEE Conference on Computer Communications Workshops. IEEE, San Francisco, 2016, http://dx.doi.org/10.1109/INFCOMW.2016.7562195,

[23] Zidek, K., et al.: *Embedded vision equipment of industrial robot for inline detection of product errors by clustering-classification algorithms.* International Journal of Advanced Robotic Systems **13**(5), 1-10, 2016, http://dx.doi.org/10.1177/1729881416664901,

[24] Simon, J.; Covic, Z. and Petkovic, I.: *Industrie 4.0 Based Customized Mass Production Overview*. Conference MECHEDU, 2017, Subotica Tech – College of Applied Sciences, Subotica, 2017,

[25] Simon, J.: *Industrial Data Acquisition Applications Using Relational Databases, IoT Environment and Multi Criteria Decision Making Systems.* International Journal of Current Research in Engineering, Science and Technology **1**(1), 11-18, 2016,

[26] Simon, J.; Trojanova, M.; Zbihlej, J. and Sarosi, J.: *Mass Customization Model in Food Industry Using Industry 4.0 Standard with Fuzzy Based Multi-criteria Decision Making Methodology*. Advances in Mechanical Engineering **10**(3), 1-18, 2018, http://dx.doi.org/10.1177/1687814018766776,

[27] Petkovics, I.; Simon, J.; Petkovics, Á. and Čović, Z.: *Selection of Unmanned Aerial Vehicle for Precision Agriculture with Multi-criteria Decision Making Algorithm*. IEEE 15th International Symposium on Intelligent Systems and Informatics. IEEE, Subotica, 2017,

[28] Simon, J.; Čović, Z. and Dobrilović, D.: *The Web of Things and Database Management Systems.* Analecta Technica Szegedinensia **10**(2), 61-68, 2016, http://dx.doi.org/10.14232/analecta.2016.2.61-68,

[29] Simon, J., et al.: *The Web of Things and Database Services.* International Conference on Applied Internet and Information Technologies. AIIT, Zrenjanin, 2015,

[30] Simon, J. and Covic, Z.: *Data Management of the Automomous Mobile Devices and Internet of Things*. International Journal of Engineering **13**(3), 265-268, 2015,

[31] Simon, J.: *Concepts of the Internet of Things from the Aspect of the Autonomous Mobile Robots*. Interdisciplinary Description of Complex Systems **13**(1), 34-40, 2015, http://dx.doi.org/10.7906/indecs.13.1.5.

[32] Sárosi, J.: *Measurement and Data Acquisition*. University of Szeged, Faculty of Engineering, Szeged, 2014,

[33] Nyikes, Z. and Rajnai, Z.: *The Big Data and the relationship of the Hungarian National Digital Infrastructure.* International Conference on Applied Internet and Information Technologies, 2015. AIIT, Zrenjanin, 2015.

Interdisciplinary Description of Complex Systems 16(3-A), 408-416, 2018

NETWORKING TECHNOLOGIES FOR SMART CITIES: AN OVERVIEW

Dalibor Dobrilović*

University of Novi Sad, Technical Faculty “Mihajlo Pupin"
Zrenjanin, Serbia

DOI: 10.7906/indecs.16.3.13
Regular article

Received: 15th April 2018.
Accepted: 31st August 2018.

ABSTRACT

Considering the complex architecture of Smart City environments it should not be forgotten that their foundation lies in communication technologies that allow connectivity and data transfer between the elements in Smart City environments. Wireless communications with their capabilities represent Smart City enabling technologies that gives the opportunity for their rapid and efficient implementation and expansion as well. In that field the evident trend is appearance of numerous technologies, which can be applied in variety of scenarios. In order to be able to make rapid deployment of the Smart City systems it is necessary to perform good analyses of performances and applicability of those technologies. By knowing the characteristics of particular technologies, the professionals will have the opportunity to develop efficient, cost effective and flexible Smart City systems by implementing the most suitable one. In this article the review and discussion on wireless technologies for enabling Smart City services is presented.

KEY WORDS

smart city services, wireless communications, wireless technologies

CLASSIFICATION

ACM: Networks, Cyber-physical networks, Sensor networks
JEL: O18, R58

*Corresponding author, η: dalibor.dobrilovic@uns.ac.rs; +381 62 801 97 60;
Djure Djakovica bb, 23 000 Zrenjanin, Serbia

INTRODUCTION

The rapid development and deployment of Smart City environments impose challenging tasks to the engineers, developers and researches working in that field. Communication technology play important role in those systems because it allows connectivity and data transfer between the elements in Smart City environments. The advantages of wireless communications are obvious, because the Smart City systems are employed on wider, preferably urban areas, and can face demand for rapid expansion and reconfiguration. The usage of wireless technology is further justified with the extensive use of movable sensor nodes, nodes deployed on various places where it is difficult to install wired infrastructure, and above all, notable decrease in sensor and communication module prices and power consumption. In order to prepare ourselves for effective and rapid deployment of the efficient Smart City systems it is necessary to perform good analyses of performances and applicability of those technologies.

In this article the review and discussion on wireless technologies for enabling Smart Cities is presented. The article is structured as follows: after the introduction, definition of Smart Cities and related trends is given. It is followed by the classification of various well-established and emerging wireless technologies targeting Smart City environments. The discussion of their applicability in accordance with their features and characteristics and author experience is presented in next section. Finally, the conclusion based on analyses and authors experience is presented at the end of the article.

SMART CITIES

In the beginning of these analyses it is important to explain definition of Smart City. Having in mind that this is complex term which demands extensive explanation, for the purpose of this article it will be simplified. A Smart City can be defined as environment that uses currently available technologies to improve living conditions by offering access to information about parameters that enhance lives of its inhabitants. These parameters can range from status of their education and employment possibilities, available utilities for citizens, transportation information, energy consumption information, health-related issues, water and air quality monitoring, waste management and other relevant information that potentially could benefit the community [1].

The term *Smart City* can be considered as the new urban environment, designed for performance through information and communication technologies (ICTs) and other forms of physical capital. Visionaries and planners hope that Smart Cities with the effective management of resources through intelligent management will lead to a higher quality of life for citizens and can improve economic and environmental conditions [1].

Smart Cities should heavily rely on ICT. So it is important to define the main ICT trends who will take the role of enablers of Smart Cities. Those two emerging trends are Machine-to-machine (M2M) and Internet of Things (IoT). Simply said, M2M communication should not be confused with IoT despite their similarity. M2M is used to connect sensors and other devices to ICT systems through wired or wireless networks. On the contrary, IoT represents paradigm including a set of technologies, systems, and design principles associated with the Internet-connected things and larger Internet network. The vision of IoT is to reach a structure similar to today's Internet, where connections merge things and real world, while the M2M technologies should act as an enabler for that. In that sense, IoT represents an extension to the existing Internet, with an automatic data collection, control, and supervision of physical infrastructure, through a remote monitoring [2].

SMART CITY ENABLING COMMUNICATION TECHNOLOGIES

The rapid development of the wireless technologies is heavily inspired by novel services planned for Smart City environments. E.g., some technologies like IEEE 802.11 (Wi-Fi), in contrast to its high popularity, are not suitable for the IoT and for the Smart Cities as well. The reason is that Wi-Fi is originally designed to offer end users high speed Internet or LAN access from limited number of stations in short distances and indoor environments. The purpose of Wi-Fi technology is to enable high speed access to multimedia data and services. In order to expand the usage of IEEE 802.11 networks to IoT, IEEE 802.11ah Task Group (TGah) is formed with a goal to design energy efficient protocol [3].

In order to realize what wireless technologies are applicable in Smart Cities and to determine their efficient appliance in particular services, the classification of the technologies should be made. Smart City wireless technologies can be categorized, according traditional classification based on range, into three classes: Wireless Personal Area Networks (WPAN), Wireless Local Area Networks (WLAN), and Wireless Metropolitan Area Networks (WMAN) [4]. The classification nowadays can be expanded with new terms such as Home Area Networks (HAN), Neighborhood Area Networks (NAN) [5], Field Area Networks (FAN) and Body Area Networks (BAN). The classification of Smart City communication technologies can also be made according to [6] where there are three groups: (i) *Cellular Mobile Networks*, (ii) *IoT-Dedicated Cellular Networks*, (iii) *Multi-Tier Networks*.

Cellular Mobile Networks are planned for new communication paradigm with little or no human interaction, e.g. for Machine-To-Machine (M2M) or Machine-Type communications (MTCs). Those networks should be implemented in Smart City applications designed for high coverage and flexibility of supported data rate. *IoT-dedicated cellular networks* are intended to answer the need for design of low-cost, low-energy M2M applications with limited traffic requirements. Those technologies have advantage comparing to cellular operators, lower costs of network equipment and network devices and include technologies such as: SigFox, LoRaWAN, Weightless, Ingenu, etc. *Multi-tier Architectures* cover variety of solutions like following: IEEE 802.15.4. ZigBee, WI-SUN (802.15.4g), ULP (802.15.4q), Wireless M-Bus, Z-Wave, Bluetooth Low Energy (BLE), WiFi Low Power (802.11ah), etc. These technologies are targeted to applications with limited number of nodes and low communication range, allowing flexible setups and easy customization.

The comparison of main characteristics of technologies is given in Table 1. In the table, related standards and governing bodies, operating frequencies, data rates, range and typical topologies are given for each technology. The technology characteristics are extracted and compiled from following sources [2, 4-12].

The model of usage of presented wireless technologies in Smart City environment is shown in Fig. 1 where technologies and possible areas of application are given according to [4, 13].

DISCUSSION ON TECHNOLOGY APPLICABILITY

In general, application for smart cities can be classified in the following groups: Smart Health, Smart office, home and residential buildings, Smart Energy (including Smart Grid and Smart Lightning), Smart Environment (Water Management, Smart Waste, Weather, Noise and Air pollution monitoring), Smart Physical safety /security, Smart Education, Smart Administration, Smart Industries and Smart Transportation (Traffic monitoring, Smart traffic lights, Smart Parking) [2, 4, 6, 13-17]. All these applications have different requirements. Two important features of the technologies related to requirements are listed in Table 1 and those features are range and data rates. Those two features have major impact on the possibility of

Table 1. Comparison of Smart City technologies (continued on p.412).

Communi-cation Technology	Standard/ governing bodies	Frequency	Range (app.)	Data rates	Topology
NFC	ISO/IEC – ISO 13157 etc.	(HF) 13,56 MHz	10 cm	106, 212, 424 Kbps	Point-to-point
RFID	ISO/IEC - ISO/IEC 18000	(LF) 125 -134 kHz (HF)13.56 MHz (UHF) 856 - 960 MHz	3-10 m (active up to 100 m)	40 Kbps-640 K	Point-to-point
Bluetooth/ Bluetooth Low Energy (BLE)	IEEE 802.15.1/ Bluetooth SIG	2.4 GHz	10 m typical 30-50m (BLE)	1-3 Mbps 1 Mbps (BLE)	Point-to-point, Piconet, Scatternet, Star-bus (BLE)
Z-Wave	Z-Wave Alliance	900 MHz	30 m (ind.) 100 m	9,6-100 kbps	Star, cluster, mesh
ZigBee	ZigBee Alliance	2,4 GHz	10-100 m	250 kb/s	Mesh
WiFi	IEEE 802.11 (a/b/g/n)	2,4/3,6/4,9/5/5,9 GHz	100 m	1-54Mbps	Star
ULP (802.15.4q)	IEEE Std 802.15.4q	868/915/2450 MHz	100 m	100 kbps	Star
WI-SUN 1606 (802.15.4g)	Wi-SUN Alliance	sub-1 GHz, 2,4 GHz	200 m	1 Mpbs	Star, Mesh, Peer-to-peer
6LoWPAN	Internet Engineering Task Force (IETF) IETF RFC4944	868MHz/ 915MHz/ 2,4GHz	200 m	250 kbps (2,4GHz) 40 kbps (915MHz) 20 kbps (868MHz)	Node-to-node, Star, Tree, Mesh
Wireless M-BUS	EN 13757-4	169/433/868 MHz	300 m	2,4 kbps-100 kbps	Star
WiFi Low Power (802.11ah)	IEEE 802.11 working group	Sub-1 GHz	1 km	150kbps ~ 346,666Mbps	Star, Tree
Weightless-W	Weightless Special Interest Group (SIG)	470-790 MHz TV white spaces	5 km	250 b/s-50 kb/s (UL) 2.5 kb/s-16 Mb/s (DL)	Star
Weightless-N	Weightless Special Interest Group (SIG)	Sub GHz (ISM)	3 km	250 b/s (UL) None (DL)	Star
Weightless-P	Weightless Special Interest Group (SIG)	Sub GHz (ISM)	2 km	200 bps-100 kbps (UL) 200 bps-100 kbps (DL)	Star

Table 1. Comparison of Smart City technologies (continued from p.411).

Communi-cation Technology	Standard/ governing bodies	Frequency	Range (app.)	Data rates	Topology
LTE-M Release 12/13	3GPP Release 12	700-900 MHz	2,5-5 km	200 kbps (DL) 200 kbps (UL)	Star
DASH7 1606	DASH7 Alliance	SUB-GHz 433/868/915 MHz	5 km	9.6,55.6,166.7 kbps	Node-to-node, Star, Tree, Mesh
LoRaWAN	LoRa Alliance	433, 863-870 MHz (EU) 902-928MHz (US)	2-15 km	250 bps-50 bps (UL EU) 250 bps-50 kb/s (DL EU)	Star
SigFox	SigFOX	868-902MHz	10-50 km	256 b/day (DL), ≤100 bps (UL)	Star
LTE	3GPP	2,5/5/10 GHz	30 km	300Mbps(DL), 75 Mbps(UL)	Star
LTE-A	3GPP	2,5/5/10/15/20 GHz	30 km	1Gbps(DL),500Mbps(UL)	Point-to-point
WiMAX	3GPP	3,5 GHz	50 km	75 Mbps	Point-to-multipoint, mesh
Ingenu	Ingenu	2450 MHz (ISM)	100 km	624 kbps (UL) 156 kbps (DL)	Star. Tree
NB-IoT	3GPP Release 13	Can be deployed in 2G/3G/4G spectrum (e.g. 450 MHz to 3.5GHz),	1 km (urb.) 10 km (rur.)	234,7 kbps (DL) 204,8 kbps (UL)	–
EC-GSM	3GPP Release 13	800-900 MHz	15 km	~300 kbps (DL) 10 kbps (UL)	–
CS IoT	–	700-900 MHz	–	200 kbps (DL) ~48 kbps (UL)	–

possibility of appliance of particular technology for particular Smart City service or application. E.g. Home automation requires short range and low data rates and Smart traffic lights service require short range, but medium to high data rate. Traffic, Air quality and noise monitoring, smart lightning and waste management applications require long range and low data rate communications [6]. Smart health requires short ranges and high data rates [18].

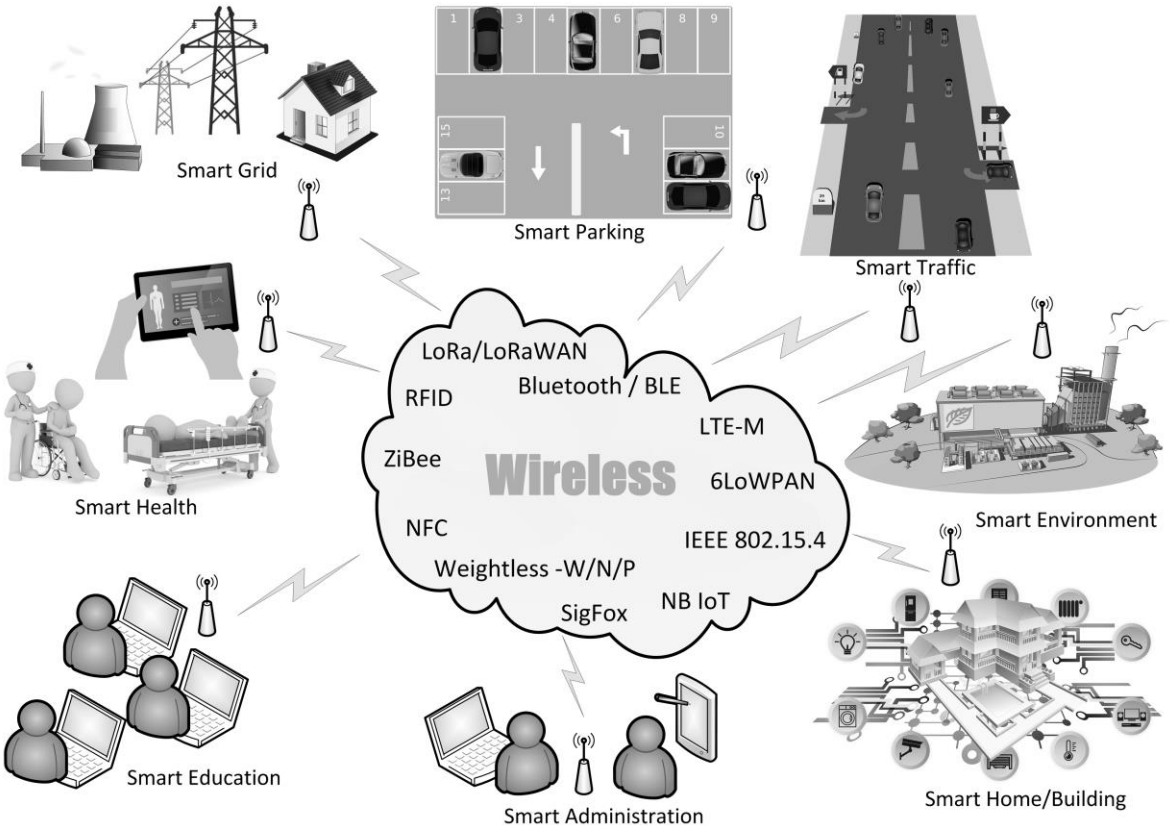

Figure 1. The usage of Wireless Technologies in Smart Cities.

Considering the range, three following categories listed in the beginning of the article can be used: WPAN, WLAN and WMAN. Despite this, some technologies like 6LoWPAN have range of 200m and are still classified like WPANs, while WI-SUN (802.15.4g) is classified as Field Area Network (FAN) by WiSUN Alliance. In order to avoid confusion, terms like short, medium and long range are used for classification in this article. Short range technologies with range from 10 cm to 3 m (see Table 1) are NFC and RFID. There is many more technologies (which can be still classified as short range) with longer range (10m-50m) such as: Bluetooth, Blue Low Energy (BLE), Z-Wave and ZigBee. Medium range technologies have extended coverage and usually have range from 100 m to 300 m. This group includes WiFi, ULP (802.15.4q), WI-SUN (802.15.4g), 6LoWPAN and Wireless M-BUS. The third group includes longer range technologies with range from 1 km to 15, 30, 50 or more kilometers. The group includes/consists of: WiFi Low Power (802.11ah), Weightless–W, Weightless–N, Weightless–P, LTE-M Release 12/13, DASH7, LoRa, LoRaWAN, SigFox, LTE, LTE-A, WiMAX and Ingenu. It should be noted that: Weightless, LoRa, LoRaWAN, SigFox and NB-IoT can be called Low-Power Wide-Area Network (LPWAN) [11, 16, 17]. Considering the data rate the networks can be also divided in three categories [6]: low, medium and high data rate technologies.

According to the presented literature and findings following conclusion can be made. Standards such as Bluetooth/Bluetooth Low Energy, IEEE 802.15.4 and ZigBee are considered as WPAN networks and are indented to be used for interconnecting the individual's workplace devices [4]. These standards are suitable for smart health monitoring and smart lighting applications as well as for other short range applications such as: Smart Home, and Smart parking and Smart traffic lights. 6LoWPAN can be used for Smart lighting [20]. WMAN or long range technologies are designed for covering large areas approximately the size of a city (with or without suburban and rural surrounding region) as point-to-point or

point-to-multipoint networks. Those networks can are usually owned by an entity, such as an Internet service provider (ISP), government, or an enterprise. [4] Low-Power WANs (LoRa, LoRaWAN, SigFox, etc) with features suitable for low-cost mobile and secure bidirectional communication can be used in most smart cities applications, such as Smart grids and metering, Smart street lighting, Smart homes, Smart health monitoring, and Smart transportation. According to authors [16] NB-IoT is a better fit for electric metering applications than SigFox and LoRa because of the required high data rate and frequent communication, while in Smart building applications LoRa and SigFox have advantage over NB-IoT.

The author of this article has experience with LoRa [20-22], ZigBee [23-25] and proprietary sub-1 GHz [26, 27] technologies. The experiments related to ZigBee technology are connected to testing its performance in indoor environments as well as for usage in wireless temperature monitoring systems. Experiments made with sub 1 GHz technology are connected to indoor propagation. Experiments with LoRa technologies are made for coverage testing, tuning outdoor propagation models and testing LoRa applicability for moving stations. ZigBee and sub 1 GHz experiments justify usage of these technologies for Smart home and building systems. Experiments with LoRa technology justify its usage for any Smart City service requiring long range (up to 5 km in urban area for stationary sensor nodes and up to 3 for movable stations) and medium to low data rates.

CONSLUSION

This article indicates one of the major challenges in designing and planning Smart City applications and services – the choice of suitable technology to be implemented. The complexity of this task is caused by variety of technologies applicable to these environments, and frequent appearance of new technologies as well. Significant difference in technology features makes this task more complex. In this article, the effort to classify available and most applicable wireless technologies for smart cities is made. The additional effort is made towards brief systematization on applicability of particular technologies for particular smart city application.

The future research in this area should be pointed in two directions. One is to determine the technology that is applicable in greater number of Smart City applications. The other one is to make more experiments in order to test these technologies in variety of scenarios.

REFERENCES

[1] Stimmel, C.L.: *Smart Cities, Analytics, ICT, and Design Thinking.*
CRC Press, Taylor & Francis Group, Boca Raton, 2016,

[2] Da Silva, I.N. and Flauzino, R.A.: *Smart Cities Technologies*.
ExLi4EvA, 2014,

[3] Khorov, E.; Lyakhov, A.; Krotov, A. and Guschin, A.: *A survey on IEEE 802.11ah: An enabling networking technology for smart cities*.
Computer Communications **58**, 53-69, 2015,
http://dx.doi.org/10.1016/j.comcom.2014.08.008,

[4] Yaqoob, I., et al.: *Enabling Communication Technologies for Smart Cities.*
IEEE Communications Magazine **55**(1), 112-120, 2017,
http://dx.doi.org/10.1109/MCOM.2017.1600232CM,

[5] Mahmood, A.; Javaid, N. and Razzaq, S.: *A review of wireless communications for smart grid*.
Renewable and Sustainable Energy Reviews **41**, 248-260, 2015,
http://dx.doi.org/10.1016/j.rser.2014.08.036,

[6] Angelakis, V.; Tragos, E.; Pöhls, H.C.; Kapovits, A. and Bassi, A.: *Designing, Developing, and Facilitating Smart Cities Urban Design to IoT Solutions*,
Springer International Publishing, Switzerland, 2017.

[7] Quinnell, R.: *Low power wide-area networking alternatives for the IoT*.
EDN Network,
https://www.edn.com/design/systems-design/4440343/2/Low-power-wide-area-networking-alternatives-for-the-IoT, accessed 15th September 2017,

[8] Radiocrafts AS: *Wireless M-Bus Technology Overview*.
https://radiocrafts.com/technologies/wireless-m-bus-technology-overview, accessed 15th September 2017,

[9] Silva, B.N.; Khan, M. and Han, K.: *Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities*.
Sustainable Cities and Society **38**, 697-713, 2018,
http://dx.doi.org/10.1016/j.scs.2018.01.053,

[10] Hammi, B.; Khatoun, R.; Zeadally, S.; Fayad, A. and Khoukhi, L.: *IoT Technologies for Smart Cities*.
IET Networks **7**(1), 1, 2018,
http://dx.doi.org/10.1049/iet-net.2017.0163,

[11] Raza, U.; Kulkarni, P. and Sooriyabandara, M.: *Low Power Wide Area Networks: An Overview*.
IEEE Communications Surveys & Tutorials **19**(2), 855-873, 2017,

[12] *Ismail*, D.; Rahman, M. and Rahman, M.: *Low-Power Wide-Area Networks: Opportunities, Challenges, and Directions*.
International Conference on Distributed Computing and Networking. Varanasi, India, 2018.

[13] Gaur, A.; Scotney, B.; Parr, G. and McClean, S.: *Smart City Architecture and its Applications Based on IoT*.
Procedia Computer Science **52**, 1089-1094, 2015,
http://dx.doi.org/10.1016/j.procs.2015.05.122,

[14] Lambrechts, J. and Sinha, S.: *Microsensing Networks for Sustainable Cities*.
Springer International Publishing, Switzerland, 2016,

[15] Al Nuaimi, E.; Al Neyadi, H.; Mohamed, N. and Al-Jaroodi, J.: *Applications of big data to smart cities.*
Journal of Internet Services and Applications **6**, No. 25, 2015,
http://dx.doi.org/10.1186/s13174-015-0041-5,

[16] Mekki, K.; Bajic, E.; Chaxel, F. and Meyer, F.: *A comparative study of LPWAN technologies for large-scale IoT deployment*.
ICT Express, 2018,
http://dx.doi.org/10.1016/j.icte.2017.12.005,

[17] Sinha, R.S.; Wei, Y. and Hwang, S.: *A survey on LPWA technology: LoRa and NB-IoT*.
ICT Express **3**(1), 14-21, 2017,
http://dx.doi.org/10.1016/j.icte.2017.03.004,

[18] Wi-SUN Alliance: *Wi-SUN for Smart Cities*.
https://www.wi-sun.org, accessed 15th March 2018,

[19] Bynam, K., et al: *Analysis of TG4q (ULP) Use Cases and ULP-PHYs*.
IEEE doc. 802.15-15-0226r0, March 2015,
https://mentor.ieee.org/802.15/dcn/15/15-15-0226-00-004q-analysis-of-ulp-use-cases-and-ulp-phys.docx, accessed 15th March 2018,

[20] Dobrilović, D.; Malić, M.; Malić, D. and Sladojević, S.: *Analyses and Optimization of Lee Propagation Model for Lora 868 MHz Network Deployments in Urban Areas*.
Journal of Engineering Management and Competitiveness **7**(1), 55-62, 2017,

[21] Dobrilović, D.; Malić, M.; Malić, D. and Stojanov, Ž.: *Analiza performansi LoRa tehnologije kod mobilnih senzorskih stanica u urbanim okruženjima*. In Serbian.
XXXV Simposia of new technologies in postal and telecommunication traffic. Belgrade, 2017,

[22] Dobrilovic, D.; Malic M.; Stojanov Z. and Sladojevic S., *Approach in Exploring Wireless Technology Performance in Smart City Environments*.
Smart City konferencia 2017. Budapest, 2017,

[23] Dobrilovic, D., Stojanov, Z., Brtka, V.; Čović, Z. and Bilinac, N.: *Software application for analyzing ZigBee network performance in university courses*.
IEEE 12th International Symposium on Intelligent Systems and Informatics. Subotica, pp.73-77, Subotica, 2014,
http://dx.doi.org/10.1109/SISY.2014.6923560,

[24] Dobrilovic, D.; Odadzic, B.; Stojanov, Z.; Sinik, V.: *Testing Zigbee RF module applicability for usage in temperature monitoring systems.*
22nd Telecommunications Forum Telfor (TELFOR). Belgrade, pp.415-418, 2014,
http://dx.doi.org/10.1109/TELFOR.2014.7034436,

[25] Dobrilović, D.; Stojanov, Ž.; Čović, Z.; Simon, J. and Petrov, N.: *Model of data center temperature monitoring system with the use of open source hardware*.
IEEE 14th International Symposium on Intelligent Systems and Informatics. IEEE, Subotica, pp.221-226, 2016,

[26] Dobrilovic D.; Odadzic, B. and Stojanov, Z.: *Approach in planning the deployment of 868 MHz RF modules in WSN scenarios*.
Proceedings of IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics. IEEE, Timisoara, pp.387-392, 2015,
http://dx.doi.org/10.1109/SACI.2015.7208235,

[27] Dobrilovic, D.; Odazic, B. and Stojanov, Z.: *Site-general indoor loss propagation model adjustment for 868 MHz RF modules*.
Scientific Bulletin of The "Politehnica" University of Timişoara, Transactions on Automatic Control and Computer Science **61(75)**(1), 65-72, 2016.

METODA NEIZRAZITOG RAČUNANJA ZA UČINKOVITO MODELIRANJE ZAGAĐENJA BUKOM U PAMETNIM GRADOVIMA

A. Nemes[1], G. Mester[1] i T. Mester[2]

[1]Sveučilište Obuda, Doktorska škola sigurnosnih znanosti
Budimpešta, Madžarska

[2]Geomant-Algotech
Budimmpešta Madžarska

SAŽETAK

Zagađenje bukom jedan je od najvažnijih problema u urbanom području. Glavni izvor zagađenja bukom je u broju i vrsti motornih vozila, ali i u dodatnim parametrima ovisno o uličnoj konfiguraciji. To je sustav kojeg je teško precizno modelirati klasičnim matematičkim metodama. Očekuje se da će pametni gradovi dinamički kontrolirati gradski promet kako bi se ne samo smanjile prometne gužve, već i osigurala prikladna razinu buke stanovnicima.

Rad daje metodu dizajna za učinkovito modeliranje prometa pametnih gradova i određivanja onečišćenja bukom temeljeno na neizrazitoj logici, pomoću višenamjenskog genetskog algoritma, optimizaciji padova gradijenta i pojedinačnoj dekompoziciji u programskom paketu MATLAB. Genetski algoritmi primjenjuju se na prethodnu identifikaciju parametara funkcija članstva neizrazitog dijela Zadehovog oblika, s ciljem minimiziranja maksimalne apsolutne identifikacijske pogreške i korijenskog srednjeg kvadrata identifikacijske pogreške te smanjenja složenosti modela i osiguravanja maksimalne numeričke robusnosti. Zatim se metoda odlaska gradijenta koristi za optimizaciju finih podešavanja, a linearni parametri, koji su posljedica neizrazitih pravila, izračunavaju se metodom pojedinačne razgradnje vrijednosti kako bi se pronašli najmanji kvadrati optimalnog prikaza učenja modela. Skup podataka za učenju izgrađen je iz mjerenih podataka, kombiniran s pažljivo odabranim simulacijskim podacima kako bi se osigurala cjelovitost modela i njegova numerička robusnost.

Detaljna analiza metode i rezultata računalnom simulacijom procesa identifikacije pokazuje valjanost predložene metode.

KLJUČNE RIJEČI

zagađenje bukom, matematičko modeliranje, neizrazita logika, pojedinačna dekompozicija, genetski algoritmi

Interdisciplinary Description of Complex Systems 16(3-A), vi, 2018

DOSEZI KIBERNETIČKE SIGURNOSTI PAMETNE UPRAVE I PROGRAMI INDUSTRIJE 4.0

M. Kiss i L. Muha

Sveučilište Obuda, Doktorska škola sigurnosnih znanosti
Budimpešta, Madžarska

SAŽETAK

Za upravjanje pametnim gradovima nužna je pravilna uprava, industrija i uslužni ekosustav koji se na tome može razvijati. Što su pametniji elementi sustava to je kompleksnija pripadna informatičko--komunikacijska infrastruktura, pri čemu jedno utječe na drugo, izravno ili neizravno. Zadnjih godina pokazalo se koliko su ranjivi takvi industrijski i uslužni sustavi sektora uprave i korporacija. Napadi u cyber-svijetu, npr. *Wannacry* ili *NotPetya* mogu utjecati na operacije neke organizacije do stupnja koji predstavlja značajan izazov upravama gradova, država ili na nekom kontinentu. Navedene kampanje djelovale su na industrijske i dostavne lance. Kako je moguće pritom opstati? Koje su kompetencije potrebne za rad naše industrije u takvom štetnom okruženju? U ovom istraživanju istaknut će se kompetencije potrebne kako bi pametni gradovi u okviru Industrije 4.0 uspješno proveli glavne projekte u korist svog razvoja.

KLJUČNE RIJEČI

kompetencije, IT upravljanje, Industrija 4.0, pametni grad, upravljanje projektom

Interdisciplinary Description of Complex Systems 16(3-A), vii, 2018

MOGUĆNOSTI OSPOSOBLJAVANJA ZA ZAŠTITARSKE RADNJE NA PRIMJERU MADŽARSKIH DRŽAVNIH ŽELJEZNICA

A. Szabó[1], E. Szűcs[1] i T. Berek[2]

[1]Sveučilište Obuda, Doktorska škola sigurnosnih znanosti
Budimpešta, Madžarska

[2]Nacionalno sveučilište državne uprave
Budimmpešta Madžarska

SAŽETAK

Pametni gradovi planiraju nekoliko praktičnih inovacija u cilju osiguravanja standarda svojih stanovnika, stanovnika prigradskih naselja i posjetitelja. Osim osiguravanja standarda, inovacije dodatno podižu standard življenja temeljen na održivim postavkama pomoću pametnih alata i logičkh metoda. U temelju je pametnih gradova sigurnost njihovih stanovnika. Zato je od vitalnog značenja omogućiti provođenje predviđenih operacija u normalnim uvjetima kritične infrastrukture. Prema zakonu iz 1997. godine, kritična infrastruktura vezana je uz aktivnosti Madžarskih državnih željeznica, tj. grupe MÁV. Zakon predviđa naoružanu zaštitarsku službu, te konzervatorsku i poljoprivrednu službu. Slijedom toga grupa MÁV uključuje i zaštitarsku službu i naoružanu zaštitarsku službu. Njihove zadaće nisu samo preventivne sigurnosne radnje nego i obrana u posebnim slučajevima u skladu s pripadnim pravilnicima. Kako bi svoje dužnosti mogli obavljati na propisani način, izrazito je značajno da zaštitarsko osoblje prolazi dugotrajno, redovito, praktično osposobljavanje. Ovaj rad ilustrira sadašnje mogućnosti osposobljavanja osoblja za provođenje sigurnosnih radnji u grupi MÁV. Također, razmotrena su moguća unaprijeđenja osposobljavanja. Navodimo u kojim internim osposobljavanjima mogu sudjelovati djelatnici grupe MÁV za područje sigurnosti. Povrh toga, ilustriramo mogućnosti dodatnih osposobljavanja i tečajeva koje svojim zaposlenicima nudi grupa MÁV u cilju njihovog osposobljavanja do razine na kojoj se uklapaju u kompleksni sustav pametnog grada.

KLJUČNE RIJEČI

pametni grad, pametni ljudi, kritična infrastruktura, željeznica, zaštita, zaštitarstvo, osposobljavanje

nterdisciplinary Description of Complex Systems 16(3-A), viii, 2018

KATEGORIZACIJA I SIGURNOST INFORMATIČKE TEHNOLOGIJE AUTOMATSKIH VOZILA

A. Albini, D. Tokody i Z. Rajnai

Sveučilište Obuda, Doktorska škola sigurnosnih znanosti
Budimpešta, Madžarska

SAŽETAK

Uz mehaničke promjene, automatizacija je sve značajnija u evoluciji vozila. Razvoj autonomnih vozila pokretačka je snaga evolucije infrastrukture informacijske tehnologije vozila. Samopouzdanje traži sve više automatike. Povećana razina automatike traži povećanu operacijsku pouzdanost. To, nadalje, rezultira u povećanoj razini sigurnosti vozila u cyber-svijetu. Ugroza u cyber-svijetu može biti prirodnog ili umjetnog porijekla. Sigurnost informatičkih tehnologija je zaštita od prijetnji prirodnog porijekla. Ona uključuje zaštitu od prirodnih ili tehnoloških utjecaja. Zbog toga je bitno povećati razinu sigurnosti informatičke tehnologije u informatičkoj infrastrukturi vozila. Ovaj rad ispituje pristupe koji povećavaju razinu sigurnosti informatičkih tehnologija sa stajališta opće informatičke infrastrukture vozila. Ti pristupi omogućuju brže procesiranje, povećanu dostupnost i veću fleksibilnost sustava. Istraživanje traži uvođenje nove kategorizacije automatizacije vozila. Pristupi su ispitani u odnosu na nove kategorije i funkcionalne razine opće informatičke infrastrukture.

KLJUČNE RIJEČI

IT infrastruktura, IT sigurnost, porast, tehnologija, vozilo

Interdisciplinary Description of Complex Systems 16(3-A), ix, 2018

TOČNO RADIOFREKVENCIJSKO IDENTIFICIRANJE I PRAĆENJE ŽELJEZNICA PAMETNIH GRADOVA POMOĆU DRONOVA

P.M. Hell i P.J. Varga

Sveučilište Obuda, Doktorska škola sigurnosnih znanosti
Budimpešta, Madžarska

SAŽETAK

Pametni promet jedan je od osnovnih djelova infrastrukture pametnih gradova. U skorijoj budućnosti, bit će korišteno sve više automatiziranih dostavnih sustava, što će umanjiti ljudski faktor u mogućim uzrocima pogreški. Drugim riječima, sigurne operacije automatiziranih sustava jedan su od najznačajnijih zadataka. Izravnoj opskrbi pametnih gradova i njihovih industrijskih pogona najbolje slui cestovni i željeznički teretni i putnički prijevoz. Uspostava zakona i automatiziranje sustava smanjuje broj nesreća, ali ih ne uklanja u potpunosti. Analizom željezničkih nesreća u zadnjih nekoliko godina ustanovili smo kako je vrijeme između nesreće i početka spašavanja i popravka jedan od najvažnijih faktora za uspješnu operaciju. Lokalizacija željezničkih nesreća često je teško provediva ili vremenski zahtjevna zbog uvjeta na licu mjesta. To vrijeme može biti značajno smanjeno radikalnim uvođenjem sustava koji pomaže pri radu agencija i ljudstva mobiliziranog za uklanjanje posljedica nesreća. Trolejbusi i tankeri su u današnje vrijeme opremljeni RFID-primopredajnikom koji omogućava praćenje kretanja pošiljke. U ovom radu istražujemo kakvu bi pomoć omogućile bespilotne letjelice opremljene RFID-čitačem, u slučaju prometne nesreće ili katastrofe, posebno kad je riječ o prijevozu opasnih materija po fiksiranoj trasi. Cilj je razviti primjenu moderne i inovativne tehnologije koja može pametni grad učiniti sigurnijim.

KLJUČNE RIJEČI

bespilotna letjelica, RFID, željeznica, komunikacija, nesreća, opasne materije

Interdisciplinary Description of Complex Systems 16(3-A), x, 2018

VJEROJATNOSNI PRISTUP I SUSTAV NEIZRAZITE LOGIKE KAO POTPORA PAMETNIH SIGURNOSNIH SUSTAVA ŽELJEZNIĆKIH POSTAJA

G. Liebmann, L. Hanka i G. Schuster

Sveučilište Obuda, Doktorska škola sigurnosnih znanosti
Budimpešta, Madžarska

SAŽETAK

Prijevoz je jedan od temelja pametnog grada. Željeznica je značajan dio javnog prijevoza i prijevoza robe, a njeno će značenje samo rasti. U današnje vrijeme porast broja ugroza i opadanje osjećaja sigurnosti generira izraženu potrebu dizajniranja pametnih, višerazinski integriranih sustava željezničkih postaja. Sigurnosni rizik tog područja zadnjih godina raste zato što javni prijevoz predstavlja bitan dio ljudske svakodnevnice, što će u budućnosti biti još izraženije. Jedna od posljedica toga je i porast broja pljački, vandalizma, čak i terorizma. Integracija konvencionalnih sustava daje nove mogućnosti i vodi na veću pouzdanost upravi i krajnjim korisnicima za izbjegavanje navedenih incidenata. Moć kompleksnog sustava ljudi i elektro-mehaničkog podsustava može biti iskorištena samo ako u središnjoj nadzornoj postaji radi kvalificirano i dobro osposobljeno osoblje.

Zbog zahtjevnosti rada višerazinskog integriranog sustava sigurnosti, bez kvalificiranih i dobro osposobljenih korisnika i operatera opadat će učinkovitost takvog sustava. Dodatno, učinkovitost integriranog sustava može biti manja od učinkovitosti uobičajenih realizacija neintegriranog sustava. To je razlog zašto su u integraciji potrebne posebne pametne funkcije.

Upravljanje pametnim, kompleksnim sustavima sigurnosti željezničkih postaja zahtjevno je zbog utjecaja ljudskog faktora, velikog broja veza i internih procesa. Međutim, nedavno razvijeni i unaprijeđeni vjerojatnosni pristup i pristup neizrazite logike mogu biti korisno matematičko rješenje navedenih razmatranja. Pripadne metode mogu biti korištene u cjelovitim, skaliranim sustavima sigurnosti ako kao prvo – slijedom pristupa neizrazite logike – ekspertna analiza pribavi dovoljnu količinu informacija o bitnim dijelovima sustava. Nakon toga nastaje mogućnost predaje i prijema podataka o određenim sustavima te mogućnost kontinuiranog preračunavanja faktora što – u nekim slučajevima – može biti mrežno provedeno. Sve navedeno omogućuje u kratkom vremenu generiranje i slanje informacija upravi postrojenja. To omogućuje maksimiziranje ukupne funkcionalne operativne učinkovitosti i smanjenje rizika. Rad daje korisne smjernice za upravljanje sustavom željezničkih postaja pametnog grada. Navodi glavne veze s rizicima za nalaženje ključnih elemenata unutarnjih i vanjskih parametara pametnih kompleksnih sustava sigurnosti. Generirana baza znanja zasigurno će sadržavati dodatne informacije o učinkovitosti i mogućim unaprijeđenjima sustava.

KLJUČNE RIJEČI

pametna sigurnost na željezničkim postajama, kompleksni sigurnosni sustavi, analiza grananja greške, vjerojatnosni pristup

Interdisciplinary Description of Complex Systems 16(3-A), xi, 2018

MOGUĆNOST UNOŠENJA KORISNIČKOG KODA U APARATE ZA PRODAJU KARATA POMOĆU SUČELJA IZMEĐU GLAVE I RAČUNALA

D. Simonyi i T. Kovács

Sveučilište Obuda, Doktorska škola sigurnosnih znanosti
Budimpešta, Madžarska

SAŽETAK

Dostupnost sučelja između mozga i računala, temeljenog na prikazu EEG, vidljivo u svakodnevnim primjenama, proširilo je skup aplikacija za mobilne uređaje. Mnogi proizvođači nastupaju s vlastitim mobilnim uređajima, koji će u skoroj budućnosti biti dostupni praktički svima, a koji otvaraju nove perspektive u suvremenom međudjelovanju čovjeka i stroja. Jedno od mogućih područja primjene je proširenje komunikacijskih mogućnosti za ljude s posebnm fizičkim potrebama, omogućavajući im prethodno nedostupna djelovanja. Jedno takvo proširenje je unošenje teksta bez tipkovnice. U Madžarskoj, u slučaju *online* kupovanja željezničkih karata, potvrda o kupljenoj karti može biti primljena nakon unošenja kôda kupca na zaslonu osjetljivom na dodir. Međutim, u slučaju nemogućnosti, fizičke ozljede ili drugog razloga, korisnici mogu biti onemogućeni upotrijebiti ruke te za njih ne postoji navedeni način plaćanja karte. To može biti nadiđeno alternativnom identifikacijom. Svrha ovog istraživanja je procijeniti mogućnost unošenja znakova u uređaje za prodaju karata pomoću sučelja između mozga i računala, temeljnog na prikazu EEG. Istraživanje se sastoji od dva dijela. U prvom dijelu izdvojeni su tehnički parametri uređaja za prodaju željezničkih karata kako bi se odredilo dozvoljavaju li oni povezivanje s vanjskim jedinicama i podatkovnu komunikaciju sa sučeljem između mozga i računala. Drugi dio istraživanja je anketiranje. Posjetili smo ustanove za brigu o ljudima umanjene pokretljivosti gdje smo pitali osoblje i štićenike ustanova da ispune upitnike. To je omogućilo procjenu potrebe za sučeljem između mozga i računala pri baratanju uređajima za prodaju željezničkih karata. Pripremeljen je i dodatni upitnik za određvanje stavova osoba prosječne pokretljivosti o uporabi navedenih uređaja.

KLJUČNE RIJEČI

sučelje između glave i računala, biometrijska identifikacija, aparati za prodaju karata, željeznički prijevoz

MOGUĆA PODRUČJA PRIMJENE BESPILOTNIH LETJELICA U ZBRINJAVANJU OTPADA NAKON ŽELJEZNIČKIH NESREĆA I KATASTROFA

G.K. Kiss Leizer*

Sveučilište Obuda, Doktorska škola sigurnosnih znanosti
Budimpešta, Madžarska

SAŽETAK

U radu su predstavljene najsuvremenije izvedbe bespilotnih letjelica (dronova) s naglaskom na sigurnijoj identifikaciji istijecanja opasnih tvari tijekom željezničkih nesreća ili katastrofa. Ova tehnologija značajna je za minimiziranje zagađenja opasnim otpadom generiranim tijekom nesreća ili katastrofa. Pritom je nužno dodatno istraživanje mogućnosti upravljanja otpadom – uz zadovoljavanje uvjeta najviše razine sigurnosti po okoliš – kao i nalaženje novih metoda profesionalnog baratanja otpadom u kratkom vremenu. Istraživanje jedinstvenih rješenja za željezničke i cestovne nesreće ili katastrofe također je mogući pristup. Značaj primjene bespilotnh letjelica izražen je posebno u slučajevima kad su drugi načini pristupa zahvaćenom području otežani ili nemogući. Tijekom neutralizacije eksploziva, opasnih ili otrovnih tvari, rizik po čovjeka može biti uklonjen uporabom suvremenih bespilotnih letjelica.

KLJUČNE RIJEČI

bespilotne letjelice, sigurnost okoliša, opasni otpad, minimiziranje štete, željezničke nesreće

Interdisciplinary Description of Complex Systems 16(3-A), xiii, 2018

JESMO LI SPREMNI ZA PAMETNI TRANSPORT? ANALIZA STAVOVA O JAVNOM PRIJEVOZU U BUDIMPEŠTI

J.I. Mezei[1] i K. Lazányi[2]

[1]Sveučilište Obuda, Doktorska škola sigurnosnih znanosti
Budimpešta, Madžarska

[2]Sveučilište Obuda, Ekonomski fakultet Keleti Károly
Budimpešta, Madžarska

SAŽETAK

Pri svakom ozbiljnom razvoju koji će utjecati na veliki dio društva, izrazito je bitno analizirati aktualni stav društva o određenoj usluzi kao i analizirati moguće posljedice elemenata razvijanog sustava. Navedeno vrijedi i za pametne gradove, posebno njihov pametni prometni sustav, iako razvoj takvog sustava unapređuje razinu življenja ljudi. Ključno je odrediti koji faktori određuju način prijevoza; koja svojstva utječu na te odabire; kakvi su stavovi različitih osoba o gradskim načinima prijevoza te jesu li ljudi spremni koristiti pametna prijevozna sredstva (npr. samovozeća vozila). Ovaj rad prikazuje odgovore stanovnika Budimpešte na navedena pitanja. Rad započinje pregledom literature o pametnim gradovima i njihovim sustavima prijevoza. Zatim su predstavljeni rezultati istraživanja kojeg je poduprijelo Madžarsko ministarstvo ljudskih mogućnosti, nakon čega su izneseni pripadni zaključci.

KLJUČNE RIJEČI

pametni prijevoz, javni prijevoz, spremnost, samovozeća vozila

Interdisciplinary Description of Complex Systems 16(3-A), xiv, 2018

PAMETNI I SIGURNI?
MILENIJSKA GENERACIJA I MOBILNI UREĐAJI

P. Holicza i E. Kaděna

Sveučilište Obuda, Doktorska škola sigurnosnih znanosti
Budimpešta, Madžarska

SAŽETAK

Pripadnici milenijske generacije, Generacije Y, neprekidno su povezani sa svojim krugom na društvenim mrežama, i čine temelj društvenih medija. Te mlade potrošače smatra se najvećom grupacijom vlasnika pametnih telefona u većini dijelova svijeta. Zapravo, mobilni uređaji postali su jedan od najvažnijih dijelova imovine te generacije koja pametno koristi tehnologiju. Međutim, napredno i rasprostranjeno korištenje mobilnih uređaja često ne prati svijest o potrebnoj razini sigurnosti. Ljudi koji su odrastali uz internet uz veću će vjerojatnost mrežno dijeliti osobne i osjetljive korporativne informacije koristeći isti mobilni uređaj i za poslovnu i za privatnu svrhu, uključivanjem u nezaštićene bežične mreže ili posuđivanjem drugih uređaja bez pripadne zaštite. Ovaj rad razmatra temeljne sigurnosne rizike pametnih telefona koje korisnici susreću pri korištenju novih tehnologija. Cilj rada je istražiti kako praksa i ponašanje korisnika dovodi do sigurnosnih rizika u njihovoj uporabi pametnih telefona. Sigurnosne prakse i svijest mogu biti unaprijeđeni povećavanjem znanja korisnika. Za postizanje toga potrebno je obrazovanje.

KLJUČNE RIJEČI

mobilni uređaji, Milenijska generacija, Generacija Y, ponašanje na društvenim mrežama, sigurnost

Interdisciplinary Description of Complex Systems 16(3-A), xv, 2018

SIGURNOST OSTVARENA DIZAJNOM SUSTAVA AUTONOMNIH INTELIGENTNIH VOZILA I INTELIGENTNOM INFRASTRUKTUROM PAMETNOG GRADA

D. Tokody[1], A. Albini[1], L. Ady[2], Z. Rajnai[1] i F. Pongrácz[3]

[1]Sveučilište Obuda, Doktorska škola sigurnosnih znanosti
Budimpešta, Madžarska

[2]Sveučilište Obuda, Elektrotehnički fakultet Kálmán Kandó, NextTechnologies d.o.o.
Budimpešta, Madžarska

[3]IBM Madžarska d.o.o.
Budimpešta, Madžarska

SAŽETAK

Rad razmatra metodičku osnovu planiranja pametne pokretljivosti. Pametna pokretljivost jedan je od značajnih elemenata pametnog sustava. Prema metodologiji prikazanoj u ovom radu prijevoz u pametnom gradu može bti razvijen na siguran način, fokusiranjem na dva glavna elementa: sigurnost i sigurnost planiranja pametne pokretljivosti. Inteligentna (prometna) infrastruktura i autonomna inteligentna vozila mogu biti integrirani u jedan sustav kako bi se ostvarila digitalna transformacija sustava prijevoza. Cilj istraživanja je razmotriti pitanja postavljena zbog kontrole i komuniciranja autonomnih vozila u sustavu vozila. Razvoj autonomnih inteligentnih vozila i sustava vozila temelji se na daljnjem razvoju kooperativnih inteligentnih prometnih sustava, kako bi se postigla pametna pokretljivost. Istraživanje nastoji iznaći metode i postupke koji pomažu sigurnom planiranju u cyber--fizičkom sustavu narastajuće kompleksnosti čiji se sve kompleksniji elementi koriste u autonomniim inteligentnim vozilima i prijevozničkom sustavu, uzimajući u obzir vidove sigurnosti i operativne rizike.

KLJUČNE RIJEČI

digitalizacija prijevoza, autonomna inteligentna vozila, pametni grad, inteligentna infrastruktura

Interdisciplinary Description of Complex Systems 16(3-A), xvi, 2018

KRITIČKI PREGLED PROBNIH PLATFORMI PAMETNIH GRADOVA U OKVIRU INTERNETA STVARI U OBLAKU

J. Simon[1] i G. Mester[2]

[1]Sveučilište u Szegedu, Fakultet inženjerstva
Szeged, Madžarska

[2]Sveučilište Obuda, Doktorska škola sigurnosnih znanosti
Budimpešta, Madžarska

SAŽETAK

Internet stvari počinje se pojavljivati posvuda u mnogim oblicima. Ali, sigurnost je jedna od najvažnijih stvari koje bi mogle usporiti rast interneta stvari. Sigurnosni principi korišteni u računarstvu poduzeća mogu pomoći u rješavanju tog problema. Već postoji više povezanih uređaja na planetu nego što je ljudi, navode vodeći istraživači na ovom području. Do 2020. godine bit će 50 milijardi povezanih uređaja, preko 6 puta više od broja stanovnika. Većina tih uređaja moći će se upravljati putem interneta i sve će više biti odgovorni za prikupljanje i prijenos osjetljivih podataka. Danas potrošači mogu posjedovati aplikaciju koja prikuplja informacije o njihovoj rutini. Za nekoliko godina te iste osobe mogu imati medicinski uređaj, upravljan putem interneta, koji kontinuirano prenosi podatke svom liječniku. U pogrešnim rukama, podaci iz sustava za upravljanje kućanstvima mogu se koristiti za procjenu korisničkih navika. Isto tako, tvrtke mogu biti ranjive kada povezuju uređaje poput onih za grijanje, ventilaciju, kondicioniranje zraka, navodnjavanje ili druge komercijalne uređaje.

KLJUČNE RIJEČI

IoT, pametni gradovi, pametna mreža, platforme u oblaku

Interdisciplinary Description of Complex Systems 16(3-A), xvii, 2018

TEHNOLOGIJE UMREŽAVANJA ZA PAMETNE GRADOVE: PREGLED

D. Dobrilović

Sveučilište u Novom Sadu, Tehnički fakultet „Mihajlo Pupin“
Zrenjanin, Srbija

SAŽETAK

Obzirom na složenu arhitekturu okruženja pametnih gradova (engl. *Smart City*), ne treba zaboraviti da njihovi temelji leže u komunikacionim tehnologijama, koje omogućuju povezivanje i prijenos podataka između elemenata u okruženjima pametnih gradova. Bežične komunikacije sa svojim karakteristikama predstavljaju tehnologije koje omogućuju stvaranje pametnih gradova i daljnje njihovo brzo i učinkovito implementiranje i proširenje. U tom je području očigledan trend pojava brojnih tehnologija koje su primjenjive u različitim scenarijima. Kako bi se moglo brzo uvesti sustav pametnih gradova, nužno je kvalitetno analizirati performanse i primjenjivost tih tehnologija. Znajući karakteristike određenih tehnologija, profesionalci će imati priliku razviti učinkovite, ekonomične i fleksibilne sustave pametnih gradova primjenom najprikladnijih tehnologija. U ovom radu prikazane su i diskutirane bežične tehnologijea koje omogućavaju razvoj usluga pametnih gradova.

KLJUČNE RIJEČI

usluge u pametnim gradovima, bežične komunikacije, bežične tehnologije

MANUSCRIPT PREPARATION GUIDELINES

Manuscript sent should contain these elements in the following order: title, name(s) and surname(s) of author(s), affiliation(s), summary, key words, classification, manuscript text, references. Sections acknowledgments and remarks are optional. If present, position them right before the references.

ABSTRACT Concisely and clearly written, approx. 250 words.

KEY WORDS Not more than 5 key words, as accurate and precise as possible.

CLASSIFICATION Suggest at least one classification using documented schemes, e.g., ACM, APA, JEL, PACS.

TEXT Write using UK spelling of English. Preferred file format is Microsoft Word. Provide manuscripts in grey tone. For online version, manuscripts with coloured textual and graphic material are admissible. Consult editors for details.

Use Arial font for titles: 14pt bold capital letters for titles of sections, 12pt bold capitals for titles of subsections and 12pt bold letters for those of sub-subsections. Include 12pt space before these titles.

Include figures and tables in the preferred position in text. Alternatively, put them in different locations, but state where a particular figure or table should be included. Enumerate them separately using Arabic numerals, strictly following the order they are introduced in the text. Reference figures and tables completely, e.g., "as is shown in Figure 1, *y* depends on x …", or in shortened form using parentheses, e.g., "the *y* dependence on *x* shows (Fig. 1) that…", or "… shows (Figs. 1-3) that …".

Enumerate formulas consecutively using Arabic numerals. In text, refer to a formula by noting its number in parentheses, e.g. expression (1). Use regular font to write names of functions, particular symbols and indices (i.e. sin and not *sin*, differential as d not as *d*, imaginary unit as i and not as *i*, base of natural logarithms as e and not as *e*, x_{n} and not x_n). Use italics for symbols introduced, e.g. $f(x)$. Use brackets and parentheses, e.g. {[( )]}. Use bold letters for vectors and matrices. Put 3pt of space above and below the formulas.

Symbols, abbreviations and other notation that requires explanation should be described in the text, close to the place of first use. Avoid separate lists for that purpose.

Denote footnotes in the text by using Arabic numerals as superscripts. Provide their description in separate section after the concluding section.

References are listed at the end of the article in order of appearance in the text, in formats described below. Data for printed and electronic references is required. Quote references using brackets, e.g. [1], and include multiple references in a single bracket, e.g. [1-3], or [1, 3]. If a part of the reference is used, separate it with semi-colon, e.g. [3; p.4], [3; pp.4-8], [3; p.4, 5; Ch.3]. Mention all authors if there are not more than five of them, starting with surname, and followed with initial(s), as shown below. In other cases mention only the first author and refer to others using et al. If there are two or more authors, separate the last one with the word "and"; for other separations use semicolon. Indicate the titles of all articles, books and other material in italics. Indicate if language is not English. For other data use 11pt font. If both printed version and the Internet source exist, mention them in separate lines. For printed journal articles include journal title, volume, issue (in parentheses), starting and ending page, and year of publication. For other materials include all data enabling one to locate the source. Use the following forms:

[1] Surname, Initial1.Initial2.; Surname, Initial1.Initial2. and Surname, Initial1.Initial2.: *Article title.* Journal name **Vol**(issue), from-to, year, http://www.address, accessed date,

[2] Surname, Initial1.Initial2. and Surname, Initial1.Initial2.: *Book title*. Publisher, city, year,

[3] Surname, Initial1.Initial2.; Surname, Initial1.Initial2., eds.: *Title*. In: editor(s) listed similarly as authors, ed(s).: *Proceedings title*. Publisher, city, year.

If possible, utilise the template available from the INDECS web page.

CORRESPONDENCE Write the corresponding author's **e**-mail address, **t**elephone and **a**ddress (i.e., *η*).

D. Tokody, A. Albini, L. Ady, Z. Rajnai and F. Pongrácz	384	Safety and Security through the Design of Autonomous Intelligent Vehicle Systems and Intelligent Infrastructure in the Smart City
J. Simon and G. Mester	397	Critical Overview of the Cloud-Based Internet of Things Pilot Platforms for Smart Cities
D. Dobrilović	408	Networking Technologies for Smart Cities: An Overview

(continuation from the front cover)

ISSN 1334-4684 (printed)

http://indecs.eu