RELIABILITY OF SECURITY SYSTEM INTEGRATION FROM THE PERSPECTIVE OF THE INTEGRATION SOLUTION

Z. Votruba

Department of Technological Equipment of Buildings, Faculty of Engineering, Czech University of Life Sciences Prague, Czech Republic

Abstract

This work deals with the issue of security system integration for so-called "intelligent buildings". It does not deal with the entire problematic which is rather wide, but it strives to answer the basic issue whether it is possible to consider such integration from the perspective of reliability parameters of integrated systems without reducing reliability of the security (or other alarm) system itself. Based on the gained findings, performed measurements and tests I have processed statistics and statistical verification of the statement included in the evaluated hypothesis. Actual trends in the alarm system integration are subsequently evaluated based on the obtained data and conclusions. Factors limiting the alarm system integration are also assessed, mainly as regards reliability of the integrated system and its parts. On the basis of theoretical calculations, experimental measurements and modelling premises are defined regarding the features of partial systems and their possible integration.

The basis of my work is verification of the base hypothesis whether an integration of a security (or any alarm) system does not reduce security and reliability of the partial systems in such extent that it will prevent their integration.

Testing of this hypothesis was performed on the basis of long-term measurements of integrated and non-integrated security systems. These results were statistically processed so that the key hypothesis could be verified or rejected and unambiguous conclusions formulated.

The author of this work does not discus legislative or normative terms of the alarm system integration.

Key words: IH&AS, security system, integration, reliability.

INTRODUCTION

Reliability of security systems is a basic parameter affecting the system use and also functioning. As concerns security systems (as well as any other alarm systems), the system reliability definition is traditionally slightly different than in the case of other systems or mechanical components. This definition is based on the definitions prescribed by the applicable industrial standard (e.g. CSN EN 50 131-1) and also especially on the overall conception of the security system (ADELI, 2008). As regards these systems, the system reliability is defined not only as the system ability to carry out the prescribed activity but also the probability of the system activation in the event of an emergency situation. We are therefore also talking about the so-called probability to overcome the system. This probability indeed changes depending on time, with regard to various abilities and on the basis of the system regular operation or climatic and other effects that cannot be deterministically described. Therefore a neuron self-learning model is an ideal tool for such system simulation. This issue, however, is not the base of this work. Security system reliability is regularly derived from the system security class related to the level of "ability" of the applicable system saboteur. The aforementioned standard relatively accurately defines 4 basic security classes. As regards the definition of reliability of the security system itself compared to a security system integrated within a larger complex, definitions of the following terms are more important:

- Probability of detection (Pd)
- Nuisance Alarm Rate (NAR)
- False Alarm Rate (FAR)
- Probability of overcoming (Vd)(ALTHOFF, 2001)

The probability of detection (Pd) corresponds to the probability of presence or movement of the violator in the area secured by the relevant detector or detection system (detection zone). This probability can differ. In general the Nuisance Alarm Rate (NAR) grows when the probability increases and under certain conditions the False Alarm Rate (FAR) increases as well. It is provided in the interval from 0 to 1 and differs for various detectors. As regards standard security systems as a whole, this value ranges for security classes 2 to 3 from 0.85 to 0.92. The project quality, its im-

plementation and regular servicing significantly affect this value.

The Nuisance Alarm Rate (NAR) is defined as the rate of nuisance alarms caused due to circumstances that can be considered as non-risk and to which the detector is basically sensible (e.g. weather conditions, movement of animals or vegetation etc.). The summary of such rates of the individual detectors can be aggregated for the entire system. The valid NAR value for the security system in security class 2 and 3 is defined by the maximum value of 1 alarm per 168 hours (per week). A too high value is a clear indicator of an erroneous project.

The False Alarm Rate (FAR) is the rate of invalid alarms caused without any clear external reason, most frequently due to circuit noises, defective electronic parts or other detector defects. It is usually provided as the number of alarms in a single detection zone per a certain time unit. With a standard security system the rate value of 1 alarm per 8,760 to 17,520 hours (according to the security class) is considered as the limit value. A high value in this case refers to an erroneous installation, poor-quality product or inappropriate service.

Probability of overcoming (Vd) is the probability with which the violator can overcome the detection technology without causing an alarm. It is most frequently done be overcoming the detection zone for example by climbing over, digging out or bridging or by using of the technical limits of the particular detection technology. According to the used technologies the values of this probability range from 0.01 to 0.2 (again in line with the security class and the type of the used system). In this case the project quality and the way of its implementation play a significant role (BOJANOVSKÝ, 2008).

The aforementioned indicators were used as base parameters on the basis of which the formulated hypothesis H0: Security system integration to other systems will not reduce security and reliability of the security system was verified. Even though standard CSN CLC/TS 50398:2009 allows for such degradation under certain circumstances!

MATERIALS AND METHODS

It is probably impossible to define a single universal test for the assessment of reliability of various ways of integration. It is possible to evaluate the overall reliability of individual integration tools, but we have to use another way of testing for each of them. Therefore we used the following methodology:

a) Integration by means of integration relays (PGM): in this case the test is performed on real objects under regular operation [1]. Sufficient operating time without integration and with integration is significant in this case. On the basis of the statistically assessed results of diagnostic signals (NAR, FAR and Vd – see above) evaluation of unambiguity of the operation difference before and after integration is performed. Selection of comparable actual high-quality installations with good operation service is significant for the aforesaid test (LIAN ET AL., 2014).

b) Security system integration by means of the EIB/KNX protocol in a higher-grade interconnected system (AULICKÝ ET AL., 2008). In this case, with regard to the smaller number of available installations, the tests were performed under laboratory conditions. Similar security systems were selected to enable comparison with the previous integration type. Testing was performed both at the physical level (verification of the information transfer from an alarm security and emergency system (ASES) to a PC by means of the KNX data using the Wireshark software) and at the application level (by means of the Loxone software) (HEŘMAN ET AL., 2008).

c) Integration by means of the CIB industrial bus of Teco a.s. was also tested mainly by laboratory means, although in this case one test was performed at an actually operated integrated system also comprising a security system. The test methodology fully complied with the way of testing according to variant of integration b). The Wireshark program was used to verify physical communication between ASES and the testing PC; a mosaic tool for the bus programming also comprising performance testing algorithms was used at the application level.

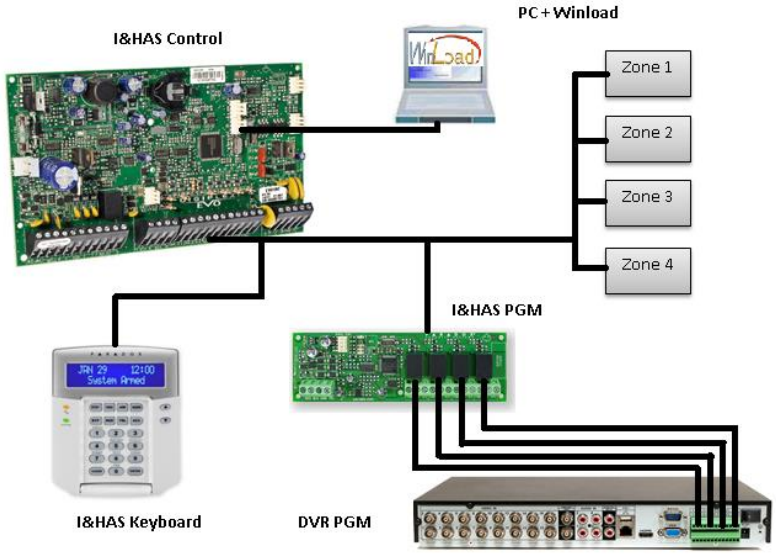

Fig. 1. – Arrangement diagram for PMG testing model according to method a)

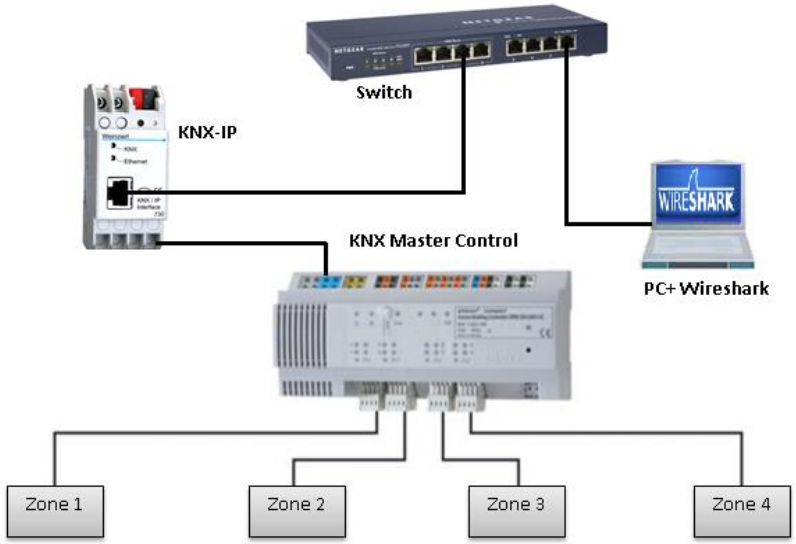

Fig. 2. – Arrangement diagram for KNX testing model according to method b)

Upon testing a set of values gained before integration was compared by means of the given method (reliability indicators NAR and VAR together with a subjective assessment of the possible change in Vd). With view to the differing numbers of measurements the parametric Student t-test or its variant, i.e. the two selection t-test was used because the base set mean value is unknown and only 2 sample data sets are compared. The following zero hypothesis is therefore tested: H0: $\mu 1 = \mu 2$.

With regard to the measurement characteristics and the requirement for testing we used a so-called "non-pair test".

The following calculation of sample characteristics was performed for the samples:

1st sample (number of members: n_1): $\bar{x}_1$, S1

2nd sample (number of members: n_2): $\bar{x}_2$, S2

As the tested samples can come from groups with the same/differing variance of the monitored characteristic value, it is necessary to first test the variance difference of both samples (a zero hypothesis, H0: $\sigma_1^2 = \sigma 2^2$) by means of the F-test.

F = greater variance (S_1^2, S_2^2) / smaller variance (S_1^2, S_2^2)

with sample variances:

$$S_1^2 = \frac{\sum x_i^2 - \frac{(\sum x_i)^2}{n_1}}{n_1 - 1} \quad (1)$$

$$S_2^2 = \frac{\sum x_i^2 - \frac{(\sum x_i)^2}{n_2}}{n_2 - 1} \quad (2)$$

To search the tabular critical values for the F-test it is necessary to determine the degrees of freedom for the numerator of the greater and smaller variance.

If $F \leq F_{0.975}$, i.e. H0 applies: $\sigma_1^2 = \sigma 2^2$ (both samples therefore come from populations with an equal variance); the non-pair t-test is used to test the difference in mean values for equal variances:

$$t = \frac{\left|\overline{x_1} - \overline{x_2}\right|}{\sqrt{\frac{(n_1 - 1) \times S_1^2 + (n_2 - 1) \times S_2^2}{n_2 + n_1 - 2} \times \frac{n_1 + n_2}{n_1 \times n_2}}} \quad (3)$$

If $F > F_{0.975}$, i.e. H0 does not apply: $\sigma_1^2 = \sigma 2^2$ (both samples therefore come from populations with a differing variance); the non-pair t-test is used to test the difference in mean values for differing variances:

$$t = \frac{\left|\overline{x_1} - \overline{x_2}\right|}{\sqrt{\frac{S_1^2}{n_1} + \frac{S_2^1}{n_2}}} \quad (4)$$

Excel functions (F.TEST and T.TEST) were used for the aforesaid calculations.

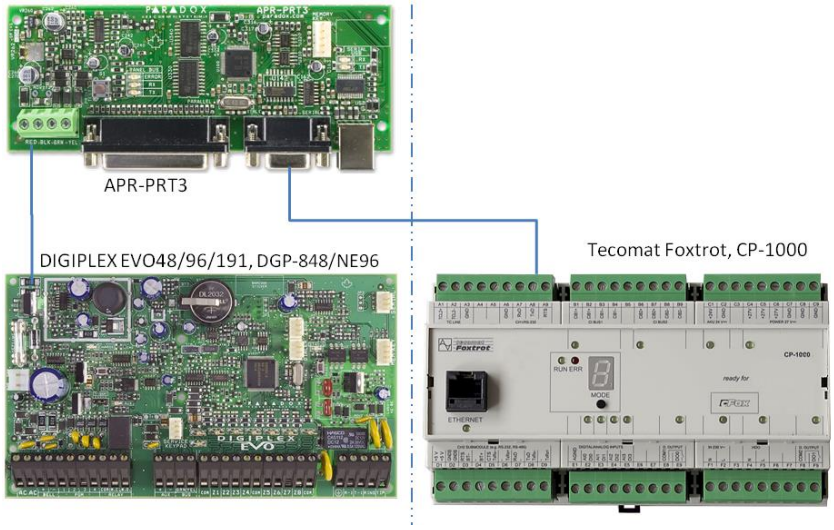

Fig. 3. – Arrangement diagram for CIB testing model according to method c)

RESULTSAND DISCUSSION

Input data for the integration testing by means of the program relay of an ASES switchboard was read from 3 different security switchboards in various operations. The age of all systems ranged from 3 to 5 years. Different times before integration rather showed as more difficult for statistic processing than as the relevant impact on the testing result.

Tab. 1. – System critical events

	System 1		System 2		System 3	
	before	after	before	after	before	after
Number of operation days (since integration)	236	628	120	142	411	123
Ratio of nuisance alarms	0.8%	1.2%	2.1%	2.0%	1.3%	2.6%
Ratio of false alarms	0.3%	0.1%	0.4%	0.5 %	0.2%	2.1%
Ratio of critical system defects	0.2%	0.5%	0.2%	0.1%	0.1%	0.7%
Ratio of critical user defects	1.4%	0.3%	4.0%	2.7%	3.2%	3.8%

Note: *the term "**before**" means before the integration date, the term "**after**" means operation after the integration date (also applies in the following tables)*

Tab. 2. – Hypothesis testing results

	System 1		System 2		System 3	
	before	after	before	after	before	after
average	0.0321	0.0187	0.0571	0.0911	0.1029	0.1108
standard deviation	0.1797	0.1178	0.355	0.1897	0.3287	0.2211
variance	0.0751	0.0385	0.2871	0.0887	0.2245	0.0871
F test significance	5E-36 p <0.05		1,28E-30 p <0.05		0,0150 p <0.05	
t test significance	0,1635 p <0.05		0,3052 p <0.05		0,8096 p <0.05	
Conclusion	at the given significance level H_0 was confirmed		at the given significance level H_0 was confirmed		at the given significance level H_0 was confirmed	

It is obvious from the performed measurements and statistic processing that integration carried out by means of program outputs/inputs in alarm systems does not cause reducing of reliability and the individual systems do not affect each other significantly from the statistical perspective. The rate of alarms (both nuisance and false), operators' errors and critical errors did not show any difference before integration and after it. It is an interesting aspect that the ratio of false alarms compared to the standard (FAR) was basically exceeded 2 times in all three systems, independent of the level of integration.

This provides obvious information regarding the quality of the project or its implementation (or service).

When testing integration by means of the KNX bus (according to variant b) of our methodology) the testing took place in two stages. First, one main line was connected to the bone KNX bus and a message transfer test were carried out (a status change at the ASES switchboard). Subsequently the 4 main lines were interconnected and statuses were read from all the lines. The test results are provided in the following Tab. 3.

It is obvious that the test results with the KNX bus confirmed the preliminary assumption that the KNX bus will show unreliable communication with more main lines. Testing of the base hypothesis is therefore quite unambiguous (VOTRUBA ET AL., 2011).

Tab. 3. – Reliability of transfer of changed ASES status by the KNX bus

	1 main line		4 main lines	
	to ASES	to PC	to ASES	to PC
Number of operating hours	64	64	52	52
Number of changes	7658	7,653	6240	4,187
Number of lost changes	0	5	0	2,053
Number of lost changes in %	0	0.0653	0	32.9

Tab. 4. – Hypothesis testing results

	1 main line	4 main lines
F test significance	0.04781 p <0.05	0.5741 p <0.05
t test significance	0.01874 p <0.05	0.1501 p <0.05
Conclusion	at the given significance level H_0 was confirmed	at the given significance level H_0 was confirmed

The aforementioned result was subsequently also confirmed by testing at the application level using the Loxone tool that confirmed the problems of the KNX bus upon packet collisions between the particular main lines. With view to the unambiguous result at the transfer level, no other result analysis at the application level was carried out.

Using of the CIB bus does not have such tradition world-wide as using of the KNX bus; however this method is quite well-known and frequently used in the Czech Republic. Therefore the test results for the integration tendency are quite significant. The test was performed similarly as in the case of the KNX bus testing, i.e. first with a single ASES switchboard per bus and subsequently with 4 switchboards (each at an independent branch). The results are summarized in the following table.

With view to the gained results statistical processing could not have been performed correctly – the standard deviation and variance have zero values or range close to zero. Surprisingly, reliability of the changed transfer by means of the CIB bus was thus evidenced.

Tab. 5. – Reliability of transfer of a changed ASES status by the CIB bus

	1 main branch		4 main branches	
	to ASES	to PC	to ASES	to PC
Number of operating hours	75	75	68	68
Number of changes	9,000	9,000	8,150	8,148
Number of lost changes	0	0	0	2
Number of lost changes in %	0	0	0	0.025

DISCUSSION

Although the aforementioned results are a significant simplification, they provide a certain notion which direction to follow in the integration tendencies concerning alarm systems for so-called intelligent buildings.

Integration by means of PGM is applicable in practice for up to approximately 20 – 30 statuses; in case of a greater number an insolvable logical problem occurs, which cannot be resolved within the ASES system logic. It however concerns one of the simplest and most effective ways of integration for small and medium systems. It was confirmed in a quite extensive test that despite some conditions provided in the literature this way is not problematic as regards reduction of the ASES system reliability.

According to the tests, integration by means of the KNX bus is also suitable for smaller and medium installations or for installations with a single main line. It is surprising because it was anticipated that KNX buses would be a good solution for the largest integration systems. It however appears that there is a problem with the power supply of elements, which is a chronic issue with KNX buses, together with irregular "unambiguity" of some users within the bus, even in the direct line. It is due to the use of the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) method as a tool preventing limitation of the number of collisions at a common bus (ANTTIROIKO ET AL., 2013). If two users transmit at the same time, the telegram whose bit sequence reads log 0 earlier shall be preferred. This procedure is quite frequently used for the communication technique but it has one great problem. The described regulation only functions at the line level. If a KNX bus is divided into more lines (which is a frequent case with larger installations), this method fails and the telegram is lost without such loss identification. If a participant tries to send the telegram more than three times but fails to get it through (due to the communication load or the set communication priority), the user may "drop out" off the communication for a certain period (which actually happened in the course of practical testing). Such drop out lasted up to several seconds and in some cases manual restarting was necessary. This was probably the reason for the quite frequent failure of the status transfer as described in the test (KNX, 2008).

In both cases the CIB bus showed almost perfect reliability (it is suspected that failures in the second part of the test were caused rather by an error in the test than in the bus). This result is quite surprising and it is most probably caused by the communication centralization. Unlike KNX, CIB does not use a decentralization model (KLABAN, 2008). Communication is controlled by a central PLC automatic machine with quite good control of the elements accessing the bus. Using of the bus (system) for integration therefore has

a great potential as regards security and reliability of information transfer to the bus.

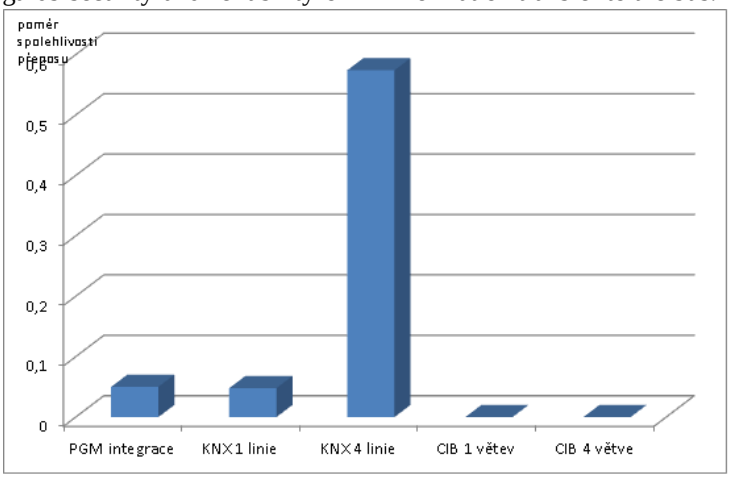

Fig. 4. – Comparative reliability values of alarm information transfer at various integration platforms

CONCLUSIONS

The partial conclusions of our three tests were described in the previous chapter. It can be generally claimed that on the basis of the performed tests we can reasonably claim that integration by means of PGM is a suitable tool for integration mainly for smaller integrated systems also comprising security systems. To the contrary, using of the most widely spread industrial bus is quite problematic for extensive systems and it cannot be recommended for the security system integration, mainly if a greater number of lines is used. The CIB bus represents a high quality way of integration, mainly for medium systems. It uses its control units to ensure quality and reliable transfer of the status information from security systems.

The author is aware that the aforementioned tests are not sufficient for all possible ways of using industrial buses as integration tools for alarm systems; they however provide a certain notion, and based on the tests the author seeks to create another way of integration at a new level, i.e. integration by means of a neuron module using the self-learning principles of neuron networks (VOTRUBA, 2016; ZHOU ET AL., 2013).

Tab. 6. – Summary of results in a table form

Technology integration	Key positive characteristics	Key negative characteristics
PGM	• price • simplicity • reliability • universal use	• only for smaller systems • problematical expandability • reduced user comfort
KNX/EIB	• expandability • large producers • extensive systems • distributed solution	• higher price • incomplete compatibility • errors in transfer (collisions) • insufficient power supply solution • problematic changes in configuration and programming
CIB	• expandability in the Czech Republic and compatibility with other solutions • proprietary preparation for alarm integration • extensive systems • clear programming	• higher price • server solution • unsolved module locking • insufficient power supply solution

Tab. 7 - Suitability of the integration technology application according to size

Technology integration	Small integration *(1 – 15 statuses)*	Medium integration *(10 – 200 statuses)*	Extensive integration *(100 and more statuses)*
PGM	80%	20%	0%
KNX/EIB	2%	80%	12%
CIB	5%	15%	80%

REFERENCES

1. ADELI, H.: Smart structures and building automation in the 21(st) century, 25th International Symposium on Automation and Robotics in Construction Location: Vilnius, LITHUANIA Date: JUN 26-29, 2008.
2. ALTHOFF, J.: Preface. In Safety of Modern Systems. Congress Documentation Saarbruecken 2001. Cologne : TŰV- Verlag GmbH, 2001, p. 5-6. ISBN 3-8249-0659-7.
3. ANTTIROIKO, A.,V., VALKAMA, P., BAILEY, S.J.: Smart cities in the new service economy: building platforms for smart services. AI and Society, 2013, p. 1-12, ISSN 0951-5666.
4. AULICKÝ, V., ET AL.: Smart buildings and ecological construction. Praha, Publishing house Dr. Josef Raabe, s.r.o, 2008. 280 s. ISBN 1803-4322.
5. BOJANOVSKÝ, J.: Smart buildings - „Control, safety and information systems in modern buildings“, SECURITY Magazine, December 2008.
6. HEŘMAN, J., ET AL.: Electrical and telecommunication installations. Praha: Verlag Dashöfer, 2008. ISSN 1803-0475.
7. KLABAN J.,Inels and bus CIB – Modern smart wiring system, Automa, 12/2008, p. 28 – 31.
8. KNX SYSTEM ARCHITECTURE. Konnex association, 2008. Available at:http://www.knx.org/_ leadmin/downloads/03 - KNX Standard/KNX Standard Public Documents/KNX System Architecture.pdf. (cit. 2015-10-5)
9. LIAN, K., HSIAO, S., SUNG, T.: Smart home safety handwriting pattern recognition with innovative technology, Computers and Electrical Engineering, Volume 40, Issue 4, May 2014, p 1123-1142
10. VOTRUBA, Z.: Integration of protective systems within the project "SMART buildings", 2016, dissertation, Prague CUA
11. VOTRUBA, Z., KOTEK, T., HART, J.: Universal interconnection protective systems in intelligent building project. Security magazine. 2011, č. 2, ISSN 1210-8723.
12. ZHOU, Q., ZHANG, Z., CUI, F.: Research on the integrated control teaching system of building based on fieldbus, Applied Mechanics and Materials 278-280 , 2013, pp. 1952-1955, ISSN 1660-9336.

Corresponding author:
Ing. Zdeněk Votruba, Ph.D., Department of Technological Equipment of Buildings, Faculty of Engineering, Czech University of Life Sciences Prague, Kamýcká 129, Praha 6, Prague, 16521, Czech Republic, phone: +420 22438 3149, e-mail: votruba@tf.czu.cz