Géza Tarnai *

METÓDA HARMONIZÁCIE HODNOTENIA ZABEZPEČOVACÍCH SYSTÉMOV

HARMONISATION METHOD OF SAFETY VALIDATION SYSTEMS

Článok sa zaoberá metódami ako harmonizovať rôzne validácie preukazov bezpečnosti podľa rôznych predpisov, ktore vznikli v rôznych dobách, navzájom a so súčasne platnými európskymi normami CENELEC v spojitosti s konkrétnym aplikačným príkladom realizácie prvého elektronického zabezpečovacieho zariadenia na MÁV (Maďarskej štátnej železnici).

This paper presents methods to harmonize different safety validations, which were created at different times and by different prescriptions, with each other and with the CENELEC standards, in connection with a concrete application example, the realization of the first electronic interlocking system of the MÁV.

Keywords: Safety validation, railway signalling, CENELEC standards, harmonization

A decision on the modernization of the main line of the Hungarian Railways (MÁV) towards West-Europe was made in the early 90's. The aim of the modernization was to reduce the travel time between Budapest and Vienna. In the frame of this project three railway stations have been equipped with electronic interlocking systems. The first electronic interlocking system of MÁV was installed in 1997 in Tata station, by Siemens Transportation Systems. The Stellwerk Ltd., a Hungarian engineering company took a considerable part in the interfacing tasks and in a number of developing and projecting tasks.

One difficulty of the project was that the most modern electronic interlocking has to work together with the existing relay-based block system. Furthermore, the trackside objects (point machines, signals etc.) are also traditional with a traditional interface. Furthermore, it had to be taken into consideration that the Traffic Rules for the Hungarian Railways are different from the rules of former applications of the Siemens interlocking (DB, SBB etc.). A special requirement was the solution of the control of the 75 Hz track circuits, which is the base of the train protection system. As the original electronic interlocking was not equipped with such a sub-system, it had to be completed with a Siemens safety programmable logical controller, PLC (Fig. 1) [2].

The complexity of the system and the fact that it was the first electronic interlocking system in Hungary, made the preparation of the safety validation and the authority approval process rather difficult. The existing, previously accepted safety validations for

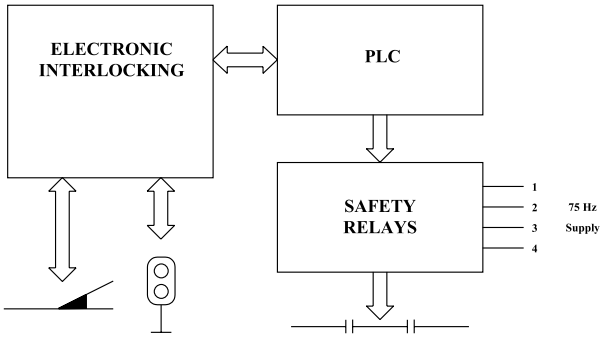

Fig. 1 Control of the 75 Hz supply

those parts, which did not have to be modified for the Hungarian Railways, were accepted by the Hungarian Transportation Authority, too. The modified parts needed a modification or completion of their safety validation, and these had to be approved by the Authority (e.g. signal system). For the brand new parts (e.g. 75 Hz control) a new safety validation had to be created. Of course the interface between the new and old sub-systems (interlocking computer, PLC, block system, relay interface and their communication) also needed a safety validation.

The preparation of the safety cases was not the heaviest task, but rather the harmonization of these different types of documentation. The existing safety validations were prepared before the appearance of the new CENELEC directives, and they followed the directives of additional different standards. Between the new and old safety validation the so called "safety validation interface" had to be created in order to harmonize the different

* **Dr. Géza Tarnai (1940) CSc., PhD., Assoc. Professor, FIRSE**
Technical University of Budapest, Department of Transport Automation, H-1111 Budapest, Bertalan Lajos u. 2.
Tel.: +36-1-463 1990 Fax: +36-1-463 3087, E-mail: tarnai@kaut.kka.bme.hu

safety validations, and the whole package had to be matched with the new CENELEC directives. [15]

In the following section the safety suitability analysis of control PLC of the 75 Hz supply will be outlined.

Proofing the suitability of the 75 Hz control PLC

Railway application of the DIN V 19250 standard

As mentioned in the case of the electronic interlocking system in Tata station, a safety PLC is applied for the control of 75 Hz supply. Of course, it had to be examined previously whether the selected type of PLC is suitable for this application from a safety point of view. To decide this, the given application's requirements from the PLC had to be specified (matching the application and the requirement class) and this had to be compared with the safety requirements that the PLC can fulfill, i.e. from which requirement class does the PLC come.

The classification of the SIMATIC S5 115F PLC that was intended to be used in Tata was carried out in accordance with the DIN V 19250 standard during the type examination [7]. Thus, we classified the safety requirements of the control of the 75 Hz track circuits also in accordance with the mentioned standard.

To match a requirement class with a given application, 4 risk parameters must be taken into consideration:

- degree of the damage (S1...S4)
- staying in the danger zone (A1, A2)
- possibility to avoid the danger (G1, G2)
- probability of the occurrence of the unwanted event (W1...W3).

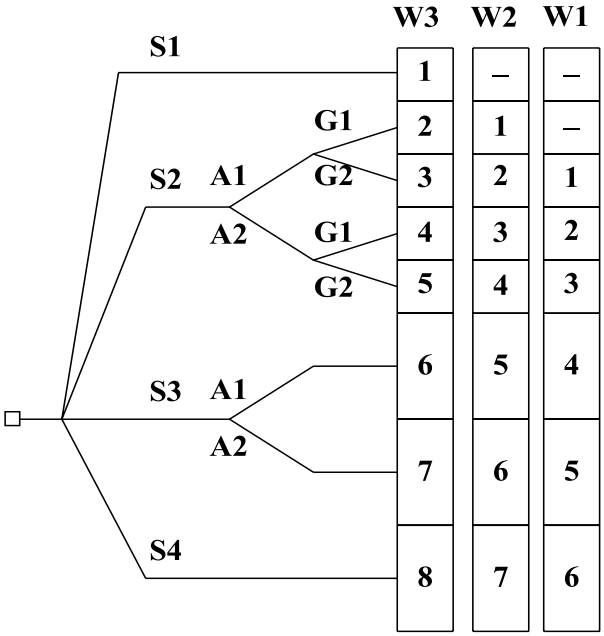

Fig. 2 Risk graph

The connection between the risk parameters and the requirement classes is shown on a risk graph (Fig. 2), where the lowest or mildest requirement class is referred to as 1 and the highest requirement class as 8 [3].

Although the DIN V 19250 is not a railway-specific, but an industrial standard, however with the consideration of some additional definitions for the interpreting of the risk parameters, it can also be applied in the field of the railway operation for the classification of the safety requirements. The required technical and operational arrangements that satisfy the demands of a given requirement class must be carried out in accordance with the DIN V VDE 0801 standard [1, 4, 10].

To match the appropriate requirement class with a given application, the application must be decomposed into sub-functions, and the examinations must be carried out for these sub-functions. To determine the sub-functions the customer requirements must be taken as a basis.

Supply of the 75 Hz track circuits

The 75 Hz track circuits are supplied with coded signal (code '1'...'4'), where code 1 orders the train to stop at the next signal, and code '4' allows to drive at the highest permitted speed. Codes '2' and '3' mean intermediate speeds. The basic safety task of the 75 Hz supply is to stop those trains with an emergency braking that are passing by a red signal at a speed more the 15 km/h [9].

To fulfill this requirement

- the 75 Hz track circuits must be supplied with code '1' (stop!) on a given length before the red signal,
- the track circuit section behind the signal must not be supplied, or only so that the aerial of the train may not receive any 75 Hz signal from the track. The latter is to solve so that the track section behind the signal must be supplied from that side where the train will enter on the track section, i.e. from the signal (Fig. 3).

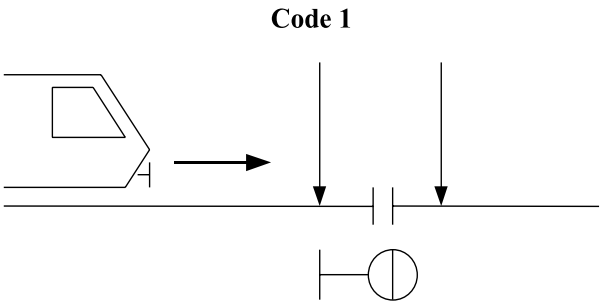

Fig. 3 Supply of the track circuits before and behind the signal

Another task of the 75 Hz supply that must be examined before the classification of the safety requirements is: the onboard repeater signal on the locomotive may not show higher speed than what the real signal beside the track shows. To this the supply code must correspond to the real signal, and in case of a failure it

may only be lower. E.g. if the main signal allows 40 km/h speed, the supply may not be code '4' (maximum speed) instead of code '2', not even in case of a failure.

The task of the PLC is to select the required code and to control the safety relays which switch the code (Fig. 1). The code-switching relay circuit is so constructed that in case of a PLC failure or break-down, or in case of a relay failure, the supplied code can only be '1' (stop!).

Result of the Examination

We examined the possible operational cases, and to the mentioned functions we fixed the requirement class 5, with one exception. In one case the requirement class 6 was established. Since for an application always the highest sub-function is significant, for the 75 Hz track circuit control PLC the requirement class 6 can be established.

According to the type examinations of the TÜV Bayern, the S5-115F PLC satisfies the demands of the requirement class 6 of the DIN V 19250 standard [16], thus the selected PLC is suitable for the presented application, i.e. for the control of the 75 Hz supply.

Comparing of the safety prescriptions

Former prescriptions

Different safety directives and safety philosophies have been formed at the railways of the different countries during the development. From the flowing different technical applications have been developed the different safety validation procedures for the railway signalling equipment. A favoured of them in Europe is the "Directives to Technical Authorization of Railway Signalling Equipment" (Mü 8004), elaborated and being regularly updated by the *Central Office of German Federation Railways* (its new name is *Federation Railway Office, EBA*). These directives are not exclusively applied by the German Railway (DB), but many other railways and other railway signalling institutions use this directives' collection during their activity.

In the case of the Siemens's electronic interlocking system in Tata, these directives are also authoritative, since the safety validations for the previous applications of this equipment, e.g. at the DB, were also elaborated in accordance with the Mü 8004. In order to keep the consistency, it seemed to be practical to carry out the safety validation of the for the MÁV application changed or new system parts also on this basis.

The intention to a unified procedure, however, could not be totally successful, because as mentioned before the suitability of the control PLC of the 75 Hz supply could be validated on the basis of the DIN V 19250 standard. A further difficulty was that the Hungarian railway authorities, from the mid-90-s intended to take the new European standards as the basis for future applications in Hungary [13]. It meant for us to examine the compatibility of the former and the new standards or preliminary standards so that the existing safety validations previously elaborated by former prescriptions should not be created again, and only the necessary modifications and additions should be done.

The New Prescriptions

In frame of the elaboration of the new European standards, the DIN V VDE 19250 German standard used as a basis up to now is put into the *IEC 65 A (Sec) 123* international standard [5], and the DIN VDE 0831 which was compulsory for the railway signalling equipment will be transferred to the *EN 50129* European standard [11].

The requirement classes of the DIN V VDE 19250 appear in the IEC 65A (Sec) 123 standard as *Required Risk Reduction* in *8 levels,* signed with letters from 'a' to 'h'. From the Required Risk Reduction levels are deducted the *System Integrity Levels (SIL),* signed with numbers from 0 to 4. These levels form the base of the technical realization by the IEC 65 A (Sec) 123. The connection between requirement classification of the DIN V 19250 and the IEC 65 A (Sec) 123 is shown on table 1. [1]

Table 1

Requirement classes	Required Risk Reduction	System Integrity Level
DIN V 19250	IEC 65 A (Sec) 123	
1	a	0
2	b	1
3	c	1
4	d	2
5	e	3
6	f	3
7	g	4
8	h	4

The main target of the harmonization activities in the frame of the CENELEC is to establish the conditions for cross acceptance of the technical safety procedures in Europe. The elaborated draft standards (prEN 501xx) are based on international preliminary standards (IEC 65 A Sec 122 and Sec 123) and national safety directives e.g. Mü 8004 and RIA 23 (Directives for Software of the British Rail). From these, the basic safety principles were taken over and a well-structured, comprehensive preliminary standard was further developed [6, 8].

The common regulations of the different railways and the general application of former international (e.g. ORE) recommendations eased the euro-norming procedure. However, the differences mainly on the field of servicing and functionality form a considerable obstacle against the general introduction of cross acceptance.

A further purpose of the application of the new standards is to keep the future developments' costs, devoted to the safety only as high as the application really requires. To achieve this aim, 4 Safety Integrity levels have been created concerning the failure probability and the risk class of a system or system-part (table 2).

Table 2

Level	Safety Integrity	Descriptive expressions (alternatives)			
4	Very high	Vital	Critical	Safety critical	Fail-safe
3	High	Vital	Critical	Safety-critical	High-safe
2	Medium	Medium vital	Essential	Safety-related	Medium-safe
1	Low	Medium vital	Essential	Safety-related	Low-safe
0	Not defined	Non-vital	Non-essential	Non-safety-related	Non-safety related

The highest Safety Integrity Level is 4. This level is valid, for example, for railway signalling equipment or a train protection system. The lowest level is 1, which is recommended for simple safety applications. For non-safety applications the level 0 was formed. The required safety class is a function of the frequency and the significance of the hazard possibilities of the controlled process and the expected safety goal.

By the establishing of the hazard, the new preliminary standard has a different basis than the former one. From the risk parameters of the DIN V 19250, it does not contain the "staying in the danger zone" (A) and the "possibility to avoid the danger" (G). It defines the "degree of the damage" (S) and the "probability of the occurrence of the unwanted event" (W) parameters in another way, too. The probability of the unwanted event is shown as probability levels and is classified. The former deterministic and implicit probability approach is exchanged with a stochastic, explicitly on probabilities based approach [14].

The new preliminary standard defines the satisfactory safety as the probability that the technical process or the system suits the determined and proved safety requirements at any time until the uninstallation of the system.

If we include the Mü 8004 standard into the examination, we can state that it does consider neither the probability of the unwanted event, nor the degree of the damage. Furthermore the classification of the system safety requirements can not be found, which is otherwise ordinary in other prescriptions. Thus, according to the Mü 8004 any safety related system should meet the highest requirements (SIL 4 according to the euro-standards). The non-safety systems correspond to the SIL 0 of the euro-standards. The intermediate levels can not be handled by the Mü 8004 standard.

The connection between the requirement classes of the different safety prescriptions is shown on table 3.

Comparing the Mü 8004 and the euro-standards, the difference is obvious in the field of safety process and the approach to safety management [15]. The safety process required by the Mü 8004 is based on a static safety management approach. Practically it focuses on the required safety at the moment of the approval of a new system and does not or hardly contains any prescriptions in connection with the further phases of the system's life cycle. It presumes that the necessary and sufficient examinations to prove the existence of the safety can be carried out. Therefore the examiner's knowledge on the examined system is critical.

In spite of this, the new euro-standards are characterized by dynamic safety management. Obviously the regulation of the approval is similar to the Mü 8004, but the safety process is completed: the whole life cycle is covered by the regulation. Thus, the required level of safety and quality is assured in frame of a properly designed and controlled process. It also means that the approval examination is less emphasized in the process than in the Mü 8004.

According to the new euro-standards it is evident that necessary and sufficient examination of the classical approach can

Table 3

Requirement class	System Integrity Level	Safety Integrity Level	System qualification
DIN V 19250	IEC 65 A (Sec) 123	prEN 50129	Mü 8004
1	0	0	Not safety-relevant
2	1	1	
3	1	1	
4	2	2	
5	3	3	
6	3	3	
7	4	4	Safety relevant,
8	4	4	fail-safe

not be practically carried out. Realization of the additional considerations besides the previously known and unified examination considerations are the responsibility of the developer and the examiner. The realized hazards and the arrangements made for their correction can be followed up. The safety can be connected to and proved at certain levels of the system's hierarchy. The reviser does not need to know the equipment in total; his main task is to control keeping the rules.

Harmonization of the former and newer prescriptions

We can conclude that the two safety validation processes based on different approaches are not to be exchanged, and it is difficult to switch from one to the other. However, the importance of the difference between the above detailed regulations is decreased by several factors: one is that the Mü 8004 recommends to apply an ISO 9000 like quality management in the development and the manufacturing. Thus, the safety as a property of the product can be controlled and followed up with the product itself. Therefore, the result of the two different regulations in the developing and manufacturing phase can be equal.

The results of the examinations of the electronic interlocking system in Tata showed that the data and results gained from the safety validation process according to Mü 8004 can be reordered and completed to reach an end-documentation that meets the requirements of the euro-standards [13]. The differences of the two prescriptions in the safety process can be handled appropriately from the viewpoint of the approval. This allows us to apply previous Mü 8004 safety validations. Furthermore, it makes possible the creation of safety validations by the former directives for changed or new system parts and to integrate them into the safety process in accordance with the euro-standards.

This paper presented the correlation between the safety requirement classes of the different safety directives. The results of the examinations of the control PLC of the 75 Hz supply by the DIN V 19250 standard can be integrated into the safety process, carried out in accordance with euro-standards.

Reviewed by: M. Kunhart, J. Zahradník

References

[1] "Anforderungsklassen für Signal- und Zugsicherungsanlagen" VDV Schriften 331, September 1994
[2] ANTWEILER, B., W. STAAB, G. TARNAI: "A Siemens elektronikus biztosítóberendezése Tatán" Vezetékek Világa Magyar Vasúttechnikai Szemle 1997/3 pp. 20-23.
[3] DIN V 19250 "Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen" Mai 1994
[4] FISCHER, W.: "Das vertretbare Risiko einer Bahn" Der Nahverkehr 9/95 pp. 48-50
[5] IEC 65A (Sec) 123 "Funktionale Sicherheit von elektrischen/elektronischen/programmierbar elektronischen Systeme" 1990
[6] JANSEN, H.: "The Safety Case - A New European Approach to Guided Transportation Safety Philosophy ..." World Congress on Railway Research Conference Colorado Springs, USA June 17-19 1996 pp. 173-185.
[7] KLEIN, S., F. RIEGER: "SICAS S5 - Stellwerke Light" Signal+Draht 87 (1995) 9 pp. 290-295
[8] LENNARTZ, K.: "Europäische Normen für die signaltechnische Sicherheit der Eisenbahnen" Signal+Draht 86 (1994) 12 pp. 416-420
[9] MACHOVITSCH, L.: "Vonatmegállító berendezések" A Vasúti Technika Kézikönyve Műszaki Könyvkiadó Budapest, 1977. (szerk.: Czére, B.) 5.2.6.2 fejezet 2. kötet, pp. 460-475.
[10] MÜLLER-HELLMANN, A.: "Anforderungen an Sicherheitssysteme aus der Sicht des VDV" Signal+Draht 86 (1994) 12 pp. 428-431
[11] Railway Applications:
- The Specification and Demonstration of Reliability, Availibility, Maintainability and Safety (RAMS) prEN 50126: 1995
- The Specification and Demonstration of Reliability, Availibility, Maintainability and Safety (RAMS) Part 2: Safety prEN 50126-2: 1994
- Software for Railway Control and Protection Systems prEN 50128: 1994
- Safety Related Electronic Railway Control and Protection Systems prEN 50129: 1994
- Basic Requirements for Safety Related System Using a Single Serial BUS prEN 50159: 1994

[12] RASTOCNY, K.. J. ZAHRADNIK, J. SLOVAK: "Classification of Risk Parameters" 2nd International Scientific Conference „Elektro '99" 23-24 June 1997 Zilina Section Information&Safety Systems pp. 55-59.
[13] RÓZSA, G., S. HŐGYE: "Az új közlekedésbiztonsági rendszerek alkalmassági tanúsítványának elkészítése" Vezetékek Világa - Magyar Vasúttechnikai Szemle 2/97 pp. 16-18.
[14] SZABÓ, G., G. TARNAI: "Dependability Analysis of Interlocking Systems - A Comparison of the Probabilistic and the Deterministic Approaches" 3rd International Scientific Conference „Elektro '99" 25-26 May 1999 Zilina Section Information&Safety Systems pp. 7-12.
[15] TARNAI, G., S. HŐGYE: "A vasutaknál alkalmazott biztosítóberendezések technikai biztonsági normái" II. Országos Vasúti Távközlési és Biztosítóberendezési Konferencia Bükfürdő, 1997. szept. 17-19. pp. 2-5.
[16] Zertifikat Nr.: U 94 12 20403 006 „Sicherheitgerichtetes Automatisierungsgerät S5-115F" TÜV Product Service 08. 12. 94