Journal of KONBiN 1(21)2012
ISSN 1895-8281
DOI 10.2478/jok-2013-0002

ProSIL SOFTWARE FOR FUNCTIONAL SAFETY MANAGEMENT IN LIFE CYCLE

APLIKACJA ProSIL DO ZARZĄDZANIA BEZPIECZEŃSTWEM FUNKCJONALNYM W CYKLU ŻYCIA

Tomasz Barnert, Kazimierz T. Kosmowski, Marcin Śliwiński

Politechnika Gdańska, Wydział Elektrotechniki i Automatyki
Gdansk University of Technology, Faculty of Electrical and Control Engineering
e-mail: t.barnert@ely.pg.gda.pl; k.kosmowski@ely.pg.gda.pl; m.sliwinski@ely.pg.gda.pl

***Abstract**: In the paper the ProSIL software to aid the functional safety management is presented. The software consists of three modules to aid: determination of the required SIL level (ProSILen), veryfication of the SIL level (ProSILver). In the aplication the method of the calibrated risk graph to determine the required safety integrity level SIL for defined safety instrumented functions is applied. The methods concerning functional safety analysis utilized in the process of the design and performing Safety Instrumented Systems (SIS) according to PN-EN 61508 and PN-EN 61511 prepared by the team during researches are implemented.*

***Keywords:** functional safety, SIL, ProSIL, ProSILer, ProSILen, BPCS, SIS*

***Streszczenie:** W niniejszym artykule przedstawiono prototypowe oprogramowanie ProSIL wspomagające zarządzanie bezpieczeństwem funkcjonalnym. Program ProSIL składa się trzech modułów wspomagających: określanie wymaganego poziomu SIL (moduł ProSILen), weryfikację SIL (moduł ProSILer). W aplikacji ProSIL zaimplementowano opracowaną w trakcie badań metodykę analizy bezpieczeństwa funkcjonalnego w projektowaniu i użytkowania systemów SIS zgodnie wymaganiami z PN-EN 61508 i PN-EN 61511. Wykorzystano metodę kalibrowanego grafu ryzyka do określania wymaganego poziomu nienaruszalności bezpieczeństwa SIL dla zdefiniowanych funkcji bezpieczeństwa*

***Słowa kluczowe:** bezp. funkcjonalne, SIL, ProSIL, ProSILen, ProSILer, BPCS, SIS*

1. Introduction

Taking into account the expectations of process engineers and functional safety analysts it is important to provide useful computer-aided knowledge-based system supporting the safety management in system life cycle. Such knowledge-based system has been designed as a ProSIL software to support designing and verifying the E/E/PE, BPCS and SIS systems according to PN-ENC 61508 and PN-EN 61511 requirements [6, 7, 8, 9]. It makes possible to determine required safety integrity level SIL using the risk graph or risk matrix method or to modify this level according to requirements imposed by the supervisory institution for defined safety functions. Computer aided verification of determined SIL is to be carried out for the architectures of E/E/PE or SIS implementing safety-related functions.
Simplified scheme and functional scope of the knowledge-based system for supporting the SIL determination and verification is shown on Figure 1.

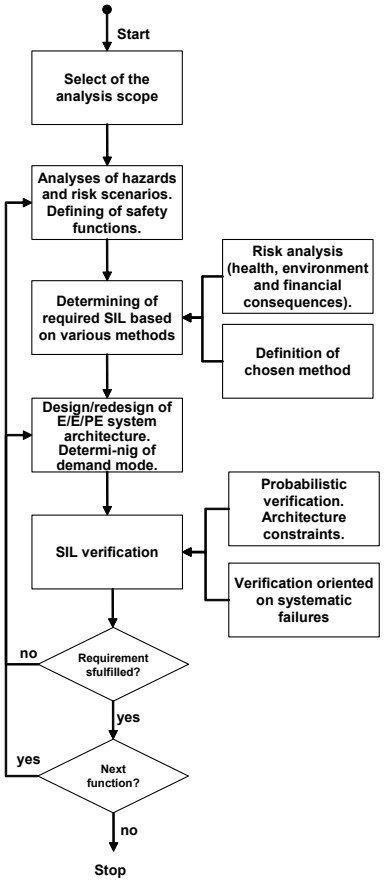


Fig. 1. Main modules of functional safety analysis system ProSIL [4, 5]

ProSIL consists of several modules connected with different aspect of functional safety analysis. There is a hazard identification and analysis module, which generates the risk scenarios and descriptions of safety-related functions. Next module is risk analysis and assessment, which allow determining required SIL for each safety function. The last module is related to verification of determined SIL for each architecture considered of given safety function.

2. Concept of ProSIL knowledge-based software

A concept of ProSIL software provides an opportunity to create projects with many safety-related functions (SRFs) described. For each SRF one of several available method of analysis can be applied. The chosen method is dependent on analyzed system's life cycle stage. The ProSIL software consists of three main modules: determining SIL (ProSILen), verifying SIL (ProSILer) and LOPA analysis module [10, 11, 12]. Each new created project has detailed description and opportunity of saving its parameters into integrated database. Figure 2 presents main window of project in the describing software. At a top belt in the application there is a direct access to one of the mentioned above modules, however for each defined SRF there is an option to enter the proper module directly from its edit window.

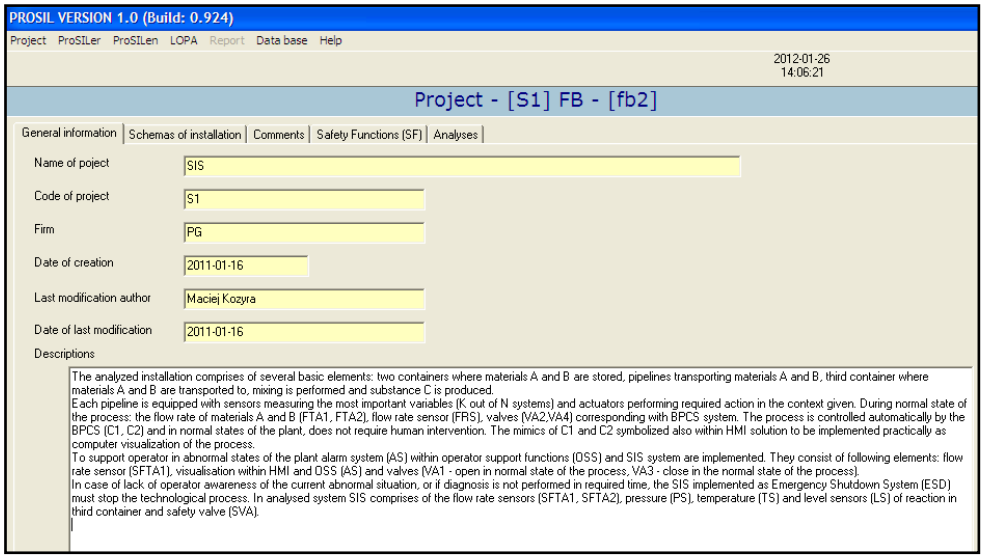


Fig. 2. ProSIL application main window

User of the application has direct insight into some overall project information as well as attached schemas and specific P&IDs of analyzed system or subsystems (see Fig. 3).

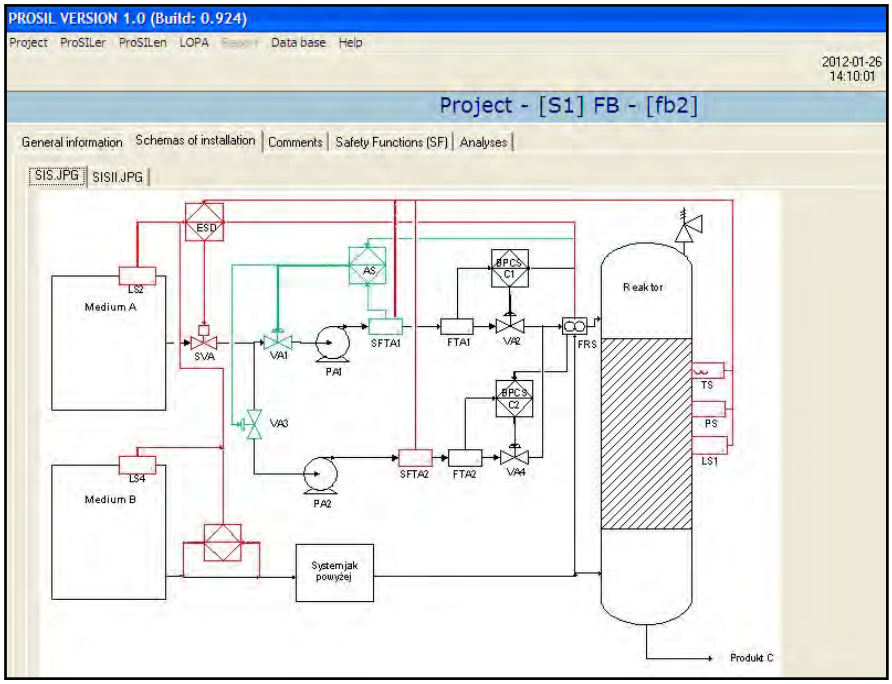


Fig. 3. Installation schemas container

The ProSIL software provides opportunity to manage set of safety functions which should be identified and described earlier in the process of hazard analysis (Fig. 4).

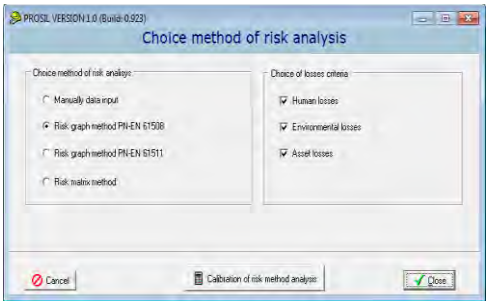


Fig. 4. Choose one of the available SIL determining method

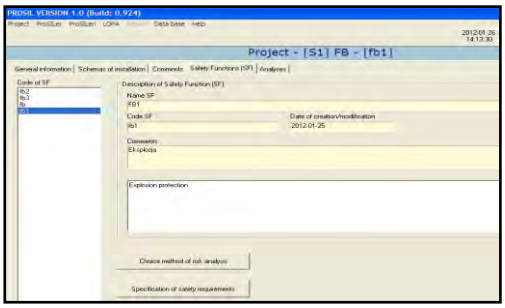


Fig. 5. Definition of new safety function

By necessity of occurrence a relationship between the results of hazard analysis and a risk assessment input information, ProSIL gives an option for including them into the application as text attachments. Those documents are also taken into account in the process of determining required safety integrity level.

3. Determining required safety integrity level

One of the main part of computer-aided functional safety analysis is a module for determining required safety integrity level of chosen safety function.
There are several methods to determine SIL for given safety function. Some of more popular ones in industrial practice are:

- Risk Matrix,
- Risk Graph,
- Layers of Protection Analysis (LOPA).

These methods are qualitative or quantitative, which means that they use descriptive or quantified information about the risk parameters. The standard (PN-EN 61508) proposes a qualitative risk graph method for determining SIL qualitatively for given safety-related system as a main one. This method is useful, but special care should be taken into account during applying the method. It should be noted that the number of parameters and their ranges describing the frequency and consequences of a dangerous event can differ for some accident scenarios. That's why a new extended approach was introduced in [3, 4, 5], based on modifiable risk graphs, which allows building any risk graph schemes with given number of the risk parameters and their ranges expressed qualitatively or preferably semi-quantitatively.

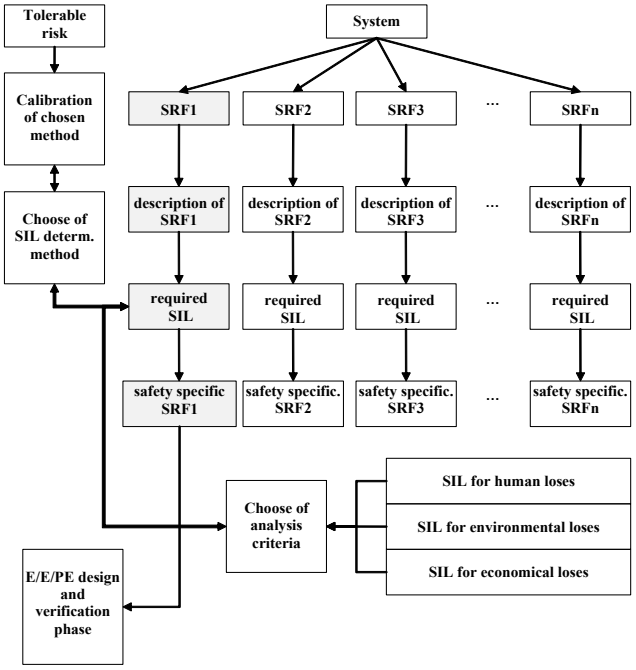


Fig. 6. Main idea of using ProSILen module

Determining of required safety integrity level for chosen safety function is realized in specialized module of ProSIL application. It is built by two main sections. If the method of determining SIL is chosen, then it should be calibrated in the proper manner, so the first section of the described module is responsible for calibration of chosen risk assessment method. A concept of ProSIL requires calibrating the method once in the project if this method is used during any analyses at least for one SRF included in the project. A process of calibrating selected method is divided into two steps. First step is related to determining a tabular part of this method and the second one is associated with proper choose of risk parameters and their risk criterion ranges (with qualitative, semi-quantitative or quantitative description). For example, one of the available method is PN-EN 61508 based risk graph which has four risk parameters: C, P, F and W. A definition of tabular part of the risk graph relies upon selection of one from seven accessible risk reduction levels, which are associated directly with four SIL levels or lack of requirements level. A process of selecting SIL determining method is presented in figure 5. The fundamental window of calibrating the selected exemplary methods is illustrated in figures 7 & 8.

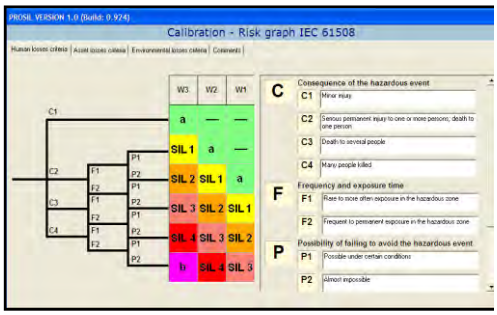


Fig. 7. Calibration of the IEC 61508 risk graph method (human losses)

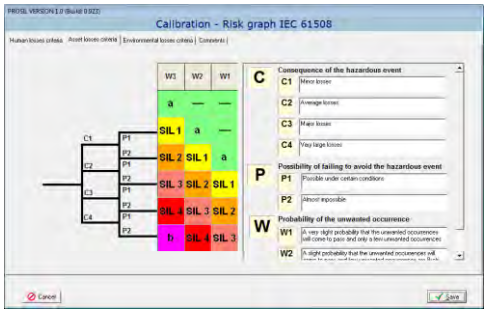


Fig. 8. Calibration of the IEC 61508 risk graph method (asset losses)

A second part of SIL determining module is associated with the usage of proper calibrated method in the specific risk analyses. An information about criteria of analysis (i.e. oriented on human, environment or asset loses) are determined during the process of calibration selected method (see Fig. 7 & 8). This is very important part of use this application module because it is related to further risk analysis and opportunity of choosing proper analysis criteria. The analysis for each criteria can give different required SIL results. If more than one criterion is chosen in this analysis, the more restrictive SIL is taken into account as a final result for analyzed safety function. Next two figures show some examples of determining required SIL.

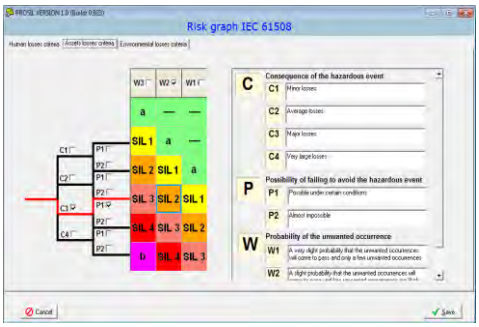


Fig. 9. Determining of required safety integrity level (asset loses)

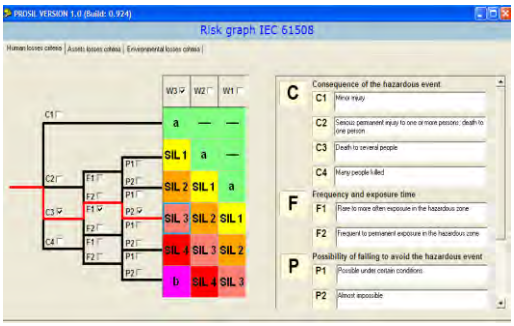


Fig.10. Determining of required safety integrity level (human loses)

4. Safety integrity level verification

Computer aided SIL verification module ProSILer (see Fig. 11) consists of a library of probabilistic models developed using the minimal cut sets method (MC). This library contains also probabilistic models of system and subsystem from PN-EN 61508-6. The architecture of the E/E/PES system realizing the safety-related function is represented basically as a functional safety reliability block diagram (RBD). Probabilistic modeling of safety-related systems is performed using *koon* subsystems architectures including dependent failures modeling for β-factor parameter obtained from a knowledge-based system. The SIL verification module includes a generic reliability database of various parameters (λ, *MTTR, MTBF, MTTF, DC, TI,* β). There is possibility to enter the reliability data from external sources with relevant explanations (providing documentary evidence).

The diagnostic coverage (*DC*) and β-factor determining is computer aided using the knowledge-based system. There is an option to draw PFD(t) probability function together with evaluated PFD_{avg} value for given mission time. The software package contains also a module for optimizing the functional test intervals and a module for sensitivity and uncertainty assessment of results obtained from probabilistic models with regard to its parameters (failure rates, diagnostic coverage, mean time to repair, test interval, β-factor, etc.).

The methodology proposed for verifying SIL is described in some recent papers [1, 2, 3]. Described above concept of SIL verification module is shown on Figure 11.

Presented module enables creating probabilistic models with *koon* subsystems' structures which may consist of different elements. Figure 12 illustrates main window of the ProSILer. It contains a main safety function information and more specific description. Next step is selection of mode of operation for SIS, i.e. "*demand mode*" as well as "*frequent or continuous mode*".

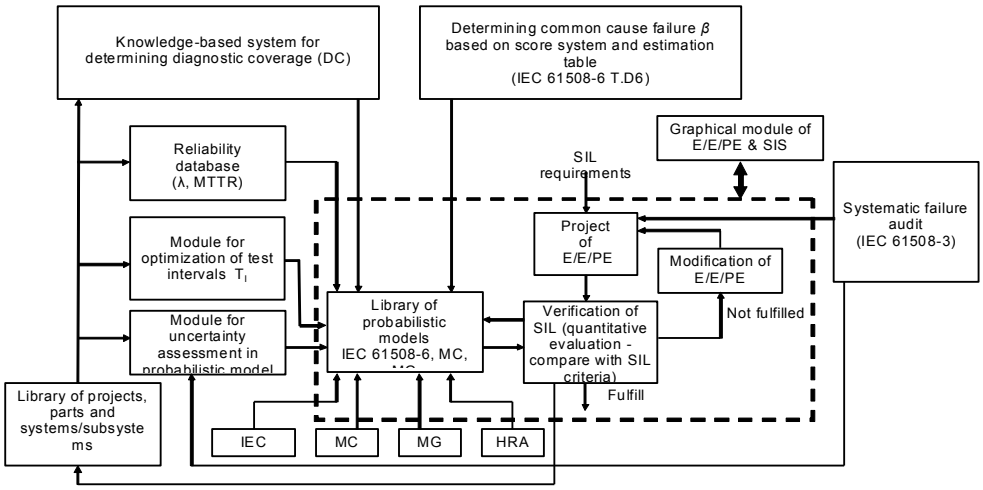


Fig. 11. Main idea of using ProSILer module [4]

Project engineer can choose one of three available methods of verification SIL and connected with them calculation algorithms: according to PN-EN 61508, minimal cut sets or simplified equations [2, 5, 8, 9, 11].
A button "*Edit hardware structure*" makes possible entering into a new window with tools designed for creating functional safety probabilistic models.

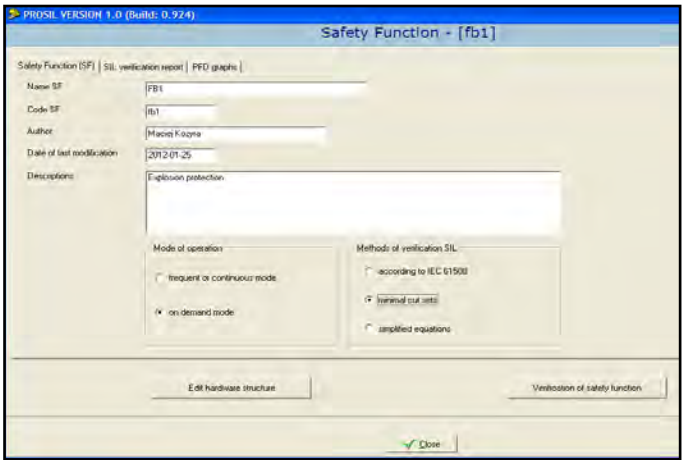


Figure 12. Main window of verification module

The project of SRF is displayed as a reliability block diagram with subsystems sections: sensor, logic (e.g. PLC, safety PLC) and actuators subsystems. The project window should be filled by engineer with some of the modules and elements available in application. After proper creation of SIS structure it can be tested by special function called: "Test structure" (see fig. 13).

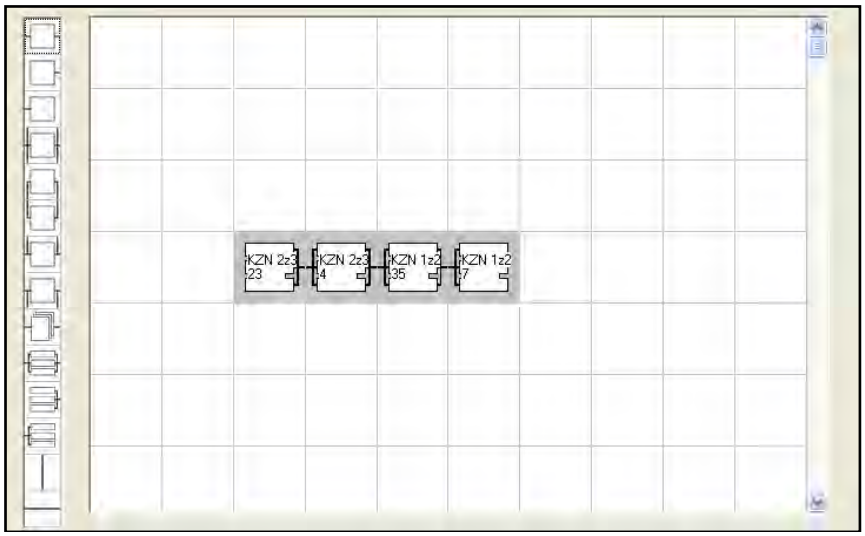


Fig. 13. Block diagram with representation of SIS hardware architecture

Reliability data for single element in the SIS structure which implements safety related function, e.g. temperature sensor, may be input in manual or automatic (from core data base ProSILcdb) manner [4, 10]. If the accurate DC (diagnostic coverage) data is available than it can be written in "*DC [%]*" input field. When that kind of data isn't present, the ProSIL software helps obtaining diagnostic coverage by special module called "*DC assessment*". In figure 14 the window for single element data is presented.

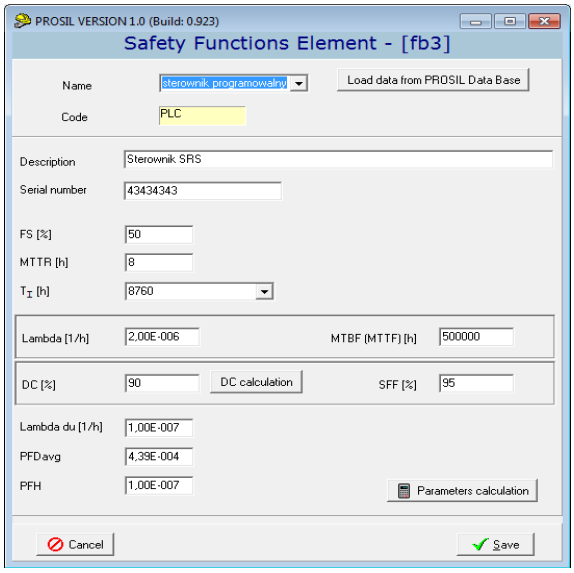


Figure 14. Reliability data for single element in the SIS structure

In the main window of SIS structure the right mouse click on "*k oo n"* element enables advanced options for this kind of structure. It is presented in figure 15.
The *koon* structure has higher priority over other single elements in the modeled system. It consists of identical elements with a specific probabilistic model. However the *koon* structure may included different elements (Fig. 15).

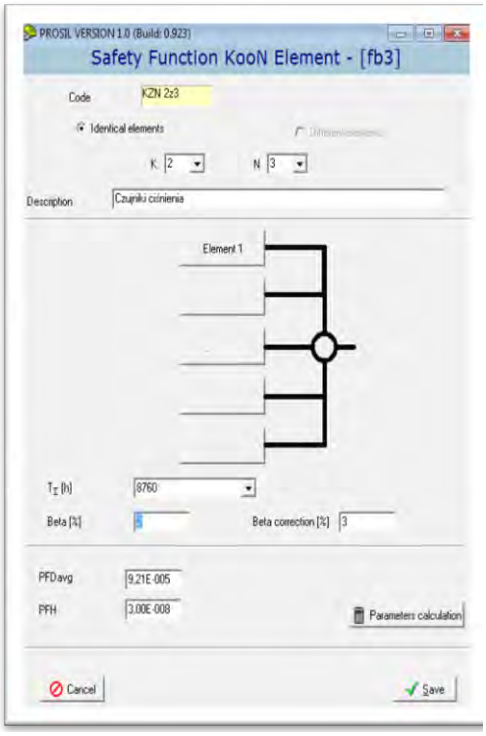


Fig. 15. KooN structure for identical elements

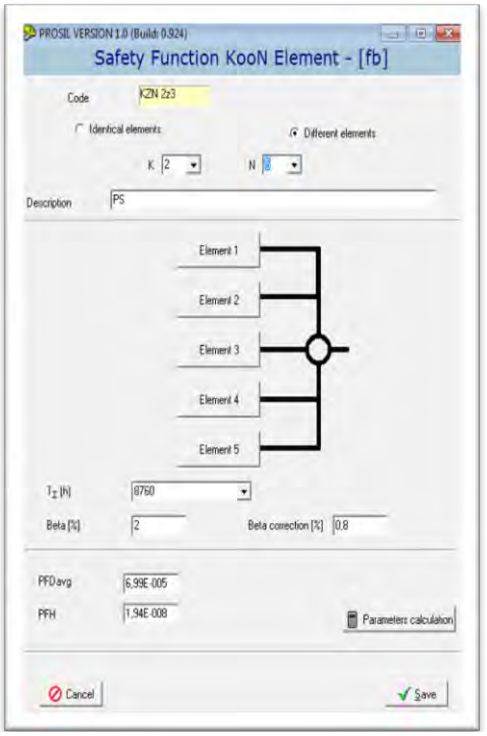
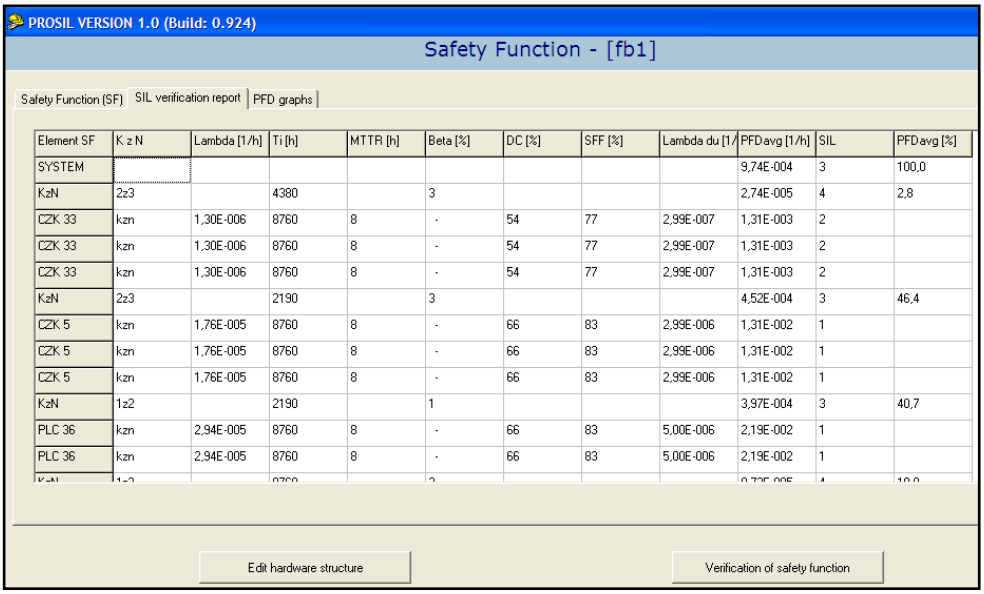


Fig. 16. KooN structure for different elements

As was mentioned above, the probabilistic model is built by single elements like: valves, pumps, sensors, servos, actuators, I/O modules, CPUs, communications channels, etc.) which are connected with nodes. The model should be created from left to right (see Fig. 13). After complete of SIL verification process a report table is accessible (the results are presented separately for SRF demand mode of operation and frequent or continuous mode). It can be viewed in figure 17.
The SIL verification process gives an access to some important results: values of PFD(t), PFD_{avg}, PFH for system, subsystems and all subsystems' elements. Another option of ProSILer module is creation of graph of functions PFD(t) and PFD_{avg}.



Element SF	K z N	Lambda [1/h]	Ti [h]	MTTR [h]	Beta [%]	DC [%]	SFF [%]	Lambda du [1/	PFDavg [1/h]	SIL	PFDavg [%]
SYSTEM									9,74E-004	3	100,0
KzN	2z3		4380		3				2,74E-005	4	2,8
CZK 33	kzn	1,30E-006	8760	8	-	54	77	2,99E-007	1,31E-003	2	
CZK 33	kzn	1,30E-006	8760	8	-	54	77	2,99E-007	1,31E-003	2	
CZK 33	kzn	1,30E-006	8760	8	-	54	77	2,99E-007	1,31E-003	2	
KzN	2z3		2190		3				4,52E-004	3	46,4
CZK 5	kzn	1,76E-005	8760	8	-	66	83	2,99E-006	1,31E-002	1	
CZK 5	kzn	1,76E-005	8760	8	-	66	83	2,99E-006	1,31E-002	1	
CZK 5	kzn	1,76E-005	8760	8	-	66	83	2,99E-006	1,31E-002	1	
KzN	1z2		2190		1				3,97E-004	3	40,7
PLC 36	kzn	2,94E-005	8760	8	-	66	83	5,00E-006	2,19E-002	1	
PLC 36	kzn	2,94E-005	8760	8	-	66	83	5,00E-006	2,19E-002	1	

Fig. 17. SIL verification report window

The graphs may be presented in logarithm scales (see Fig. 18).

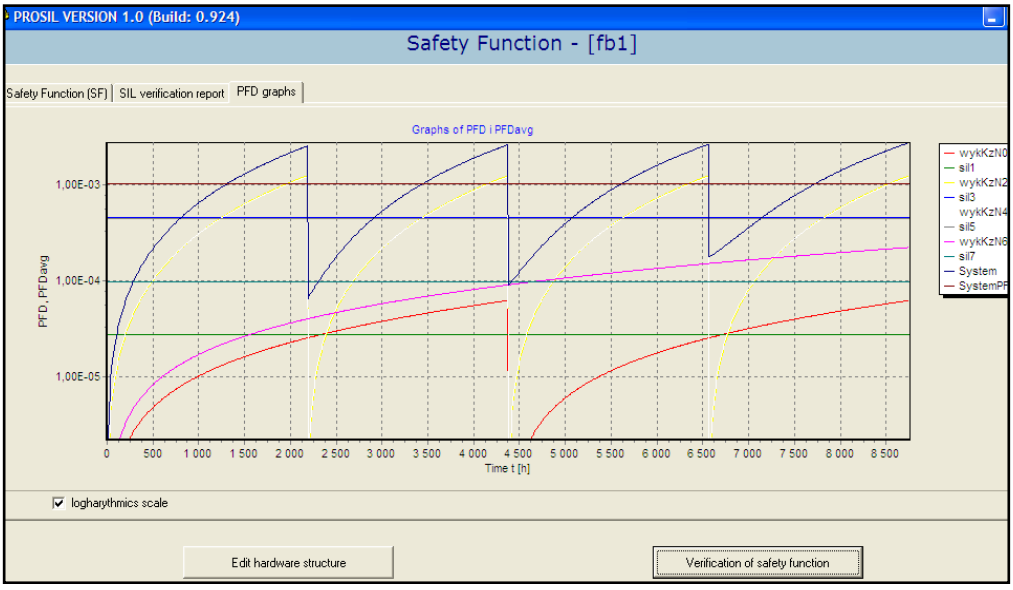


Fig. 18. PFD(t) and PFDavg graphs in logarithm scales

The last window of ProSILer is summary results of SIL verification for all described safety related functions in the project. It is presented in figure 19.

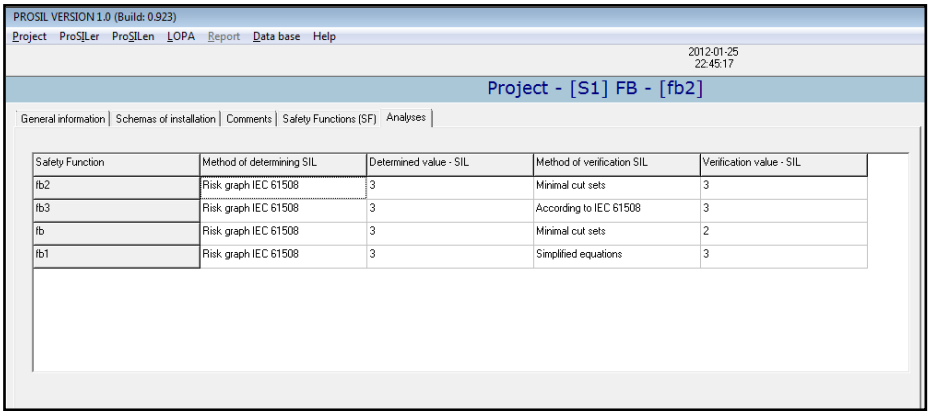


Fig. 19. Summary results of SIL verification

5. Conclusion

Due to a complexity of functional safety concept and its usage in practice, the ProSIL software was made as an alternative tool for particular computer aided safety analyses. It is designed especially to ensure easier access to functional safety analysis methods for each stage of safety-related systems' life cycle with main accent laid on processes of determining required safety integrity level for safety-related functions as well as verifying its level for designed hardware which implements those functions. A conceptual design of ProSIL assumes that the process of designing safety-related systems (SRSs) should be based on PN-EN 61508 and PN-EN 61511 framework

A special module designed for determining requirements for safety-related functions (SRFs) consists of several methods and tools intended for calibrating them in case of proper further risk reduction analyses. A module for verifying SIL is based on reliability block diagrams. They let users of application building complex probability models of hardware structures.

Moreover, the ProSIL software contains also a LOPA module which is designed especially to create reliable layers of protection datasheets with results of this kind of analyses (not described in this paper). The new aspects of including the security issues in the functional safety analyses are also under development and they are implemented in new version of ProSIL-EAL software. It will also include some human factors issues (like HRA) in determining and verification SIL modules.

4. Literature

[1] Barnert T., Kosmowski K.T., Sliwinski M. Methodological aspects of functional safety assessment. Zagadnienia Eksploatacji Maszyn. Instytut Technologii Eksploatacji - Panstwowy Instytut Badawczy. 2006

[2] Barnert T., Sliwinski M. Methods for verification safety integrity level in control and protection systems. Functional Safety Management in Critical Systems. Fundacja Rozwoju Uniwersytetu Gdanskiego. Gdansk, 2007

[3] Barnert T., Kosmowski K.T., Sliwinski M. Determining and verifying the safety integrity level of the control and protection systems under uncertainty. ESREL 2008 European Safety & Reliability Conference, Valencia, 2008.

[4] Barnert T., Kosmowski K.T., Śliwiński M.: A knowledge-based approach for functional safety management, Taylor & Francis Group, European Safety & Reliability Conference ESREL, Praga, Czechy 2009.

[5] Barnert T., Kosmowski K.T., Sliwinski M., Integrated functional safety and security analysis of process control and protection systems with regard to uncertainty issue, PSAM 2010, Seattle, USA, 2010

[6] PN-EN 61508. Functional safety of electrical/electronic/programmable electronic safety – related systems. Parts 1-7. International Electrotechnical Commission (IEC), 2010

[7] PN-EN 62061. Safety of machinery – Functional safety of safety-related electrical/ electronic and programmable electronic control systems (E/E/PE). International Electrotechnical Commission (IEC), 2005

[8] PN-EN 61508. Functional safety of electrical/ electronic/ programmable electronic (E/E/PE) safety related systems. Parts 1-7. International Electrotechnical Commission (IEC), 1998

[9] PN-EN 61511. Functional safety: Safety instrumented sys-tems for the process industry sector. Parts 1-3. International Electrotechnical Commission (IEC), 2000

[10] Reliability Data for Safety Instrumented Systems - PDS Data Handbook, 2010

[11] Reliability Prediction Method for Safety Instrumented Systems - PDS Method Handbook. SINTEF, 2010

[12] Layer of Protection Analysis, Simplified Process Risk Assessment. American Institute of Chemical Engineers, Center for Chemical Process Safety. New York, 2000

Acknowledgements

The authors wish to thank the Ministry for Science and Higher Education in Warsaw for supporting the research and the Central Laboratory for Labour Protection – National Research Institute (CIOP-PIB) for cooperation during preparation and realization of a research project VI.B.10 for 2011-13 concerning the safety management of hazardous systems including the functional safety aspects as well as human reliability and security issues.

M.Sc. Tomasz Barnert, *received M.Sc. in 2005 from Gdansk University of Technology (GUT). From 2006 researcher and since 2008 assistant at Faculty of Electrical and Control Engineering, GUT. Specialization: functional safety aimed at risk assessment and determining required safety integrity level (SIL); security of distributed control and protection systems.*

Prof. Kazimierz Kosmowski, *received Ph.D. in 1981 and D.Sc. in 2003 from Gdansk University of Technology (GUT). Since 2006 to 2012 the manager of Division of Control Eng. at Faculty of Electrical and Control Eng. and since 2007 a vice-chairman of Polish Safety and Reliability Association (PSRA). Specialization: reliability and safety of technical systems, human reliability, functional safety of programmable control and protection systems.*

Ph.D. Marcin Śliwiński*, received Ph.D. in 2006 from Gdansk University of Technology (GUT). From 2001 researcher and since 2006 lecturer at Faculty of Electrical and Control Engineering, GUT. Specialization: functional safety of control and protection systems aimed at SIL verification, probabilistic modeling of technical systems*