Barnert Tomasz

Kosmowski Kazimierz T.

Śliwiński Marcin
Gdańsk University of Technology, Gdańsk, Poland

Knowledge-based functional safety management using ProSIL software

Keywords

hazardous plants, functional safety management, control and protection systems, safety integrity level (SIL)

Abstract

In the article the ProSIL software for computer aided functional safety management is presented. The software consists of three modules for the determination of the required SIL level (ProSILen) and verification of the SIL level (ProSILver). In the ProSIL the calibrated knowledge-based risk graph method for determining the required safety integrity level (SIL) of the safety functions identified in hazard analysis is implemented. The SILs are then verified for safety-related control and protection systems implementing relevant functions with regard to random failures and potential systematic failures. The assessment methods are compatible with international standards IEC 61508 and IEC 61511. Some current challenges and methodological issues concerning knowledge-based functional safety management in life cycle are also discussed.

1. Introduction

Modern industrial plants are equipped with complex programmable control and protection systems operating usually within a computer network. For designing of such systems a functional safety concept [5], [10], [11] is now widely of interest [6], to be implemented in various industrial sectors, e.g. machinery [8] and the process industry [7].

The primary objective of functional safety management is to reduce the risks associated with operation of hazardous installation to an acceptable level introducing a set of defined safety functions (SFs) that are to be implemented using programmable control and protection systems, e.g. electric/electronic/programmable electronic (E/E/PE) safety-related systems (S-RSs) [6], basic process control systems (BPCSs) or safety instrumented systems (SISs) [7].

Taking into account expectations of functional safety analysts and process industry engineers it is worthwhile to develop and provide an useful in practice computer-aided knowledge-based system for supporting the functional safety analysis and management in system life cycle. Such prototype knowledge-based system has been designed under name ProSIL software. It supports relevant functional safety analyses and their documenting during the design and operation of the E/E/PE, BPCS and SIS systems taking into account the requirements and criteria given in international standards IEC 61508 [6], IEC 61511 [7], IEC 62061 [8].

The SIL software supports the determination of required safety integrity level SIL of SFs using the risk graph or risk matrix method [1], [2], [3], [4]. The required SIL can be also taken from a regulatory institution and documented for given safety function. Then the computer aided verification of determined SIL is to be carried out for the architectures of E/E/PE or SIS that implement safety-related functions.

Due to complexity of analyses, to overcome difficulties in decision making under significant uncertainties [9] we propose to adapt in the ProSIL some elements of the risk informed decision making (RIDM) methodology [12]. The methodology proposed is compatible with the functional safety management methodology described in IEC 61508. It enables the decision making in a more systematic way. In the methodology proposed the overall functional safety management (FSM) in life cycle includes the RIDM and continuous risk assessment (CRA) based on performance monitoring.

A module of layer of protection analysis (LOPA) [13] is now at final developing stage that will enable systematic analyses of protecting barriers, which generally can be to some extend dependent. Selected from mentioned above modules are described in more details below in this article.

2. Outline of ProSIL knowledge-based software modules

Simplified scheme and functional scope of the knowledge-based system for supporting the SIL determination and verification for safety functions is shown in *Figure 1*.

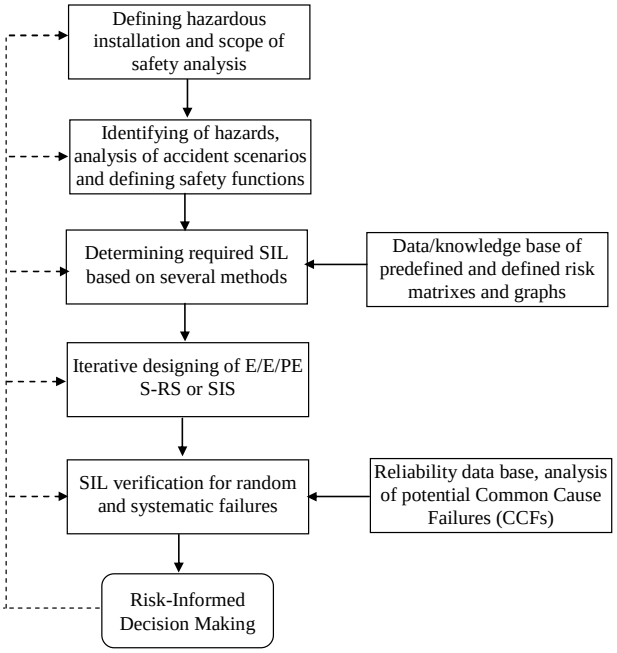

Figure 1. Main modules of the functional safety analysis system ProSIL

The ProSIL consists of several modules covering different aspects of functional safety analysis. There are modules for hazard identification and analysis of accident scenarios for defining of safety-related functions. Next module is for supporting the risk analysis and assessment, which allow determining required SIL for consecutive safety functions. The final module was developed for verification of SIL for architectures of E/E/PE S-RSs or SISs considered.
The ProSIL software provides mechanisms to create projects with many safety functions defined. It consists of three macro modules for: determining SIL (ProSILen), verifying SIL (ProSILer) and LOPA analysis module [1], [2], [3]. Each new created project has detailed description and possibility of saving its parameters into integrated knowledge/database.

Figure 2 presents main window of newly defined or selected project from a data/knowledge base. From this window there is a direct access to mentioned above modules. For each defined safety function being implemented using E/E/PE S-RS or SIS there is an option to enter proper module directly for consecutive steps of the analysis.

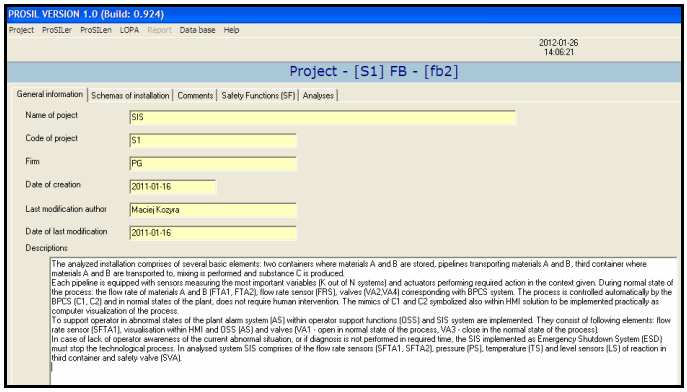

Figure 2. ProSIL software main window

The user of the software has direct insight into some overall project information as well as attached schemas and specific P&ID (*piping and instrumentation diagram*) of analyzed system or subsystems (see *Figure 3*).

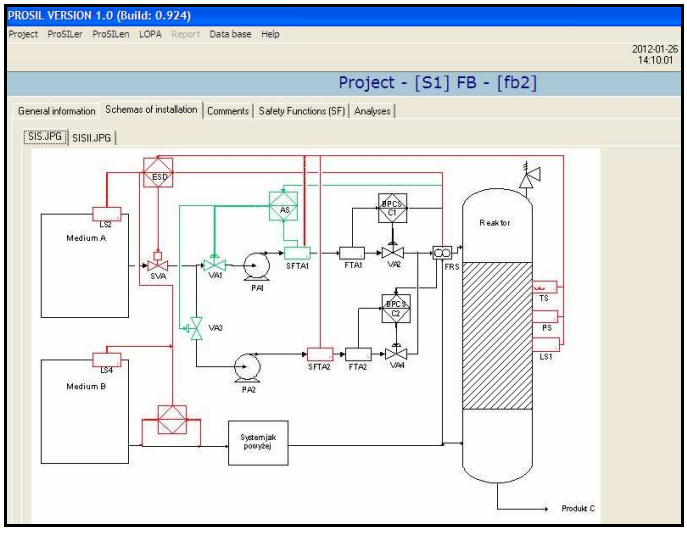

Figure 3. Installation P&D for functional safety analysis

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

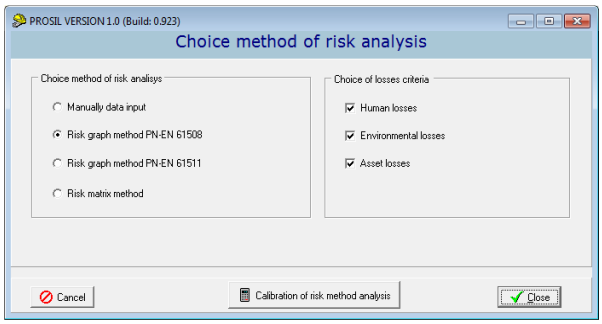

Figure 4. Window for selecting one of the available SIL determination methods

Each new function is defined within defined and characterised project (*Figure* 5).

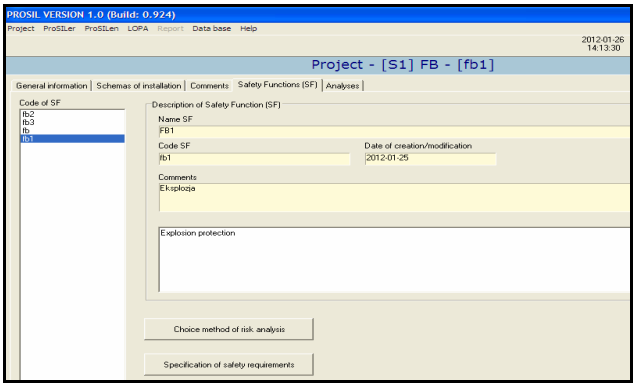

Figure5. Window for defining new safety function

The data documented in the ProSIL modules can be printed out during analyses or as a part of the final documentation of given project.

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 (SIL) of given safety function. There are available several methods to determine SIL for given safety function. Some of more popular ones in industrial practice are [6], [7], [13]:

- 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 IEC 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 hazardous event can differ for some accident scenarios. That is why a new extended approach was proposed in works [1], [2], [3], [4], 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.

Determining of required SIL 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* 6. The fundamental window of calibrating the selected exemplary methods is illustrated in *Figures 7* and *8*.

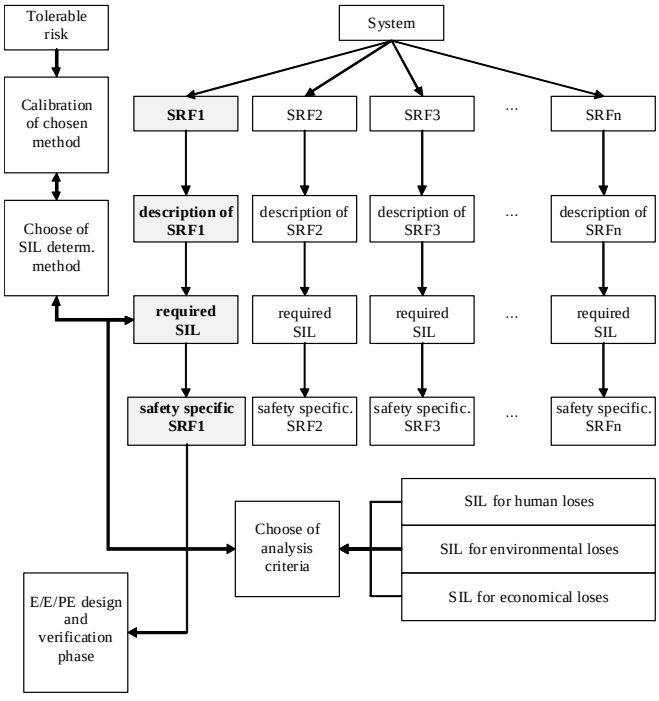

Figure 6. Main idea of using ProSILen module

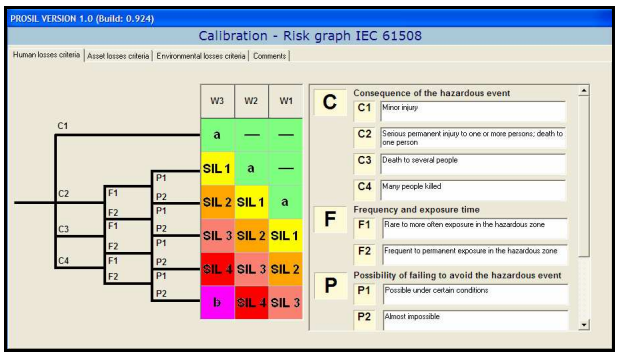

Figure 7. Calibration of the IEC 61508 risk graph method (human losses)

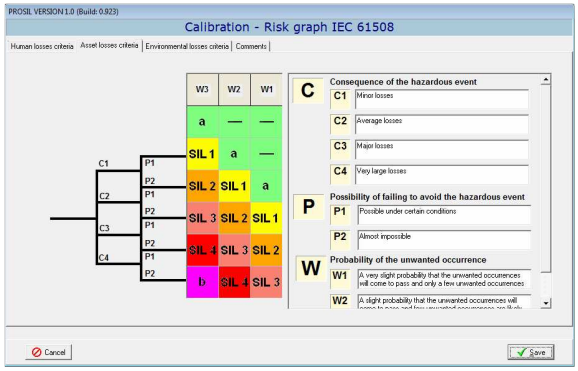

Figure 8. Calibration of the IEC 61508 risk graph method for assets losses

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 *Figure* 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.

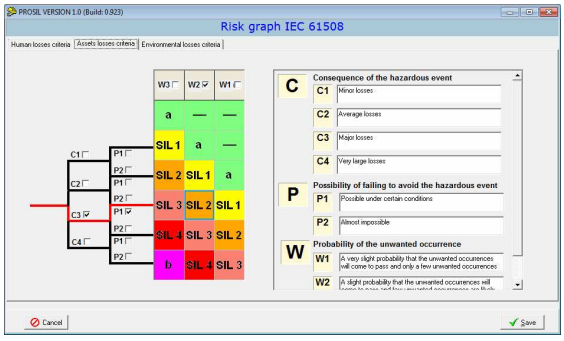

Figure 9. Determining of required safety integrity level for assets losses

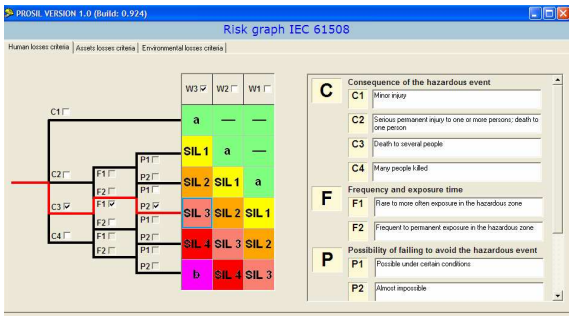

Figure 10. Determining of required safety integrity level for human losses

4. Safety integrity level verification

Computer aided SIL verification module ProSILer (*Figure 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 IEC 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 models using β-factor method (parameter evaluated from a knowledge-base). 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 methods proposed for verifying SIL are described in papers [1], [3]. Described above concept of SIL verification module is shown in *Figure 11*.

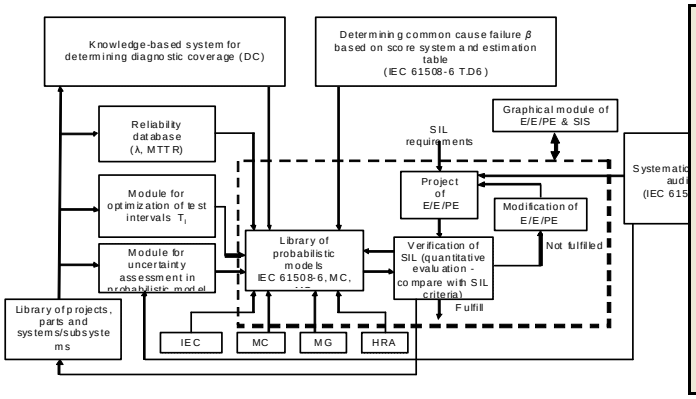

Figure 11. Main idea of using ProSILer module

Presented module enables creating probabilistic models with *KooN* subsystems' structures which may consist of different elements. *Figure 12* shows 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*" of E/E/PE system operation.
Project analyst can choose one of three available methods of verification SIL and associated with it model and calculation algorithm: according to IEC 61508, based on minimal cut sets or using simplified equations [1], [2], [3].

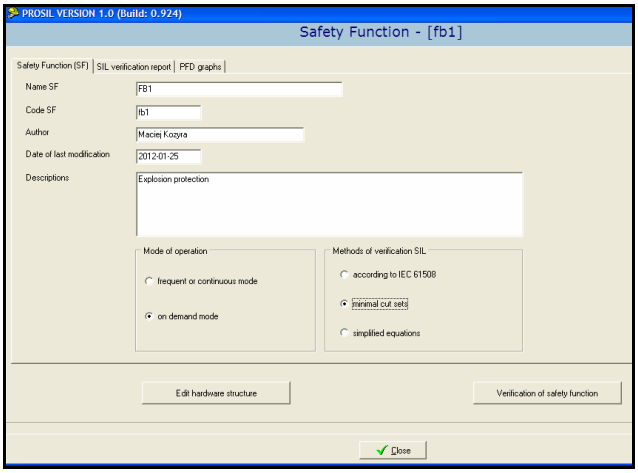

Figure 12. Main window of verification module

The E/E/PE S-RS or SIS is defined using special reliability block diagram with subsystems of: sensors, logic (e.g. safety PLC) and actuators. After proper creation of E/E/PE S-RS or SIS structure see *Figure 13*) it can be tested by special function called: "Test structure".

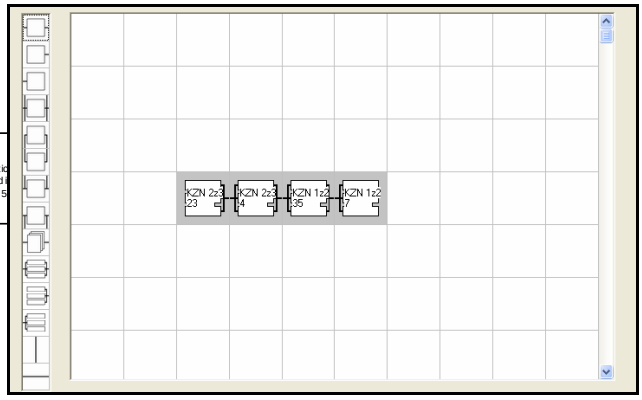

Figure 13. Block diagram with representation of SIS hardware architecture

Reliability data for single element in the E/E/PE S-RS or SIS structure which implements safety related function, e.g. temperature sensor, is introduced from core data base ProSILcdb) or manually, e.g. from he literature [14], [15]. If the accurate DC (diagnostic coverage) data is available than it can be written in "*DC [%]*" input field. When that kind of data is not available the ProSIL software helps obtaining diagnostic coverage by special module called "*DC assessment*". In *Figure 14* the window for defining given element reliability data is presented.

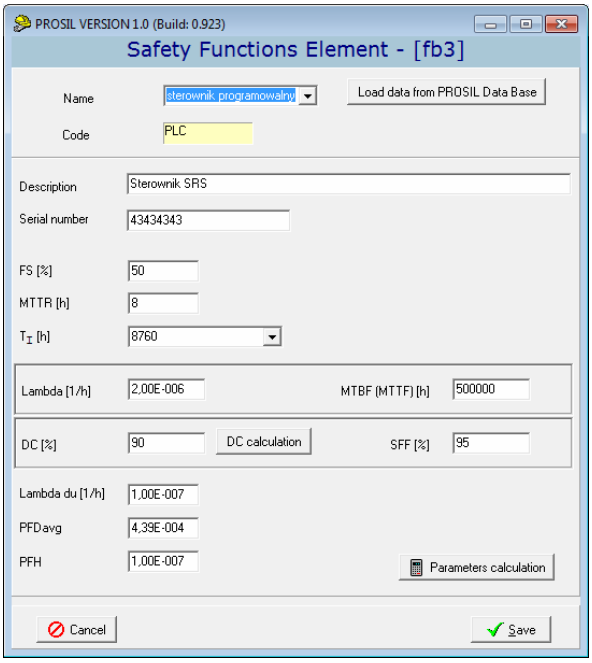

Figure 14. Reliability data for given element of E/E/PE S-RS or SIS

In the main window of E/E/PE S-RS or SIS structure the right mouse click on given system enables advanced option of its defining as presented in *Figure 15*.
The KooN structure has higher priority over single elements in the modeled system. It consists of

identical elements with a specific probabilistic model. However the KooN structure may include also different elements *(Figure 16*).

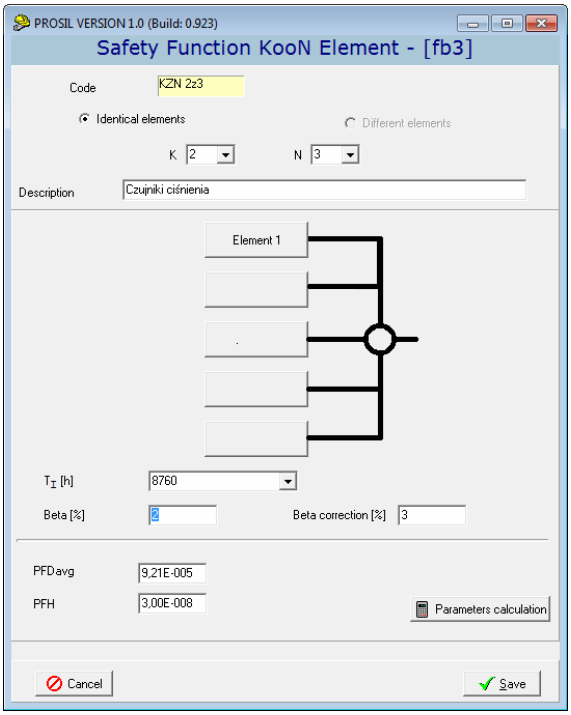

Figure 15. KooN structure of identical elements

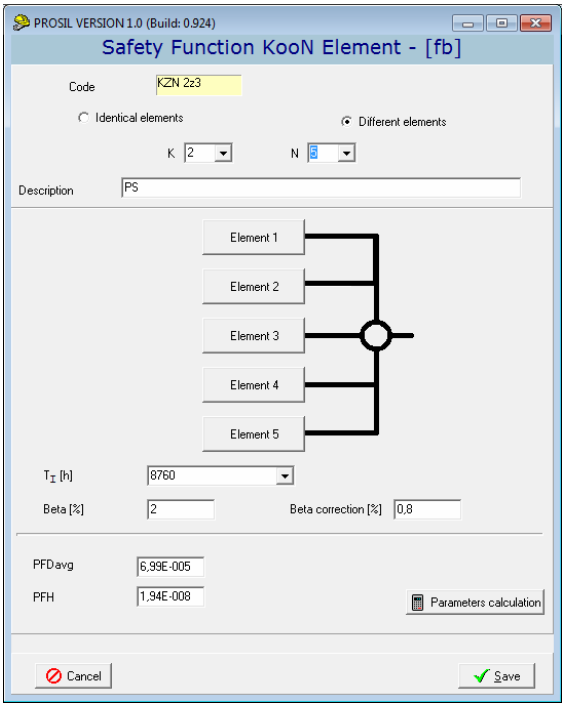

Figure 16. KooN structure of different elements

As it was mentioned above, the probabilistic model can be developed using single elements like: valves, pumps, sensors, servos, actuators, I/O modules, CPUs, communications channels, etc.) which are connected with nodes. The model is to be created from left to right (see *Figure 13*).
After completing the SIL verification process a report table is generated including the results separately for low demand mode of operation and frequent/continuous mode *(Figure 17*).

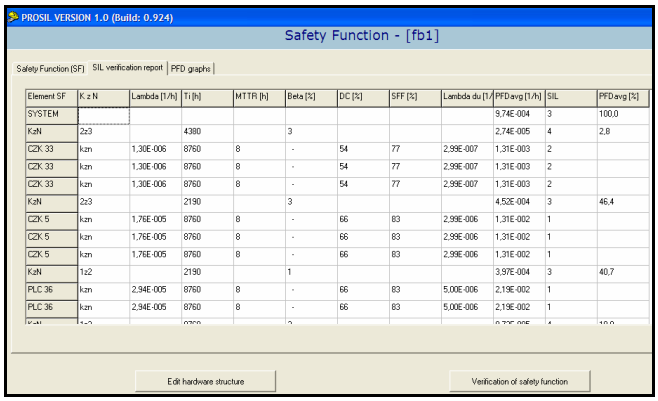

Figure 17. Report window of SIL verification

The SIL verification process gives an access to some important results: values of *PFD(t)*, PFD_{avg}, *PFH* for system, subsystems and all elements. Another option of ProSILer module is creation of graph of functions PFD(t) and PFD_{avg}. The graphs may be presented in linear and logarithm scales (*Figure 18*).

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

The last window of ProSILer is a summary of results of SIL verification for all described safety functions defined in the project *(Figure 19*).

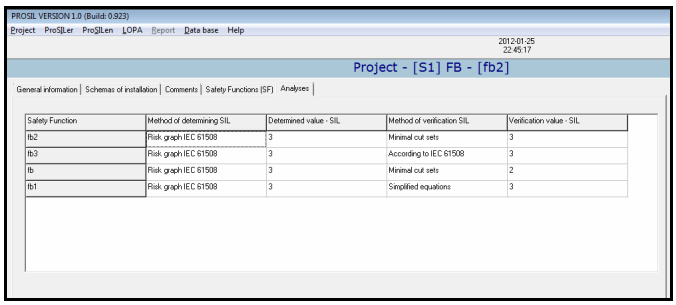

Figure 19. Window with summary of SIL verification results

5. Functional safety management with regard to RIDM framework

A concept of risk-informed decision making (RIDM) has been developed at some regulatory and research institutions of nuclear industry in USA. In the safety philosophy created the importance of addressing uncertainties as an integral part of decision-making with regard to the results of *probabilistic risk assessment* (PRA) has been emphasized.
Taking into account these principles some main areas of functional safety-related decision making were identified, which are shown in *Figure 20*. As it was mentioned, nowadays the programmable control and protection systems operating in networks play an important role in maintaining high performance and safety of many technical systems, in particularly in complex hazardous plants. Therefore, the relevant risk-informed analyses performed for identification of more important factors influencing performance and risk should be of a considerable interest for operators and regulators [12].

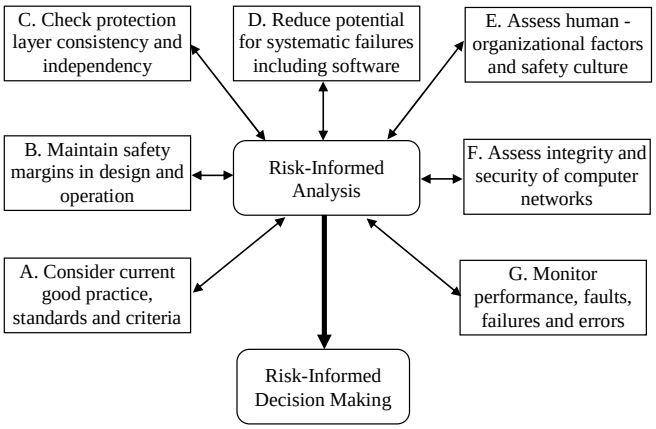

Figure 20. Main areas of functional safety analyses for decision making

In complex technical system different types of subsystems are distinguished and their malfunctions can be caused by hardware, software and human components. Their operation is influenced by various factors: environmental, technical and human. Human errors are rooted in organisational deficiencies, so potential causes of human failures should be carefully considered in probabilistic modelling of these systems.
The RIDM methodology can be useful in functional safety analysis because the analysts use the qualitative and quantitative information in developing relevant risk models and probabilistic models of E/E/PE S-RSs or SISs. These models are significantly influenced by expert opinions and assumptions. The ProSIL software is very useful for functional safety assessment extended to sensitivity analysis of changing parameters of the models on results obtained.

6. Conclusion

In the article capabilities of prototype software package ProSIL for computer aided functional safety management are described. This software tool comprises several modules and databases to perform functional safety analyses for complex industrial installations.
The software package enables defining accident scenarios using results from HAZOP study or simplified event trees with consideration of defined hazards and initiating events. The analyst has possibility to construct risk matrix appropriate for analyzed accident scenarios. In application there exists also a library of risk graphs with possibility to define and modify risk parameters.
ProSIL gives specialists opportunity to determine a set of safety functions associated with analyzed scenarios in order to mitigate risk to tolerable level. Determining of required safety integrity level SIL for selected safety function can be performed with utilization of the risk graph and risk matrix methods.
As the next step the architecture of hardware for implementing safety functions is modeled by reliability block diagram (RBD) method for distinguished subsystems. The subsystems have generally *KooN* configuration consisting of the same or different elements.
The ProSIL contains also a library of probabilistic models of subsystems consistent with IEC 61508 and extended models calculated with utilization of minimal cut set technique based on RBD or fault tree.
The basic version of this software includes general database of reliability parameters with flexible updating possibility. The second option is to use own data from industrial experience with indication of data sources.
The advantage of ProSIL software is also possibility to assess and optimise the time intervals between testing of subsystems within E/E/PE S-RS or SIS. The module for verifying SIL enables determination and graphical representation of probability of failure on demand PFD(t) and calculating average value PFD_{avg} of E/E/PE S-RSs and SISs consisting of subsystems for two operation modes.
Among described above options, the ProSIL module for evaluating the quality and integrity of the software of programmable safety-related systems is at implementing stage. It is based mainly on

recommendations of the IEC 61508-3, which specifies a set of techniques and methods of quality assurance which should be applied during the various phases of software life cycle. The aim of this module is to assist performing tasks in the process of inspection and testing of the software by presenting the techniques and measures recommended for the required SIL level, collecting the data from inspection process and printing the appropriate reports.

Due to a complexity of functional safety analysis and its importance in industrial practice, the ProSIL software seems to be a useful tool for computer aided functional safety analyses. It is designed to enable easy access to functional safety analysis models on consecutive stages of functional safety management in life cycle.

The ProSIL is in final stage of its development. At present the layers of protection analysis (LOPA) method compatible with IEC 61511 and human reliability analysis (HRA) using SPAR-H method [16] is tested. New aspects of including the security issues in the functional safety analyses are also under development to be implemented in a new version of ProSIL-EAL software.

Acknowledgments

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 the 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.

References

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

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

[3] Barnert, T., Kosmowski, K.T. & Śliwiński, M. (2009). A knowledge-based approach for functional safety management. Taylor & Francis Group. *Proc. European Safety & Reliability Conference ESREL*, Prague.

[4] Barnert, T., Kosmowski, K.T. & Sliwinski, M. (2010). Integrated functional safety and security analysis of process control and protection systems with regard to uncertainty issue. *Proc. PSAM 2010*, Seattle.

[5] Gruhn, P., Cheddie, H. (2006). *Instrumented Systems: Design, Analysis and Justification.* ISA – The Instrumentation, Systems and Automation Society.

[6] IEC 61508 (2010). Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems, Parts 1-7. International Electrotechnical Commission. Geneva.

[7] IEC 61511 (2003). Functional safety: Safety Instrumented Systems for the Process Industry Sector. Parts 1-3. International Electrotechnical Commission, Geneva.

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

[9] Kosmowski, K.T. (2004). Modelling and uncertainty in system analysis for safety assessment. *Proc. of the International Conference on Probabilistic Safety Assessment and Management, PSAM 7 - ESREL '04*, Berlin, Springer.

[10] Kosmowski, K.T. (2006). Functional Safety Concept for Hazardous System and New Challenges. *Journal of Loss Prevention in the Process Industries* 19(1), 298-305.

[11] Kosmowski, K.T. (Ed.) (2007). *Functional Safety Management in Critical Systems.* Gdansk University of Technology. Publishing House OF Gdansk University (Wydawnictwo Fundacji Rozwoju Uniwersytetu Gdańskiego).

[12] Kosmowski, K.T., Barnert, T., Śliwiński, M. & Porzeziński, M. (2012). Functional Safety Assessment within the Risk Informed Decision Making Process. *Proc. PSAM 11 – ESREL 2012*, Helsinki.

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

[14] SINTEF (2010a). Reliability Prediction Method for Safety Instrumented Systems - PDS Method Handbook.

[15] SINTEF (2010b). Reliability Data for Safety Instrumented Systems - PDS Data Handbook.

[16] SPAR-H (2005). Human Reliability Analysis Method, NUREG/CR-6883, INL/EXT-05-00509, US NRC.