CHOOSING FMECA-BASED TECHNIQUES AND TOOLS FOR SAFETY ANALYSIS OF CRITICAL SYSTEMS

Oleg ILLIASHENKO and Eugene BABESHKO

Abstract: There is no universally valid approach for deciding on a technique for reliability analysis. This paper presents a methodology for assessing safety and choosing the most appropriate FMECA-based technique, as well as tools supporting the implementation of this technique.

Keywords: Failure Modes, Effects and Criticality Analysis, FMECA, safety analysis, decision-support.

Introduction

Safety analysis is an important and quite complicated part of critical systems development life cycle. Terms and rules of safety analysis for electronic components are widely described in well-known ISO/IEC international standards series [1] and technical report.[2] Because of its complexity the risk of improper safety assessment takes place in most cases. Besides, incorrect information about safety of assessed objects could lead to risks of overestimation and risk of low estimation. In the first case the developer faces the challenge of spending more resources than it is necessary to provide required level of safety. In the latter case failure probability of hypothetic system is significantly high, because of incorrect information. Besides, there is a lack of appropriate developers knowledge and good guidelines that simplify the selection process, which causes dependence on human factor. This in turn may lead to human made errors, company specific solution and unrepeatability of the whole process.

The risk of improper safety assessment could be caused by several reasons:

- chosen safety analysis technique is not suitable for I&CS safety analysis;
- incorrect use of chosen safety analysis technique (it is expected that this technique is appropriate for particular task).

INFORMATION & SECURITY. An International Journal, Vol.28, No. 2, 2012, 275-285.

There are a lot of well-known techniques that can be used for critical information and control systems (I&CS) dependability analysis and assessment of its attributes (e.g. FMEA – Failure Modes and Effects Analysis and its modifications, FTA – Fault Tree Analysis, HAZOP – Hazard and Operability Analysis, RBD – Reliability Block Diagram, MM – Markov Models, etc). Using these techniques it is possible to perform quantitative and/or qualitative assessment. Every assessment method or technique has its own pros and cons. FMEA is one of techniques that is often used. The process defined for FMEA addresses: (1) planning, (2) worksheet formats, (3) ground rules and assumptions, (4) coding system, (5) contributing information, (6) indenture level (including hardware and functional approaches), (7) failure definition, (8) identification of failure modes, (9) effects (local, sub-system and system level), (10) detection methods and corrective actions, (11) identification of corrective design and (12) severity classification. A number of publications describe the basic concept of FMEA.[3] Initially, FMEA should be performed during the design stage, but it also may be used throughout the life cycle of a product to identify possible failures as the system ages.

Failure mode and effect analyses may vary in the level of detail reported, depending upon the detail needed and the availability of information. As a development matures, assessment of criticality is added in what becomes a Failure Mode, Effects, and Criticality Analysis, or FMECA. The first application rules of this technique were declared as a military standard by the U.S. Department of Defense.[4] Nowadays FMECA procedure is regulated by a variety of international, national, company standards and other normative documents.[5]

Usually safety-critical systems are operated in harsh environment and cause different types of failures taking into account increasing of their multi-component complexity. On this basis there are two ways of safety analysis techniques improvement:

- to develop a new technique and tool to support this technique; this however is not the best way;
- to analyze existing techniques and tools, make a right choice of them in accordance to particular task, or combine use and further adaptation (or minimal remake).

The main idea of FMECA is the determination of all possible failure modes for I&CS as a whole, its subsystems or components. At the same time possible failure effects and failure causes are presented. The procedure is concluded with criticality assessments in “probability-consequences” space by special criticality matrix and optional specification for optimization actions. The aim of method is to recognize the risks and weak points of a system as early as possible in order to enable execution improvements in a timely manner.[6] Results of FMECA are usually presented in tables as ar-

ranged lists. Some modifications of FMECA-techniques in according to analyzing attributes are:

- Software FMECA (SFMECA) for components;
- Design FMECA (DFMECA) for processes;
- Intrusion-oriented FMECA (IMECA) for types of faults and influences, etc.

There are a lot of tools which support these methods and quantity of these tools is constantly increasing. The use of appropriate software tools can increase the integrity of the development process, and hence product safety by reducing the risk of introducing faults in the process.

Analysis of related works shows that combined usage of reliability and safety analysis techniques and tools is needed to be investigated. The familiarization of an organisation with FMECA goes under a number of stages.[7] Expanded FMECA provides solutions in risk priority definition and in comparing corrective actions.[8] The understanding of safety and reliability analysis techniques and their application, provides for efficient combined use in regard to safety-critical systems.[9] Program packages for reliability and safety analysis also evolved depending on the stage of programming evolution.[10]

The main goal of this study is to reduce the risk of incorrect safety assessment. The second goal is to examine FMECA-based techniques and supporting tools in order to propose a methodology of their choice according to a particular tasks and features of applications.

Selection of a safety analysis technique

Combination of techniques

As previously said we decided to use a Failure Modes, Effects and Criticality Analysis technique as base and widely used reliability analysis technique during the work on this paper. Software tools that are compared in the research support not only FMECA analysis but others. It is not sufficient to use only FMECA during critical I&CS analysis because of its restrictions:

- FMECA does not take into account multiple-failure interactions, meaning that each failure is considered individually and the effect of several failures is not accounted for;
- FMECA does not analyze dangers or problems that may occur when the system is operating properly;
- critical failure modes, causes, or effects that are not recognized by the designer(s) will not be addressed;

- human factors are not considered, etc.

Results of possible combination of techniques are shown in Figure 1. Results of FMECA and IMEA are used during further FTA (Fault Tree Analysis), RBD (Reliability Block Diagram), CCF (Common Cause Failure Analysis), and also during Markov Modelling. During RBD it is possible to use list of all components that can cause I&C system failure which has been obtained during FMECA. In FTA results of FMECA are used to get list of all possible failures. To perform Markov modelling it is required to know component's failure rates and recovery time so as to get state-to-state transitions. Finally in most cases I&CS operation may be analyzed using a Markov model.

Selection criteria

The following criteria for analysis and comparison of T&Ts were used in this research. Their features are briefly described below.

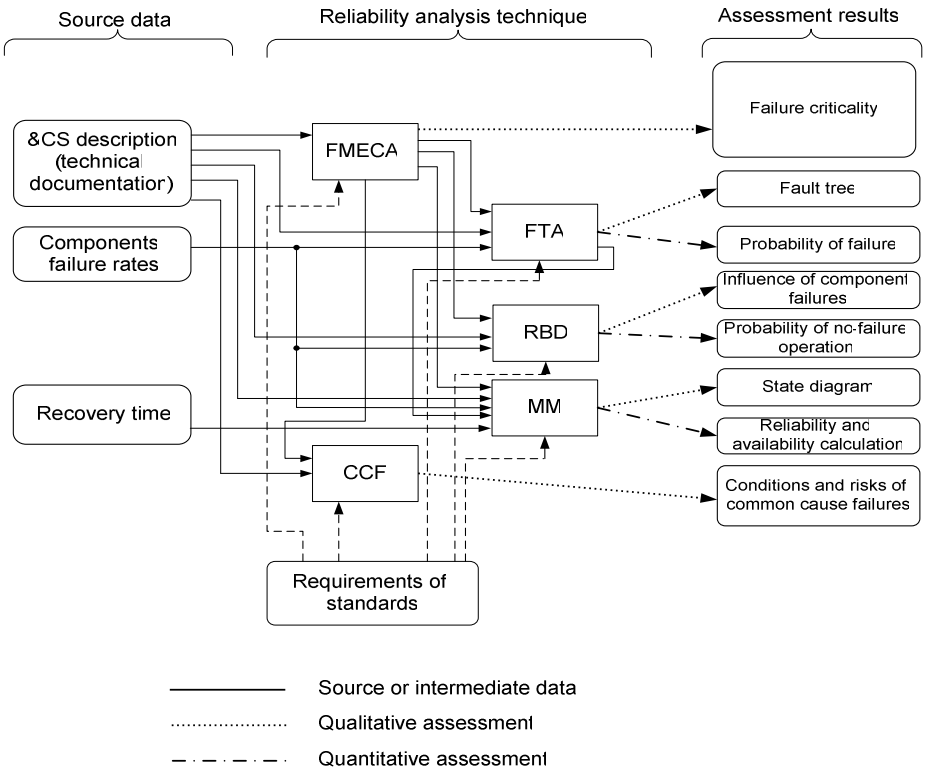

Figure 1: Combined use of reliability analysis techniques.

Compliance to normative documents. Nowadays most of companies work for standardization of their productions and software compliance to international standards is the cornerstone of technique and tool choice. The meaning of "compliance" is exact fulfilment of requirements and functions described in document. This criterion is divided to following: international ISO/IEC standards, guidance/procedures, national standards; industry standards, other normative documents.

Experience of application in industry. Field of software application in industry partially could show industrial area that software is suitable for.

Methods used for assessment of system NPP I&C safety. This criterion shows techniques, indexes, functions, etc. which results could be automatically calculated using reliability software.

Tool architecture/framework. Tool architecture largely determines the possibility of flexibility in using the software. The analysis showed that currently the following types of architectures are presented: desktop system (1 PC), server system, web-based system, multi-user system (two or more computers).

Reporting. Report about work that was done, its correctness, the right calculation of results, understandability are very important when using the results of the program. This criterion shows the possibility of saving data in certain file formats or it representation in the form of a report.

Vendor support Almost all companies provide customer support by phone, using webinars, e-mail correspondence, or by fax. Free technical support is available for a certain period (usually no more than 4 months).

The criteria listed above were selected to understand which software products are oriented to international (project-independent) needs and which are oriented to individual customers.

Selection sequence

To choose the most appropriate tool and technique we use simple mathematical apparatus. Our arguments are described below.

1. There is a set of techniques for reliability and safety analysis (e.g. FMECA, FTA, HAZOP, etc.):

$$MTechniques = \left\{Technique_i\right\}_{i=1}^{n_{Tech}}; \quad (1)$$

2. There is a set of tools (e.g. Reliability Studio, FMEA-Pro, RAM Commander, etc.):

$$MTools = \left\{Tool_j\right\}_{j=1}^{m_{Tool}} \quad (2)$$

Every tool has it's quantitative and qualitative characteristics (or criterion as previously determined, e.g. compliance to normative documents, reporting, vendor support, etc.):

$$Tool_j \sim \left\{ X_{1j}, ... X_{rj} \right\} \tag{3}$$

Every characteristic has a set of constraints:

$$X_{vj} = \left\{ \alpha, ..., \zeta \right\} \tag{4}$$

3. There is such tool, which includes a set of techniques from MTechniques set:

$$\forall Tool_j \sim \Delta_j MTechniques, \Delta_j MTechniques \subset MTechniques \tag{5}$$

There is an indicator, that indicates an existence of certain characteristic in the corresponding tool ("0" – characteristic is not available, "1" – characteristic is available):

$$\gamma_{jk} = \left\{ 0,1 \right\} \tag{6}$$

This model can be represented as a Boolean matrix (Tool-Technique). An example of such matrix is shown in Table 1.

Table 1. An example of "Tool-Technique" matrix.

		Tools			
		Tool1	Tool2	Tool3	Tool4
Techniques	Technique1	***1***	***1***	0	0
	Technique2	0	***1***	***1***	0
	Technique3	***1***	0	0	***1***
	Technique4	0	0	***1***	0

Thus a verbal task can be formed in the following way:

> *It is necessary to choose one or several such tools Tool* from MTools set which cover required subset of MTechniques set and other required characteristics and provide minimal optimal criterion value.*

There can be different combinations of characteristics X for coverage task solving. They are listed below:

$X_{1j} \geq X_{required}$, e.g. "MTTF must be more than 50000 hours";

$X_{assessed} \leq X_{2j}$, e.g. "Time of analysis must be less than 30 minutes";

$X_{3j} \in X_l$, e.g. "Average probability of failure on demand must be calculated as part of IEC 61508 compliance";

$X_{rj} \to \min$ - Optimality condition (e.g., “The lowest cost”).

As an example we solve task from Table 1 and define more appropriate Technique and Tool. As optimality condition we will use the tool cost.

The first step is to write a function using discrete mathematics from Boolean matrix:

$$F = (T_1 \cup T_3) \cap (T_1 \cup T_2) \cap (T_2 \cup T_4) \cap T_3 = (T_2 \cup T_1 \cap T_4) \cap T_3 = T_2 \cap T_3 \cup T \cap T_3 \cap T_4 \quad (7)$$

The formula (7) in fact is Conjunctive Normal Form. So we receive two sets of tools:

$$\Delta M * T_1 = \{T_2, T_3\}, \Delta M * T_2 = \{T_1, T_3, T_4\} \quad (8)$$

Next step is choosing of set that meets optimality criteria (that has the lowest cost).

If in the end of this algorithm we still have several techniques and tools that comply to initial requirements, the necessity of an Expert Systems will be necessary.

Table 2 (a and b) shows appropriate tools and criteria for FMEA-analysis (and its modifications). During work on this paper, about 20 software tools for reliability and safety analysis, as well as many techniques were analyzed. Results of analysis of Tools and Techniques (T&T) are presented in matrix form. This matrix could be used for Decision-Making Tool as the source of input data.

Decision Support System

The proposed technique is implemented as special tool for decision making. This tool consists of database of tools and techniques, database of standards, logic modules of T&T choosing, graphical interface, etc. Figure 2 shows simple model of this tool.

It is also planned to create a Web-service to support decision-making in choosing methods of reliability analysis. The proposed technique was used for development of company standard CStd 66 (RPC Radiy, 2010). This guide contains requirements and procedures of FMECA analysis of developed and produced NPP I&C systems based on RADIY platform.

Conclusion

To assess safety of I&CS it is not enough to use only one of known analysis technique. Combined usage of different methods and further methods' enhancements are possible solutions. An approach of “technique of techniques’ choosing” for I&C systems safety assessment is proposed. The importance of right choice of most appropri-

Table 2a. Matrix for FMECA-based techniques and tools – Regulatory documents.

Criteria	TOOLS									
	FMEA-Pro (Dyadem)	**Relex FT** (Relex)	**ITEM QT** (Item)	**RAM Commander** (ALD)	**Relex Reliability Studio** (Relex)	**XFMEA** (Reliasoft)	**IQ-RM PRO** (APIS)	**CARE** (BQR)
International ISO/IEC Standards	ISO 9001 ISO/TS 16949	IEC TR 62380/RDF 2000	IEC 62380, IEC 61508, ISO 9000, ISO 14971	n/a	IEC 61508, IEC 60812	IEC 60812, ISO 14971	ISO CD 26262, ISO/TS 16949, IEC 61508	IEC62380-RDF2000/ UTEC80810
Guidance/ Procedures	AQAP Reliability Centered Maintenance (RCM)	FIDES Guide 2004, PRISM	n/a	FIDES Guide 2004	FIDES Guide 2004, HAZOP, AIAG	AIAG (Automotive Industry Action Group)	AIAG (2nd, 3rd, 4th edition)	n/a
National Standards	vda 6.1, mil-std 1629a, mil-std 882	China 299B, MIL-STD 1629A	China 299B, MIL-STD 1629A	MIL STD 1629, IRPH 93, GJB 229	MIL-STD 1629A, BS 5760 Part 5	MIL-STD-1629A	MIL 1629 A (101,102)	GJB299
Industry Standards	SAE J1739, ARP 5580	British-Telecom HRD5	NSWC 06 (mechanical)	NSWC-98, UTEC 80810 (French Telecom 2000), British Telecom HRD 5	ARP 5580, SAE J1739, NAVAIR-AS-4613 Class A/B/C	VDA-4, SAE J1739	n/a	British-Telecom HRD5
Other Normative Documents	n/a	MIL HDBK 217-F, Siemens SN-29500, Telcordia/ Bellcore SR/TR-332	MIL HDBK 217-F, MIL HDBK-472, Telcordia/ Bellcore SR/TR-332	MIL HDBK 217-F, Telcordia/Bellcore SR/TR-332, RADC 85-91	MIL HDBK -217F, MIL-472, MIL-1547, Telcordia/ Bellcore SR/TR-332, MIL-STD-975 M, MIL-STD-1388 2B LSAR, FMD-97	n/a	n/a	MIL HDBK 217-F (N 2), M217, HRD5, Bellcore, Siemens SN-29500, NSWC 98/LE1

Table 2b. Matrix for FMECA-based techniques and tools – Other criteria.

Criteria		TOOLS							
		FMEA-Pro (Dyadem)	**Relex FT** (Relex)	**ITEM QT** (Item)	**RAM Commander** (ALD)	**Relex Reliability Studio** (Relex)	**XFMEA** (Reliasoft)	**IQ-RM PRO** (APIS)	**CARE** (BQR)
Experience of application in industry		Automotive, Electronic Aerospace, Nuclear	Nuclear, Oil, Aerospace, Chemical, Electronic. Pharma, Automotive, Machinery	n/a	Electronic Electrical Mechanical	Aerospace, Automotive, Mechanical, Electrical, Nuclear	Automotive Machinery	n/a	n/a
Methods used for assessment		FMEA, FMECA, etc	FMEA, FMECA, FRACAS,WA, FTA, ETA, MM, LCC	FMEA, FMECA, FMEDA, etc	Process FMEA, Design FMEA, FMECA, etc	FMEA, FMECA, etc	DFMEA, Process FMEA, Machinery FMEA, System FMEA, Service FMEA, FMECA, etc.	FMEA, etc.	FMECA, etc
Architec-ture	Desktop	+	+	+	+	+	+	+	n/a
	Server	n/a	+	+	+	n/a	n/a	+	n/a
	Multi-user	+	+	+	+	n/a	n/a	n/a	n/a
Technical support		+	+	+	+	+	+	+	n/a

ate T&Ts is justified. It is planned to create more universal decision making system based on described tool.

We are planning to refine developed approach and create a unified methodology. Discussed approaches were implemented in company standard (*NQA STP-66. Reliability Analysis. Failure Modes, Effects and Criticality Analysis. STC "Radiy", 2010. – 30 pages*.) Also tool that implements methodology of decision-making was developed. It is planned to create more universal decision making system based on described tool and to create a unified methodology.

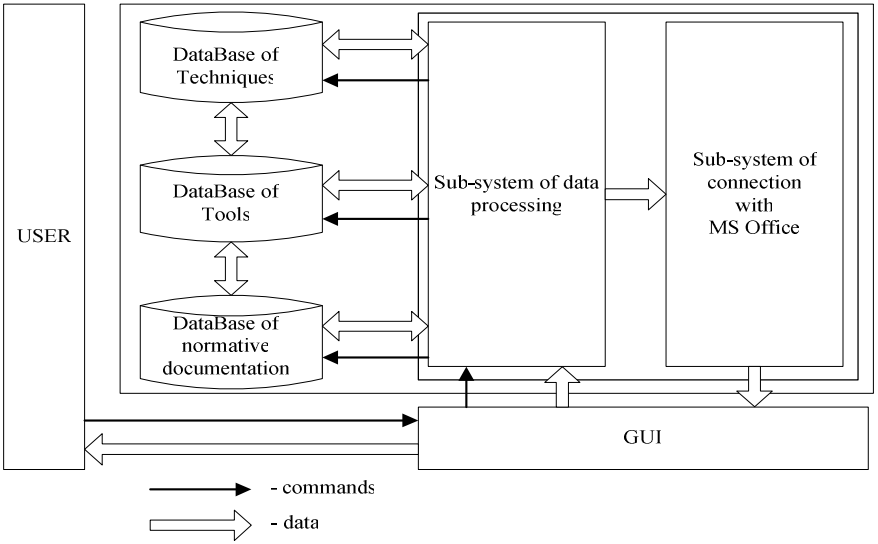

Figure 2: Simple model of the "Support Plus" Tool.

Notes:

[1] IEC 61508: 2010. *Functional safety of electrical/electronic/programmable electronic safety related systems*.

[2] IEC TR 62380. 2004-08. *Reliability data handbook –Universal model for reliability prediction of electronics components, PCB's and equipment*.

[3] D.H. Stamatis, *Failure Mode and Effect Analysis: FMEA from Theory to Execution*, Second edition (Milwaukee, WI: ASQ Quality Press, 2003); Robin E.McDermott, Raymond J. Mikulak, and Michael R. Beauregard, *The Basics of FMEA*, Second edition (New Yourk, NY: Productivity Press, 2008); William M. Goble, *Control Systems Safety Evaluation and Reliability*, 3rd edition (ISA Press, 2010).

[4] Mil-Std-1629: 1949. *Procedures for performing a failure mode, effects and criticality analysis.*

[5] IEC 60812: 2006. *Analysis techniques for system reliability – Procedure for failure mode and effects analysis* (FMEA); SAE J 1739: 2009. *Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and assembly Processes (Process FMEA) Reference Manual*; Tellcordia (Bellcore) SR-332, Issue 1. *Reliability Prediction Procedure for Electronic Equipment*.

[6] Oleg Illiashenko, Eugene Babeshko, and Vyacheslav Kharchenko, "Multistage Reliability and Safety Analysis of Information and Control Systems," *Radioelectronic and Computer Systems* 48 (2010): 283-287.

[7] Gunter Kersten, Vaihinqen, ENZ. *Fehlermoglichkeits-und-enfinbanalyse (FMEA). Handhuch Qualitats- Management* 3. Auflaqe, 469-490.

[8] Zigmund Bluvband, Pavel Grabov, and Oren Nakar, "Expanded FMEA (EFMEA)," Annual Reliability and Maintainability Symposium (RAMS), 2004 Proceedings, 31-36.

[9] Oleg Illiashenko and Eugene Babeshko, "Choice and Complexation of Techniques and Tools for Assessment of NPP I&C Systems Safety," ICONE'19, 2011 (in print); Vyacheslav Kharchenko, Eugene Babeshko, Vladimir Sklyar, et al., "Approaches to NPP I&C Systems Dependability Assessment: Analysis and Implementation,"ICAPP'10, 2010.

[10] Reid Willis, *Survey of support software for reliability engineering* (Washington Chapter, Society of Reliability Engineers, April 2006).

OLEG ILLIASHENKO, MSc student at the National Aerospace University named after N.E. Zhukovsky "KhAI". Research interests: Safety Case technologies, Reliability analysis techniques and software tools, regulation aspects of safety and critical systems applications. *E-mail*: illiashenko_oleg@hotmail.co.uk.

EUGENE BABESHKO, PhD-student at the National Aerospace University named after N.E. Zhukovsky "KhAI". Research interests: Safety Case, Reliability and safety analysis techniques and tools. *E-mail*: e.babeshko@csac.khai.edu.