Independent Verification and Diversity: Two Echelons of Cyber Physical Systems Safety and Security Assurance

Vyacheslav Kharchenko[a]

[a] *KhAI - National Aerospace University "Kharkiv Aviation Institute", Chkalov st. 17, Kharkiv, Ukraine*

Abstract

Conceptions of safety and security for cyber physical systems (CPS) in context of interaction with environment are analysed. Models and interconnection of safety and security and its attributes (functional safety, Internet safety, labor and occupational safety; cyber security, confidentiality, integrity, accessibility and physical security) for CPS functioning in conditions of information and physical environment are discussed considering common cause and time failures issue. Independent verification and validation (IV&V) and D3 (Defence-in-Depth and Diversity) approach are two echelons for protection of CPSs against cyber and physical attacks and failures caused by physical and design faults. The techniques of IV&V (XMECA, XBD, XTA, XIT etc.) are analysed in point of view different safety and security attributes. Multi-FIT technique is described as an example for CPS safety assessment. Application of diversity for safety and security assurance is discussed.

Keywords

Cyber physical systems, safety, security, independent verification and validation, diversity, common cause failure

1. Introduction

Cyber physical systems (CPSs) for critical applications such as NPP reactor trip systems, aerospace board and launch-abort control systems, railway interlocking and block signal systems and so on are important factor of safety for any country. Assurance of CPS safety and security of CPSs is one of key problems researched and advanced by scientists and engineers. High level of CPS safety and security can be achieved by enhancing and implementing methods, techniques and technologies of regulation, assessment and improving of dependability and its attributes.

There are two main approaches to assurance safety and security. Firstly, it's rigorous verification and validation allowing to minimize number or theoretically exclude design faults and vulnerabilities. This is process-based echelon of protection for created CPS.

The second echelon of protection is grounded on application of redundant structures, especially version redundancy tolerating component failures caused by physical, design and interaction faults [1]. Diversity is one of the general principles of fault- and intrusion-tolerant computer-based CPS designing and increasing dependability, decreasing the risks of the common cause failure (CCF) and optimizing costs considering consequences of severe accidents [2-4].

Objectives of the paper are the following:

- to analyse conceptions of safety and security for CPS in context of interaction with physical and information environment;
- to discuss CPS safety and security assessment and assurance problem considering CCF issue;

[1] *ICT&ES-2020: Information-Communication Technologies & Embedded Systems, November 12, 2020, Mykolaiv, Ukraine*
EMAIL: v.kharchenko@csn.khai.edu (V. Kharchenko)
ORCID: 0000-0001-5352-077X (V. Kharchenko)

- to research the independent verification and validation techniques (XMECA, XBD, XTA, XIT etc.) and D3 (Defence-in-Depth and Diversity) approach as two barriers against attacks and failures caused by physical and design faults.

Structure of the paper corresponds to objectives. Section 2 describes conceptions of CPS safety and security in context of CCF. Sections 3 and 4 discuss two echelons of CPS protection such as independent verification and validation and D3 principle. Section 5 concludes and formulates future research directions.

2. CPS safety and security in context of common cause failure

2.1. Safety and security model

Interconnection between functional safety and information (cyber) security as attributes of big safety is described by Figure 1. According with [4,5] safety is an attribute defining how CPS directly or via controlled object impacts on physical environment (PE) and information (IE) environment (Figure 1,a) and decreases risks of accidents. Failures of safety critical I&C systems increase such risks. Information (cyber) and physical security defines the degree of influence of IE and PE on system (blue and brown arrows, Figures 1,b-d). Insecure influence of IE on safety critical system can cause failures and unsafe influence of system on environment (dotted blue arrow, Fig.1,c). More detailed analysis of influence of IE and PE of safety critical system and its influence on environment is illustrated by Figure 1,d, elements of notation are described by Figure 1,e.

There are two types of attacks on CPS integrity (and accessibility or availability) and confidentiality. First of them causes failures and can be reason of unsafe impact of CSP on IE and PE. Second one causes receiving confidential data and can be reason more successful attacks on integrity and accessibility. Influence of PE can cause fatal failures and corresponding influence of CPS on PE and IE. If CPS safety depends on cyber security as a part of information security it's justifiable using of concept "cyber safety" as a part of safety [6].

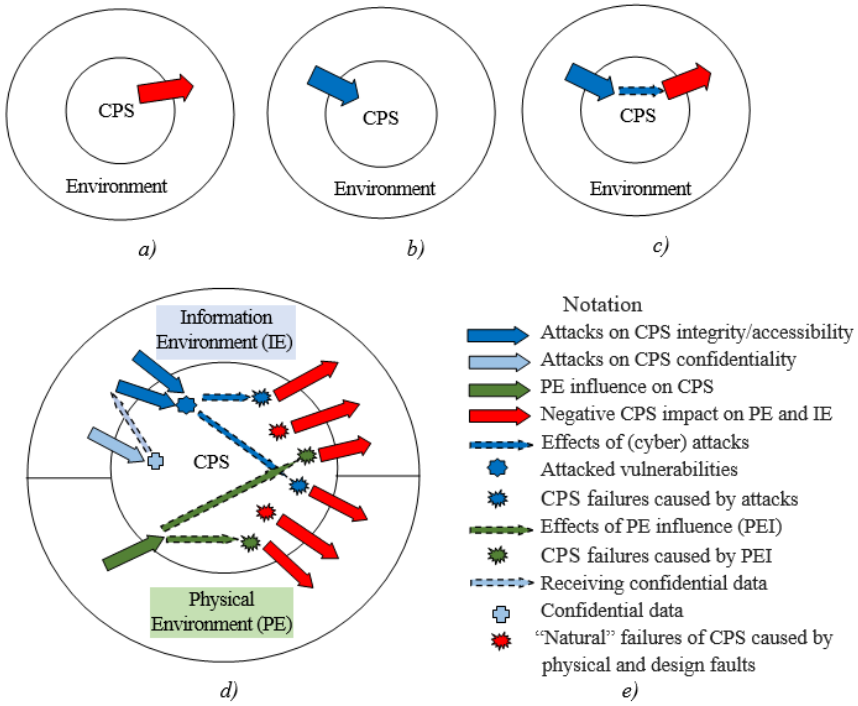

Figure 1: Models of CPS safety and security: model of safety (a), models of security (b) and influence of security on safety, model of interaction of CPS and environment (d), notation of models

More detailed analysis of different attributes of safety including functional, Internet and labour safety, and security including information security (confidentiality, integrity and accessibility), and physical security is given in Table 1. It describes influence of physical and information environment for all types of safety and security, and influence of attributes of safety and security on physical and information environment. Besides, it is analysed level of potential effects (local, for controlled object only, and global similar NPP accidents). Influence of attributes is marked by "+".

Table 1

Influence of safety and security attributes on environment

Safety& Security	Types		Influence of environment		Influence on environment		Effects	
			PE	IE	PE	IE	Local	Global
Safety	Functional safety		+	+	+ (via controlled object)		+	+
	Internet safety			+	+	+		+
	Labor safety		+		+ (via controlled object)		+	
Security	Information (cyber) security	Confidentiality		+		+ (via integrity, accessibility)	+	+
		Integrity		+	+ (via functional safety)	+	+	+
		Accessibility		+	+ (via functional safety)	+	+	+
	Physical security		+		+ (via human)		+	+

2.2. Common cause and common time failures

One of the key problem of CPS safety (and security as well) assurance is minimization or exclusion in general of common cause failure (CCF) risks. CCF is event when e_f (two or more) channels (versions) of redundant e-channel (e-version) system fail one by one or simultaneously and there is common reason causing this event. In any case, CCF is a multiple failure (MF) of CPS unlike single failure (SF) one of the redundant channels.

It should be emphasized that MF occur as a result of not only one (common) cause. It may be caused by a few different reasons concurring or spreading of failure time value does not exceed the response time of on-line testing and reconfiguration. Such type of multiple failures is called as a common time failure (CTF) which is common event failure (CEF) as CCF [6]. Classification of common cause and time failures is shown on the Figure 2. In addition to considered concepts, three attributes should be specified:

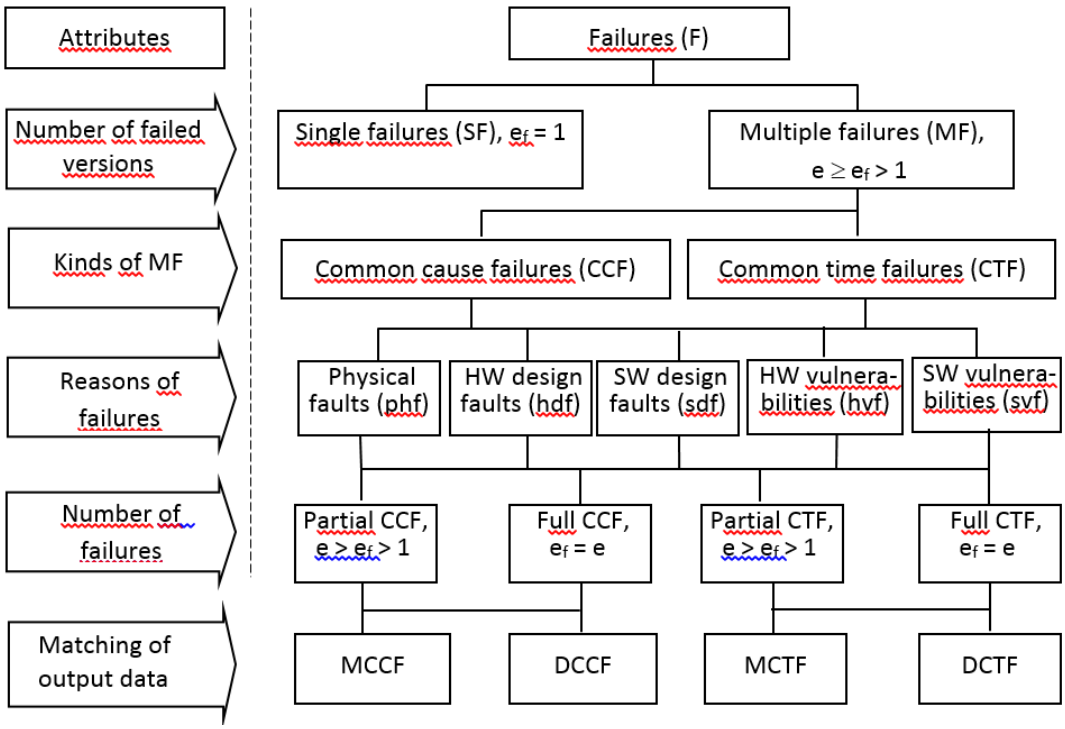

Figure 2: Classification of common cause and common time failures types and its reasons

- reasons (physical, design faults and vulnerabilities of hardware (HW) and software (SW));
- number of failed channels (versions) (partial and full CCFs, i.e. PCCFs and FCCFs, and partial and full CTFs, i.e. PCTFs and FCTFs);
- matching of output channel data in case of failures, i.e. matching (MCCFs, MCTFs) and different (DCCFs, DCTFs) failures.

Two preliminary conclusions which are important for safety critical CPSs. Firstly, CTFs are important objective of research because there are examples of serial failures caused by attacks on vulnerabilities of redundant channels and combined reasons. Secondly, very important tasks is analysis and assurance, if it's possible, of distinguishability of failure effects (output data of failed channels) to fix fact of partial or full common cause and time failures.

2.3. IV&V-D3: two echelons of common failures protection

Problem of CCF decreasing risks can be solved by use of two approaches (Figure 3):

- minimizing of latent faults, first of all, design faults and vulnerabilities. For that techniques of verification and validation (V&V) of developed or modernized CPSs (hardware, software, FPGA components, platforms etc.) have to be applied. There is rigorous requirements to V&V including requirement to independence of verification and validation teams, process, techniques and tools for safety critical CPSs such as NPP I&C systems. V&V which are performed by an organizational and/or financially independent team is called independent V&V (IV&V). Implementing IV&V allows detecting faults which haven't been detected by developers or QA specialists of company;
- application of diversity as a part of more general so-called principle D3 (Defense-in-Depth&Diversity) [7] to provide trusted fault-, vulnerability and intrusion-tolerance during CPS operation. D3 is a horizontal/vertical defense echelon consisting of n subechelons e_i and m version redundancy types vr_j (Figure 3) [6, 8, 9]. Diversity and multi-diversity when a few types version process-product redundancy are applied allows decreasing risks of common cause failure and common time failure as well during operation stage of CPSs.

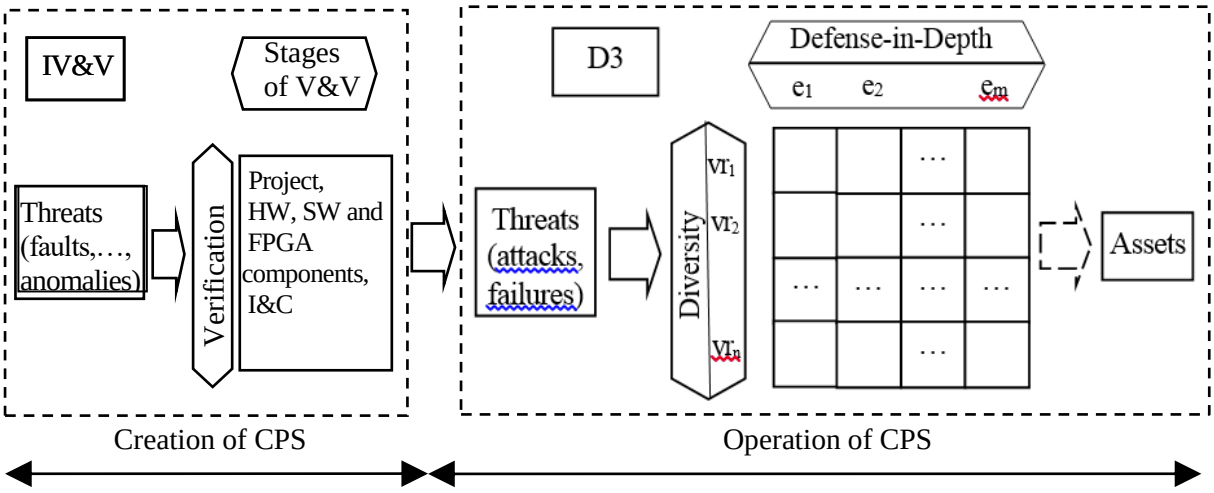

Figure 3: Two echelons of CCF protection: independent verification and validation and D3 (defence-in-depths and diversity) approach: e_i – echelons of protection in depth, v_r – types of version redundancy

These approaches are two echelons of CCF/CTF protection implementing DET principle "to detect – to eliminate (detected faults during V&V) – to tolerate (residual/undetected faults during operation)".

3. Independent verification and validation techniques: the first echelon

3.1. Methods of safety and security assessment and V&V techniques

There are a lot of methods of CPS safety and security assessment and V&V techniques which are used by developers/QA engineers of companies and independent verifiers as well such as [4, 9, 11]:

- XME(C/D)A, X (Failure, Software failure, Intrusion, …) Modes and Effects C/D (Criticality/Diagnostics) Analysis;
- XBD, X (Reliability, Safety, Security, Trustworthiness, …) Block Diagrams;
- XTA, X (Failure, Attack, Non-availability, …) Tree Analysis;
- XIT, X (Fault, Software fault, Vulnerability, …) Injection Testing;
- HAZOP(X), Hazard Operation Analysis (X – for safety, security);
- MM(X), Markov's Models (X – availability, dependability, safety, security).
- other techniques based on CCF analyses, model checking, formal methods and so on.

The V&V techniques include more software and documentation based procedures as review of documents (static analysis, verification and validation plans and reports review, check-list based analysis and so on). Table 2 summarizes the results of analysis of these techniques applicability for assessment of different safety and security attributes. The following marks are used:

- applicable technique, + ;
- can be applicable, (+);
- can't be applicable, x.

Two preliminary conclusions are the following:

- in fact, all methods and techniques which were initially developed and are used to assess functional safety have analogues to assess security and cyber security. For example, FME(C)A technique (Failure ME(C)A) was modified for security assessment as IME(C)A (Intrusion Modes and Effects (Criticality) Analysis). Feature of IMECA is considering failure as a pair "vulnerability-attack" or as a combination of threats, vulnerabilities and attacks/intrusions [4, 11];

Table 2
Analysis of applicability of assessment methods and V&V techniques for safety and security analysis

Safety& Security	Types		Methods of safety and security assessment and V&V techniques						
			XME(C/D)A	XBD	XTA	XIT	HAZOP(X)	MM(X)	Others
Safety	Functional safety		+	+	+	+	+	+	+
	Internet safety		**(+)**	**x**	**(+)**	**x**	**(+)**	**x**	+
	Labor safety		+	**x**	+	**x**	+	**(+)**	+
Security	Infor-mation (cyber) security	Confi-den-tiality	+	**(+)**	+	+	**(+)**	+	+
		Integrity	+	**(+)**	+	+	**(+)**	+	+
		Accessi-bility	+	**(+)**	+	+	**(+)**	+	+
	Physical security		+	+	+	**(+)**	**(+)**	+	+

- the methods of assessment and V&V procedures can be used by combining ones. For that a special graph-model describing a different ways to get searched measures or V&V results or to assure high level of trustworthiness by getting searched measures using different combinations of the techniques.

3.3. Multi-FIT based verification

Fault (and vulnerability) injection testing is one of the techniques applied for IV&V according with standards requirements to safety critical CPS. The goals of FIT are to assess the test quality considering test coverage/trustworthiness issues, efficiency of online testing, analyse fault- and intrusion-tolerance (to design and physical faults). "Natural" failures for complex SW and HW, CPS are multiple ones caused by physical and design faults, attacks with different scenarios.

Main challenges of multiple fault injection (multi-FIT): complexity and time of verification (in general number of faults equals 2kmn, n – number of faults, k – number of fault types, m – number of CPS levels), mutation/masking of faults and blockage of verifiable performance. The standard NUREG/CR-7151 recommends employing a multi-FIT, but it does not describe procedures of injection. To tolerate these challenges two approaches can be applied [12]:

- development of injectable projects, i.e. assurance of ability to inject faults regarding to actual/specified physical scheme or code (FITability) to optimize points and means of injection;
- implementing technique of multi-FIT based on application of modified t-wise procedure and operations of de-masking and de-blockage of injected fault subsets (Figure 4).

The future steps are important from research and practical point of view:

- development of techniques and tools that take into account the possibilities of injecting different fault/vulnerability types for different CPS components and system levels. For FPGA-based systems it may be physical faults injecting at the module and chip levels, design faults and vulnerabilities injecting into VHDL code and top-level software code);
- development of methods assuring ability to multi-fault injections, i.e. multi-FIT-ability.

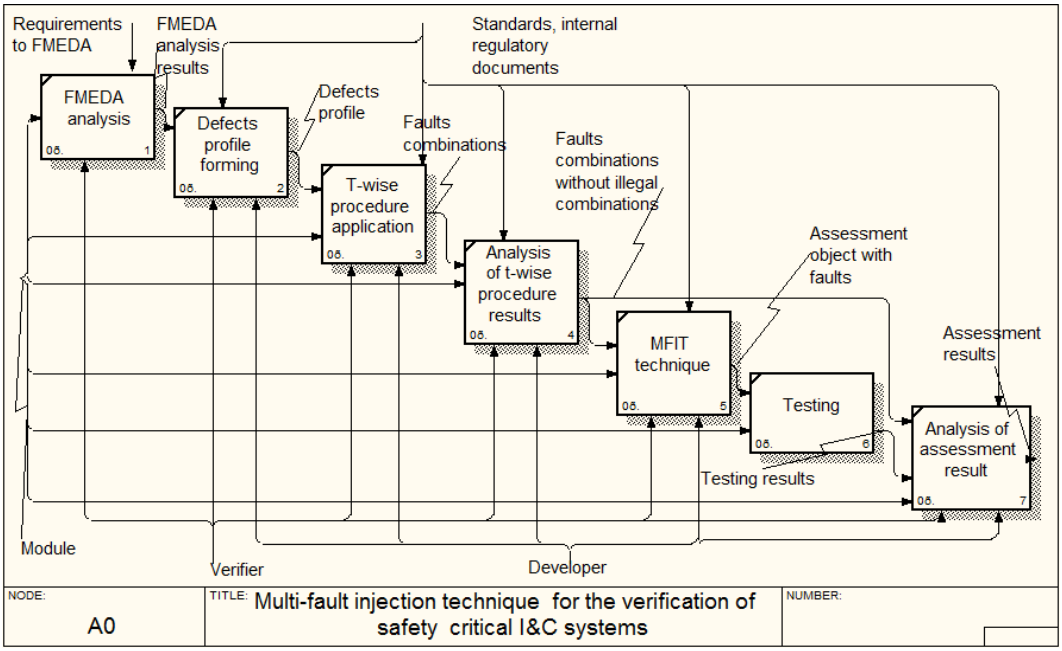

Figure 4: IDEF diagram of multi-FIT technique [12]

4. Diversity and defence-in-depth: the second echelon

4.1. Multi-version computing and classification of version redundancy

Diversity is a basic principle of multi-version computing. Main concepts of multi-version computing are the following:

- *version* is an option of different product or/and process realization of CPS function(s);
- *version redundancy* (VR) is a type of redundancy when different versions are used;
- *diversity or multiversity* (MV) is the principle providing use of several versions;
- *multi-version system* (MVS) is a system in which a few versions are used;
- *multi-version technology* (MVT) is set of the interconnected rules and design actions in which a few versions-processes leading to development of two or more intermediate or end-products are used;
- *multi-version project* (MVP) is a project in which the MVT is applied to create one- or multi-version system;
- *strategy of diversity* (MV) is a collection of general criteria and rules defining principles of formation and selection of version redundancy types and volume or MVTs;
- *diversity metric* is indicator to assess level of diversity of versions.

To assess CPS safety measures especially a probability of common cause failure it is necessary to evaluate the diversity metrics [4, 9]. Figure 5 presents set model of version faults (attacked vulnerabilities) causing failures. For one-version and cannel system (Figure 5,a) number of single faults equals N (N = Card SF). In this case, any faults of set SF is fatal and is, in fact, CCF. Hence β - factor as a metric of CCF determining relation of number of faults caused CCFs to total number of such faults equals one (and $\alpha = \beta = 1$).

The metrics of two-version system (Figure 5,b,c) can be evaluated as following: $\beta = N_{CCF} / N$, $N_{CCF} = Card\ (SF_1 \cap SF_2)$; $N = (N_1 + N_2) / 2$, $N_i = Card\ SF_i$; $\alpha_i = 1 - \beta$; $\beta_d = N_{MCCF} / N$; $\beta_{\bar{d}} = N_{DCCF} / N$; $\beta = \beta_d + \beta_{\bar{d}}$. Metrics of relative number of MCCFs and DCCFs (see Figure 2): $\beta^*_d = \beta_d / \beta$, $\beta^*_{\bar{d}} = \beta_{\bar{d}} / \beta$. For three-version system (Figure 5,d) $\alpha = 1 - \beta - 2\gamma$, where γ is metric determining part of CCFs of any two versions (PCCF), $\gamma = 2N_{PCCF} / N$). If $\gamma = 0$ (Figure 5,e), $\alpha = 1 - \beta$.

These types of faults and vulnerabilities and metrics can be used to add a profile of injected faults for FIT based verification of multi-version CPSs. Values of metrics α and β are determined using statistics of testing and operation failures and expert methods [9].

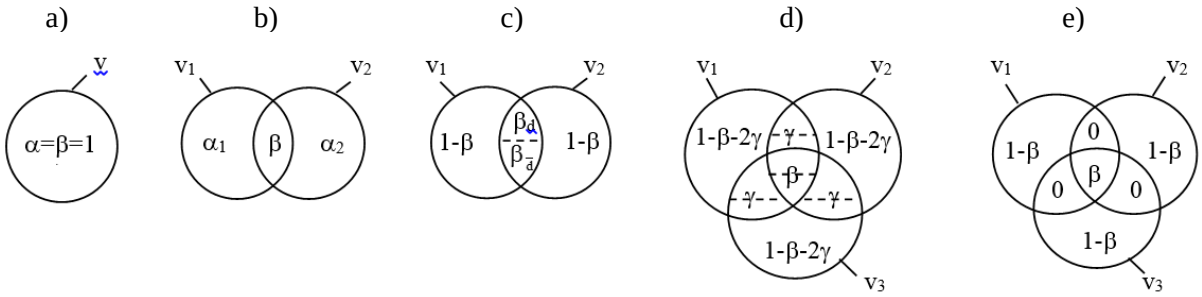

Figure 5: Models of faults sets of one-version (a), two-version (b,c) and three-version (d,e) CPS

4.2. Application of defence-in-depth and diversity for safety and security assurance

Classification of different diversity types and D3 in general is described in [7]. Table 3 contains the results of diversity and defence-in-depth (DiD) applicability analysis for assurance of CPS safety and security. The following marks are used:

- applicable type of diversity, + ;
- type of diversity can be applicable, (+);
- type of diversity can't be applicable, x.

Table 3

Influence of diversity and defence-in-depth on safety and security assurance

Safety & Security	Types		Influence of diversity						Influence of DiD
			Signal	Functional	Equipment	Software	Design	Human	
Safety	Functional safety		+	+	+	+	+	+	+
	Internet safety		x	x	x	x	x	x	(+)
	Labor safety		+	x	+	x	+	+	+
Security	Information (cyber) security	Confidentiality	x	(+)	(+)	(+)	(+)	+	+
		Integrity	+	+	+	+	+	+	+
		Accessibility	+	+	+	+	+	+	+
	Physical security		+	+	+	+	+	+	+

Let's analyse two examples of application of diversity to assess and improve safety and security. In the first case CPS has hardware and software diversity. Dependencies of up-state probabilities on time for the two-version structures are illustrated by Figure 6 [6]. Initial data for modeling are the following: failure rate of version (channel) $\lambda_{version} = 3 \cdot 10^{-5}$ 1/h, metrics of diversity for physical and design HW faults $\beta_{Hp}=0$, $\beta_{Hd} = 0.2$, metric of diversity for SW design faults $\beta_{Sd} = 0.8$; values of SF metrics for one version $\alpha_{hp}= \alpha_{hd} = \alpha_{sd} = 1/3$.

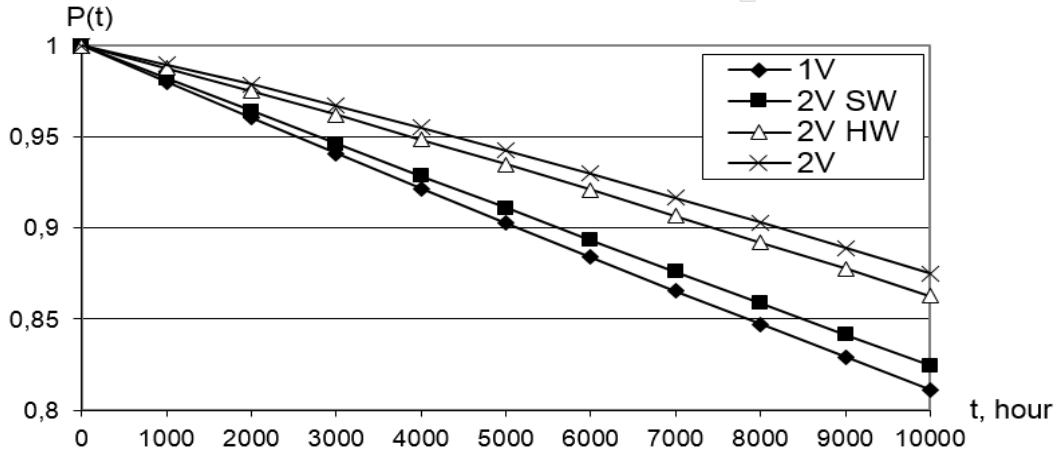

Figure 6: Dependencies of CPS probability of up-state on time for one-version system (1V), two-version system with diverse SW (2V SW), HW (2V HW) and as SW and HW (2V) versions

The second case describes security assessment of FPGA-based MVS. Table 4 summarizes some attacks and the results of assessment using IMECA-analysis. The table contains countermeasures strategies which could be applied as a requirements from Regulatory Guide 5.71:2010 (Cyber Security Programs For Nuclear Facilities, U.S. NRC) to eliminate the attack causes and, moreover, FPGA-based MVS diversity type and its attributes as a countermeasures [4].

Table 4

The results of FPGA-based MVS security assessment using IMECA technique

No	Attack mode	Attack nature	Attack cause	Occurrence probability	Effect severity	Type of effects	Countermeasures (including RG 5.71)	FPGA-based CPS diversity types and its attributes
1	Readback	Active	Absence of chip security bit and/or availability of physical access to chip interface (e.g. Joint Test Automation Group, JTAG)	M	H	Obtaining of secret information by adversary	• The use of security bit; • Application of physical security controls; (B.1.18 Insecure and Rogue Connections, Appendix B to RG 5.71, Page B-6)	Diversity of electronic elements (EEs): • Different technologies of EEs production;
3	Brute force	Active	• Search for a valid output attempting all possible key values; • Exhaustion of all possible logic inputs to a device in order; • Gradual variation of the voltage input and other environmental conditions	L	M	Leak of undesirable information	Detecting and documenting unauthorized changes to software and information, (C.3.7, Appendix C to RG 5.71, Page C-7)	Diversity of project development languages • Combination of couples of diverse CASE-tools and HDLs

3	Fault injection (glitch)	Active	• Altering the input clock; • Creating momentary over- or under-shoots to the supplied voltage	M	H	• Device to execute an incorrect operation • Device left in a compromising state • Leak of secret information	• Making sure all states are defined and at the implementation level, verifying that glitches cannot affect the order of operations; • Detection of voltage tampering from within the device; • Clock supervisory circuits to detect glitches	<u>Diversity of EE:</u> • Different manufacturers of EEs; • Different technologies of EEs production; <u>Diversity of scheme specification (SS)</u> • Different SSs; • Combination of diverse CASE tools and SSs

5. Conclusions and recommendations

The problem of the "last faults" is one of the most challengeable for critical cyber physical systems and reputational for commercial applications. There are two key approaches to minimizing risk of failures caused by design (SW/FPGA) faults and attacks on vulnerabilities using independent V&V and diversity.

X (fault, vulnerability, anomaly) injection based techniques (X/FIT) are one of the efficient V&V techniques. Important tasks are fault profiling; FIT coverage and FIT-ability; multi-FIT and tools. Systematization and aggregating of V&V techniques allow achieving higher accuracy and trustworthiness.

Diversity assures minimizing common cause failure (CCF) risk. Key problems are assessment CCF risk and implementation of new types of internal/external diversity, formal choice and combining of different types of version redundancy, multi-fault/vulnerabilities injection for multi-version systems and so on.

6. References

[1] A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr, Basic Concepts and Taxonomy of Dependable and Secure Computing, IEEE Transactions on Dependable and Secure Computing 1 (2004) 11-33.

[2] N. Leveson, Safeware: System Safety and Computers, Addison-Wesley, 1995.

[3] C. Harvey, N. Stanton, Safety in System-of-Systems: Ten key challenges, Safety Science 70 (2014) 358-366.

[4] M. Yastrebenetsky, V. Kharchenko (Eds.), Security and Safety of Nuclear Power Plant Instrumentation and Control Systems, Hershey, Pennsylvania, United States of America, IGI Global, 2020, 501 p.

[5] A. Kornecki, N. Subramanian, J. Zalewski, Studying Interrelationships of Safety and Security for Software Assurance in Cyber-Physical Systems Proceedings of the Federated Conference on Computer Science and Information Systems, 2013.

[6] V. Kharchenko, Big Data and Internet of Things for Safety Critical Applications: Challenges, Methodology and Industrial Cases, International Journal on Information Technologies and Security 4 (2018) 3-16.

[7] NUREG7007:2009. Diversity Strategy for Nuclear Power Plant Instrumentation and Control Systems. URL: https://www.nrc.gov/docs/ML1005/ML100541256.pdf

[8] V. Kharchenko, Diversity for Safety and Security of Embedded and Cyber Physical Systems: Fundamentals Review and Industrial Cases, in: Proceedings of 15th Biennial Baltic Electronics Conference, 2016, pp. 21-30.

[9] V. Kharchenko, A. Siora, E. Bakhmach, Diversity-Scalable Decisions for FPGA-Based Safety-Critical I&Cs: from Theory to Implementation, in: Proceedings of the 6th ANS International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology, NPIC&HMIT2009, Knoxville, TN, USA: American Nuclear Society, 2009, pp.11-18.
[10] IEC 60812:2018. Failure modes and effects analysis (FMEA and FMECA), 2018. URL: https://webstore.iec.ch/publication/26359
[11] E. Babeshko, V. Kharchenko and A. Gorbenko, Applying F(I)MEA-technique for SCADA-Based Industrial Control Systems Dependability Assessment and Ensuring, in: 2008 Third International Conference on Dependability of Computer Systems DepCoS-RELCOMEX, Szklarska Poreba, Poland, 2008.
[12] O. Odarushchenko, V. Kharchenko, Sklyar, V. Multi-Fault Injection Testing: Cases for FPGA-Based NPP I&C Systems, in: Proceedings of ICONE-23 23rd International Conference on Nuclear Engineering, May 17-21, Chiba, Japan, 2015, pp.31-38.