Diversity for Safety and Security of Embedded and Cyber Physical Systems:

Fundamentals Review and Industrial Cases

Vyacheslav Kharchenko
Department of Computer Systems and Networks
National Aerospace University KhAI
Centre for Safety Infrastructure Research and Analysis
Kharkiv, Ukraine
v.kharchenko@csn.khai.edu

***Abstract*— Fundamentals of diversity and multi-version systems (MVS) are overviewed. Main concepts and taxonomy of multi-version computing, methods of diversity assessment and technologies of development are analyzed. Principle D3 (Defense-in-Depth&Diversity) is researched using FTA (failure tree analysis) to understand its influence on safety and security considering physical, design faults and attacks on vulnerabilities of hardware, software, FPGA components and system configuration. Several industrial cases related to application of diversity in NPP I&Cs, aviation control systems, post-accident monitoring system and service-oriented architectures to improve safety and security are analyzed.**

Keywords—embedded systems, cyber physical systems, common cause failure, diversity, safety, security,

I. INTRODUCTION

A. *Diversity against common cause failure*

Safety critical instrumentation and control systems (I&Cs) are the most challengeable, important and complex applications in which reliability and security of hardware and software components, information technologies are key attributes. There are a lot of critical applications such as a cyber physical systems (NPP reactor trip systems and smart power grids, railway blocking and signaling systems, intellectual transport systems and infrastructures, etc) and embedded software and FPGA-based on-board aviation and piloted space systems, mobile medical devices and so on.

Hardware and software failures of these systems can be fatal and cause fatal consequences. To decrease risks of fatal failures a set of the tasks must be solved: to develop and ground the requirements to safety and other related attributes; to assure required values of safety indicators; to assess that the requirements are implemented in system project and approved during operation time.

Key problem of safety assurance is decreasing of common cause failure (CCF) probability. Common cause failures are dangerous reason of I&C violations. The most probable reasons of CCFs are design faults of software components, multiple physical faults of redundant hardware caused by different environment impacts, intrusions attacks on identical vulnerabilities of software and hardware.

Ordinary redundancy, first of all, structure redundancy does not mitigate CCF risks as the same channels have the same design faults. Using of structure redundancy can not decrease CCF as the same software and hardware components have the same vulnerabilities. Time redundancy is not efficient as well.

Critical system CCF risks can be radically decreased by application of one or several types of version redundancy (diversity). Diversity principle is based on the simple idea “The same products/processes have the same anomalies, the different product/processes have different anomalies”. “Different” means that products have the same functionality and processes have the same goals but are developed and implemented by different ways. There are a lot of diversity types for software, hardware, FPGA-based designs and development, verification, maintenance processes [1,2]. Application of diversity is requirement of standards for safety critical domains [3].

B. *Challenges of diversity principle implementation*

Main challenges of diversity principle implementation are the following:

- for regulatory bodies: how define the frameworks and formulate the requirements to application of diversity in sufficient detail;
- for developers: how choice the types and capacity of version redundancy to meet requirements and assure optimal design according to criteria “required safety-minimal costs”;
- for (independent) verifiers and validators: how to assess actual level of diversity and confirm or refute that diversity related decisions completely meet requirements;
- for operation engineers and managers: how to maintain diversity-based systems considering more complex architecture and recovery activities.

The problem is compounded by application of modern software technologies and electronic components including

978-1-5090-1393-7/16/$31.00 ©2016 IEEE

FPGAs and systems-on-programmable-chips improving functionality, productivity, reliability and possibilities to diversify design, on the one side, and creating new deficits of the safety, because they have specific weaknesses and vulnerabilities which must be taken into account.

Security related threats are more and more challengeable for safety critical applications. Security informed safety approach becomes no alternative for embedded systems and complex cyber physical systems [4-7]. Hence, it is very important to analyze how diversity influences on risks of successful attacks on vulnerabilities considering features of systems and environment.

C. Goals

In spite of the diversity principle implementation into industry and business domains and research of diversity-scalable systems there are a new challenges of their assessment, development and operation.

Goals of the paper are to review fundamentals of diversity and multi-version systems (Section II) and to analyze several industrial cases related to their application in NPP I&Cs, aerospace computer systems, post-accident monitoring system and service-oriented architectures (Sections III-V) and to present directions of future researches (Section VI). The main issues of analysis are safety, security and survivability.

II. Fundamentals of Multi-Version Systems. State-of-Art

A. Basic concepts

A set of concepts regarding development and implementation of diversity principle is united by general term "multi-version computing" described by taxonomy scheme (Fig.1). Multi-version computing is one of general types of dependable (reliable, safe and secure) computing and includes the following concepts [2,7]:

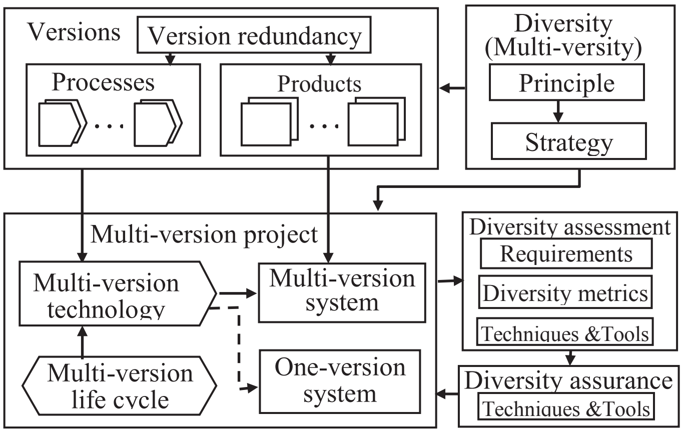


Fig. 1. Taxonomy scheme of multi-version computing

- version (product or/and process) is an option of different implementation of project tasks. Version redundancy is a type of redundancy when different versions are used. This redundancy is based on different ways and/or means of achieving a specified objective. The degree of diversity or version difference is measured by diversity metrics. Using metrics it is assessed accordance to requirements to diversity application;
- diversity or multiversity is the principle providing use of several versions. This principle means performance of the same function (product or/and process) by two and more options and processing of data received in such ways for checking, choice or formations of final or intermediate results and decision-making on their further use;
- multi-version system (MVS) is a system in which a few versions-products are used. MVS is multi-diversion system if two or more types of version redundancy are used;
- multi-version technology (MVT) is set of the interconnected rules and design actions in which in accordance with diversity strategy a few versions-processes leading to development of two or more intermediate or end-products are used;
- diversity strategy is a set of general criteria and rules defining principles of choice and complexing of version redundancy (types and volume);
- multi-version project (MVP) is a project in which the MVT is applied (by version redundancy of processes) leading to creation of one- or multi-version system (by implementation of products version redundancy);
- multi-version life cycle is based on combing processes of versions development, verification and integration or using of a few life cycle models.

B. Safety, security and D3 approach

Safety (Fig.2,a) is an attribute defining how I&C system (via controlled object) influences on environment (other systems and objects, people and so on) and decrease risks of emergencies. Failures of safety critical I&C can increase these risks, i.e. cause unsafe influence (USFI).

Security (computer security, cyber security) defines the degree of environment influence on system (Fig.2,b). Insecure influence (ISCI) of environment on safety critical system can cause unsafe influence of system on environment.

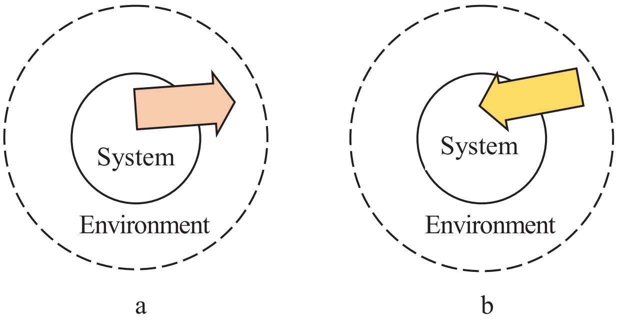


Fig. 2. General models of safety (a) and security (b)

In general, unsafe behavior of system can be caused by:

- hardware anomalies (physical faults f_p, manufacture design and physical faults f_m, vulnerabilities of hardware components v_{hw} attacked by intruders A_{hw};
- software anomalies (design faults f_{d1} and f_{d2} tolerating by changing data environment, for example by restart, and changing of software code/ design correspondingly, faults caused by software ageing fa and vulnerabilities of software components v_{sw} attacked by intruders A_{sw};
- FPGA anomalies similar hardware physical faults and software design faults, and two types of hardware and software vulnerabilities;
- system anomalies (configuration faults fc and system vulnerabilities v_{sl} attacked by intruders A_{sl}.

The results of FTA (failure tree analysis) of irredundant system is illustrated by Fig.3. System failure F_S is caused by failures of component and system levels F_{hw}, F_{sw} and F_{sl}.

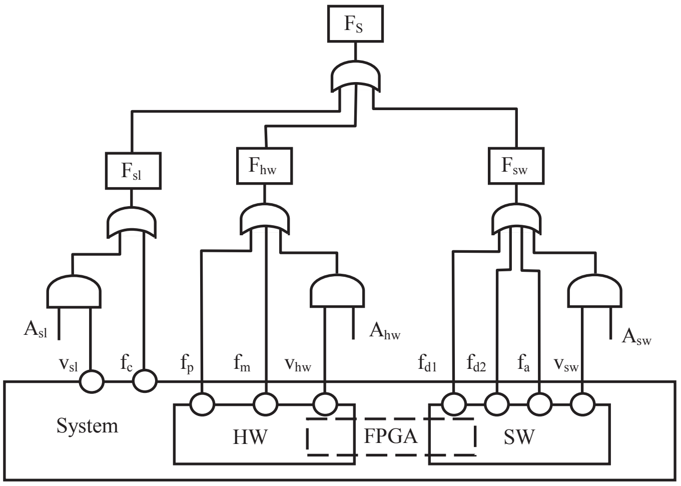


Fig. 3. FTA of irredundant system

Diversity is a part of more general so-called principle D3 (Defense-in-Depth&Diversity) [1,2] applied to provide trusted, fault- and intrusion-tolerant design and operation of I&Cs. Defense-in-Depth is a horizontal/sequential echelon of defense consisting of n subechelons ei and m diversity (version redundancy) types vrj is a vertical/parallel part of once (Fig.4). The D3 principle is used to assure safety and security as well.

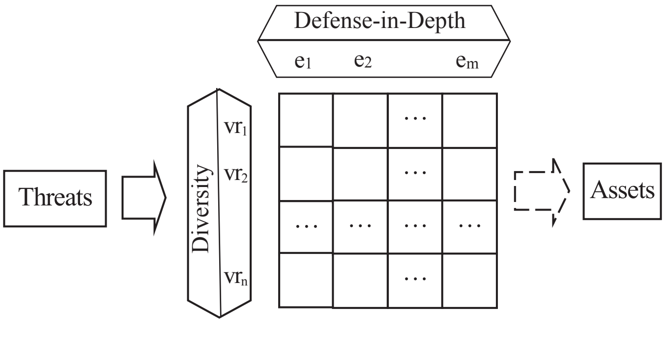
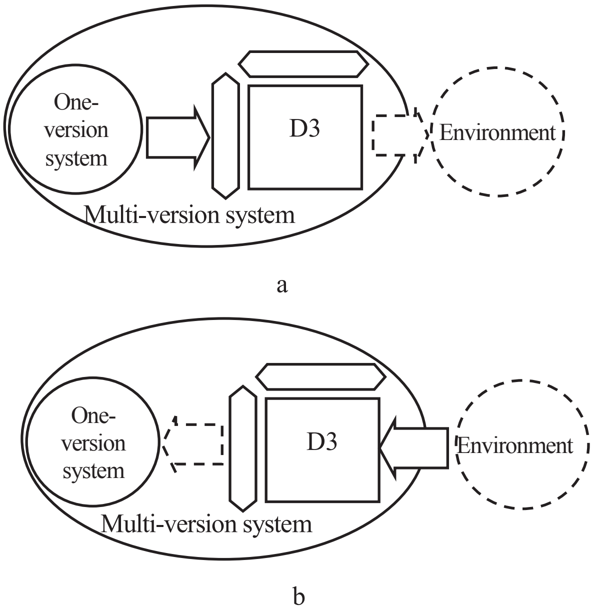


Fig. 4. D3 principle

D3 principle allows protecting assets of systems against threats. Application of D3 principle mitigate unsafe influence of I&C system on environment in multi-version system (Fig.5, a) and vice versa, i.e. mitigate unsecure influence of environment on system (Fig.5,b).



a

b

Fig. 5. Mitigation of unsafe influence of system (a) and unsecure influence of environment (b)

Mitigation of failures by application of structure and version redundancies is described by FTAs (see fig.6). In first case failures caused by physical faults (and some others depending on conditions) can be tolerated (Fig.6,a).

System with version redundancy, i.e. multi-version system can tolerate failures caused by all types of faults (Fig.6,b).

C. Diversity types and classifications

Diversity types and their classifications are described and analyzed in [1,2,7]. The standard [1] samples two-level hierarchy and includes the following types of diversity:

- human or life cycle diversity (different design IT-companies; different managers, designers, programmers and testers teams; different maintenance personnel);
- design diversity (different technologies, design approaches, architectures);
- software diversity (different algorithms, operating systems, languages);
- functional diversity (different underlying mechanisms, logics, actuators);
- signal diversity (different sensed parameters, physical effects, different manufacturers and sensor designs; different set and location of sensors);
- equipment diversity (different manufacturers and design technologies).

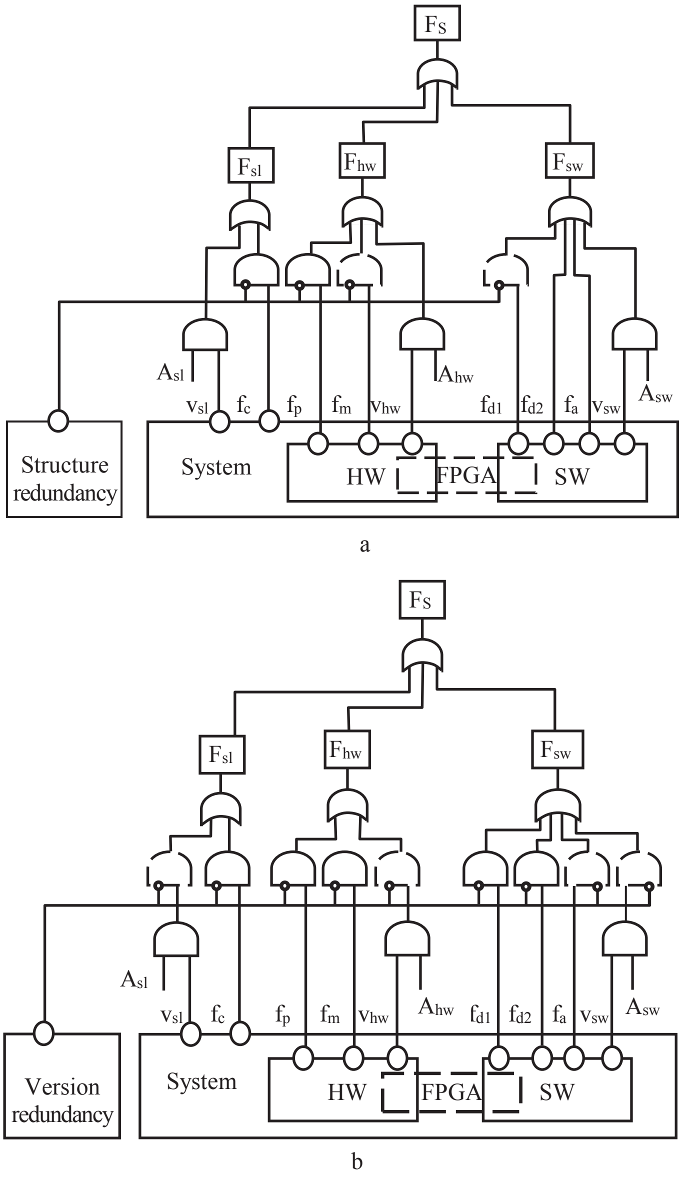


Fig. 6. FTA for system with sturcture (a) and version (b) redundancy

Other system diversity types are:

- conceptual diversity based on different number systems – positional (binary, decimal) and non-positional (modular, vedic, etc);
- implementation diversity – linear-parallel (for example, reactor trip systems [2]) and matrix (A340, A380 control systems [8]) diversity.

Besides, there are detailed classifications for software and FPGA-based systems [7,9]. Software diversity types are the following:

- diversity of life cycle models and processes (V-model, waterfall model, agile etc);
- resources and means (different human resources, languages and notations, tools);
- project decisions (different architectures and platforms, protocols, data formats, etc).

FPGA diversity types are the following:

- diversity of electronic components (different electronic chips manufactures, different technologies – SRAM, flash, anti-fuse, different chip families and chips);
- diversity of CASE-tools (different types and configurations of tools);
- diversity of project development languages (different graphical scheme languages, different hardware description languages and different IP-cores);
- diversity of specifications (specification languages) and others.

The most general three-space (stage of life cycle, level of project decisions and version redundancy types) classification of diversity types is presented by "cube of diversity"[2,7].

D. Models of multi-version systems

Multi-version system W is described by formula [10]:

$$W = \{X, F, Z, V, U\}, \qquad (1)$$

where X, Z are sets of input and output signals; F is a set of functions performed; V is a set of versions/channels; U is a function of version execution results processing (transformation of output version signals Zi in output system signal Z).

Multi-diversion system is additionally described by a set of version redundancy R and procedure F mapping R into V. Besides, I&Cs performing safety-critical functions, for example ESFAS [2], may be represented by a composition of two interconnected subsystems – monitoring (checking) subsystem and control subsystem (monitoring and control automata).

Monitoring automaton Ac analyses output signals X from monitoring and control object and forms its status code ZC. Control automaton Au forms control signals Z in accordance with signals ZC. Several options of MVS architectures are possible for a FPGA-based I&Cs. Those options may be classified according with attributes: degree of diversity coverage (I&Cs with a complete A_f and partial A_p diversity); diversity depth (I&Cs with a common A_{com} and separate A_{sep} diversity).

E. Multi-version systems technologies

Multi-version system models and technologies of development are analyzed in [2,7,10]. Selection of version redundancy types are based on a model of multi-version life cycle (MVLSC, a special graph and their modifications [10,11];

MVLC is formally presented as a bipolar G-level graph called graph of multi-version technologies [10]. Each graph node corresponds metrics of diversity and cost; way connecting initial and final nodes corresponds one of the development process options and one of the architectures. This way is characterized by indicators of “summarized” diversity and general costs.

Algorithms of MVT selection or choice of optimal way in the graph according with criteria “diversity (safety)-reliability-cost” are described in [10.11].

F. *Methods of diversity assessment*

There are following assessment methods of actual diversity level and evaluation techniques of MVS dependability and safety described in [2,7,12,13]:

- theoretical-set and metric-oriented methods based on: Eiler’s diagram for sets of version design, physical and interaction faults (including vulnerabilities for assessment intrusion-tolerance); matrix of diversity metrics for sets of different faults (individual, group and absolute faults of versions); calculation of diversity metrics by use of Eiler’s diagrams or other data about results of testing and faults of different versions;
- probabilistic methods using reliability block-diagrams (RBDs), their modifications (security, survivability and safety block-diagrams), Markovian chains, Bayesian method, etc;
- statistical methods including: receiving and normalization of version fault trends using testing data; choice of software reliability growth model (SRGM) taking into account features of version development and verification processes and fitting SRGM parameters; metrics diversity assessment; calculation of reliability and safety indicators;
- fault injection-based assessment consisting of: receiving project-oriented fault profiles; performing of faults injection procedure; proceeding of data and metrics diversity calculation; calculation of reliability and safety indicators;
- expert-oriented methods using two groups of metrics: diversity metrics for direct assessment of versions and MVS reliability and safety (direct diversity metrics); indirect diversity metrics (product complexity metrics and process metrics); values of these metrics may be used to assess direct diversity metrics. Expert method is added by other techniques founded on interval mathematics-based assessment of diversity metrics and MVS indicators, soft computing-based assessment (fussy logic, genetic algorithms), risk-oriented approach and so on.

III. Industrial Cases. Diversity for Safety and Security

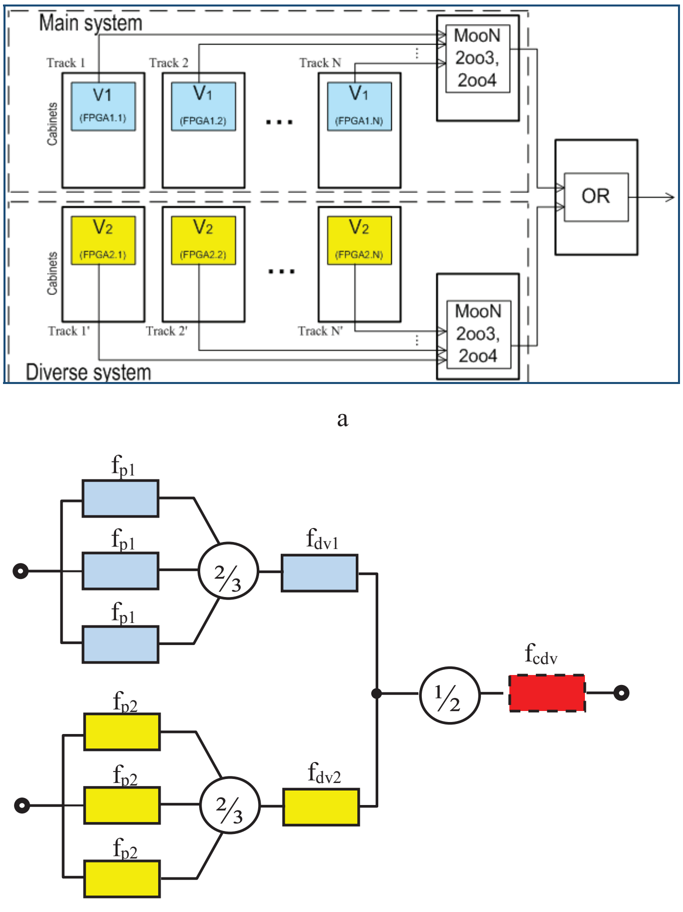
A. *Reactor trip system*

Application of diversity approach in safety critical NNP I&C systems is normative requirement of national and international standards [1-3]. An example of two-version system is reactor trip system (RTS) based on FPGA platform developed and implemented by RPC Radiy [2,7].

The RTS (Fig.7,a) consists of two identical in point of view functionality and structure systems (main and diverse) connected according with logic 1-out-of-2 (OR). Both systems have M-out-of-N structure as a rule 2-out-of03, but channels of systems are based on different hardware, FPGA and software designs.

Reliability block diagram of the RTS is shown on the Fig.7,b. This model describes a case with ideal diversity when system versions have not join design faults (components f_{d1} and f_{d2}). Hence such system tolerates design (software or FPGA) faults and physical (hardware and FPGA) faults.

This RBD takes into account common design faults of the versions (red element). They can cause CCF. Detailed research results of this system and RTS with other two-version structure considering version CCF risks are described in [12].



a

b

Fig. 7. Strucuture (a) and reliability block diagram (b) of RTS

Application of FPGA technology and FPGA-based platforms increase a number of diversity types and enlarge a set of possible diversity-oriented decisions. The following cases are possible and applied in NPP I&C systems:

- Central processing unit CPU1 vs CPU2 (different chips, manufacturers, languages and tools);
- FPGA vs CPU (main system is developed using FPGA, diverse system is developed using microcontroller);

- FPGA1 vs FPGA2 (different manufacturers, sub-technologies: SRAM-based, Flash, Anti-fuse, different development and verification techniques and tools).

Diversity allows improving some attributes of security (integrity and availability) for safety critical systems. Table 1 shows how different diversity types (according with classification [1]) can influence on security (integrity) of safety critical system [14]. Fuzzy expert scale of assessment (H – high, HM – high to medium, M – medium, L – low) has been chosen because calculating of quantitative metrics is complex separate task.

TABLE I. INFLUENCE OF DIVERSITY APPLICATION ON SECURITY

iversity Attributes (NUREG-CR/7007:2009)	*Vulnerability mitigation*
Design	
Different technologies	H
Different approaches within a technology	M
Different architectures within a technology	L
Equipment Manufacturer	
Different manufacturers of fundamentally different equipment designs	H
Same manufacturer of fundamentally different equipment designs	HM
Different manufacturers of same equipment design	M
Same manufacturer of different versions of the same equipment design	L
Logic Processing Equipment	
Different logic processing architectures	H
Different logic processing versions in same architecture	HM
Different component integration architectures	M
Different data flow architectures	L
Function	
Different underlying mechanisms to accomplish safety function	H
Different purpose, function, control logic, or actuation means of same underlying mechanism	M
Different response time scale	L
Life-Cycle	
Different design companies	H
Different management teams within the same company	HM
Different designers, engineers, and/or programmers	M
Different implementation/validation teams	L
Signal	
Different reactor or process parameters sensed by different physical effect	H
Different reactor or process parameters sensed by the same physical effect	M
The same process parameter sensed by a different redundant set of similar sensors	L
Software	
Different algorithms, logic, and program architecture	H
Different timing or order of execution	HM
Different runtime environments	M
Different functional representations	L

Gradation is based on risk reduction of successful attacks on version vulnerabilities depending on applied diversity types or subtypes.

Hence diversity is considered as a countermeasure for elimination of harmful consequences after successful attacks on vulnerabilities.

It must be emphasized that application of version redundancy can worsen other important security attribute such as confidentiality. This is partly because the intruder can attack one of the systems and access information. Besides, failed (interim) shutdown may be caused such intrusion as well. Hence in this case effect of "weak link in the chain" is possible and must be taken into account.

B. On-board aviation system

Very interesting multi-version structure of on-board flight control system (FCS) has been developed for A-340 and A-380 (Fig.8) [8]. The BCS consists of two diverse systems: primary (PCS) and secondary (SCS). Both systems consist of duplicated subsystems (three and two correspondingly). All five duplcated susbsystems have the same two CPU-based channels.

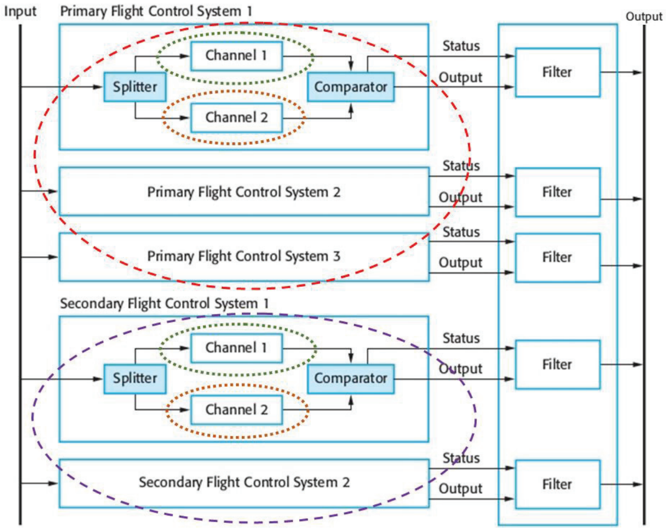
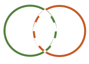
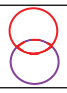
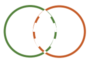
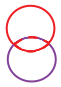


Fig. 8. Structure of control system of A340, A380 [8]

Applied diversity types are described by Table II. The following diversity types are implemented:

TABLE II. ANALYSES OF DIVERSITY TYPES IN CONTROL SYSTEM OF A340, A380

Systems	Components		Versions		CCF Model
			Ch1	Ch2	
PCS 3×(Ch1, Ch2)	HW	CPU	V_{CPU1}	V_{CPU2}	
		PCB	V_{PCB1}	V_{PCB2}	
	SW	ASW	V_{ASW1}		
		OS	V_{OS1}		
SCS 2×(Ch1, Ch2)	HW	CPU	V_{CPU1}	V_{CPU1}	
		PCB	V_{PSB1}	V_{PSB2}	
	SW	ASW	V_{ASW2}		
		OS	V_{OS2}		

- Equipment diversity of CPUs (different manufacturers and designs of CPUs for first and second channels Ch1 and Ch2 of all five subsystems);
- Equipment diversity of printed circuit boards (PCB) (different manufacturers and designs of PCSs for channels Ch1 and Ch2 of all five subsystems);
- Software diversity of PCS and SCS (different algorithms, different operation systems (OS) and applied software (ASW)).

The models of CCF for different diversity types are illustrated by last column of the table. Colors of version fault subsets corresponds to Fig. 8.

In contrast to RTS where diversity is divided on two systems (linear-parallel diversity) the FCS is based on so called matrix diversity. This principle of diversity distribution on systems has more complex model of CCF and must be supported high reliable on-line testing. Model for security assessment of such embedded system is more complex as well.

C. *On-board vehicle and railway systems*

The standard IEC 26262 contains requirement to application of diversity in on-board vehicle computer-based systems [15]. Two types of diversity are described in the standard: hardware based on use of different hardware platforms and software diversity based on use different system or/and applied software.

This huge industry domain hasn't experience on application of the diversity for on-board computer safety critical systems. However taking into account requirements and recommendations of the high level standard they will be implemented [16,17]. In this case experience of other safety critical domains including aviation and NPP I&C systems can be used [18].

In contrast to automotive domain diversity (functional, hardware and software) is applied in railway safety related systems very intensively (see review of design decisions in [19] .

IV. SOA-Based System Case. Diversity for Security

A. *Basic approach to architecture development*

Diversity can be successfully applied in business systems, in particular, in SOA(service oriented architecture)-based systems. It's explained existing a lot of targeted services with identical functionality and different configuration and components. In this case natural redundancy and diversity can be implemented.

Usually SOA consists of four components: operation system (OS), web-server (WS), application server (AS) and database (DB). Possibilities of use of diverse components in one SOA are formally described by four-level graph.

The functionally identical components are located at the one level, links between nodes (components) describe compatibility of the component [20]. Fig. 9 is a fragment of complete graph [21]).

SOA-based multi-version system is developed by selection and configuration of the compatible components linked in two or three different ways at the graph (for two- or three-version systems respectively).

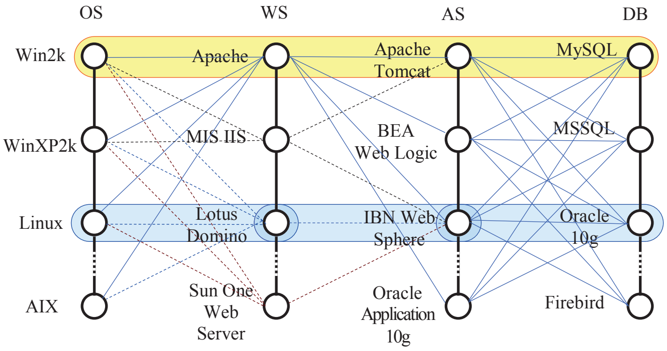


Fig. 9. Graph of SOA components compatibiity and version choice

Every node of the graph relates a set of vulnerabilities. Information about vulnerabilities for commercial software components is acceptable in open databases (NVD and others [21,22]).

B. *Security block diagram*

Using such information the sets of component and configuration vulnerabilities V_{Ci} can be obtained and used to develop the security block diagram for one SOA version (Fig. 10,a). Different configurations (versions) have different sets of vulnerabilities

Hence all pairs of configurations (ways of graph) can be assessed by diversity metrics considering a subset of common vulnerabilities and relation number of common and individual vulnerabilities [21]. For such pairs simplified security block diagram (Fig.10,b) takes into account "insecurity" of components and the configuration as a whole (red element).

Thus all diverse configurations are assessed and ranked according with security indicators similar RBD-based reliability assessment. Then complexity, costs and other metrics are calculated and optimal SOA for two-version system can be selected. Due to graph-based description of multi-version life cycle task of MVS development (choice and complexing diversity types) can be formulated and solved as a task of numeration and selection of ways on graph.

More detailed technique and tool to assess and configure the best architecture according with criterion "security-cost" and taking into account reliability and security metrics of configurators and connectors (for separated reservation of components) as well, attack profile and possibilities of dynamical reconfiguration of multi-version SOA in clouds, Markov's models and benchmarking experiences are described in [21,23,24].

These results confirm effectiveness of application of diversity approach in web- and cloud-based business systems and possibilities realization of some safety related functions using such technologies.

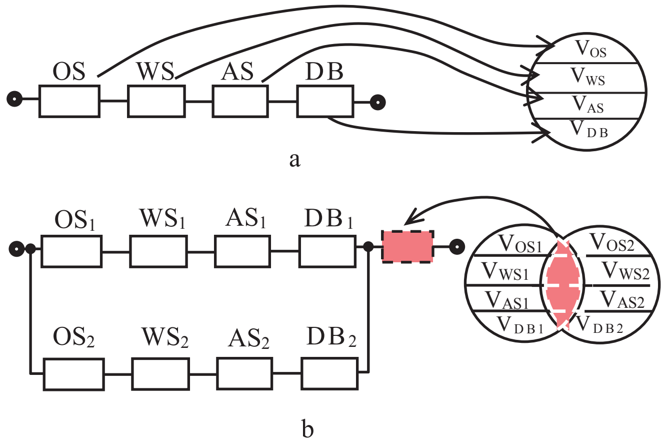


Fig. 10. Security block diagrams for one-(a) and two(b) version SOA

V. Industrial Case. Diversity for Survivability

A. *Post-accident monitoring system for critical infrastructure*

Diversity principle are applied to assure safety, security and survivability more complex cyber physical systems such as smart energy grid including digital substations and NPPs [25], pre- and post-accident monitoring system of nuclear reactor and power plant as a whole.

After Fukushima emergency the implementation of reliable and survivable post-accident monitoring systems (PAMS) is requirement of national and international regulatory bodies. PAMSs are necessary for other critical infrastructures (chemical enterprises, oil-gas transport systems and so on).

Existed NPP PAMSs are based on wired networks (WRN) connecting sensor area with the crisis centre. Reliability and survivability of such systems are assured by redundancy of equipment, cable communications and other components. In case of severe accident WRN-based PAMS can be added by wireless network (WLN) more resilient to physical failures.

To assure stable work of WLN-based PAMS subsystem after accident in conditions of powerful jamming a special means are required to support reliable transmission of data considering probable failures of WRN. For that and to improve survivability of PAMS introduction of drone fleet subsystem (DS) has been suggested in [26]. The structure of integrated WRN&WLN&DS-based PAMS is shown on Fg.11.

The following principles of embedding of drone fleet system functioning are the following.

- The drone fleet is located permanently at a considerable distance from the NPP. The communication network (WLN +DS) is deployed after the accident and drones fly to the accident zone.
- Drones fleet is divided by the role and equipment into: repeaters (Slave), that work together on a principle of “one leader” and if the “leading drone-repeater” (Master) is damaged then other drone-repeater takes Master functions; observers (equipped with a TV camera), that enable to run the continuous visual monitoring of the accident location; additional sensors, that can be located in drones or be dropped down in certain places). Drones should be able to change their role by upgrading equipment at the location base.
- Measurement and control modules are equipped with backup batteries, blocks of wireless communication, as well as, self-testing and self-diagnostic systems.
- To meet the system requirements the self-adaptability, self-testing and self-healing procedures are used.

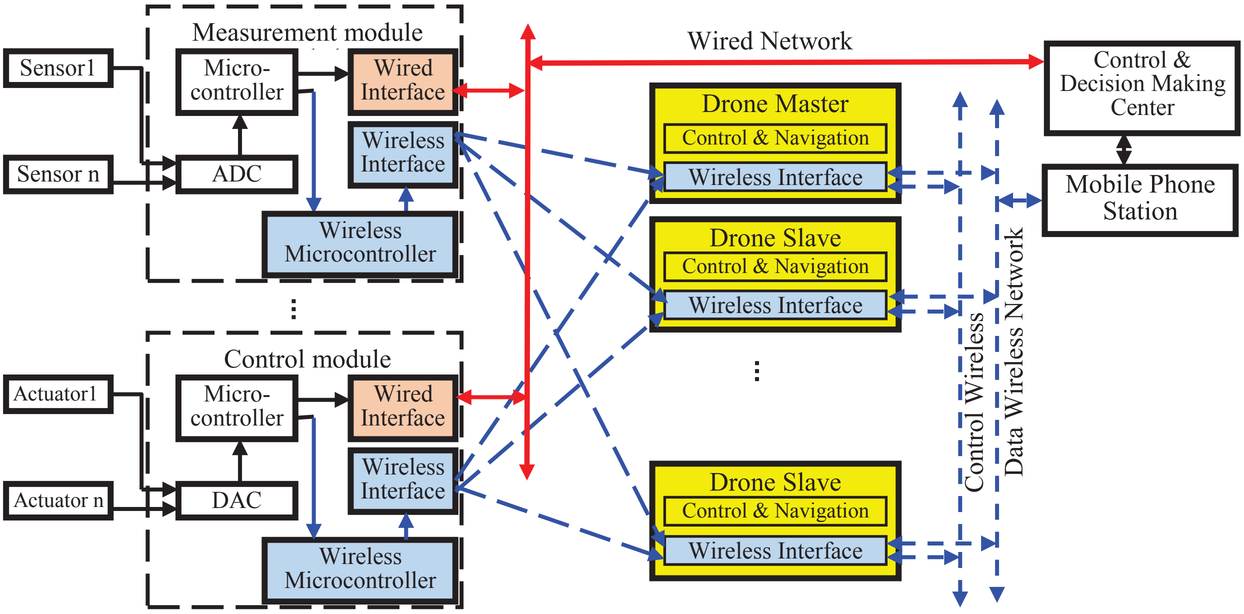


Fig. 11. The structure of integrated PAMS [25]

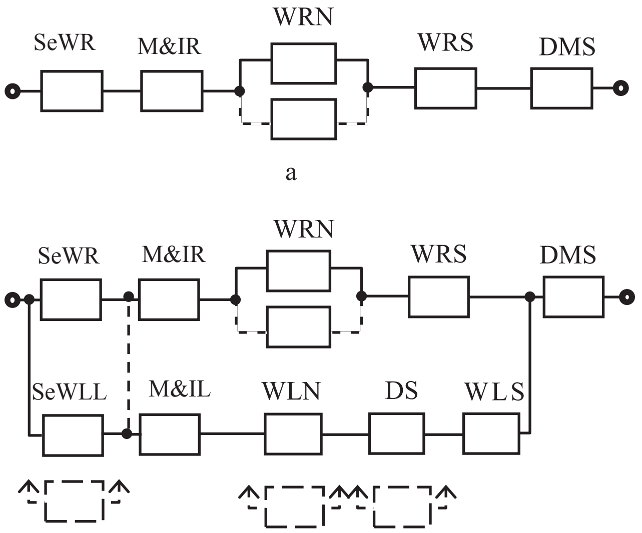
B. *Reliability and survivability models*

Reliability block diagrams for initial WRN-based PAMS (a) and for one of the possible most simple options of integrated system (b) are shown on Fig.12. These models take into account failure of the following elements:

- sensors for WRN and WLN (SeWR and SeWL);
- microcontrollers with AD/DA convertors and interfaces for WRN and WLN (M&IR and M&IL relatively);
- WRN and station WRS; WLN,
- drones (DS) and station WLS;
- decision making systems located at the crisis centre.

In fact WLN&DS system of PAMS is diverse for WRN system. Both systems have redundant elements. For first one sliding redundancy of sensors, wireless network and drones are applied. Such flexible redundant structure has more high reliability and survivability because decreases risk of common cause multiple failures [27].

Survivability of integrated PAMS is calculated using diagrams of degradation and combinatorial assessment of probabilities for different states.



a

b

Fig. 12. Security block diagram of one (a) channe and multi-version (b) SOA

VI. Conclusion

In spite of long time experience of multi-version systems in safety, mission, data and business critical domains these systems remain unique and in certain sense exotic. On the other side diversity is single, efficient and which is why unique principle of decreasing CCF risks.

Implementation of diversity and D3 principle is “expensive pleasure” therefore its application must be grounded, actual diversity level must be assessed by quantitative way (or qualitative if assumed by regulator), and required level of diversity or acceptable risks of CCF in developed system must be proved.

Diversity allows improving not only of reliability and safety and security as well. As safety and security are very important and closely related (there is circle “safety-security” via system and environment) application of diversity can assure multiple effect.

On the other side there are limitations of diversity application for improving of some security attributes, for example confidentiality.

Analysis of industrial cases allows concluding that implementation of diversity requires high level of design, verification and maintenance teams.

Future research could be related to development and adaption of existed assessment techniques and tools [28,29] for complex cyber physical systems and more deep and accurate assessment of application diversity for cyber security.

Acknowledgment

It is my pleasure to thank my colleagues from research group on dependable computing and Department of Computer Systems and Networks, National Aerospace University KhAI, Centre for Safety Infrastructure-Oriented Research and Analysis, RPC Radiy and participants of TEMPUS and FP7 projects MASTAC, SEREIN, SAFEGUARD, KhAI-ERA for all-round discussion of results described in the paper.

References

[1] NUREG/CR 7007-2009. Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, ONL, Oak Ridge, USA, 2009.

[2] M. Yastrebenetsky, V. Kharchenko (editors). Nuclear Power Plant Instrumentation and Control Systems for Safety and Security, IGI Global, Hershey PA, 2014.

[3] IEC 61508-2009. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, 2009.

[4] R. Bloomfield, K. Netkachova, R. Stroud. Security-Informed Safety: If It’s Not Secure, It’s Not Safe. Proceedings of the 5th WS Software Engineering for Resilient Systems, SERENE2013, Kyiv, Ukraine/A. Gorbenko, A. Romanovsky, V.Kharchenko (edits), Springer, 2013.

[5] V. Kharchenko, E. Brezhnev, O. Illiashenko, A. Boyarchuk. Security Informed Safety Assessment of Industrial FPGA-Based Systems. Proceedings of the 12th International Probabilistic Safety Assessment and Management Conference, PSAM 2014, Honolulu, Hawaii, USA, 2014.

[6] 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.

[7] V. Kharchenko, A. Siora, E. Bakhmach. Diversity-Scalable Decisions for FPGA-Based Safety-Critical I&Cs: from Theory to Implementation. 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.

[8] I. Sommerville. Software Engineeringh, 9th Edition, Addison-Wesley, 2011.

[9] L. Pullum. Software Fault Tolerance Techniques and Implementation, Artech House Computing Library, 2001.

[10] S. Vilkomir, V. Kharchenko. A Diversity Model for Multi-Version Safety-Critical I&C Systems. Proceedings of the 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference, PSAM-ESREL 2012, Helsinki, Finland, 2012.

[11] V. Kharchenko, T. Nikitina, S. Vilkomir. Optimal Selection of Diversity Types for Safety-Critical Computer Systems. Proceedings of the 12th International Probabilistic Safety Assessment and Management Conference, PSAM 2014, Honolulu, Hawaii, USA, 2014.

[12] V. Kharchenko, A. Volkoviy, O. Siora, V. Duzhyi. Metric-Probabilistic Assessment of Multi-Version Systems: Some Models and Techniques. Dependable Computer Systems: Advances in Intelligent and Soft Computing, Springer, Volume 97, 2011.

[13] B. Littlewood. The Impact of Diversity upon Common Mode Failures. Reliability Engineering and System Safety,Vol.5, 1, 1996.

[14] V. Kharchenko, O. Illliashenko. Diversity for Security: Case Assessment for FPGA-based Safety Critical Systems. Proceedings of the 20th Internation Conference on Conference on Circuits, Systems, Communications and Computers, CSCC2016, Corfu Island, Greece, 2016.

[15] ISO 26262-1-2011. Road vehicles – Functional safety, 2011.

[16] D. Negi, N. Bagri, V. Agarwal, Redundancy for Safety-Compliant Automotive and Other Devices, EDN Network, 2014

[17] C.Turner Safety and Security for Automotive SoC Design, WS ARM, Seul-Korea, Taibei-Taiwan, 2016 http://www.arm.com/files/pdf/20160628_B02_ATF_Korea_Chris_Turner.pdf

[18] V. Kharchenko. Diversity for Safety of Systems and Software in Context of the Standard ISO/IEC26262. 13th Workshop on Automotive on Software and Systems, Milano, Italy, 2015. http://www.ices.kth.se/upload/events/76/7577a93992a142f9b6e51b0a40698831.pdf

[19] I. Malynyak. Functional Diversity Design of Safety Related Systems. Proceedings of 11th International Conference ICT in Education, Research and Industrial Applications: Integration, Harmonization and Knowledge Transfer, ICTERI-TheRMIT2015, Lviv, Ukraine, 2015.

[20] A. Gorbenko, V. Kharchenko, O.Tarasyuk, A. Furmanov. F(I)MEA-Technique of Web-services Analysis and Dependability Ensuring Rigorous Development of Complex Fault-Tolerant Systems, LNCS 4157. Springer. 2006.

[21] V. Kharchenko, A. Gorbenko (editors). Web, Grid Cloud Technologies for Dependable IT-Infrastructures.-Project TEMPUS-SAFEGUARD, National Aerospace University KhAI, 2013.

[22] National Vulnerability Database, National Institute of Standards and Technologies, USA, 2016 https://nvd.nist.gov/

[23] V. Kharchenko, Alaa Mohammed Abdul-Hadi, A. Boyarchuk, Yu. Ponochovny. Web Systems Availability Assessment Considering Attacks on Service Configuration Vulnerabilities. Proceedings of DepCoS-RELCOMEX 2014, Brunow, Poland, Springer, 2014.

[24] V. Kharchenko, A. Abdul-Hadi, A. Boyarchuk, Yu. Ponochovnyj. Web Systems Availability Assessment Considering Attacks on Service Configuration Vulnerabilities. Seria «Information and Communication Technologies in Education, Research, and Industrial Applications Communications in Computer and Information Science» Vol. 469 / V. Ermolayev et al (edits), Springer International Publishing Switzerland, 2014

[25] E. Brezhnev, V. Kharchenko, A. Boyarchuk, J. Vain. Cyber Diversity for Security of Digital Substations under Uncertainties: Assurance and assessment. Proceedings of the 19th Internation Conference on Conference on Circuits, Systems, Communications and Computers, CSCC2015, Zakynthos Island, Greece, 2015.

[26] A. Sachenko, V. Kochan, V. Kharchenko et al. Mobile Post-Emergency Monitoring System for Nuclear Power Plants. Proceedings of the 12th ICT in Education, Research and Industrial Applications: Integration, Harmonization and Knowledge Transfer, ICTERI-TheRMIT2016, Kyiv, Ukraine, 2016.

[27] V. Kharchenko, A. Sachenko, V. Kochan, H. Fesenko. Reliability and Survivability Models of Integrated Drone-Based Systems for Post Emergency Monitoring of NPPs. Proceedings of the International Conference on Information and Digital Technologies, IDT2016, Rzeszow, Poland, 2016.

[28] V. Kharchenko, V. Sklyar, E. Brezhnev, V. Duzhyi. FPGA Platform-Based Multi-Version NPP I&C Systems: Diversity Assessment and Selection of Variants. Proceedings of the 6th ANS International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology, NPIC&HMIT 2015, Charlotte, NC, USA: American Nuclear Society, 2015.

[29] V. Kharchenko, A. Siora, V. Sklyar, A. Volkoviy. Multi-Diversity Versus Common Cause Failures: FPGA-Based Multi-Version NPP I&C Systems. In Proceedings of the 7th ANS International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technologies, NPIC&HMIT 2010, Las-Vegas, Nevada, CA, USA: American Nuclear Society, 2010.