Diversity for Safety of Systems and Software in Context of the Standard ISO/IEC26262

Vyacheslav Kharchenko, Eugene Brezhnev,

Centre for Safety Infrastructure-Oriented Research and Analysis

National Aerospace University KhAI, Department of Computer Systems and Networks

Kharkiv, Ukraine

13th WS on Automotive Software and Systems

November 12, 2015, Milan, Italia

Research and Production Corporation Radiy: Location

NPPs Capacity: 13,880 MW (8th position in the world, more 50% of total Ukrainian energy)

Belarus

Centre for Safety Infrastructure Research and Analysis, R&V&T of the RPC Radiy

Poland

Slovakia

Rivne NPP
2×VVER-1000
2×VVER-440

Kyiv

Russia

Khmelnitsky NPP
2×VVER-1000

Poltava (V&V Group)

Kharkiv
(KhAI DCSN, STC)

South-Ukrainian NPP
3×VVER-1000

Kirovograd
(RPC Radiy)

Zaporizhya NPP
6×VVER-1000

Hungary

Romania

Moldova

Research and Production Corporation Radiy: Our team

NPPs Capacity: 13,880 MW (8th position in the world, more 50% of total Ukrainian energy)

Belarus

Centre for Safety Infrastructure Research and Analysis, R&V&T of the RPC Radiy

Poland

Slovakia

Rivne NPP
2×VVER-1000
2×VVER-440

Kyiv

Khmelnitsky NPP
2×VVER-1000

Poltava (V&V Group)

Russia

Kharkiv
(KhAI DCSN, STC)

South-Ukrainian NPP
3×VVER-1000

Kirovograd
(RPC Radiy)

Zaporizhya NPP
6×VVER-1000

Hungary

Romania

Moldova

Main activities of KhAI&STC (15 years): R&D&IVV in safety and security critical domains (NPP, aerospace, automotive,…)

Outline

Introduction

- Motivation and objectives

Challenges of diversity approach application

- Uniqueness of multi-version I&Cs
- Standards review. IEC26262
- Assessment issues

Techniques and tools for diversity assessment and choice. Our experience

- NUREG 7007-based technique
- Check-list and Graph-based techniques and tools
- Technique of version generation and choice

Proposals and activities to implement diversity in automotive SW&S

Conclusions

- Discussion and next steps

Techniques and tools for assessment and assurance of cybersecurity

-V

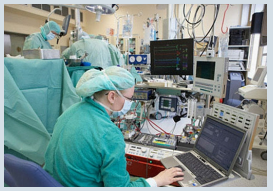
- V2V
- V2I

1. Introduction: Common Cause Failures and Diversity

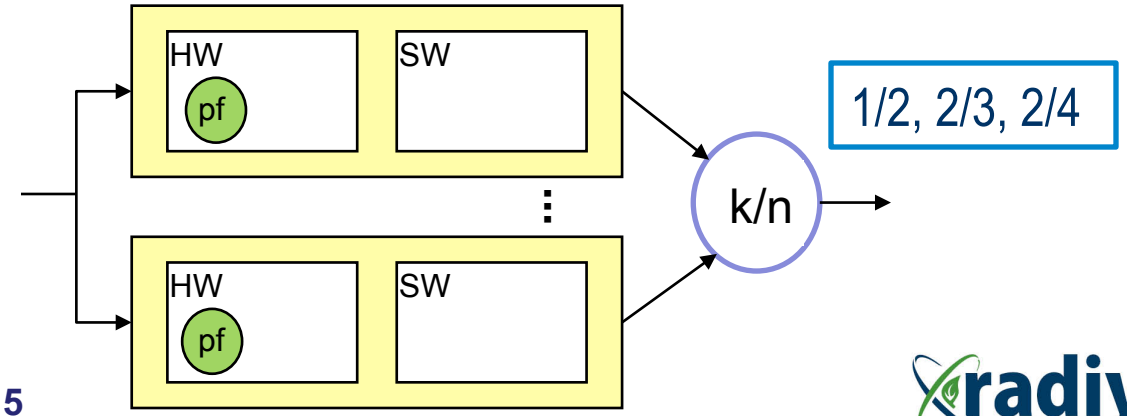
- **Problem of computer-based I&Cs safety** ≈ problem of decreasing common cause failure (CCF) probability
- **Three most probable reasons of CCFs:**

- **multiple (common) physical faults (pf)** of redundant channels HW caused by external or internal factors and element deterioration);







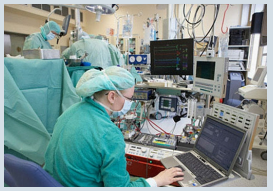


1. Introduction: Common Cause Failures and Diversity

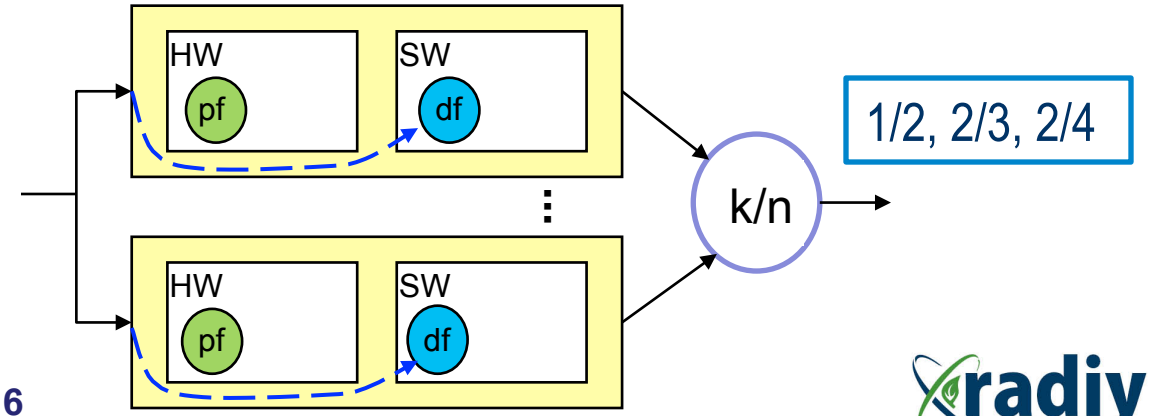
- **Problem of computer-based I&Cs safety** ≈ problem of decreasing common cause failure (CCF) probability
- **Three most probable reasons of CCFs:**

- **multiple (common) physical faults (pf)** of redundant channels HW;
- **replicated design faults (df)** of SW (or FPGA design) components (all redundant channels, 20-50% of failures for space systems (1990-2012));







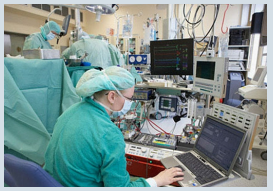


1. Introduction: Common Cause Failures and Diversity

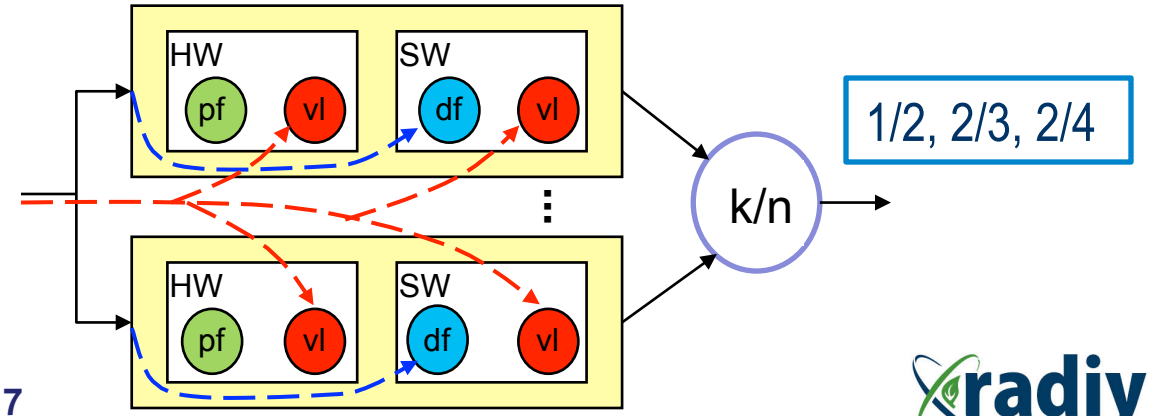
- **Problem of computer-based I&Cs safety** ≈ problem of decreasing common cause failure (CCF) probability
- **Three most probable reasons of CCFs:**

- **multiple (common) physical faults (pf)** of redundant channels HW;
- **replicated design faults (df)** of SW (or FPGA design) components (all redundant channels, 20-50% of failures for space systems (1990-2012));
- **multiple interaction faults** caused by SW/FPGA/HW **vulnerabilities (vl)** and **intrusions (attacks)** to ones





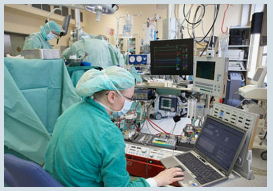




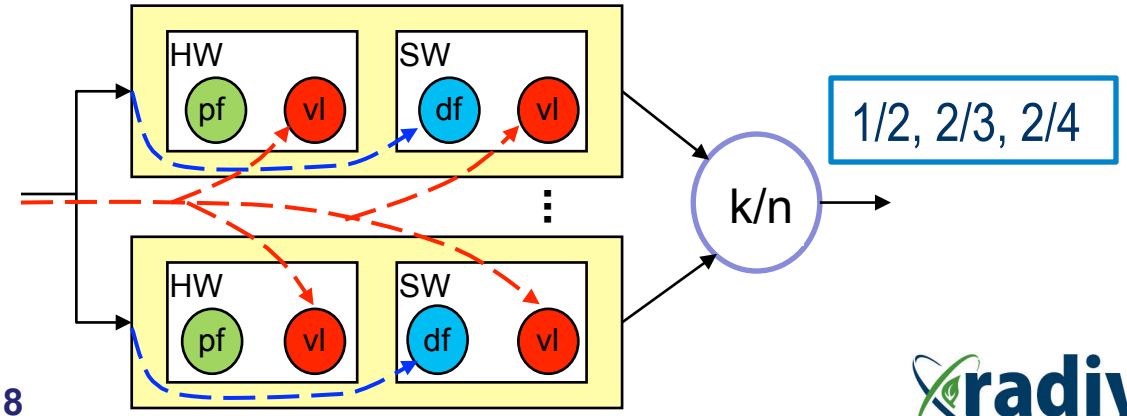
1. Introduction: Common Cause Failures and Diversity

• **Ordinary structure (and time) redundancy does not** decrease probability of different CCF types and is not effective in context of design and interaction faults.









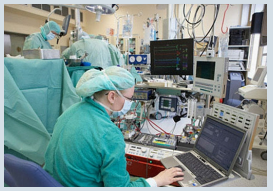
1. Introduction: Common Cause Failures and Diversity

• **Ordinary structure (and time) redundancy does not** decrease probability of different CCF types and in not effective.

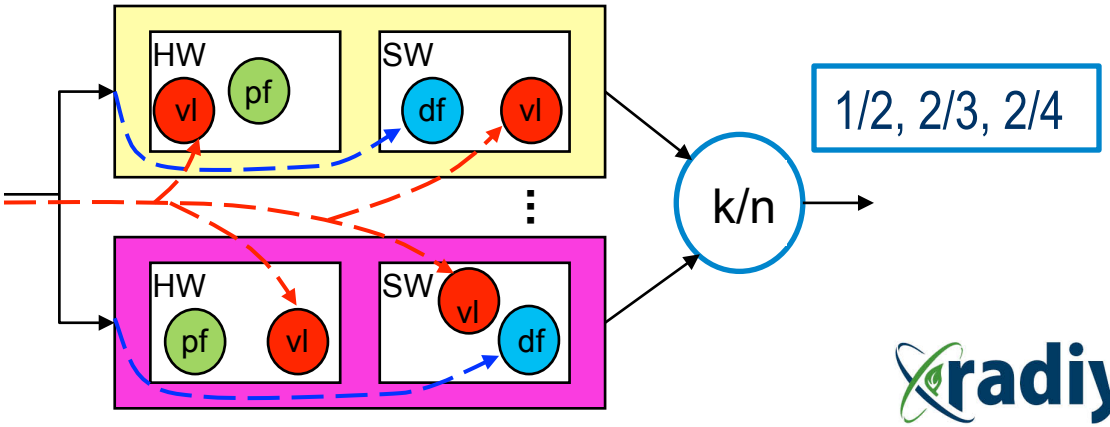
• **Diversity** (multiversity, multi-diversity) (**IEC60880**, NPP I&C) is a principle providing use of several versions (version process/product redundancy) to perform the same function by two and more options.
(**IEC61508**: different means of performing a required function).
(**IEC26262**: different solutions satisfying the same requirement with the aim of independence).

• **Application of diversity can avoid or appreciably decrease risk of CCF. Is it axiom, theorem or supposition?**









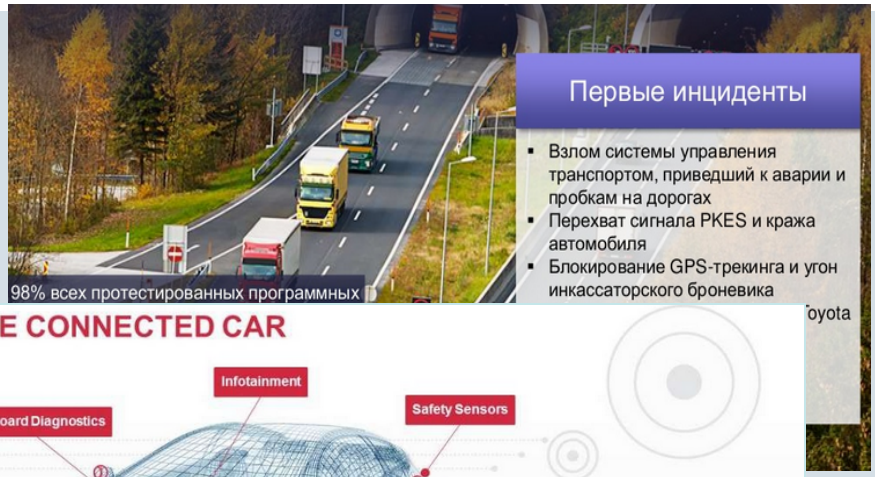
1. Introduction: Safety and Security for Automotive Domain

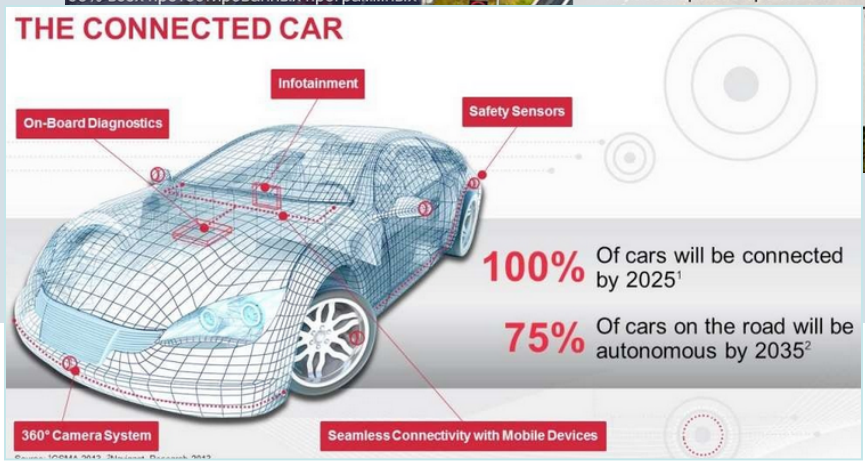
Hot facts

- lines of (VehSW) code > lines of (SpaceSW)
- VehSW ~ 1 GB, ~ 3800 interfaces
- VehSW supports 90% innovations
- 98% VehSW has faults
- domino effect for V2V and V2I ("automotive" blackout via CCF!)

A lot of attacks

- changing of route,
- arbitrary self-acceleration,
- breaking of traffic control system…





http://www.smileexpo.ru/ru/prezentatsiya-cisco-ob-avtomobilnoy-kiberbezopasnosti

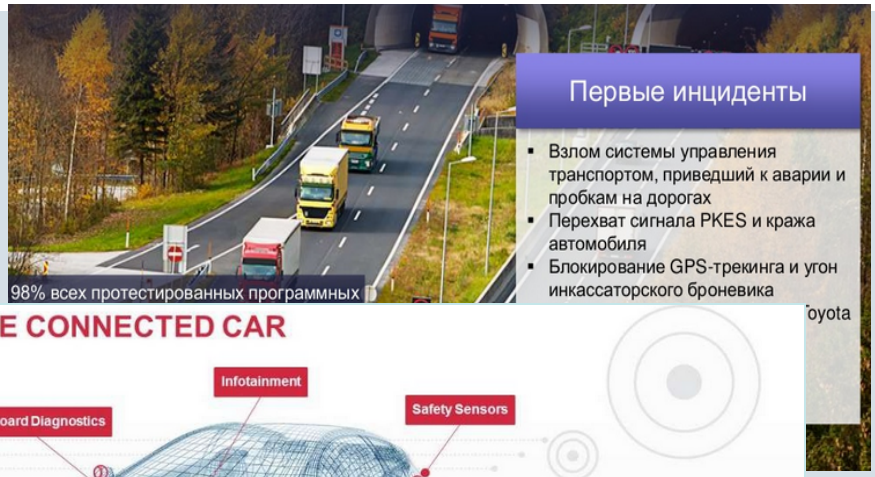
1. Introduction: Safety and Security for Automotive Domain

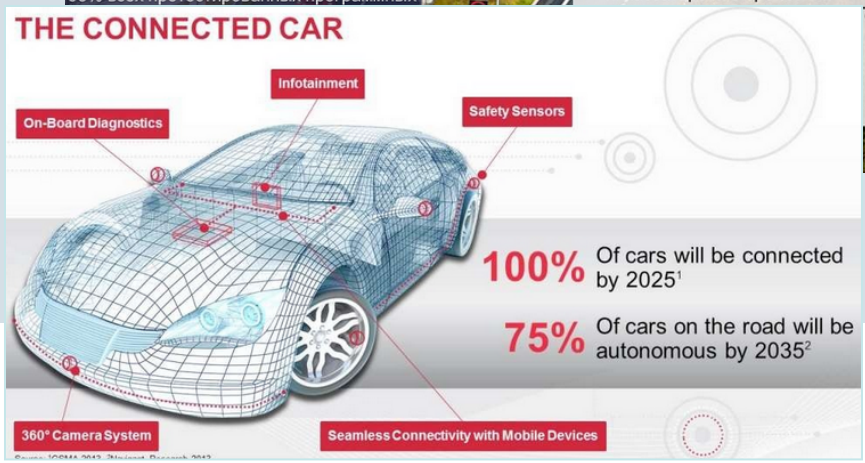
Hot facts

- lines of (VehSW) code > lines of (SpaceSW)
- VehSW ~ 1 GB, ~ 3800 interfaces
- VehSW supports 90% innovations
- 98% VehSW has faults
- domino effect for V2V and V2I ("automotive" blackout via CCF!)

A lot of attacks

- changing of route,
- arbitrary self-acceleration,
- breaking of traffic control system…





Hence physical, design and interaction faults are possible.

How diversity can help?

http://www.smileexpo.ru/ru/prezentatsiya-cisco-ob-avtomobilnoy-kiberbezopasnosti

Objectives

- Analysis of challenges regarding diversity application in industrial I&Cs
- Review of some diversity-oriented industrial decisions
- Comparison of standards (ISO/IEC 26262, ISO/IEC 60880, NUREG 7007) requirements, techniques and tools for diversity assessment/development supporting
- Our experience and discussion of R&D activities for automotive SW&S

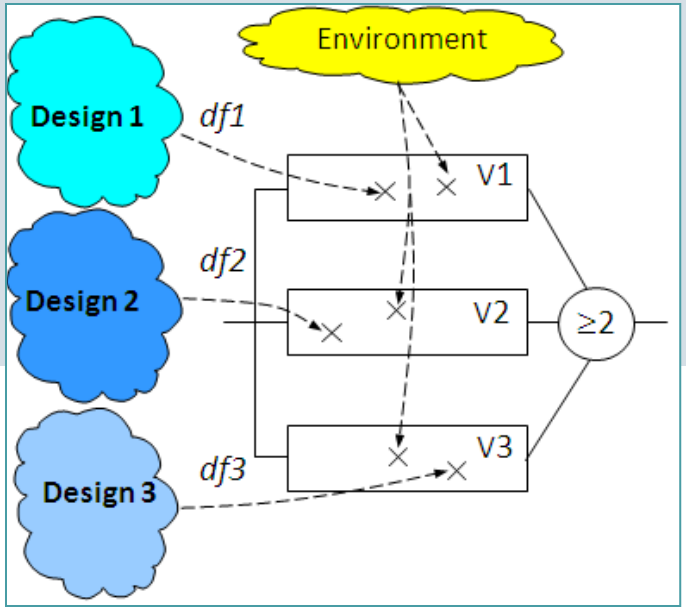
Could experience in other critical domains (NPP I&C, aerospace) be adopted and applied in automotive domain?

Which and How?

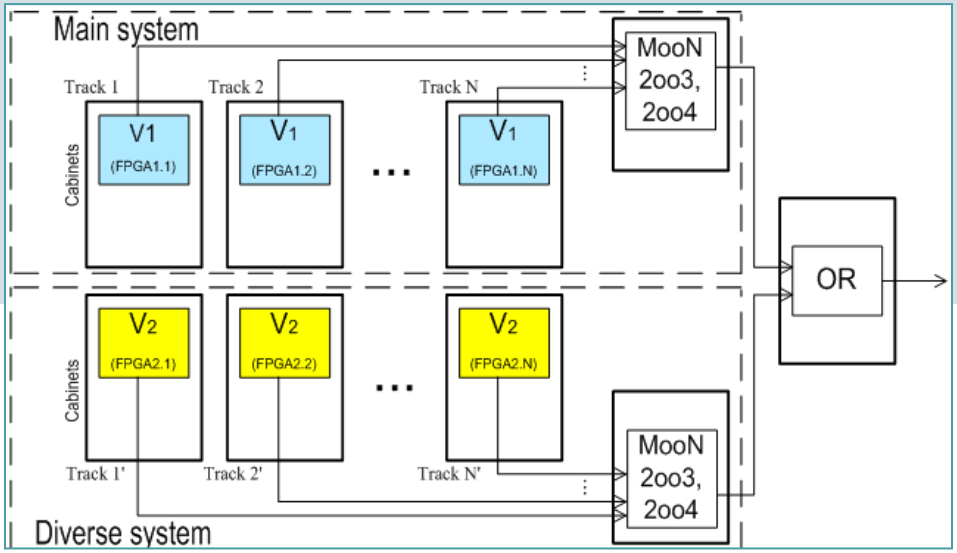
2. Diversity Related Concepts and Questions

- **Main conceptions of diversity:**

Multi-version system (a system in which n>1 versions-products are used; in general case (n,l)-system or (n,m,l)-system, l - number of channels).



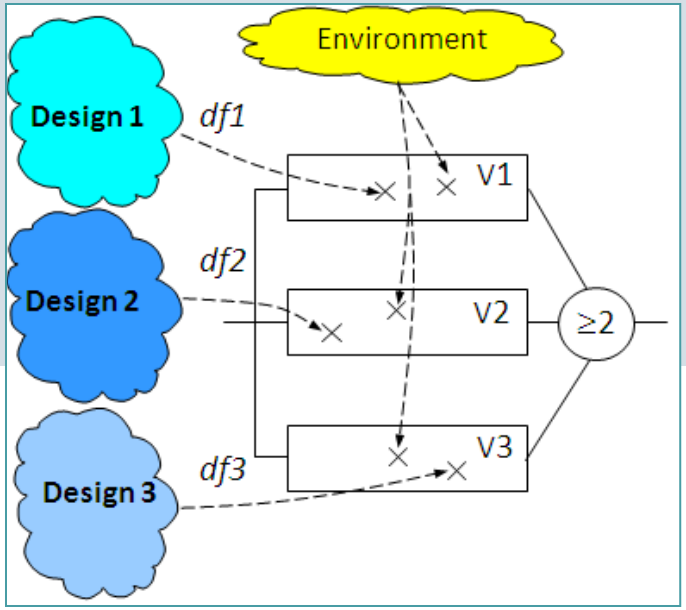
NPP Reactor Trip System (2,m,6(8))



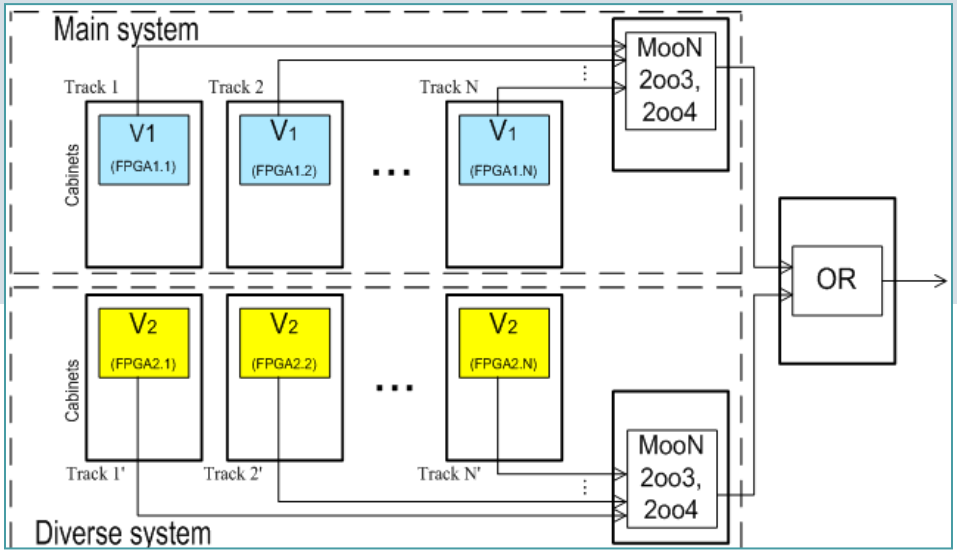
2. Diversity Related Concepts and Questions

- **Main conceptions of diversity:**

Multi-version system (a system in which n>1 versions-products are used; in general case (n,l)-system or (n,m,l)-system, l - number of channels).



NPP Reactor Trip System (2,m,6(8))



A340,380 on-board control systems (2,4,10)

Cloud Computing service system (2,1,2/3)

2. Diversity Related Concepts and Questions

- **Main conceptions of diversity:**

Multi-version system (a system in which n>1 versions-products are used; in general case (n,l)-system or (n,m,l)-system, l - number of channels).
Strategy of diversity (a set of general criteria defining principles of VR types/volume choice).
Multi-version technology *(*a set of the interconnected rules and design decisions leading to development of two or more intermediate or end-products).
Multi-version life cycle, multi-version project, diversity metrics…

- **There are two key ("eternal") questions regarding diversity:**

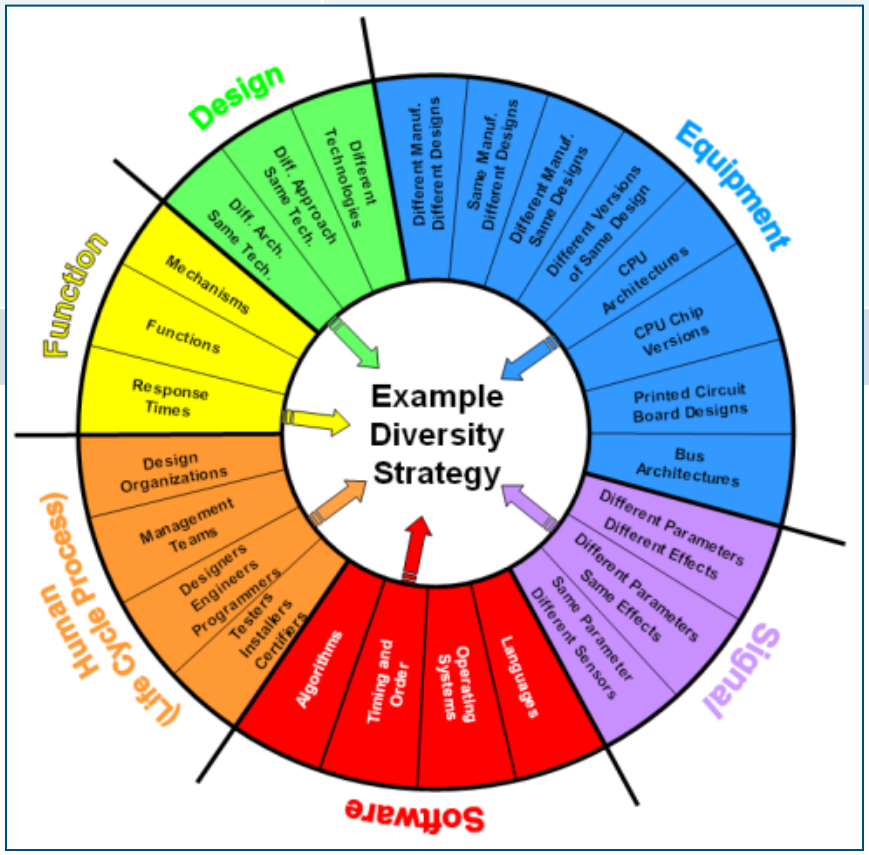
  How to assess actual value of diversity?
  How to ensure required value of diversity?

- **Practical issue:**

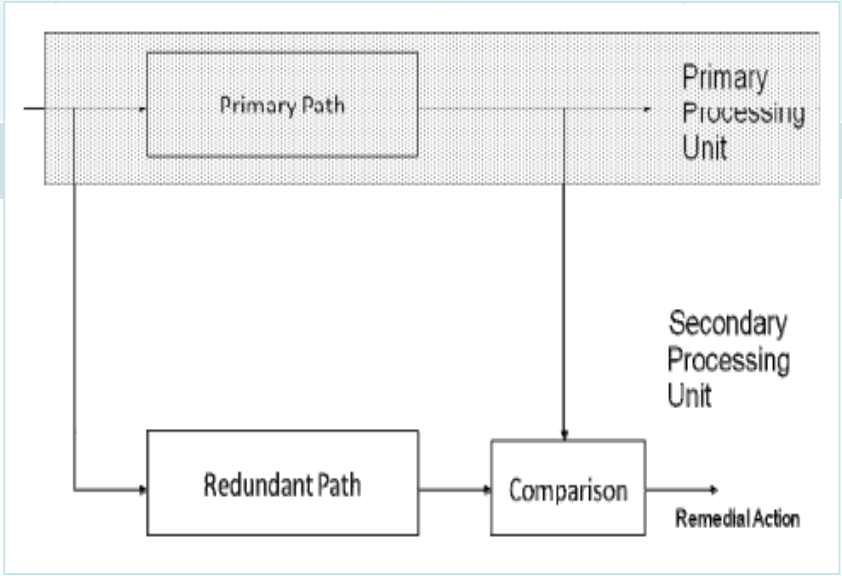
  How to assess of I&C diversity value to meet standard requirements and choice diversity types and volume by optimal (required safety / minimal cost) way?

3. Challenges: Uniqueness of MVSs

Aspect	Challenge	Question
1. Uniqueness of multi-version systems	There are a lot of DA implementations *but*: - MVSs are applied in NPPs (NUREG7007, R. Wood et.al.), aviation, railway, automotive (IEC26262)… in different way	?



This approach allows for hardware and software diversity if different processor types are used as well as separate algorithm designs, code and compilers.



radiy

XAI

classification:
- design, - equipment.
- signal, - software,
- human, - function
+ second level

IEC26262:
- SW,
- HW

Diversity types (NUREG 7007)	Diversity types (IEC 26262)
Design	
Equipment / Manufacturer	Yes
Function	
Human	
Signal	
Software	Yes

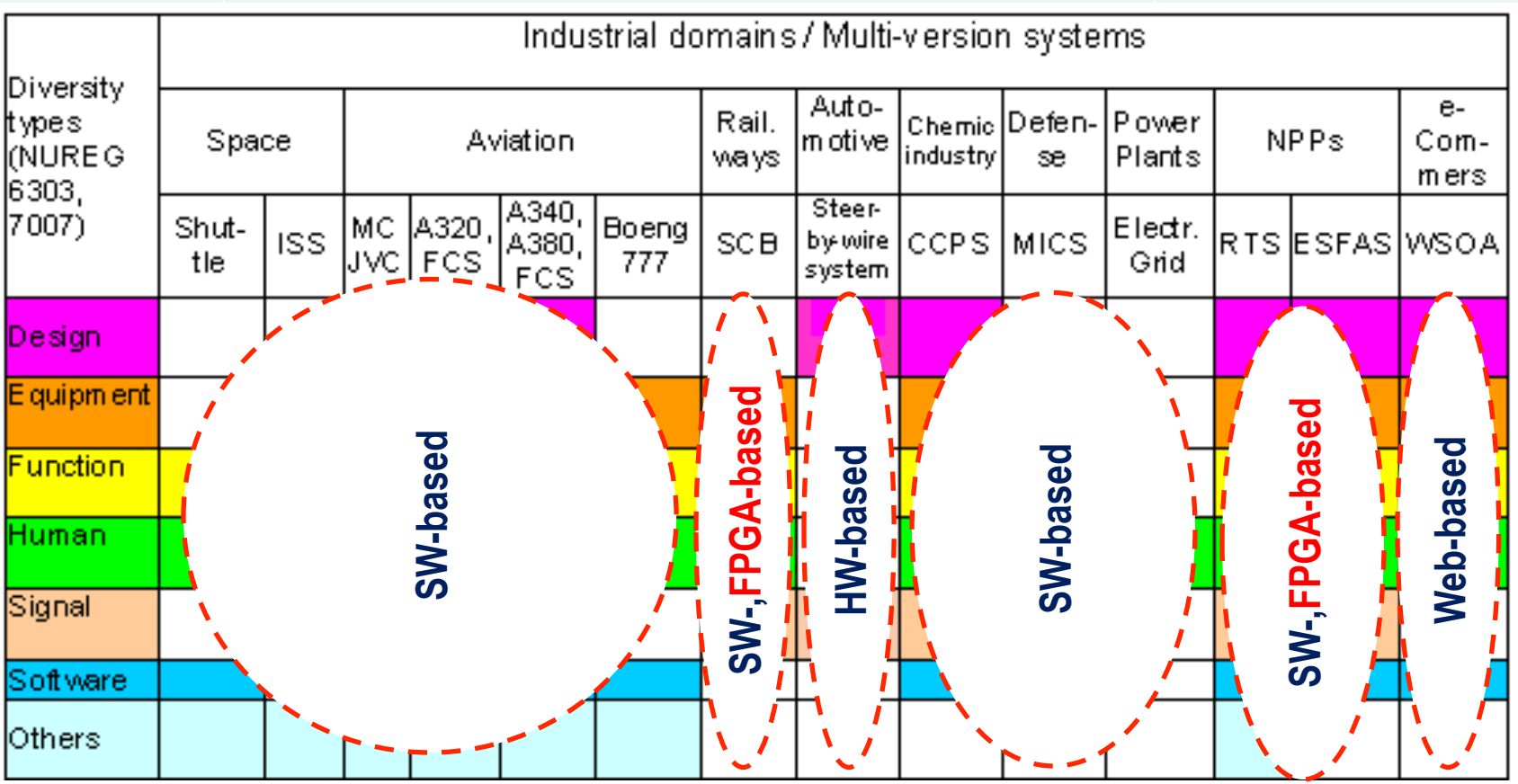
3. Challenges: Uniqueness of MVSs

Aspect	Challenge	Question
1. Uniqueness of multi-version systems	There are a lot of DA implementations *but*: - MVSs are applied in NPPs, aviation, railway,… in different way;	?

Diversity types (NUREG 6303, 7007)	Industrial domains / Multi-version systems													
	Space		Aviation				Rail. ways	Auto-motive	Chemic industry	Defen-se	Power Plants	NPPs		e-Com-mers
	Shut-tle	ISS	MC JVC	A320, FCS	A340, A380, FCS	Boeng 777	SCB	Steer-by-wire system	CCPS	MICS	Electr. Grid	RTS	ESFAS	WSOA
Design														
Equipment														
Function														
Human														
Signal														
Software														
Others														

3. Challenges: Uniqueness of MVSs

Aspect	Challenge	Question
1. Uniqueness of multi-version systems	There are a lot of DA implementations *but*: - MVSs are applied in NPPs, aviation, railway,… in different way;	?



3. Challenges: Uniqueness of MVSs

Aspect	Challenge	Question
1. Uniqueness of multi-version systems	There are a lot of DA implementations but: - MVSs are applied in NPPs, aviation, railway,… **in different way;** **- component failures occur rarely** (Radiy more 105 years experience); **- use of statistical evaluation methods is limited**; **- comparative analysis** of MVS failures for different domains is not enough.	***How we should compare experience for different domains and take features of DA use into consideration?*** ***Standard IEC 26262?***

3. Challenges: New Technologies and Risks

Aspect	Challenge	Question
2. Technologies and risks	**… FPGA technology (as "the third force")**: - ensures **new possibilities** for implementation of diversity approach (DA): • MP1 vs MP2 (SW-based), • FPGA vs MP, • FPGA1 vs FPGA2, etc; - can create **additional risks** and **deficits of safety** or **transform pre-existed;** - stipulates necessity: • to use positive features of MP/FPGA, • to analyze and decrease such risks.	***How we can use the features of MP/FPGA technology take into account and decrease specific risks?***

Standard 26262 doesn't contain any requirements/ recommendations concerning actual diversity assessment

3. Challenges: Standard Requirements

Aspect	Challenge	Question
3. Standards	**Existed standards** don't contain the **detailed requirements and techniques:** - **to assess** multi-version I&Cs (including MP/FPGA-based), - **to apply DA** for MP/FPGA-based I&Cs development, i.e. **to determine** requirements to processes and products for MVSs.	?

- → IAEA and IEC documents:
  - → IAEA NS-R-1: Safety of Nuclear Power Plants: Design (6.14, 6.34, 6.40, 6.85);
  - → IAEA NS-G-1.1: Software for Computer Based Systems Important to Safety in NPPs;
  - → IAEA NS-G-1.3: I&Cs important to safety in NPPs:
  - → IAEA NP-T-1.5: Protecting against CCFs in Digital I&C Systems of NPPs
  - → IEC 61513: NPPs - I&Cs important to safety – general requirements for systems;
  - → IEC 60880: NPPs - I&Cs important to safety - Software aspects for computer-based systems performing category A functions;
  - → IEC 62340: NPPs - I&Cs important to safety - Requirements for coping with CCF…
  - → IEC 26262: Road Vehicles Functional Safety

3. Challenges: Standard Requirements

Aspect	Challenge	Question
3. Standards	**Existed standards** don't contain **detailed requirements and techniques:** - **to assess** multi-version I&Cs (including MP/ FPGA-based systems), - **to apply DA** for MP/FPGA-based I&Cs development, i.e. **to determine** requirements to processes and products for MVSs.	***What should be severity of regulation for DA implementation?*** ***What requirements and procedures of assessment and development of MP/FPGA-based I&C should be?***

IAEA and IEC documents:

→ IAEA NS-R-1: Safety of Nuclear Power Plants: Design (6.14, 6.34, 6.40, 6.85);

US documents:

→Regulatory Guide 1.152, Revision 2: Criteria for Use of Computers in Safety Systems of NPPs;

→IEEE Std 603: IEEE Standard Criteria for Safety Systems for NPP;

→IEEE Std 7-4.3.2: IEEE Standard Criteria for Digital Computers in Safety Systems of NPPs;

→Branch Technical Position 7-19 - Guidance for evaluation of D3 in digital I&Cs;

ISO/IEC262622 is not complete!

Summary:

The standards contain (should contain, for automotive SW/systems) requirements to:

(a) types of systems where diversity should/ must be applied (No);

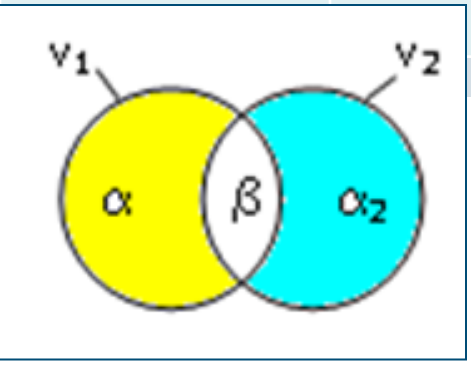
(b) types of version redundancy (Yes);

(c) recommendations to assessment procedures (No)

…

3. Challenges: Safety Assessment

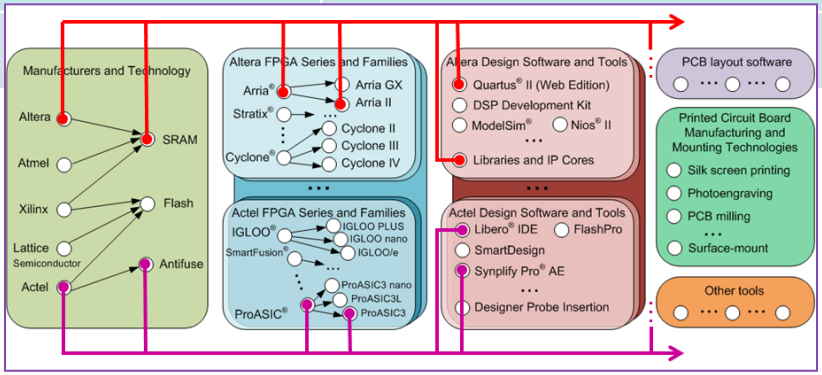
Aspect	Challenge	Question
4. Safety assessment	**There is a problem of CCF risks assessment and MVS safety assessment as a whole.** ▪ Inaccurate assessment either increases risk of fatal failure (overstated assessment) *or* increases risk of unreasonable costs (understated assessment). ▪ β-factor (indicator of CCF risk: common faults of the version sets / all faults of the version)	***What indicators (metrics), techniques and tools we should use*** ***- to assess actual diversity level (β-factor) and multi-version (MP/FPGA-based) I&C safety,*** ***- to compare different structures of MVS according with criterion "safety-cost"?***

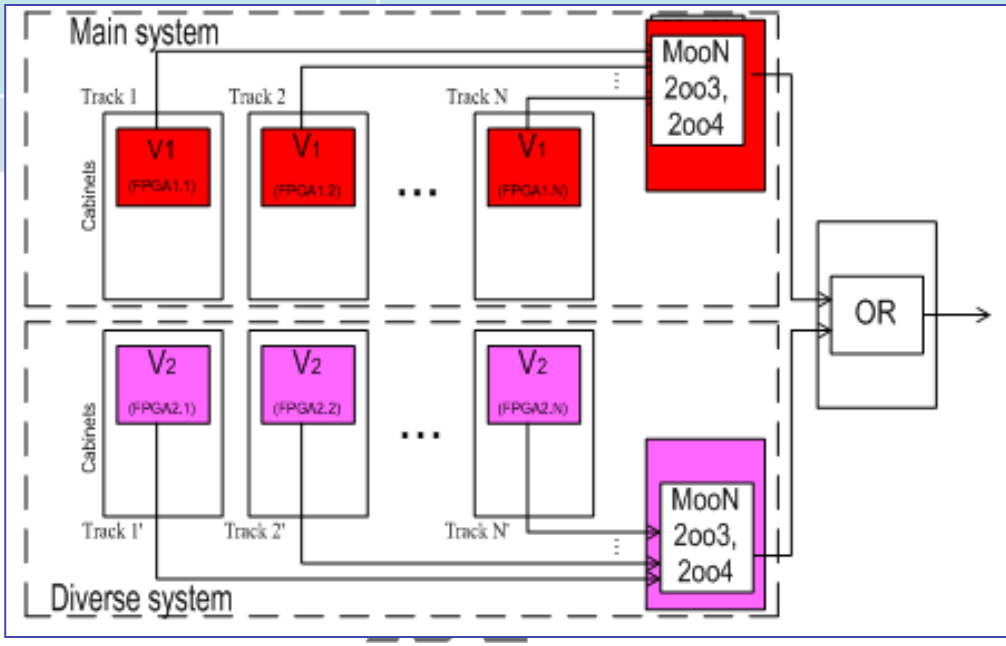


Standard 26262 doesn't contain any requirements/ recommendations concerning actual diversity assessment

3. Challenges: MVS Safety Ensuring

Aspect	Challenge	Question
5. CCF risk decreasing and MVS safety	There is a problem of **decreasing number of common version faults (CVF)**. The CVF number (and probability of CCF) may be decreased using several types of diversity (**multi-diversity or "diversity of diversity"**). There are subproblems of compatibility, dependence and choice of diversity types.	***What type (types) and how much versions developers should use to ensure required MVS safety?*** ***How to take into account dependencies of diversity types?***





4. Techniques of Diversity Assessment: Initial Remarks

There are a few techniques to assess diversity value in multi-version I&Cs:

- NUREG7007- based diversity assessment (**technique NUREG-A**);
- check-list-based diversity assessment integrated with metric and RBD (or MM)-based assessment of safety (**technique CLB-A**);
- graph model-based diversity assessment (**technique GMB-A**);
- other techniques, based on probabilistic model

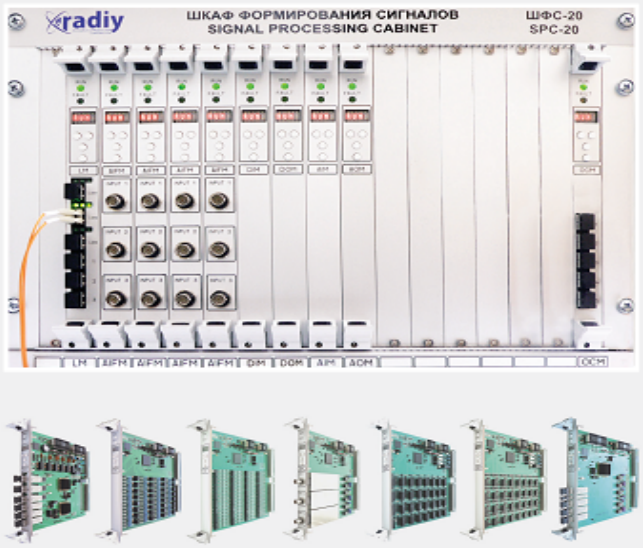
(Bayesian model of assessment of two-version systems (B. Littlewood et.al.) ,…).

To compare the techniques we should:

- to analyze basic conception and assumptions, procedures (algorithm)s and advantages/disadvantages of these techniques,
- to evaluate diversity metrics for identical MVSs.

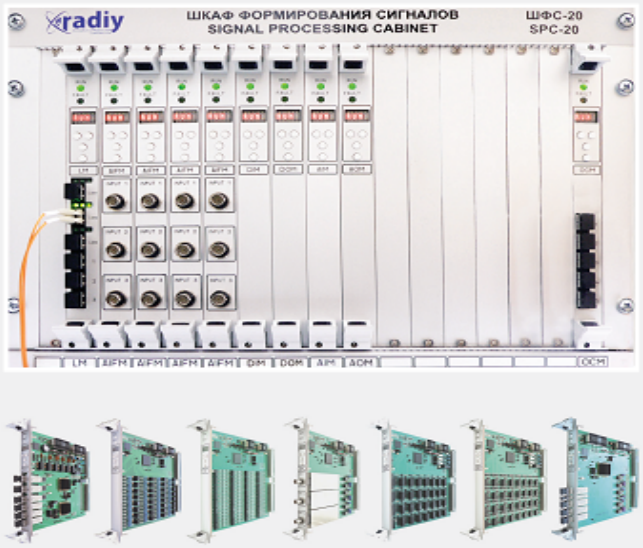
4. Techniques of Diversity Assessment: MVPs for NPP I&Cs

Radiy FPGA-based platform



4. Techniques of Diversity Assessment: MVPs for NPP I&Cs

Radiy FPGA-based platform



Multi-version projects

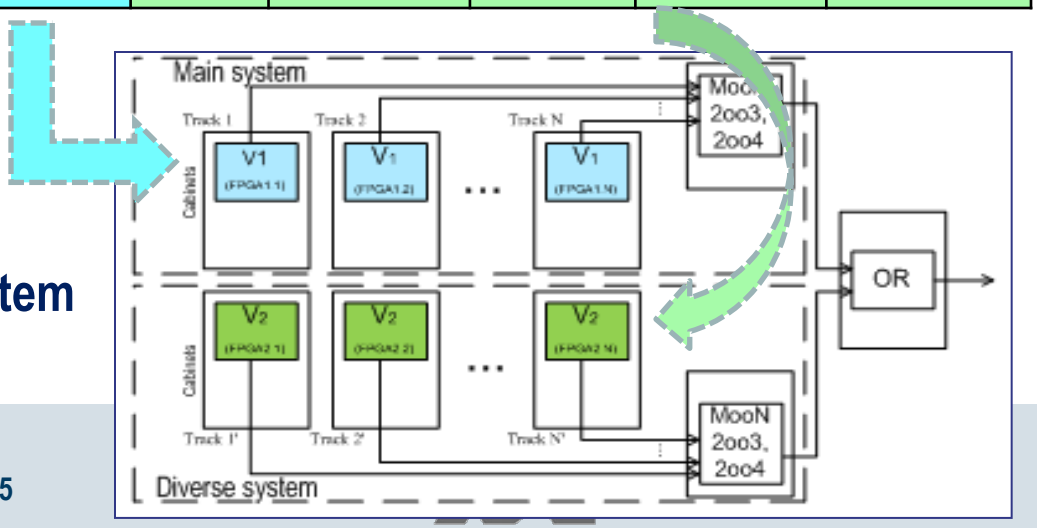
Main system	Diverse system				
	MVP1	MVP2	MVP3	MVP4	MVP5
FPGA (Altera, Radiy)	FPGA (Altera / MP, Radiy)	FPGA (Altera, another manufac-turer)	MP (Radiy)	MP (another manufac-turer)	Analog (another manufac-turer)

4. Techniques of Diversity Assessment: MVPs for I&Cs

Radiy FPGA-based platform

Multi-version projects

Main system	Diverse system				
	MVP1	MVP2	MVP3	MVP4	MVP5
FPGA (Altera, Radiy)	FPGA (Altera / MP, Radiy)	FPGA (Altera, another manufac-turer)	MP (Radiy)	MP (another manufac-turer)	Analog (another manufac-turer)



2-version Reactor trip system

4. Techniques of Diversity Assessment: NUREG-A

Attribute criteria		Indicators		Strategy name		
		Rank	DCE WT	INT	INH	Score
DESIGN	Different technologies	1	0.500			
	Different approaches within a technology	2	0.333			
	Different architectures	3	0.167			
	DAE weight and subtotals		1.000			
EQUIPMENT MANUFACTOR	Different manufacturers of fundamentally different equipment designs	1	0.400			
	Same manufacturer of fundamentally different equipment designs	2	0.300			
	Different manufacturers of same equipment design	3	0.200			
	Same manufacturer of different versions of the same equipment design	4	0.100			
	DAE weight and subtotals		0.250			
LOGIC PROCESSING EQUIPMENT	Different logic processing architectures	1	0.400			
	Different logic processing versions in same architecture	2	0.300			
	Different component integration architectures	3	0.200			
	Different data flow architectures	4	0.100			
	DAE weight and subtotals		0.644			
FUNCTION	Different underlying mechanisms to accomplish safety function	1	0.500			
	Different purpose, function, control logic, or actuation means of same underlying mechanism	2	0.333			
	Different response time scale	3	0.167			
	DAE weight and subtotals		0.600			
LIFE-CYCLE	Different design companies	1	0.400			
	Different management teams within the same company	2	0.300			
	Different designers, engineers, and/or programmers	3	0.200			
	Different implementation/validation teams	4	0.100			
	DAE weight and subtotals		0.683			
SIGNAL	Different reactor or process parameters sensed by different physical effect	1	0.500			
	Different reactor or process parameters sensed by the same physical effect	2	0.333			
	The same process parameter sensed by a different redundant set of similar sensors	3	0.167			
	DAE weight and subtotals		0.867			
LOGIC	Different algorithms, logic, and program architecture	1	0.400			
	Different timing or order of execution	2	0.300			
	Different runtime environments	3	0.200			
	Different functional representations	4	0.100			
	DAE weight and subtotals		0.733			

4. Techniques of Diversity Assessment: NUREG-A (2)

Attribute criteria				Category / Strategy name		
		Rank	DCE WT	INT	INH	Score
DESIGN	Design					
	Different technologies	1	0.500			
	Different approaches within a technology	2	0.333			
	Different architectures	3	0.167			
	DAE weight and subtotals		1.000			
EQUIPMENT MANUFACTURER	Equipment Manufacturer					
	Different manufacturers of fundamentally different equipment designs	1	0.400			
	Same manufacturer of fundamentally different equipment designs	2	0.300			
	Different manufacturers of same equipment design	3	0.200			
	Same manufacturer of different versions of the same equipment design	4	0.100			
	DAE weight and subtotals		0.250			
	(X) INT = intentional use, (i) INH = inherent use					
	DCE WT = Diversity Criterion Effectiveness Weights					

4. Techniques of Diversity Assessment: NUREG-A (3)

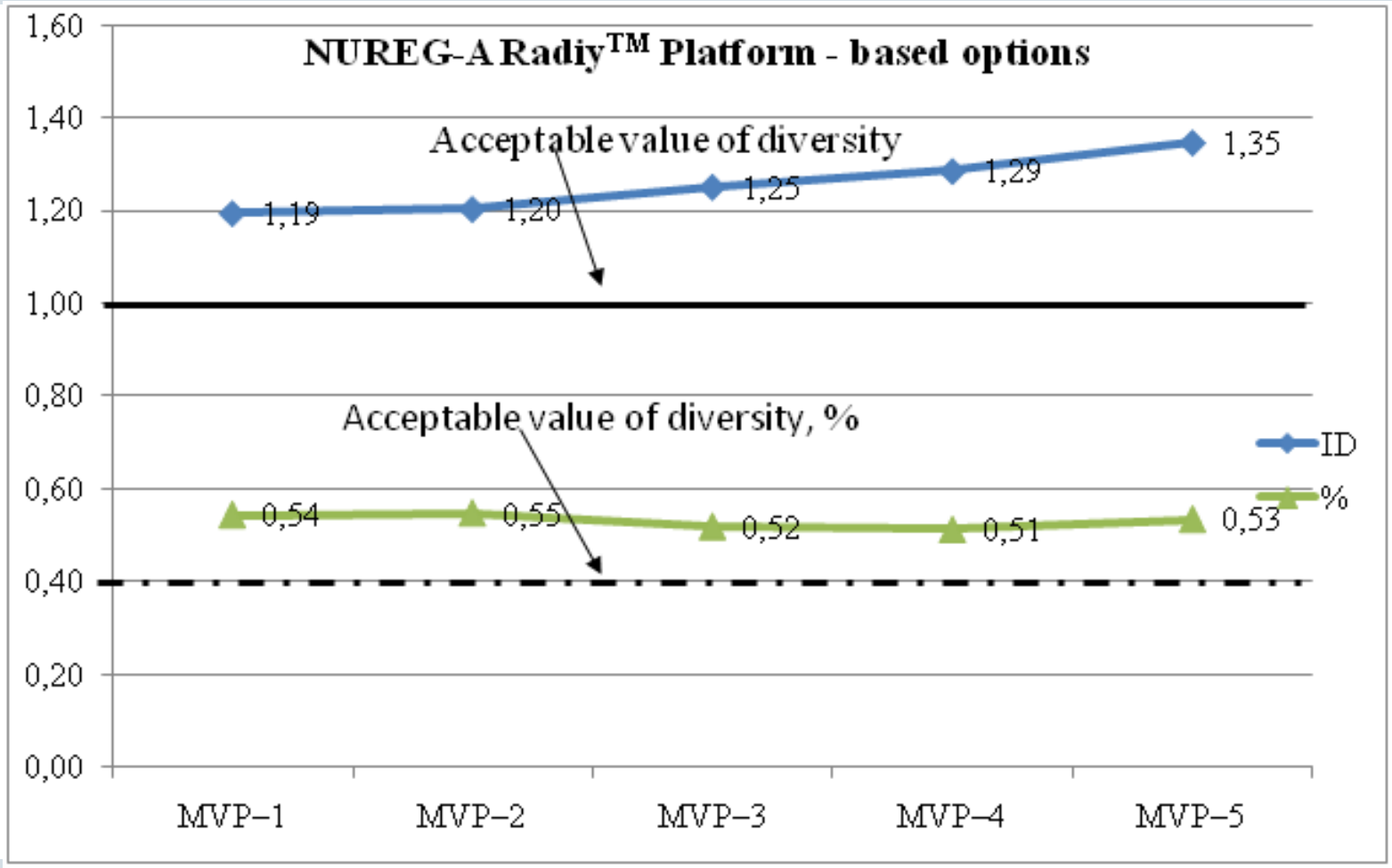
Attribute criteria				Category: Strategy name		
		Rank	DCE WT	INT	INH	Score
DESIGN	Design					
	Different technologies	1	0.500	X		0.500
	Different approaches within a technology	2	0.333			
	Different architectures	3	0.167		i	0.167
	DAE weight and subtotals		1.000		0.667	0.667
EQUIPMENT MANUFACTURER	Equipment Manufacturer					
	Different manufacturers of fundamentally different equipment designs	1	0.400			
	Same manufacturer of fundamentally different equipment designs	2	0.300			
	Different manufacturers of same equipment design	3	0.200			
	Same manufacturer of different versions of the same equipment design	4	0.100			
	DAE weight and subtotals		0.250			

(X) INT = intentional use, (i) INH = inherent use

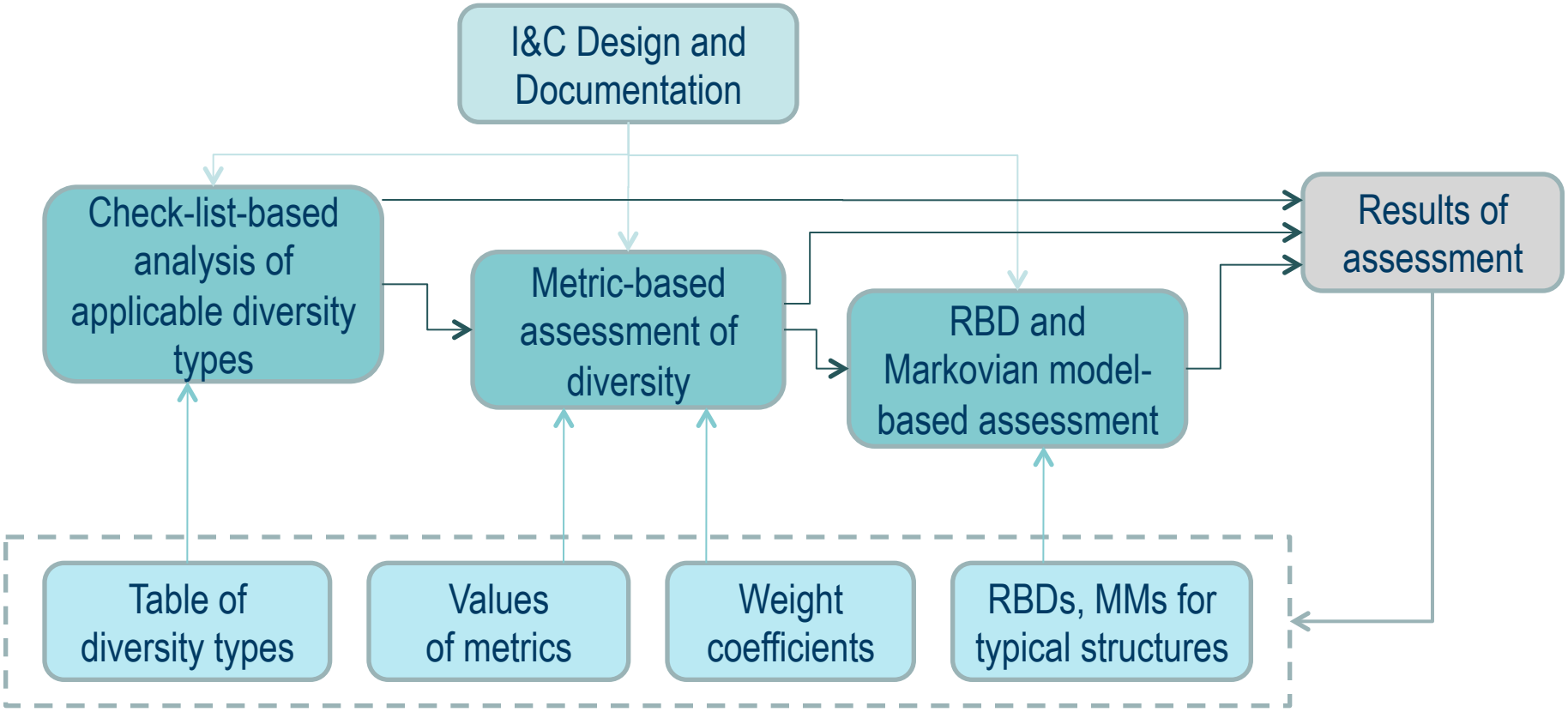
DCE WT = Diversity Criterion Effectiveness WeighTs

Result

4. Techniques of Diversity Assessment: NUREG-A (5)



4. Techniques of Diversity Assessment: CLB-A (2)

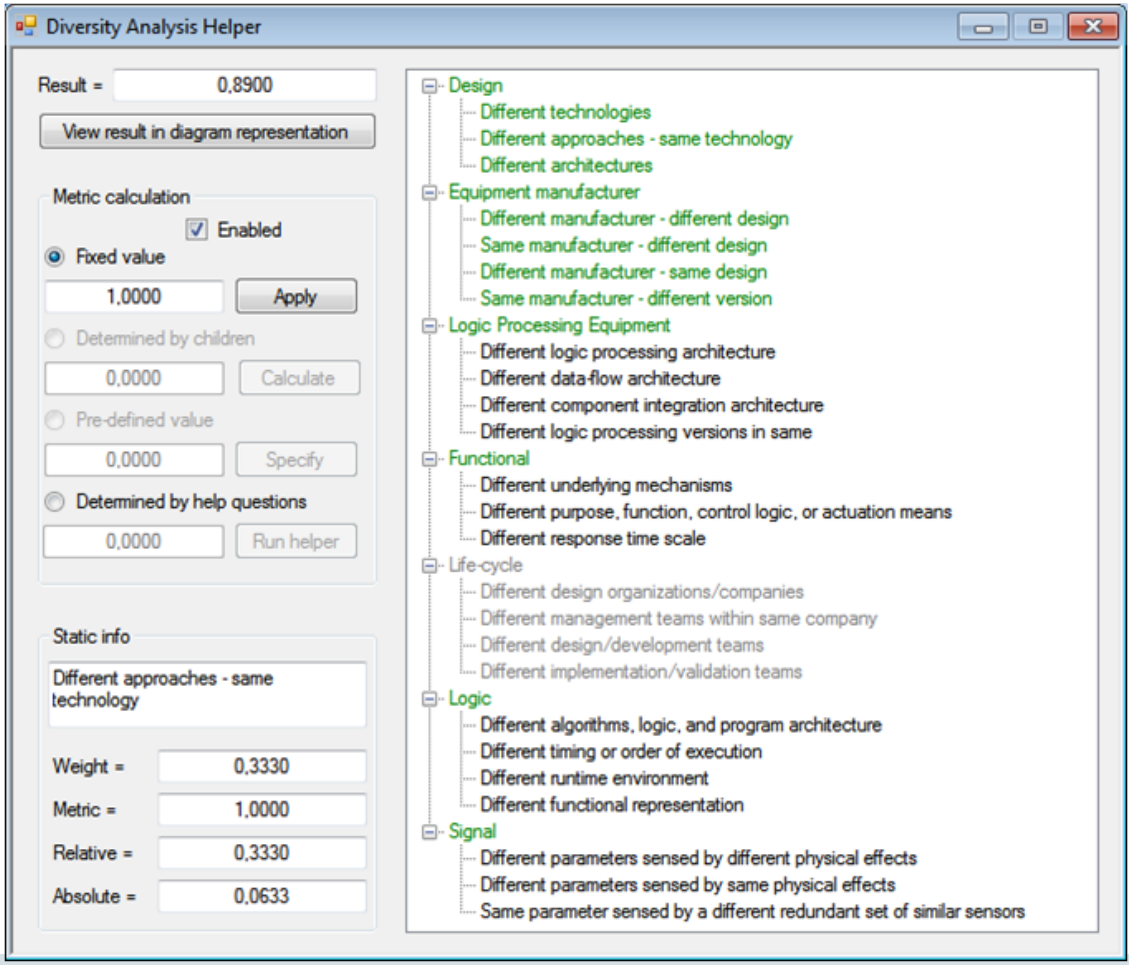


4. Tool for Diversity Assessment: Main Window

(V. Kharchenko et al. Standards analysis and tool-based assessment technique of I&C systems diversity// Proceedings of the Conference ICONE22, July 7-11, 2014, Prague, Czech Republic (accepted))

Tool DivA (Diversity Analysis*)

- ➞ Hierarchy (multi-level and extensible) of diversity types
- ➞ Calculated results (weights, metrics,…)
- ➞ Options for metric calculations
- ➞ Green colours mean diversity type is included in result of calculation
- ➞ Gray colours mean diversity type is disabled for managing



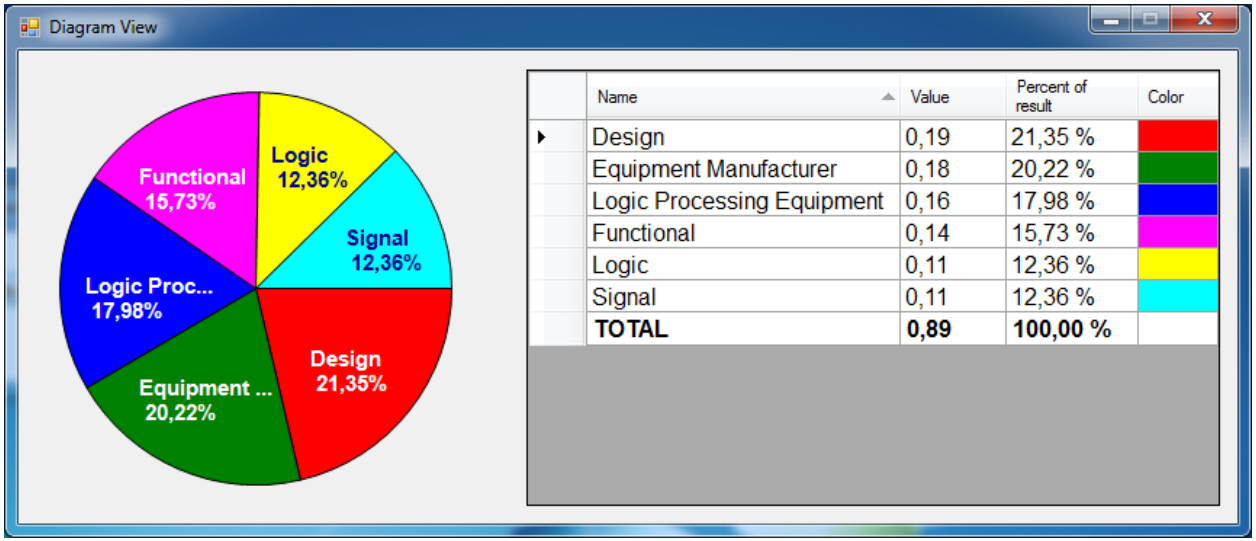
4. Tool for Diversity Assessment: Results

Diagram view:

➞ Result is represented in table and by coloured radial diagram

➞ Absolute value and percentage of result are shown for each diversity type

(on all levels of diversity hierarchy)

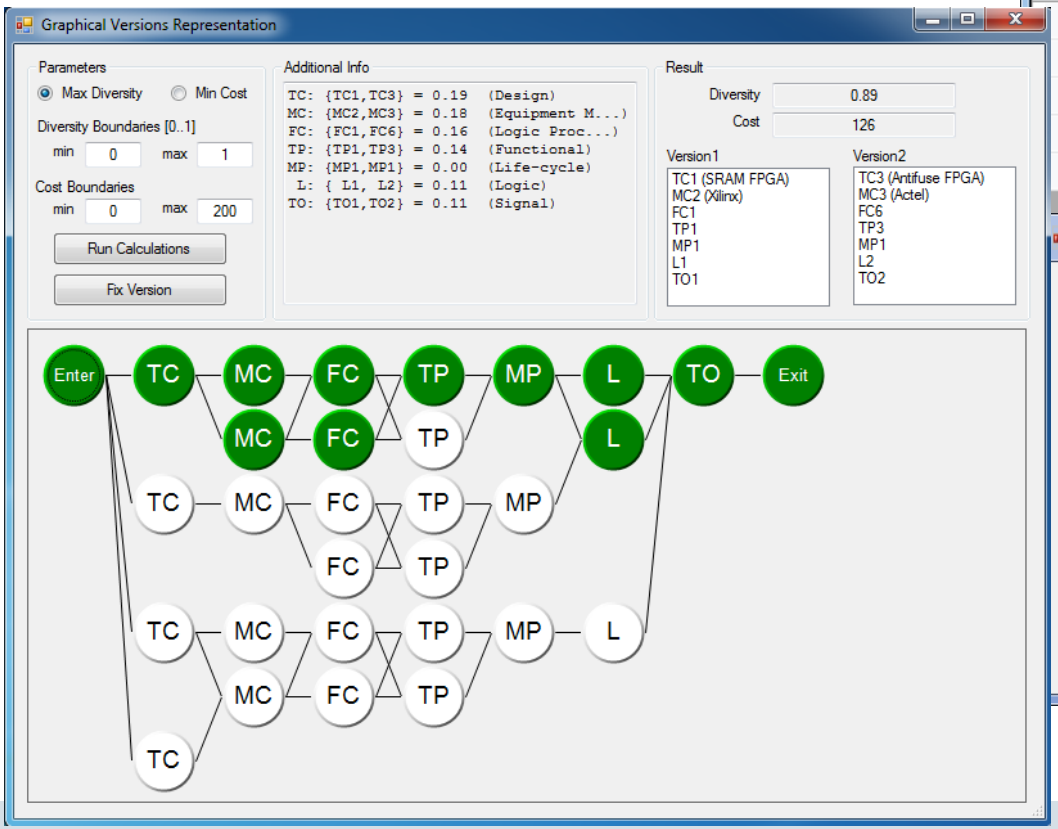


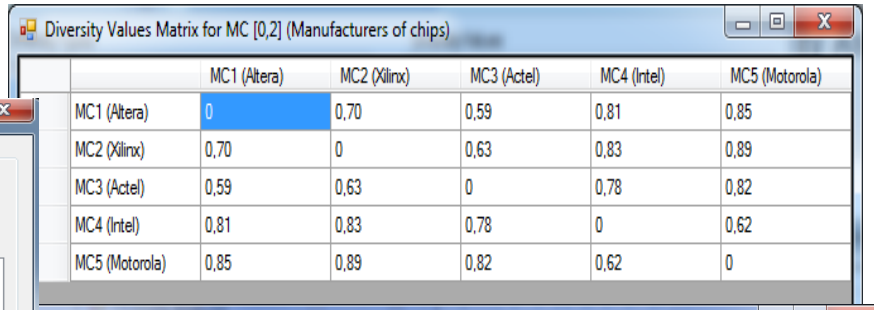
Name	Value	Percent of result	Color
Design	0,19	21,35 %	
Equipment Manufacturer	0,18	20,22 %	
Logic Processing Equipment	0,16	17,98 %	
Functional	0,14	15,73 %	
Logic	0,11	12,36 %	
Signal	0,11	12,36 %	
TOTAL	**0,89**	**100,00 %**	

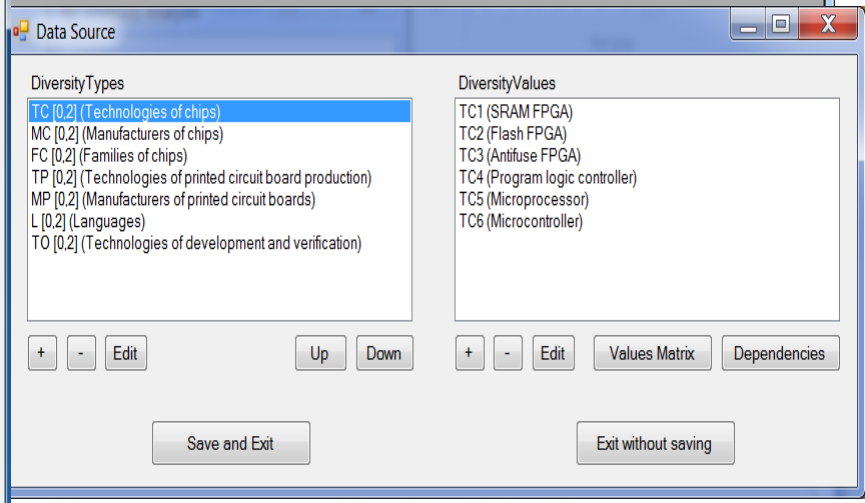
5. Choice of Diversity Types: Tool Support

(S. Vilkomir (ECU, NC, USA), V. Kharchenko., A Diversity Model for Multi-Version Safety-Critical I&C Systems// Proceedings of the PSAM11/ESREL2012, Helsinki, 24-28, June, 2012)

Tool DivA-C
(Diversity Analysis and Choice)







Conclusion (1)

Key challenges related to multi-version I&Cs

- **uniqueness of ones**

  can we use experience of NPP, aerospace I&C for automotive and vice versa? Yes!

- **existing standards** (are not enough detailed)

  comparative analysis of IEC60880,… (NPP), … and IEC26262 (automotive)

  where diversity should/shall be applied? … restrictions of applications?

- **approved diversity-oriented safety assessment techniques & tools**

  initial data, choice of technique

  diversity metrics and safety indicators calculation

- **techniques for development of multi-version systems**

  criteria “required safety(diversity)-minimal cost” (+ restrictions)

  development technique based on selecting of 2(n) ways in multi-version graph

Conclusion (2)

Our experience for automotive SW& systems allows :

- to improve concepts and methodology of diversity application;
- to add set of version redundancy (process/product considering FPGA);
- to adapt and apply developed techniques and tools:
  - to assess actual diversity metrics;
  - to analyse limitations/restrictions of diversity application;
  - to choice capacity and types of diversity
- to join safety and security issues in point of view diversity.

DESSERT Conference, Kiev, Ukraine, May 19-23, 2016, www.dessertcon.com/adaland)

- WS on cyber safety and security for V, V2V, V2I

Education and training activities:

- join TEMPUS projects on safety and security
- special training related to diversity application

Cyber security projects of KhAI CSN Department and their applicability to vehicle security assessment and assurance

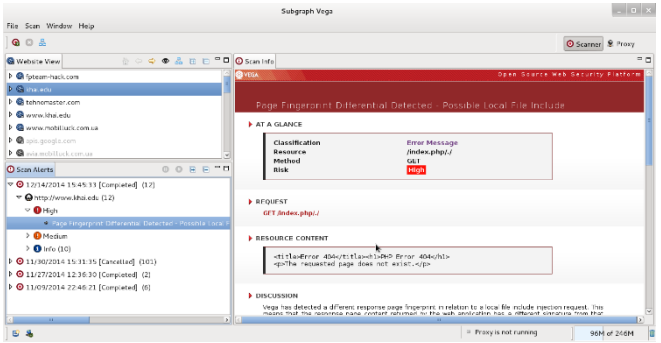
- **Project 1. Penetration testing for vehicle web services (P1)**
- **Project 2. CloudSec: CLOUD-Platform for web based application deployment (P2)**
- **Project 3. Development of Advanced Security Assurance Case based on application and adaptation of ISO/IEC 15408 standard (P3)**
- **Project 4. Application of techniques and tools for joint safety & security vehicle assessment and assurance (GAP-IMECA analysis) (P4)**
- **Project 5. Software diversity assessment (similarity assessment of SW versions based on soft techniques)**

	Vehicle	V2V	V2I
Regulatory tasks	P3	P3	P3
Safety& security assessment tasks	P1, P4, P5	P1, P4, P5	P1, P4, P5
Safety&security assurance tasks	P2, P4, P2	P2, P4, P2	P2, P4, P2

Penetration testing for vehicle web services and on-board systems

- Regulatory basis have been analyzed (ISO/IEC 15408, ISO 27k and others, Penetration Testing Execution Standard, Open Web Application Security Project (OWASP), Open Web Application Security Project (OWASP))
- Tool selection and configuration (to increase the test coverage)
- Site vulnerabilities testing (http://stc-dessert.com, ttp://www.khai.edu
- Audits reports were prepared and recommendations are given to site owner

These results might be used for PT of web services that provide support of vehicle (web based navigation system, etc)



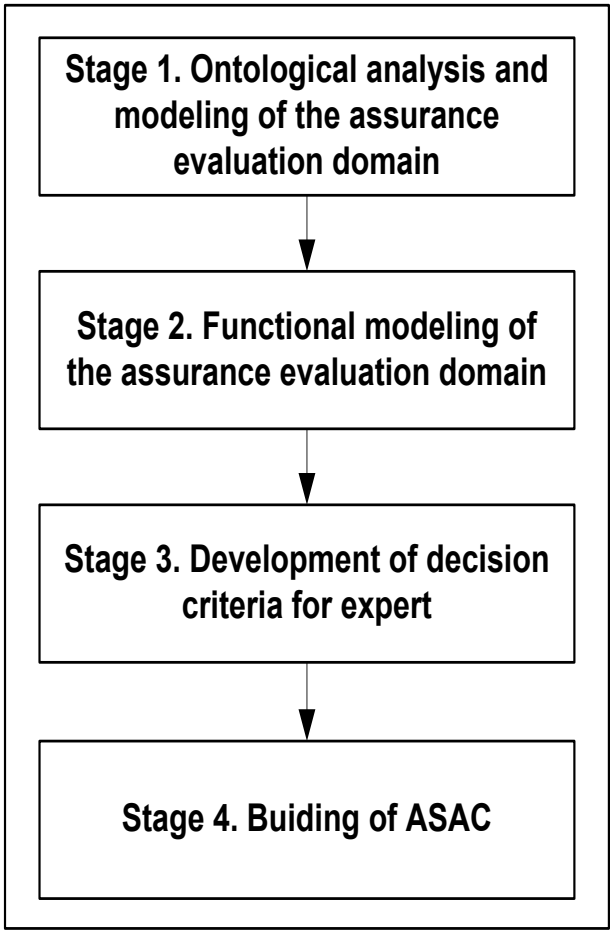
Development of Advanced Security Assurance Case based on application and adaptation of ISO/IEC 15408 standard

Project goal - To develop a unify methodology for IT security assurance for both parties (developers, evaluators, others). This methodology should be based on international standards (ISO/IEC 15408, ISO/IEC 18045, ISO/IEC TR 15443) and should contain requirements how to prove that the decision of conformity to the standard is solely correct.

What has been done -

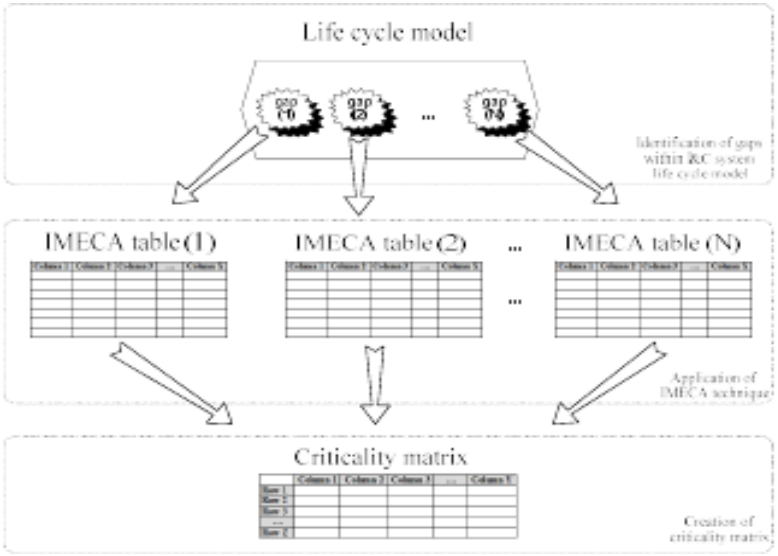
- Enhanced structure of security assurance case called *Advanced Security Assurance Case* was proposed
- Improvement of proposed security assurance case formalization technique
- Development of tool for support of proposed methodology

<u>These results might be used for ASAC development for vehicle security assurance</u>

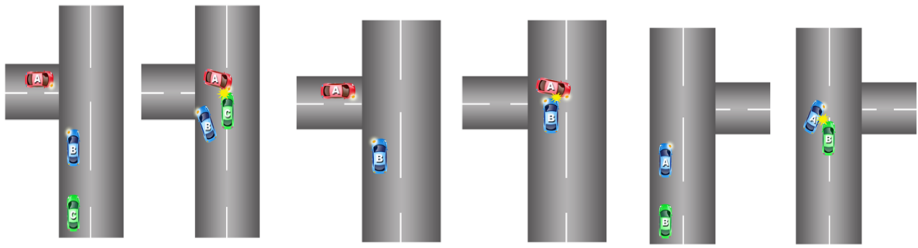


Cyber security risk analysis. Application of techniques and tools for joint safety & security vehicle assessment and assurance

Gap IMECA analysis for vehicle cyber risk analysis. This method has been used for NPP I&C security analysis



The accident situations are to be analyzed



Vehicle 1

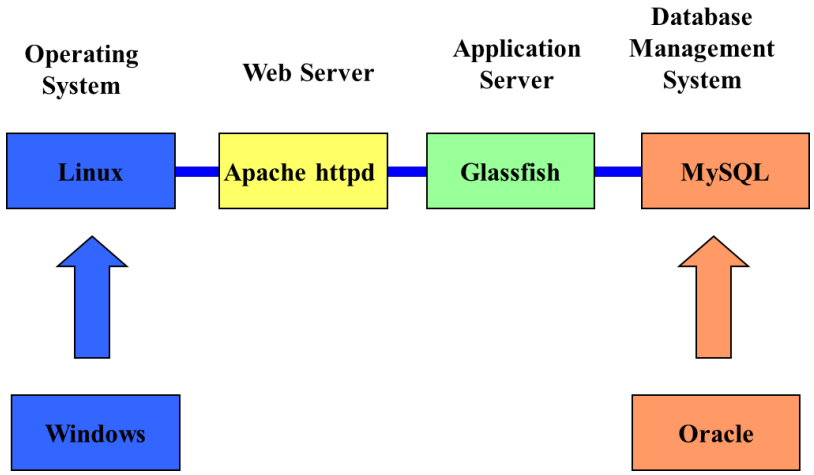
Row number	Gap in stage of	Attack mode	Accident scenarion	Occurrence probability	Effect severity	Consequence on security	Consequence on safety	Countermeasures
1	Operation	Man in the middle	Overtaking a vehicle turning right	High	High	Lost of data integrity	Injuries	Application of encryption key

CloudSec: CLOUD-Platform for web based application deployment

Project goal – development of PaaS Cloud-platform for secure deployment of cross-platform application services. Main project idea – dynamical reconfiguration of system environment (OS, system software) in the way when the most vulnerable system components are automatically exchanged with the similar (in function, purposes, etc) but less vulnerable.

This project includes the following components:

1. Zero day vulnerabilities monitor;
2. Cloud-platform «Secure PaaS».



Results of project might be used for:

– development of security scanner, interacting with zero day vulnerability monitors trough the set of API;
– development of secure PaaS Cloud-platform for provate data centers based on OpenStack

Thank you for attention
Welcome to Ukraine!

RPC Radiy, 29 Geroyev Stalingrada str., Kirovograd, Ukraine
http://www.radiy.com
National Aerospace University "Kharkiv Aviation Institute"
17 Chkalov str., Kharkiv, Ukraine, Tel.: +38 (057) 788 45 03
E-Mail: v.kharchenko@khai.edu, v_s_kharchenko@ukr.net