# GREEN AND SAFE COMPUTING: CHALLENGES AND SOLUTIONS FOR INDUSTRY AND HUMAN


**Vyacheslav Kharchenko**

**National Aerospace University KhAI, Kharkiv, Ukraine**

*Department of Computer Systems& Networks*

**Research & Production Company Radiy, Ukraine**

*Centre for Safety Infrastructure Research and Analysis*


**PERCCOM Summer School, June 19-23, 2017, LBU, Leeds, United Kingdom**

# Outline

About our team and projects
Introduction. Green vs Safe ITs
Green Computing. Key principles
Safe Computing. Principles and Industry Solutions
Conclusions

# Outline

About our team and projects

Introduction. Green vs Safe ITs

Green Computing. Key principles

Safe Computing. Principles and Industry Solutions

Conclusions

# Map of Ukraine: National Aerospace University KhAI and RPC Radiy

**Kharkiv (1.5 mil):**

- ✓ 250 IT companies,
- ✓ 30000 work in IT,
- ✓ more 2000 IT graduates yearly

# National  Aerospace University KhAI and RPC Radiy Location

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

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


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

# National Aerospace University KhAI: CSN Department

**Computing Systems and Networks (CSN) Department** is a part of Faculty of Aircraft Radio Engineering, Computing and Communications (**National Aerospace University KhAI, about 10000 students**)

- **About 700 students** (**BSc, MSc / full and part time**)
- **12 PhDs and 3 Doctors of Science students**
- **English language studies** of **BSc&Msc&PhD (2006)**
- **45 lecturers** (6 Professors and Doctors of Science, 20 Associate Professors and PhDs)
- **10 centers and labs**

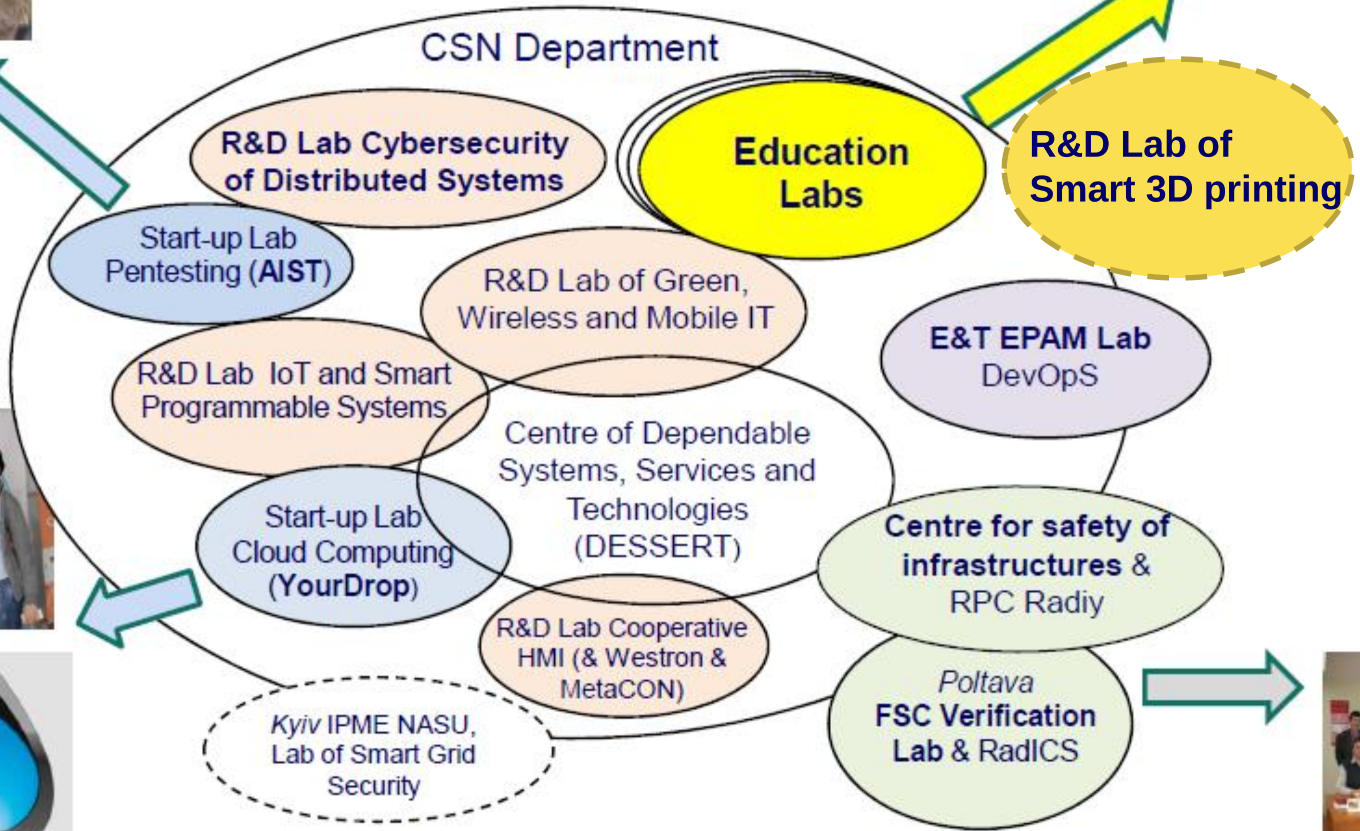
**Department of Computer Systems and Networks**

**Educational laboratories:**
- BS courses;
MS courses

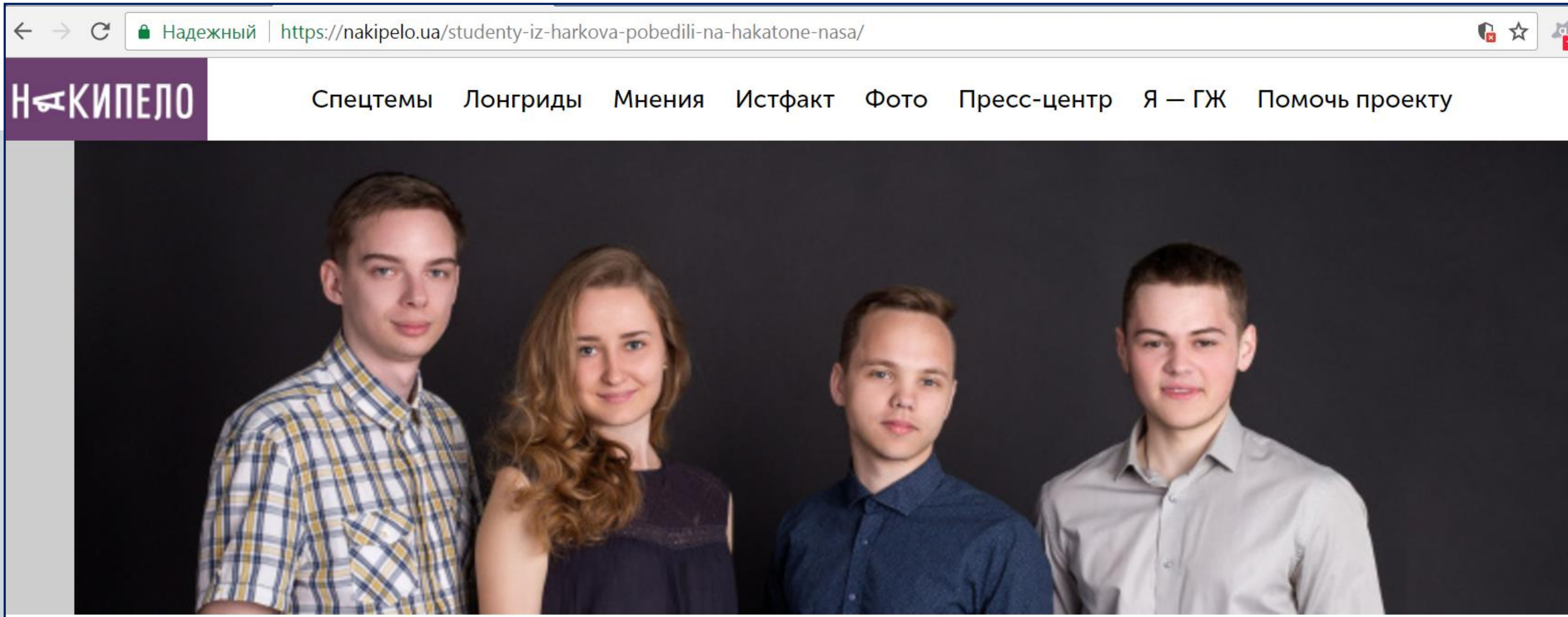
**Industrial laboratories and centres:**
- STM; CISCO, De-Link;
- RPC Radiy, Polisvit Inc., etc.

**Research&Training Centres:**
- Centre of Dependable Systems, Services and Technologies; Centre for Safety Infrastructure Research and Analysis, EPAM Centre, R&D Labs

# National Aerospace University KhAI: Department of CSN (5)




# CSN Department: Student's Team won on the NASA Hackathon




**During 5 days after call of the NASA Space Apps Challenge-2017 Hackathon (ecology and forest monitoring) our students developed, produced, tested and demonstrated mobile platform and software for fire detection system https://nakipelo.ua/studenty-iz-harkova-pobedili-na-hakatone-nasa/**

# CSN Department: Student's Team won on the NASA Hackathon


https://nakipelo.ua/studenty-iz-harkova-pobedili-na-hakatone-nasa/

# Student Startup: High Precise 3D Printer and Networked Factory

https://atn.ua/obshchestvo/v-harkove-mozhet-poyavitsya-fabrika-3d-printerov

# KhAI CSN Department EU funded projects


CERES

AEROSPACE CRITICAL COMPUTING MASTAC 2006-2009

NETWORK OF SAFEWARE ENGINEERING CENTRES SAFEGUARD 2010 2013

GREENCO GREEN COMPUTING & COMMUNICATIONS

Tempus 2013 SEREIN 2016

2014 2016 CABRIOLET

KhAI-ERA

# KhAI CSN Department EU funded projects: ALIOT, Internet of Things for Human and Industry Domains (2017-2019)

# ERASMUS+ Project: Internet of Things

**Title:** "**I**nternet **o**f **T**hings: Emerging Curriculum for Industry and Human **A**pp**l**ications / **ALIOT**"

**Project Number**: 573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP

**Duration**: 3 years (15/10/2016-14/10/2019)

**Total Budget**: 816 725,00 Euro

**Grant Holder**: University of Newcastle upon Tyne (UK)

**National Coordinator**: KhAI

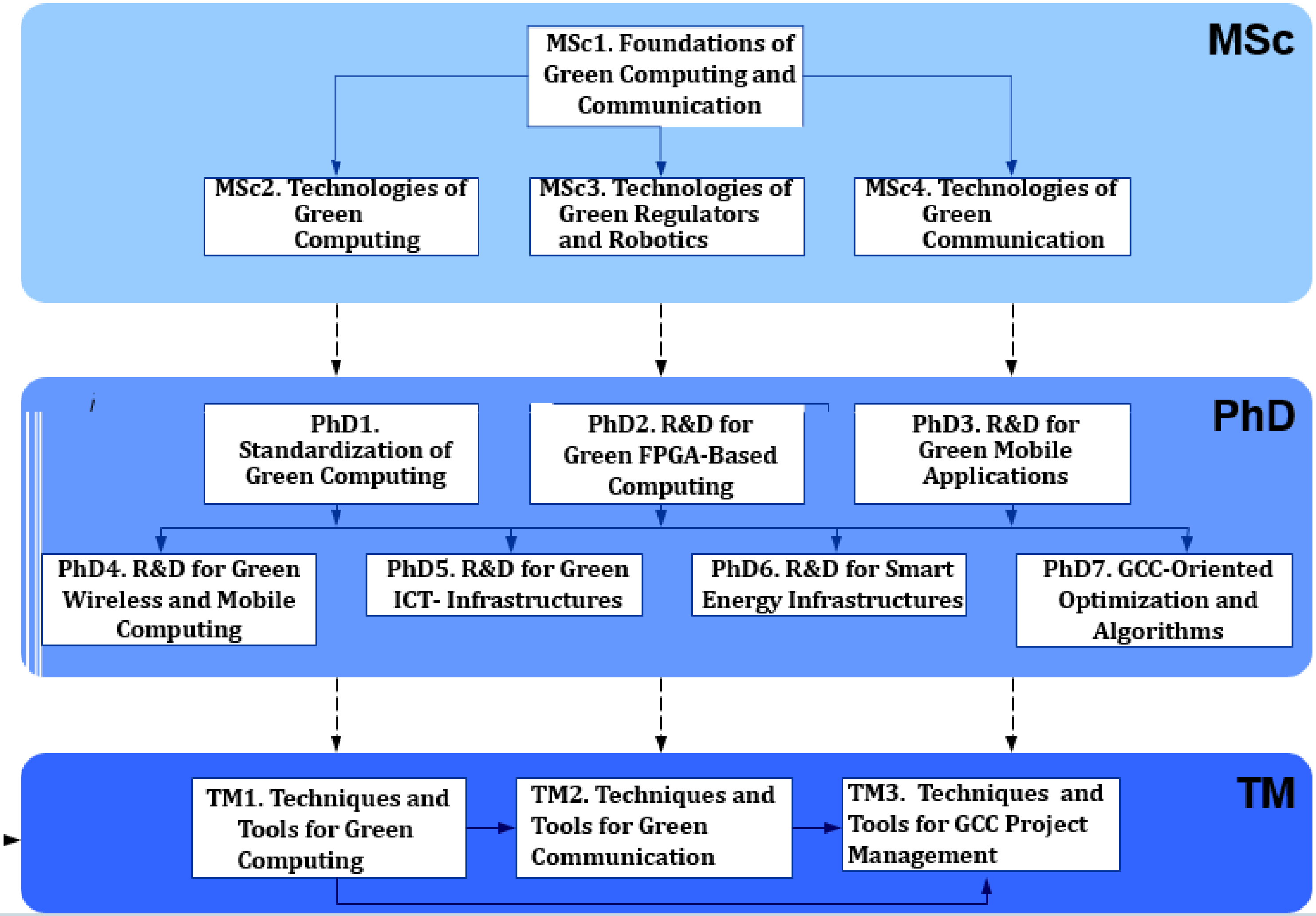
**Consortium**: 8 Ukrainian Universities + UK (Newcastle U, Leeds Beckett U), Sweden (KTH), Italy (Naples U), Portugal (Coimbra U)

**MSc programme on IoT (4 modules):**
MC1 Fundamentals of IoT and IoE
MC2 Data science for IoT and IoE
MC3 Mobile and hybrid IoT-based computing
MC4 IoT technologies for cyber physical systems

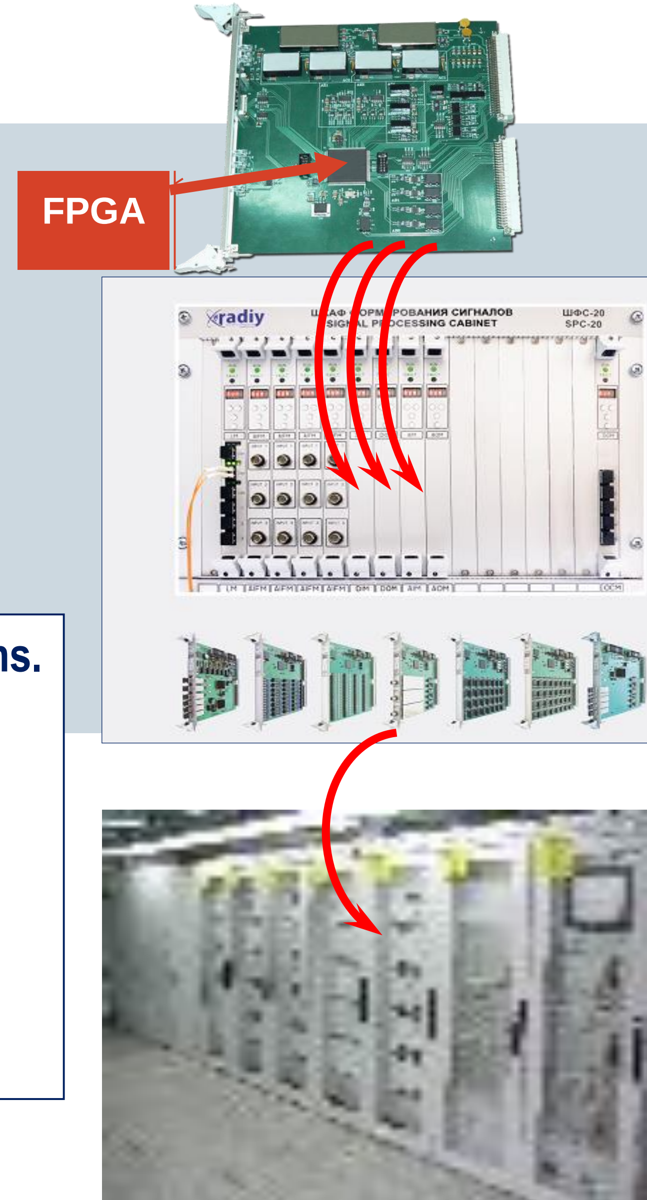
**PhD programme on IoT (4 courses):**
PC1 Simulation of IoT and IoE-based systems
PC2 Software defined networks and IoT
PC3 Dependability and security of IoT
PC4 Development&implementation of IoT systems

**Industrial training modules (6 modules):**
ITM1 IoT for Smart energy grid
ITM 2 IoT for Smart building and city
ITM 3 IoT for intelligent transport systems
ITM 4 IoT for health systems
ITM 5 IoT for ecology monitoring systems
ITM 6 IoT for industrial systems

# TEMPUS Project: Green Computing and Communication



# Research and Production Corporation Radiy




- Safe and secure FPGA-based I&C platform RadICS
- Safety critical NPP systems (RTS, ESFAS, RCS,…)
- I&C systems of research reactors
- Electric power supply equipment
- Control room panels
- Fire alarm and suppression systems
- Seismic sensors and seismic monitoring systems,….

- All 15 Ukrainian reactors were modernized using Radiy platforms.
- Over 60 NPP I&C systems have been commissioned since 2003 (Ukraine, Bulgaria, Canada, Argentina, France,…).
- SIL3 Certificate of the Radiy I&C (RadICS) platform (in one chassis, 1st in the world for such type)
- Development, manufacturing, implementation, training, maintenance
- Research, IV&V and certification support

# Outline

About our team and projects

Introduction. Green vs Safe ITs

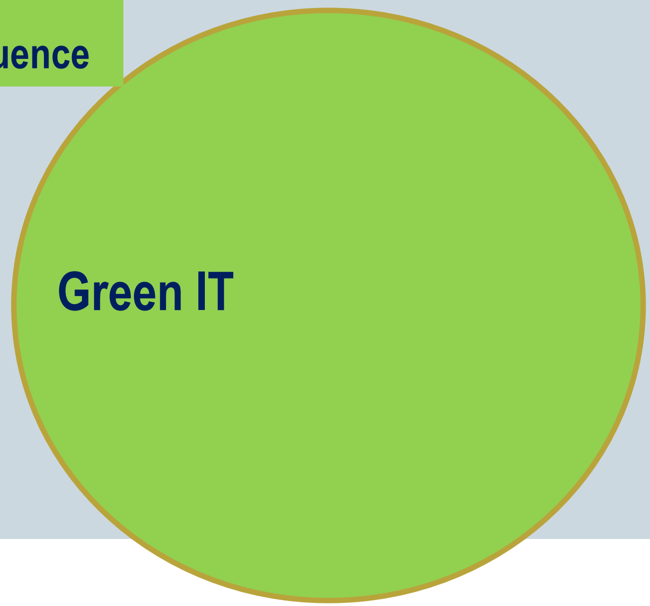
Green Computing. Key principles

Safe Computing. Principles and Industry Solutions

Conclusions

# Introduction: Green *vs* or *and* Safe IT?

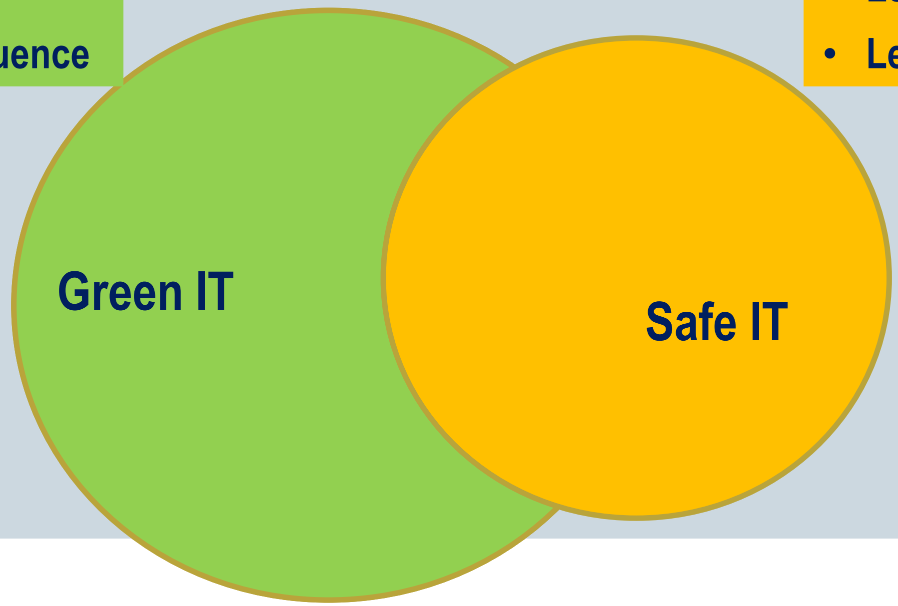
- Less energy/resources
- Less environmental influence



# Introduction: Green *vs* or *and* Safe IT?

- Less energy/resources
- Less environmental influence

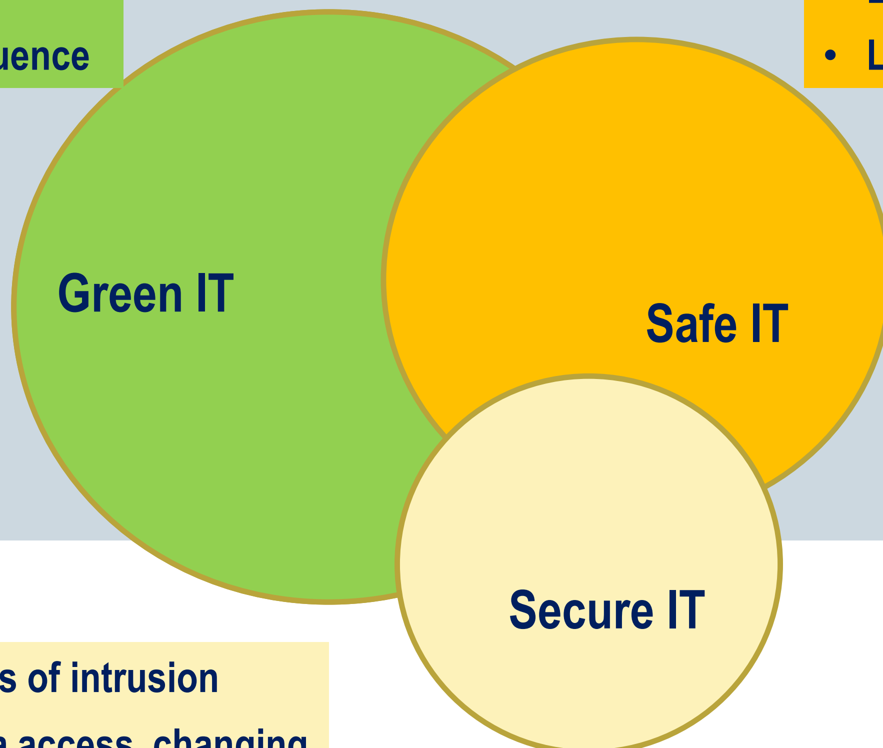
- Less risks of emergencies
- Less emergency consequences



# Introduction: Green *vs* or *and* Safe IT?

- Less energy/resources
- Less environmental influence

- Less risks of emergencies
- Less emergency consequences

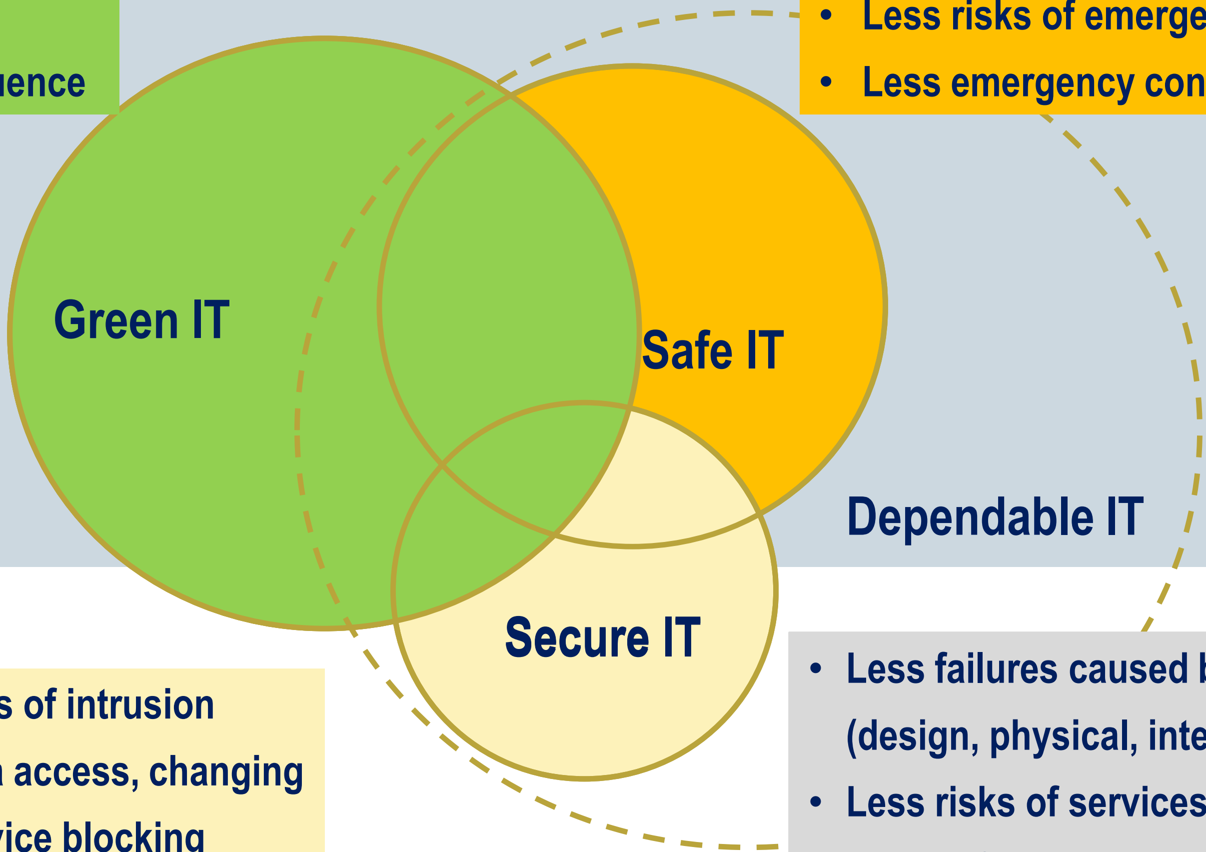



- Less risks of intrusion
- Less data access, changing
- Less service blocking

# Introduction: Green *vs* or *and* Safe IT?

- Less energy/resources
- Less environmental influence

- Less risks of emergencies
- Less emergency consequences




- Less risks of intrusion
- Less data access, changing
- Less service blocking

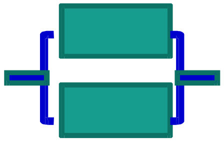
- Less failures caused by any faults (design, physical, interaction)
- Less risks of services/functions non-performance

# Introduction: Green *vs* or *and* Safe IT?

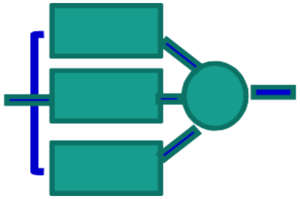
**Lectures on probabilistic logics and the synthesis of reliable organisms from unreliable components**, delivered by Professor J. von Neumann, The Institute for Advanced Study Princeton, N. J. at the California Institute of Technology, January 4-15, 1952, Notes by R. S. Pierce

**VN's paradigm: how to create reliable organism from unreliable components?**

**$P = p = 0.9$**



**$P = 2p - p^2 = 0.99$**



**$P = 3p^2 - 2p^3 = 0.972$**

# Introduction: Green *vs* or *and* Safe IT?

**Lectures on probabilistic logics and the synthesis of reliable organisms from unreliable components**, delivered by Professor J. von Neumann, The Institute for Advanced Study Princeton, N. J. at the California Institute of Technology, January 4-15, 1952, Notes by R. S. Pierce

**VN's paradigm: how to create reliable organism from unreliable components?**

**Post VN's paradigm: how to create "good" (reliable, safe, secure,…, fast, power low/green) systems from "not enough good" (unreliable, unsafe, …, non-green) components?**

# X Critical Software/FPGA Systems: Domains

## Critical computing and IT application domains

- **Safety** critical (NPP I&Cs, aviation, automotive,… on-board SW systems)
- **Mission** critical (space/unpiloted SW systems)
- **Data critical/security critical** (defense, health,…, research data systems)
- **Business** critical (banking… IT-infrastructures)

# X Critical Software/FPGA Systems: Domains and Challenges

## Critical CPS and IT application domains

- **Safety critical (NPP I&Cs, aviation, automotive,… on-board SW systems)**
- **Mission critical (space/unpiloted SW systems)**
- **Data critical/security critical (defense, health,…, research data systems)**
- **Business critical (banking… IT-infrastructures)**

## Safety related challenges

**Dependence of humanity, environment and artificial** (created by people) **systems safety / security** on **IT-system reliability**

- **NPP I&Cs.** 2000th:20% of the NPP failures
- **Space I&Cs.** 90th:20%→2000th:50%→2010th:60% of the crashes

# X Critical Software/FPGA Systems: Domains and Challenges

## Critical CPS and IT application domains

- **Safety critical (NPP I&Cs, aviation, automotive,… on-board SW systems)**
- **Mission critical (space/unpiloted SW systems)**
- **Data critical/security critical (defense, health,…, research data systems)**
- **Business critical (banking… IT-infrastructures)**

## Safety related challenges

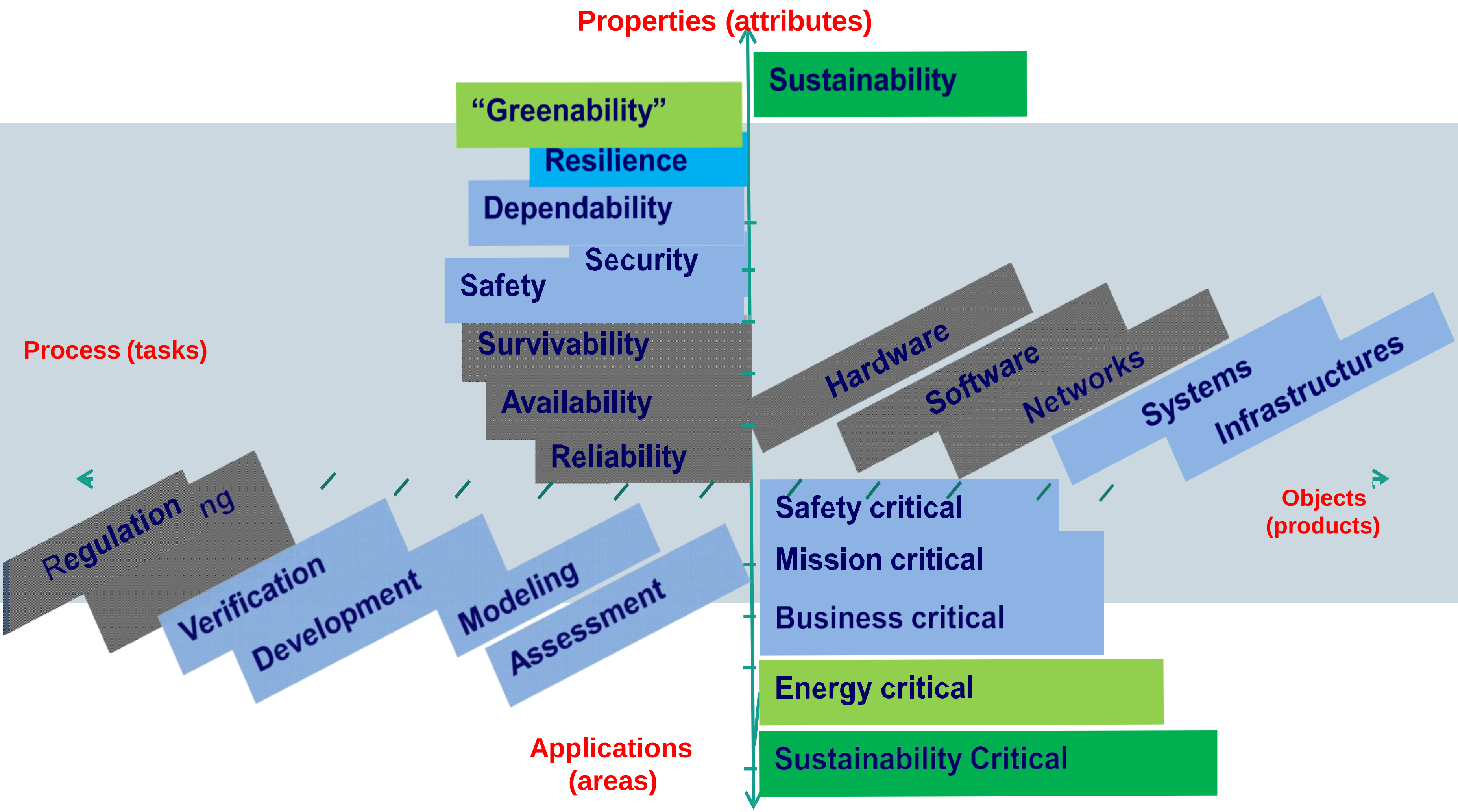
- **Dependence of humanity, environment and artificial** (created by people) **systems safety / security** on **IT-system reliability**
  - **NPP I&Cs.** $2000^{th}$:20% of the NPP failures
  - **Space I&Cs.** $90^{th}$:20%→$2000^{th}$:50%→$2010^{th}$:60% of the crashes

## Resource related challenges

- **IT:** 3-4 % of power consumption (green issues) → **energy critical**
- **IT:** 3% 16,5 % of global GHG emissions in 2020 → **ecology critical**

**Energy/ecology critical systems**

# X Critical (Safe and Green) Software/FPGA Systems: Taxonomy



# Outline

About our team and projects

Introduction. Green vs Safe IT

Green Computing. Key principles

Safe Computing. Principles and Industry Solutions

Conclusions

# Green Computing: Directions

**Green Computing** vice versa (or jointly with) Dependable, Safe, Secure and Resilient Computing

**Green Computing** as a part of Sustainable Computing and Sustainable Development

**Green Computing** and Education Activities

**Green Computing:** University and IT-industry Cooperation

**Green Computing** and Green IT-culture and Green Culture as a whole

# Green Computing: Sustainability Matrix

Main entities in the field of sustainable development (sustainability) and green IT, as an "**IT Sustainability Set**" (ITSS) can be described by the Cartesian product of two subsets:

- **Sustainability Development Set** (SDS):
  - energy and resource (EnF),
  - ecology (EcF),
  - safety (SF)
  - social and economic factors (CF);

- Two-element set (**Means-Object Set** – MOS):

*ITSS = SDS x MOS = (EnF, EcF, SF, CF) x (Means, Object)*

# Green Computing: Sustainability Matrix

(Green IT-Engineering. Concepts, Models, Complex Systems Architectures, Kharchenko Vyacheslav, Kondratenko Yuriy, Kacprzyk Janusz (Eds.), 2017, Springer Seria. – 305 p. )

| MOS | | Sustainability Development Set, SDS | | | |
|---|---|---|---|---|---|
| | | EnF | EcF | SF | CF |
| Means | | Means x EnF | Means x EcF | Means x SF | Means x CF |
| Object, IT-compo-nents | HW | EnF x HW | EcF x HW | SF x HW | CF x HW |
| | SW | EnF x SW | EcF x SW | SF x SW | CF x SW |
| | NW | EnF x NW | EcF x NW | SF x NW | CF x NW |
| | IS | EnF x IS | EcF x IS | SF x IS | CF x IS |
| | IT | EnF x IT | EcF x IT | SF x IT | CF x IT |

**Factors:**

Energy&resource (EnF),

Ecology (EcF),

Safety (SF),

Social&economic (CF)

**IT components:**

HW/FPGA

SW

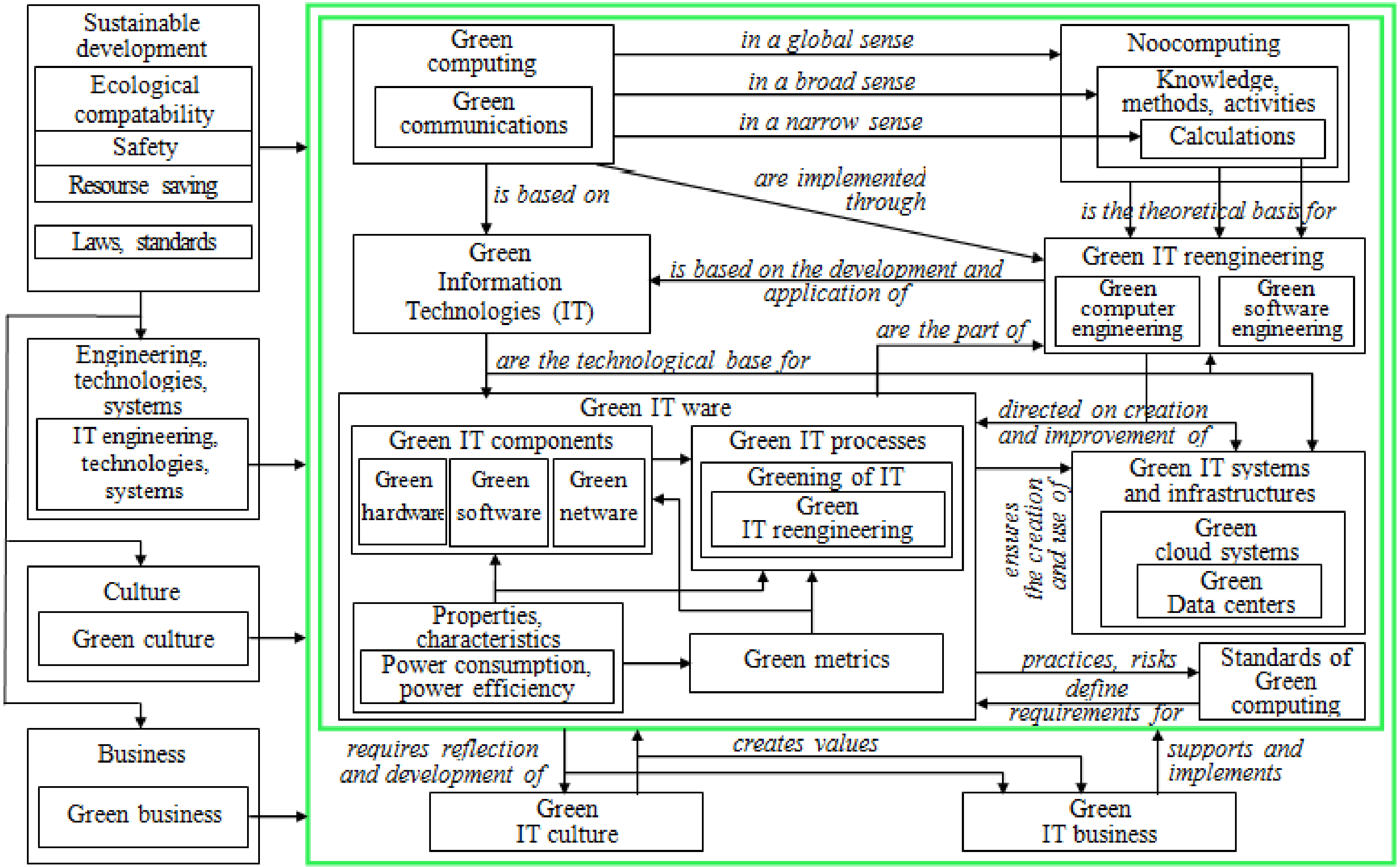
NW

IS

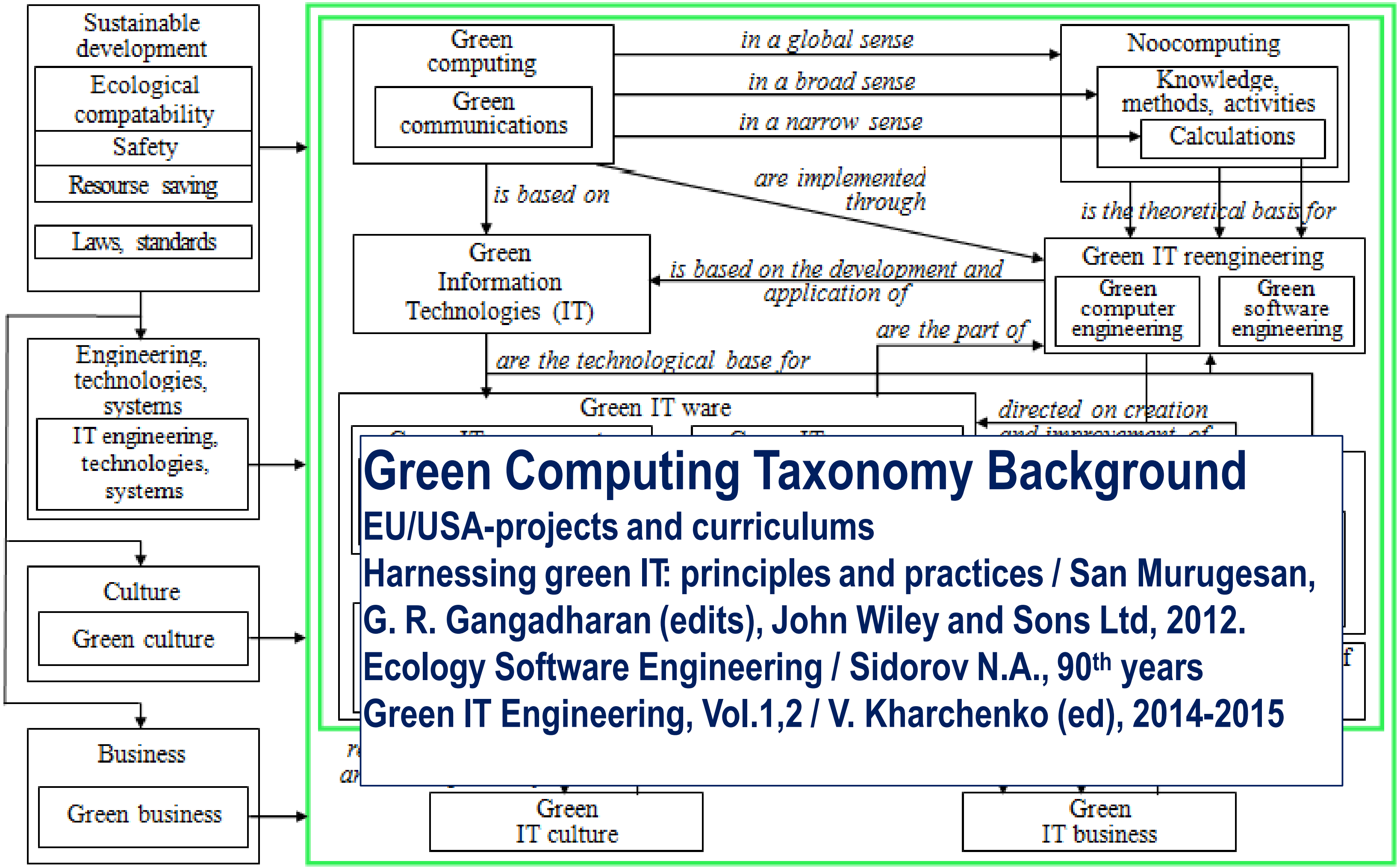
IT

# Green Computing: Taxonomy

**(Green IT-Engineering. Concepts, Models, Complex Systems Architectures,**
**Kharchenko Vyacheslav, Kondratenko Yuriy, Kacprzyk Janusz (Eds.), 2017, Springer Seria. – 305 p. )**



# Green Computing: Taxonomy




## Green Computing Taxonomy Background

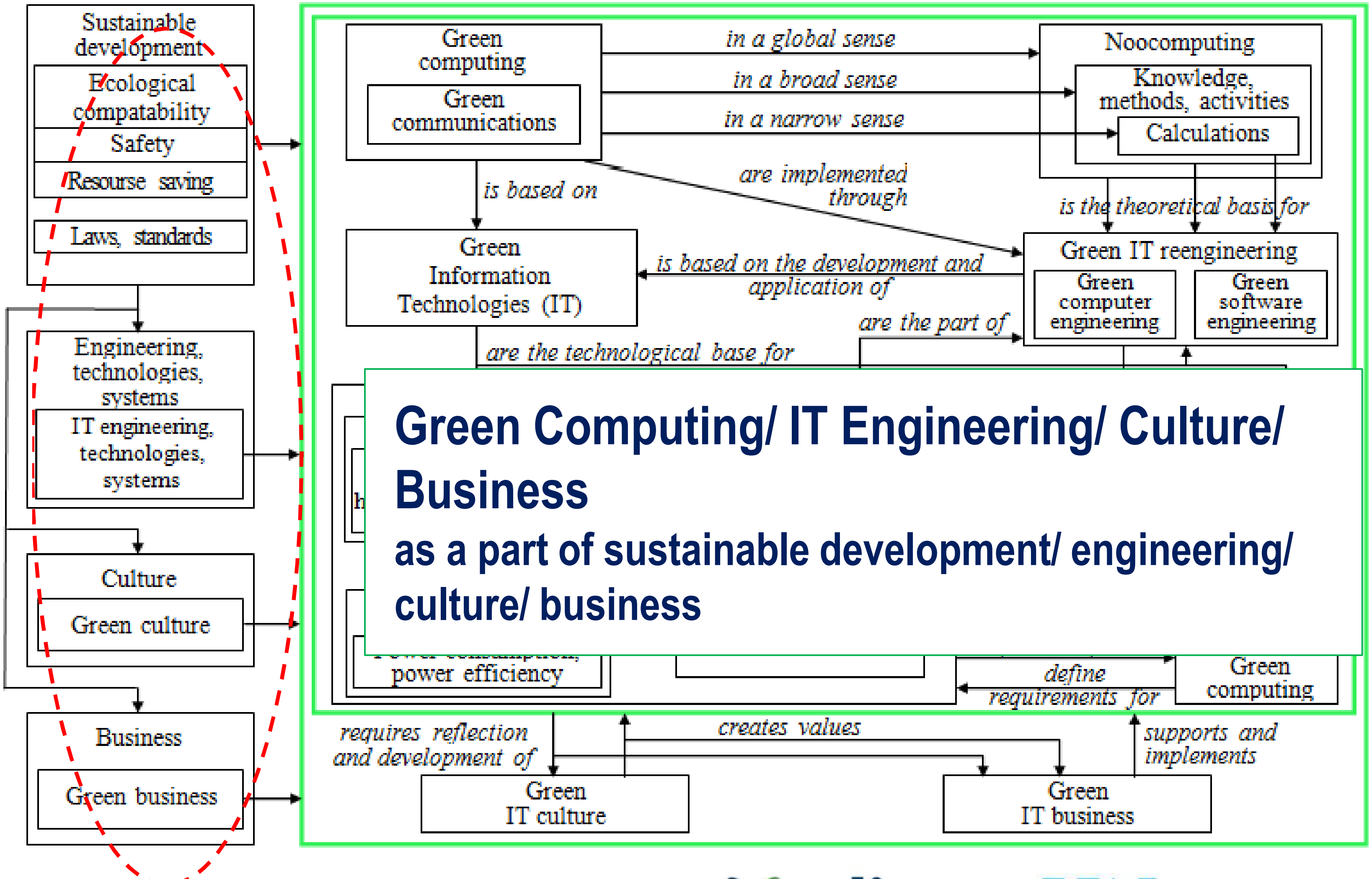
**EU/USA-projects and curriculums**

**Harnessing green IT: principles and practices / San Murugesan, G. R. Gangadharan (edits), John Wiley and Sons Ltd, 2012.**

**Ecology Software Engineering / Sidorov N.A., 90th years**

**Green IT Engineering, Vol.1,2 / V. Kharchenko (ed), 2014-2015**

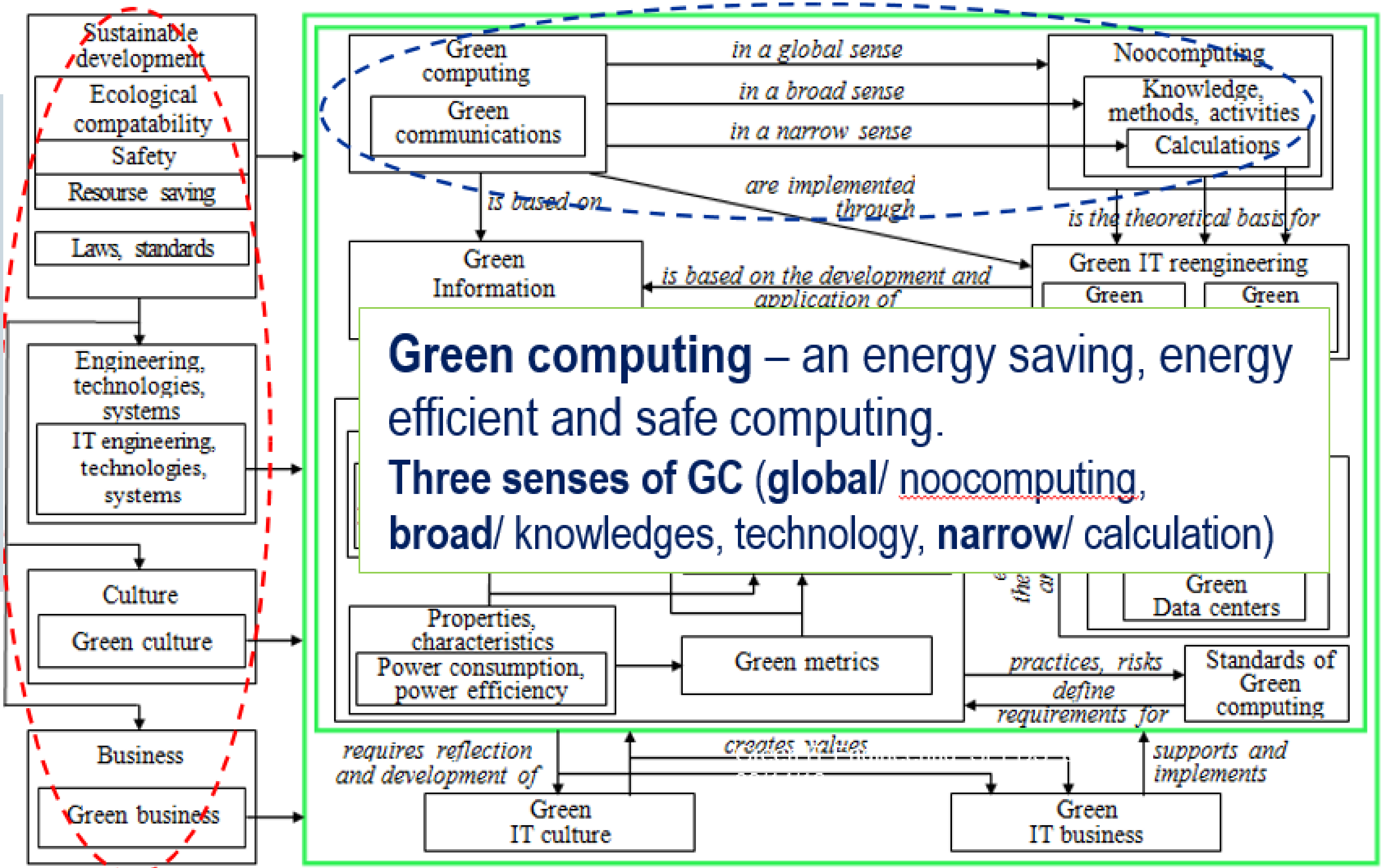
# Green Computing: Taxonomy




## Green Computing/ IT Engineering/ Culture/ Business

**as a part of sustainable development/ engineering/ culture/ business**

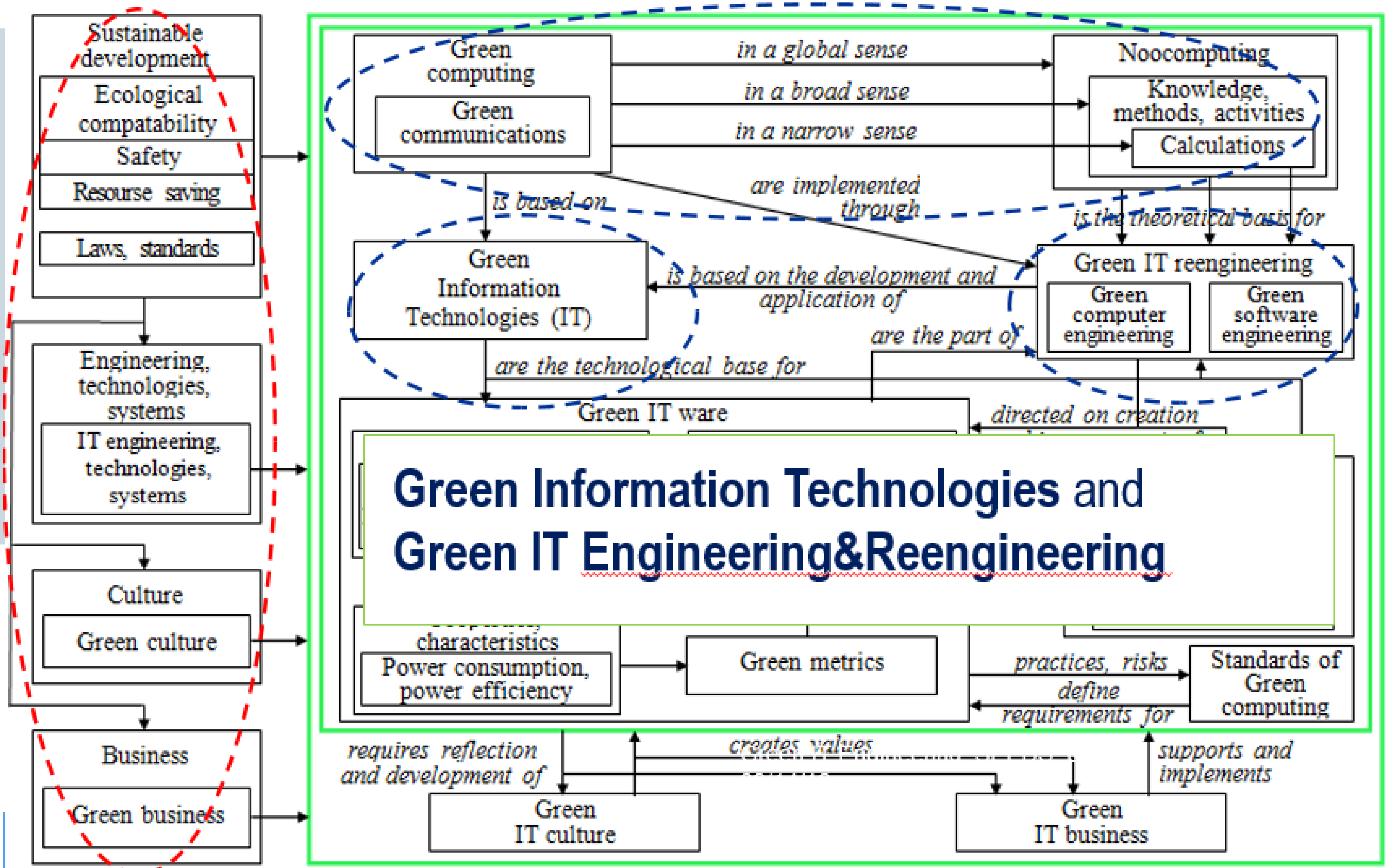
# Green Computing: Taxonomy




**Green computing** – an energy saving, energy efficient and safe computing.

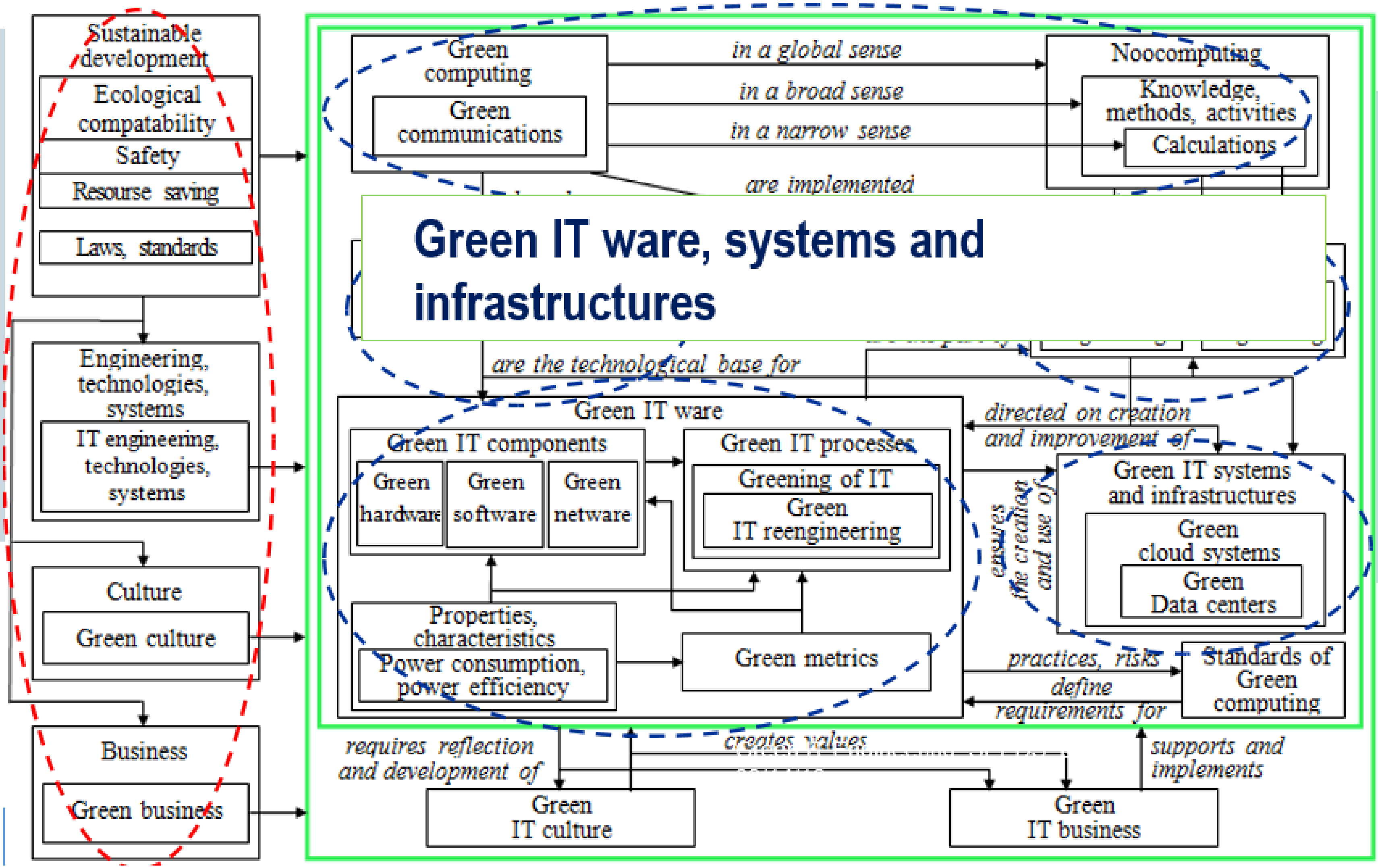
**Three senses of GC** (**global**/ noocomputing, **broad**/ knowledges, technology, **narrow**/ calculation)

# Green Computing: Taxonomy

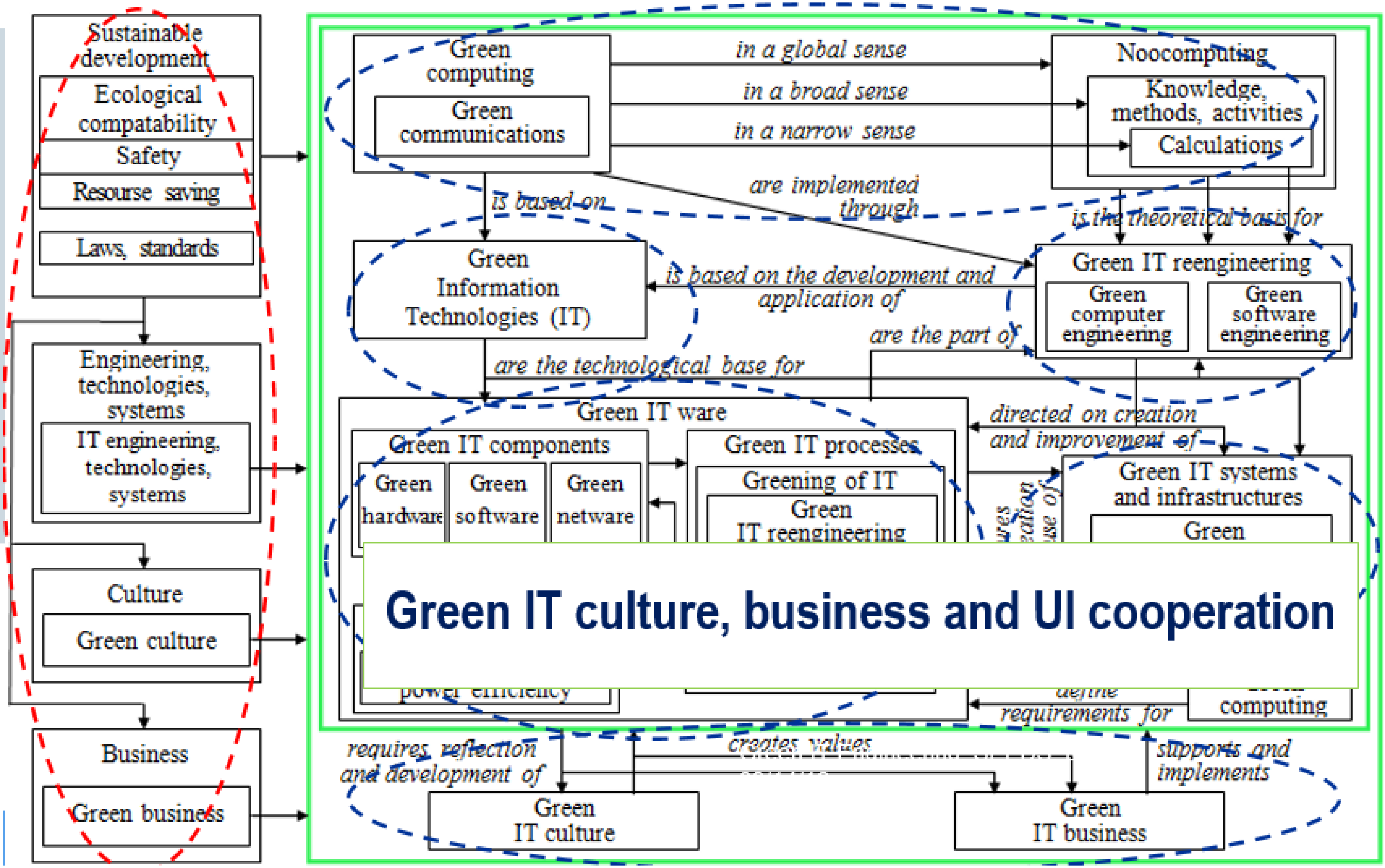



**Green Information Technologies** and
**Green IT Engineering&Reengineering**

# Green Computing: Taxonomy



# Green Computing: Taxonomy



# Green IT Culture Motion in Ukraine

**Green as a Core Value**

Green IT society as a part of Green society as a whole

**Do more with less for Win-Win-Win strategy**

Lean for Win-Win-Win (Green becomes a business goal and a competitive advantage)

**Green Culture**

Green Culture (Eco-culture) as main value of IT-society.

Safety Culture & Quality Culture as a part of Green Culture

**Green IT activity directions**

Green IT teaching

Green IT R&D and Green IT start-ups

Green IT business and communications

Green IT responsibility and social activities

# Green Computing: Some Principles

**General principles of green IT implementation:**

- the green-oriented life cycle model should be specified and implemented (similar safety life cycle);

- balancing of green and other characteristics (dependability, performance, cost,…);

- the green gap analysis based on determining of the discrepancies of requirements and existed project solutions (similar gap analysis for safety) may be applied to modernize existed I&C systems;

- the decisions concerning application of green processes and products should be made taking into account summarized costs for all life cycle including utilization (as a cost-effective approach for safety assurance).

# Green Computing: VN's Paradigm and Safety Again

**Key question of the Von Neumann's paradigm:**

**Can green system be developed out of not enough green components?**

**We can say "Yes" taking into account that safe ITs can be the part of green ITs at the specified conditions.**

# Green Computing: VN's Paradigm and Safety Again

**Key question of the Von Neumann's paradigm:**

**Can green system be developed out of not enough green components?**

**We can say "Yes" taking into account that safe ITs can be the part of green ITs at the specified conditions.**

**Techniques minimizing power consumption (PC) for dependable/safe systems:**

?

?

?

# Green Computing: VN’s Paradigm and Safety Again

**Key question of the Von Neumann’s paradigm:**

**Can green system be developed out of not enough green components?**

**We can say “Yes” taking into account that safe ITs can be the part of green ITs at the specified conditions.**

**Techniques minimizing power consumption (PC) for dependable/safe systems:**

**- decreasing of voltage up to acceptable or extreme (in point of view of soft fault rate) value for redundant channels (DVE);**

**?**

**?**

# Green Computing: VN's Paradigm and Safety Again

**Key question of the Von Neumann's paradigm:**

**Can green system be developed out of not enough green components?**

**We can say "Yes" taking into account that safe ITs can be the part of green ITs at the specified conditions.**

**Techniques minimizing power consumption (PC) for dependable/safe systems:**

- decreasing of voltage up to acceptable or extreme (in point of view of soft fault rate) value for redundant channels (DVE);
- introducing PC-oriented mode adaptation for chip (active/sleep modes switching) and separate redundant channels (PMA);
- controlled diverse clocking for internal redundant channels (CDS).

# Outline

About our team and projects

Introduction. Green vs Safe IT

Green Computing. Key principles

Safe Computing. Principles and Industry Solutions

Conclusions

## Safe Computing. Some Challenges

**There are problems of “last” faults for extra-safe IT-systems**

Detection and elimination (development stage), tolerating (operation stage)

- ***How we can tolerate design (SW), physical (HW), interaction (SW&HW) faults and vulnerabilities&attacks?***

  Common cause failure (CCF) problems for critical SW/FPGA-based systems and diversity application to decrease CCF risks

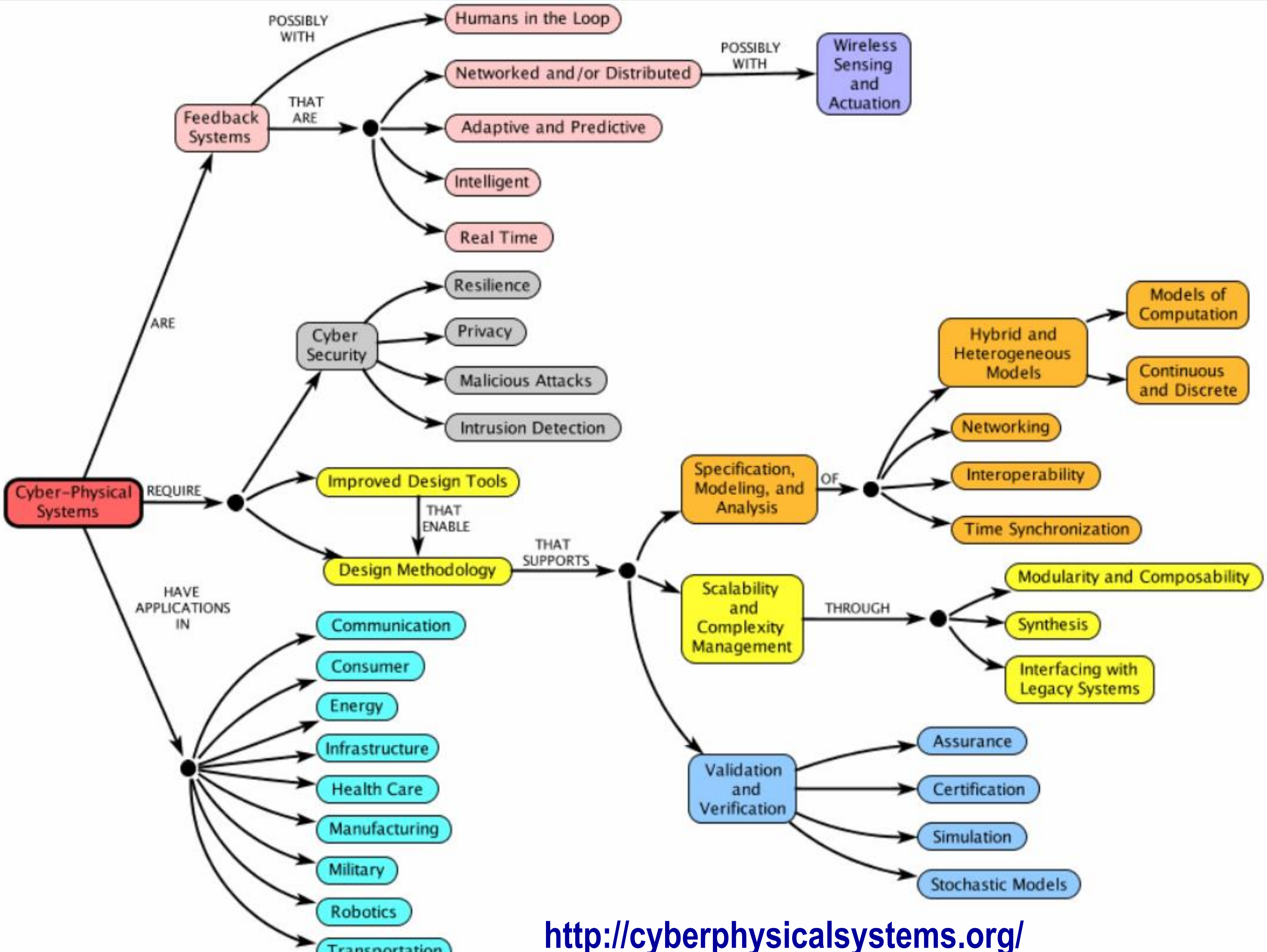
- ***How we can verify critical SW/FPGA systems, assess test cases quality (coverage), on-line testing trustworthiness and fault and intrusion tolerance?***

  Fault and multi-fault/vulnerability injection-based techniques of verification and validation

- ***How to assess influence of security on safety of SW systems?***

  Security informed safety approach: regulation, IMECA technique and security case

# Embedded/Cyber physical systems: Cyber security vs Cyber safety. Is this taxonomy correct?

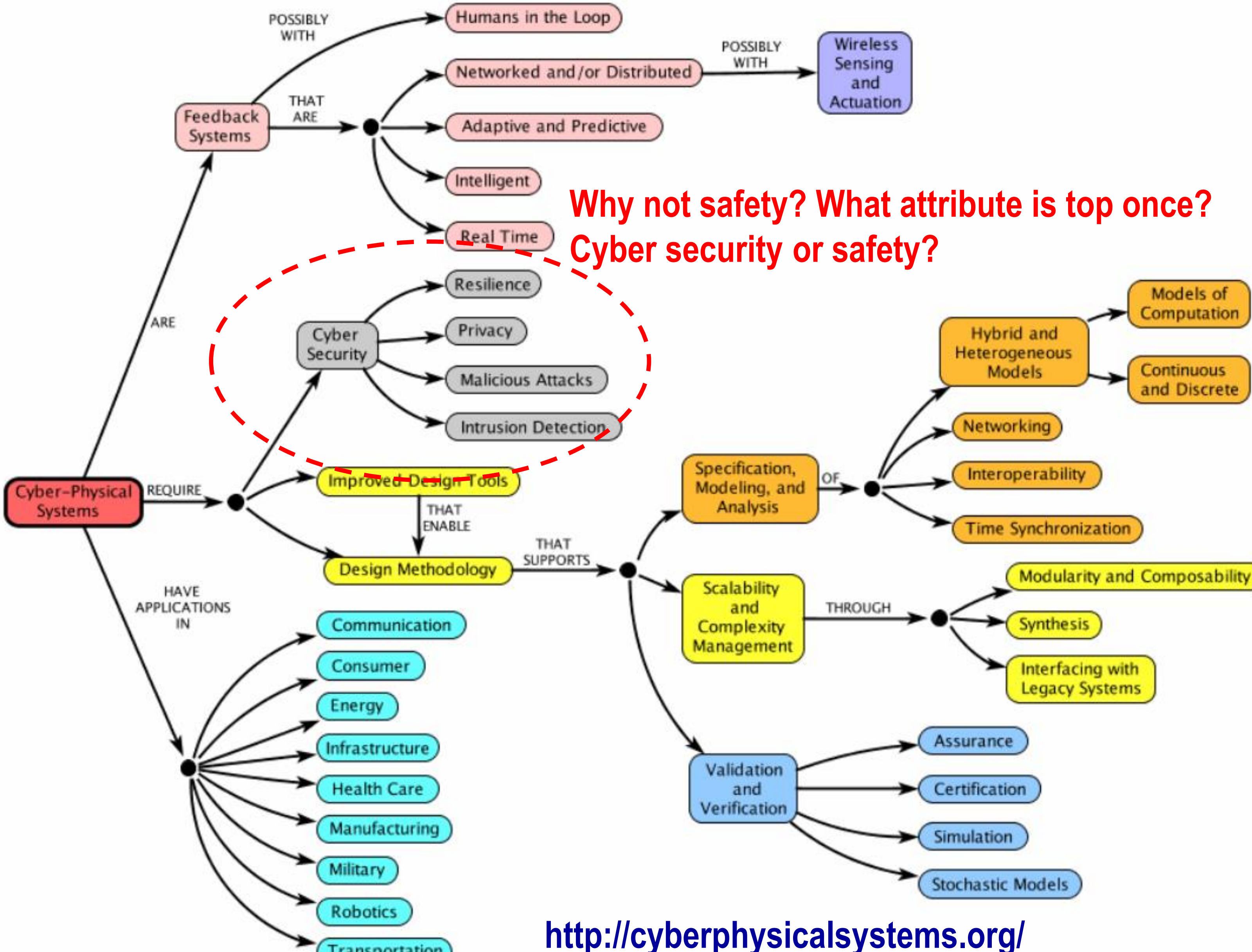



http://cyberphysicalsystems.org/

# Embedded/Cyber physical systems: Cyber security vs Cyber safety. Is this taxonomy correct?








**Why not safety? What attribute is top once? Cyber security or safety?**

http://cyberphysicalsystems.org/

# Safety of Critical Software/FPGA Systems: Some Challenges

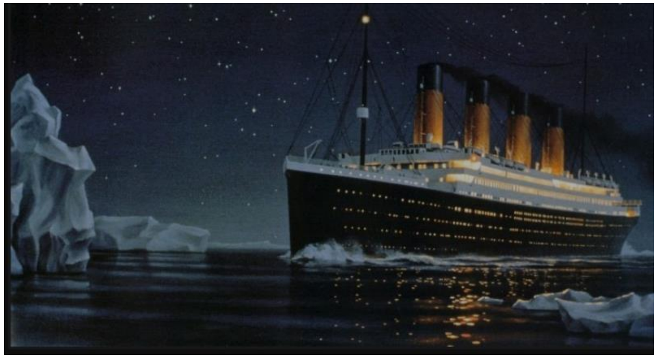
Complexity,  human (design, V&V, environment, decision making) →

new uncertainties & faults & errors

Let’s remember tragedies

Titanic

Challenger …





radiy

# Safety of Critical Software/FPGA Systems: Some Challenges

**Complexity, human (design, V&V, environment, decision making) →**
**new faults & errors**

**Security/cybersecurity issues →**
**new vulnerabilities & threats & attacks & failures**

# Safety of Critical Software/FPGA Systems: Challenges/Automotive

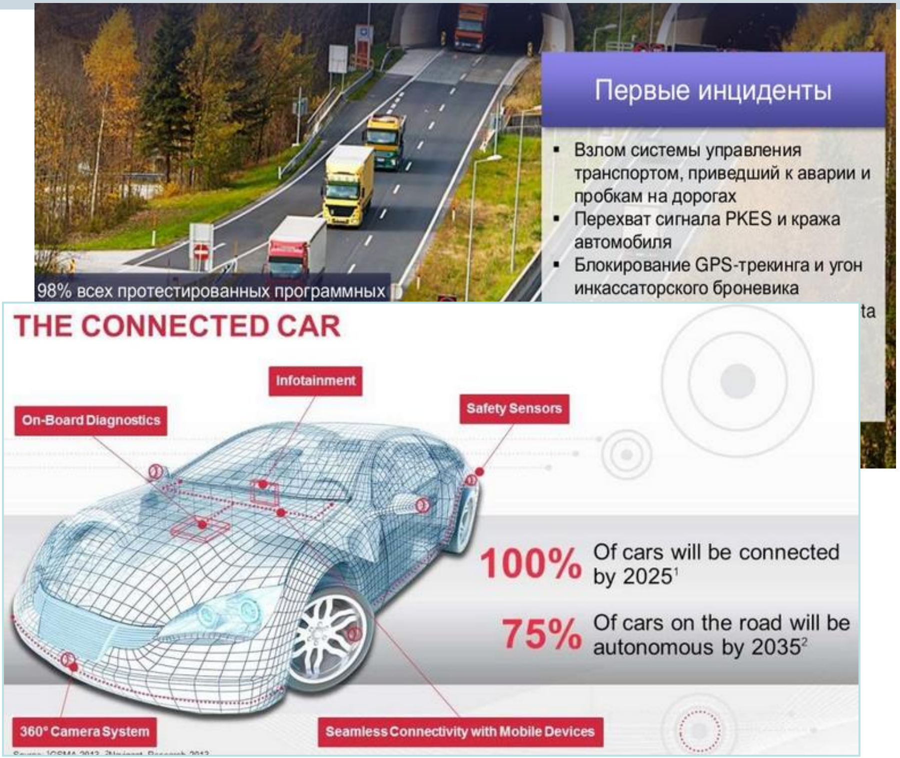
## Hot facts

- 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”/ITS 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

# Safety of Critical Software/FPGA Systems: Some Challenges

Complexity, human (design, V&V, environment, decision making) → new faults & errors

Security/cybersecurity issues → new vulnerabilities & threats & attacks & failures

+ New components (SW, FPGA) and ITs (cloud, IoT) → new risks & deficits of safety/security

# Critical Computing Concepts: Safety vs Security

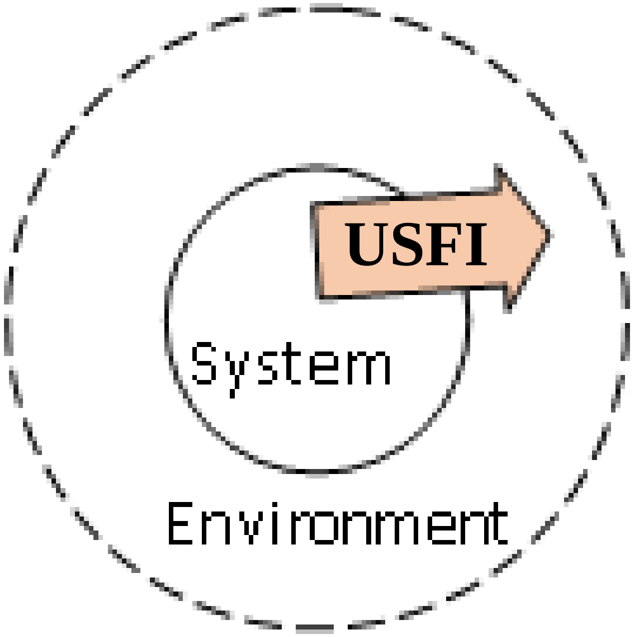
(Cyber) Safety

(Cyber) Security

**What is difference?**
**(system, environment, influence)**

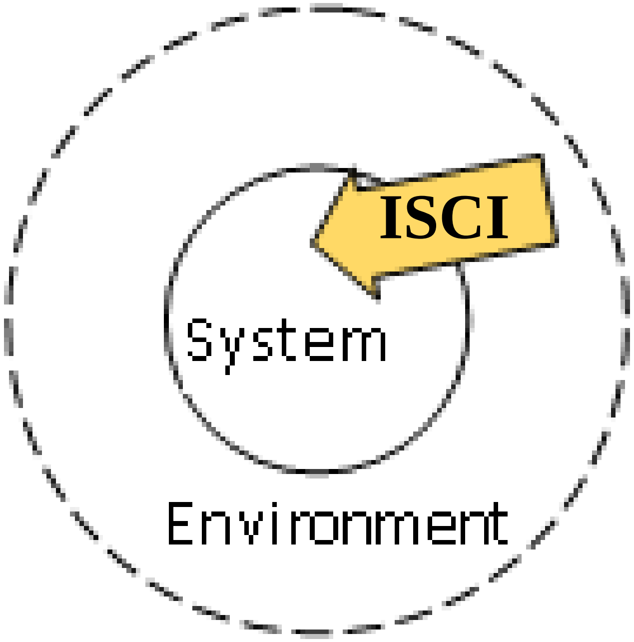
# Critical Computing Concepts: Safety vs Security

(Cyber) Safety



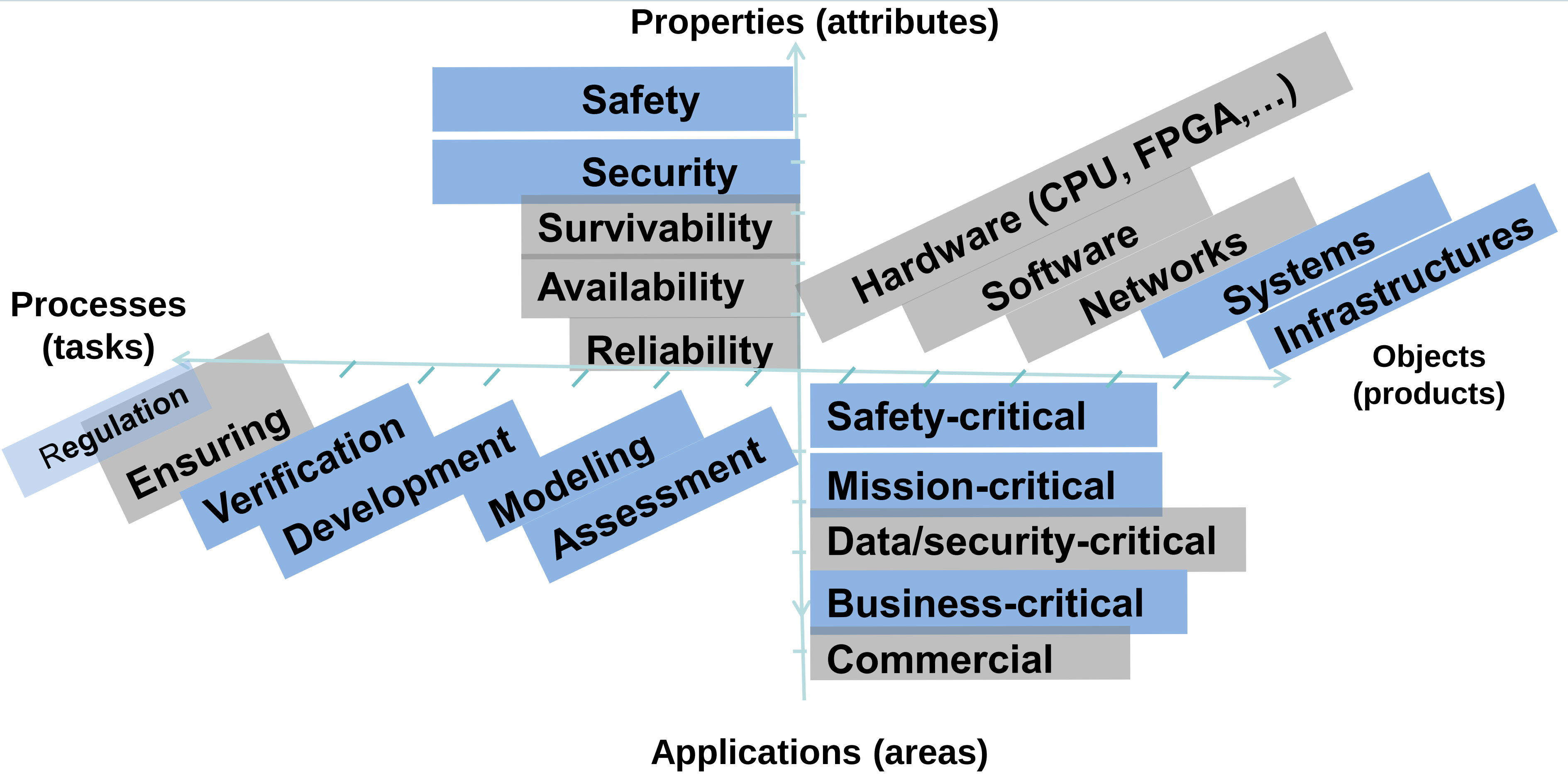

USFI – unsafe influence
of system on environment
(other systems, people,…)

(Cyber) Security

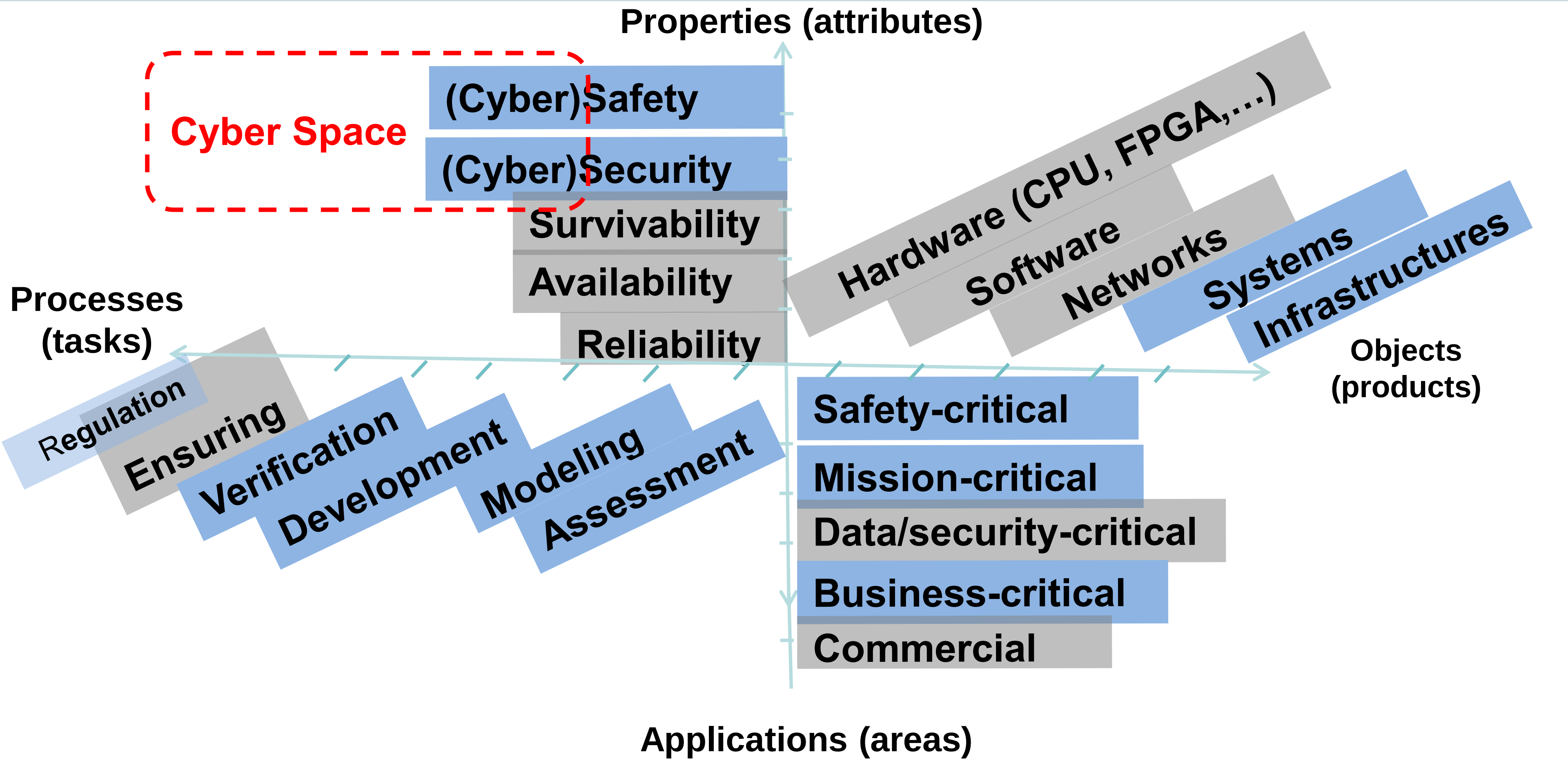



ISCI – insecure intrusion
of environment (…) on system

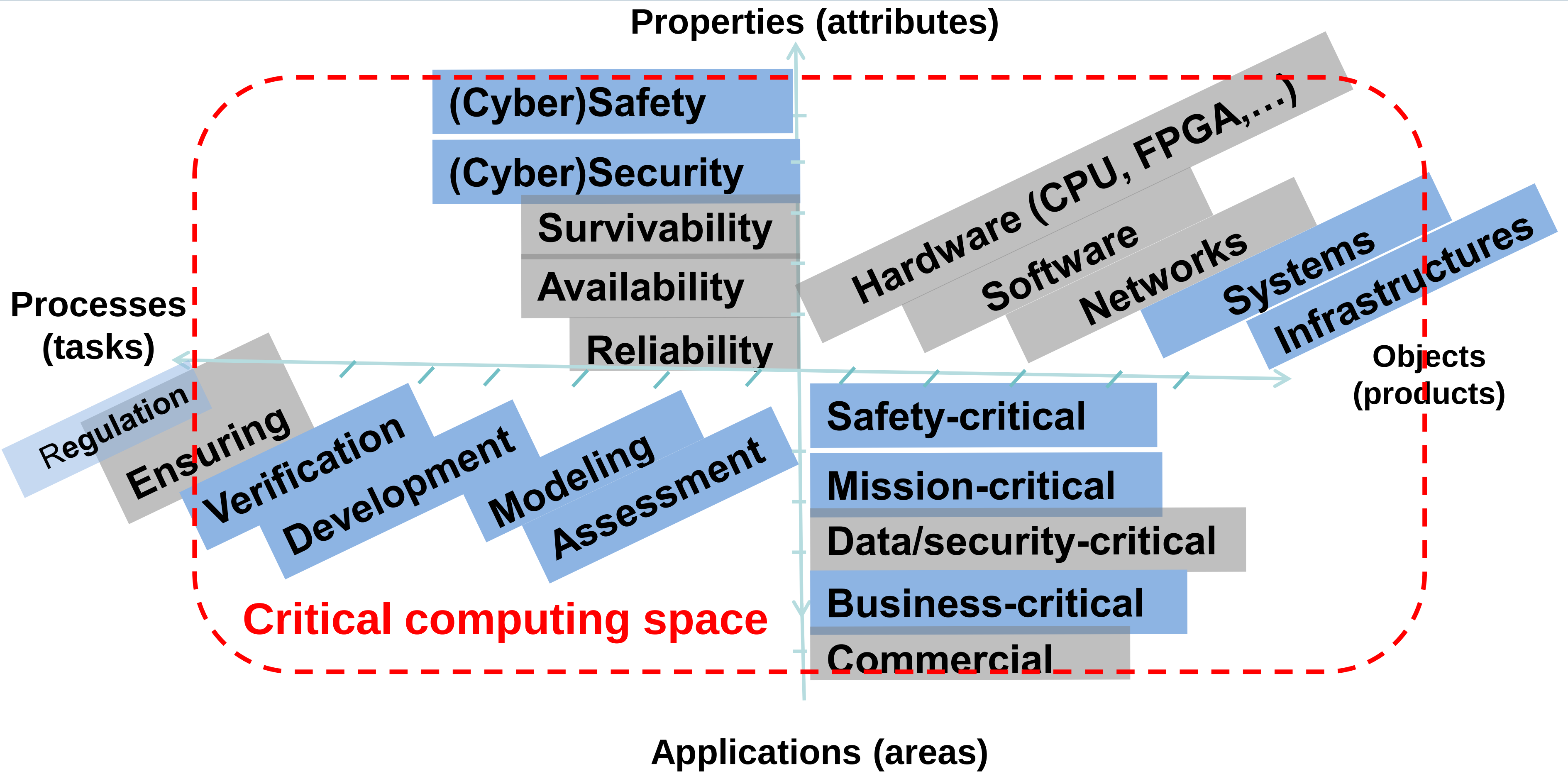
# Critical Computing Concepts: Space



# Critical Computing Concepts: Space



# Critical Computing Concepts: Space

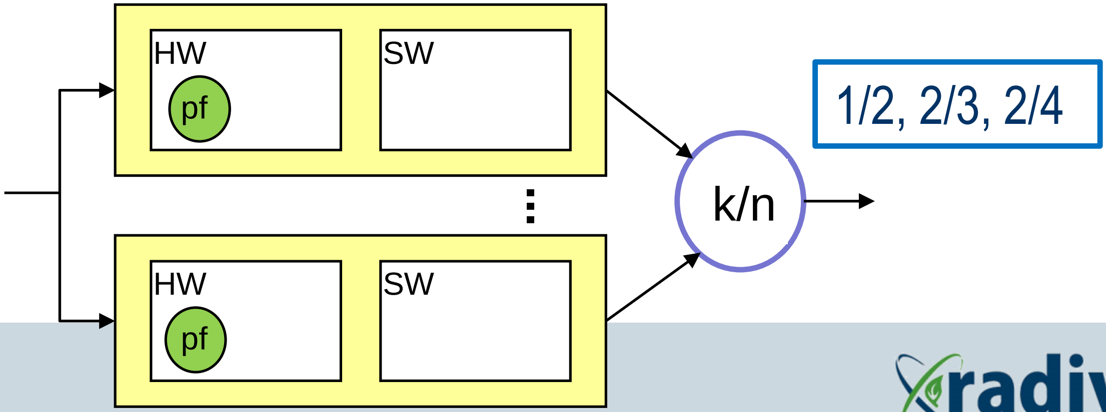


# Common Cause Failures: Reasons

- **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);

\+ ?





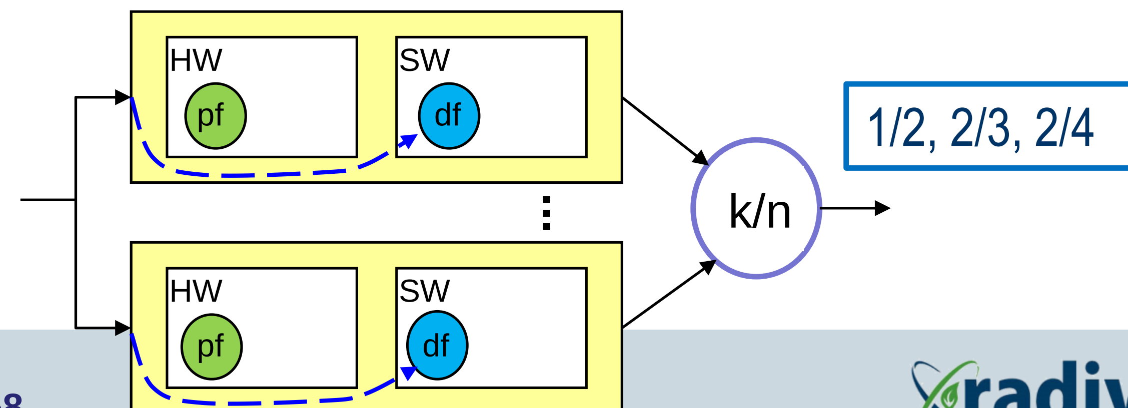

radiy

# Common Cause Failures: Reasons (2)

- **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 (1990-2015));



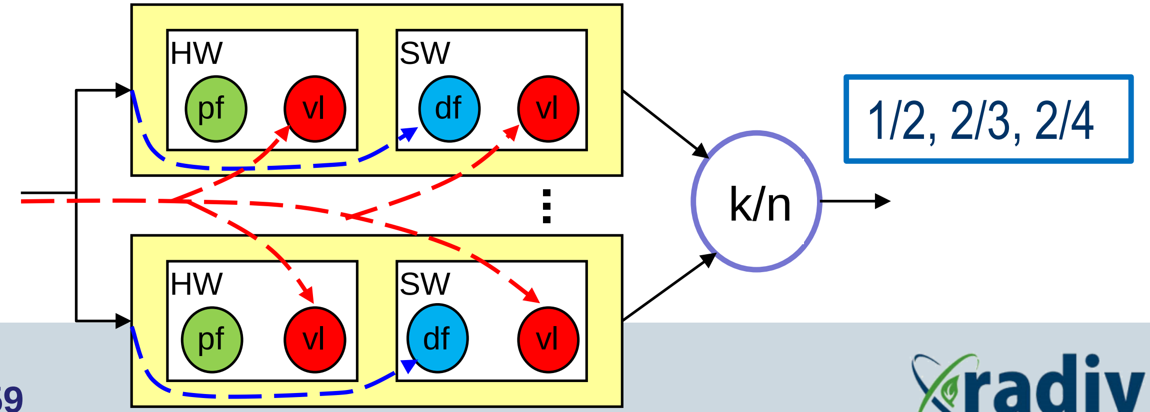
# Common Cause Failures: Reasons (3)

- **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 (1990-2015));

\- **multiple interaction faults** caused by SW/FPGA/HW **vulnerabilities (vl)** and **intrusions (attacks)** to ones

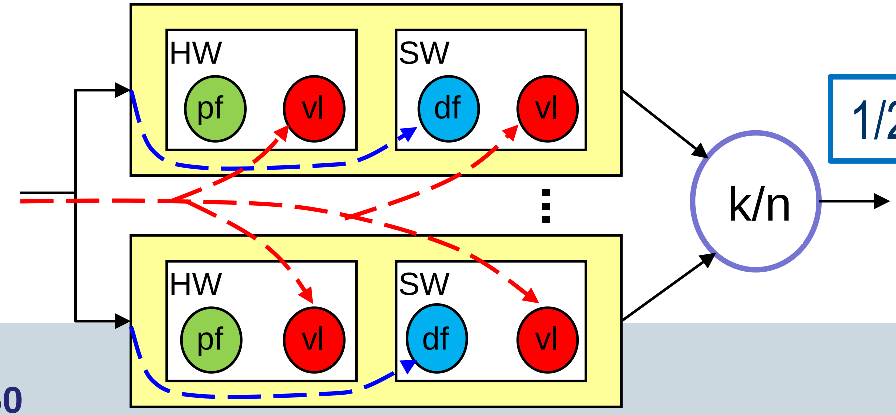



# Common Cause Failures. Preliminary conclusion

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








1/2, 2/3, 2/4

# Common Cause Failures. Question?

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

**Any suggestion how to minimize/exclude CCF risk?**

**For:**

**Security lock systems**

**Banking systems/Our money in banks**

**…**

**Aviation/car on-board systems**

**Reactor trip systems**

**Health monitoring & control**

**Railway…**

# Common Cause Failures. Simple example: Diversity of Locks

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

**Any suggestion how to minimize/exclude CCF risk?**


**Security entrance system with a lot of different locks**

# Common Cause Failures. Simple example: Diversity of Locks

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

**Any suggestion how to minimize/exclude CCF risk?**

**Perpetrator cannot open door using one key**

# Common Cause Failures. Simple example: Diversity of Bank Accounts

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

**Any suggestion how to minimize/exclude CCF risk?**

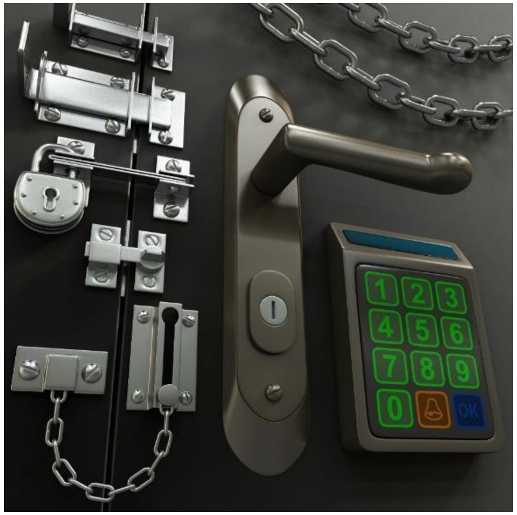

**All banks cannot be simultaneously liquidated**




radiy

# Common Cause Failures. 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.



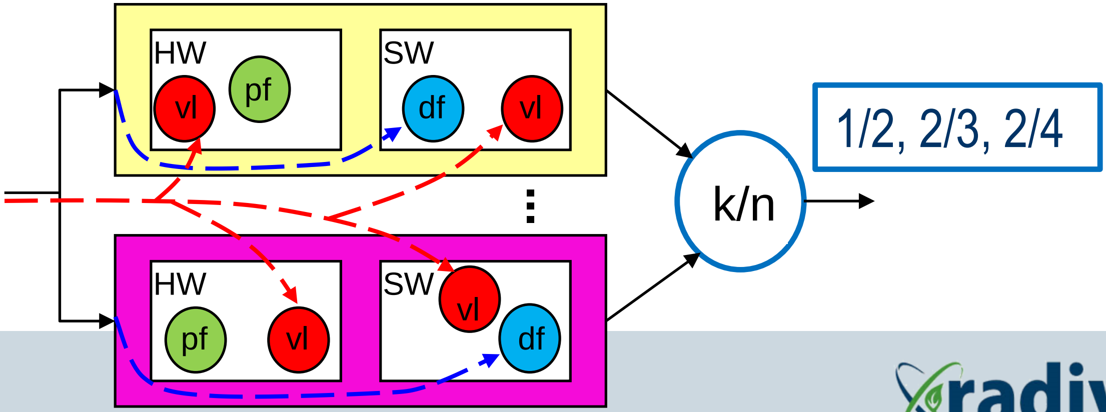

**We have to apply diversity to minimize risk of common failure for redundant systems!**

# Common Cause Failures. Multi-Version Computing

- **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.

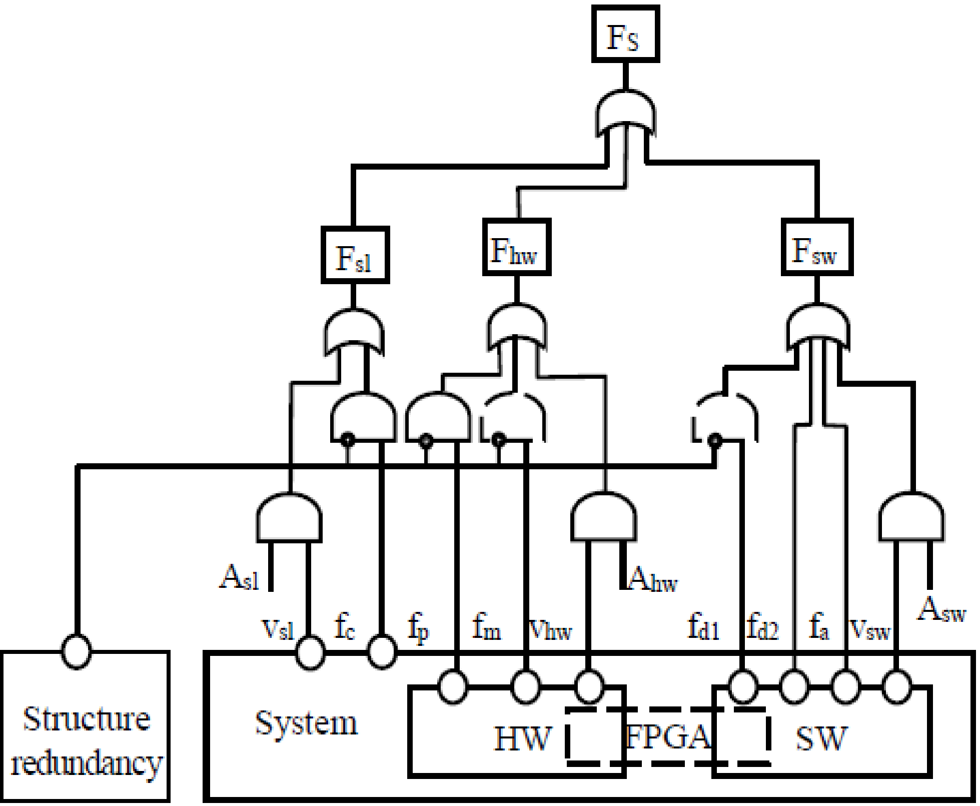
(**IEC61508**: different means of performing a required function).
(**IEC26262**: different solutions satisfying the same requirement with the aim of independence).

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




# Diversity Fundamentals: Structure Redundancy

## F/ATA - Structure redundancy

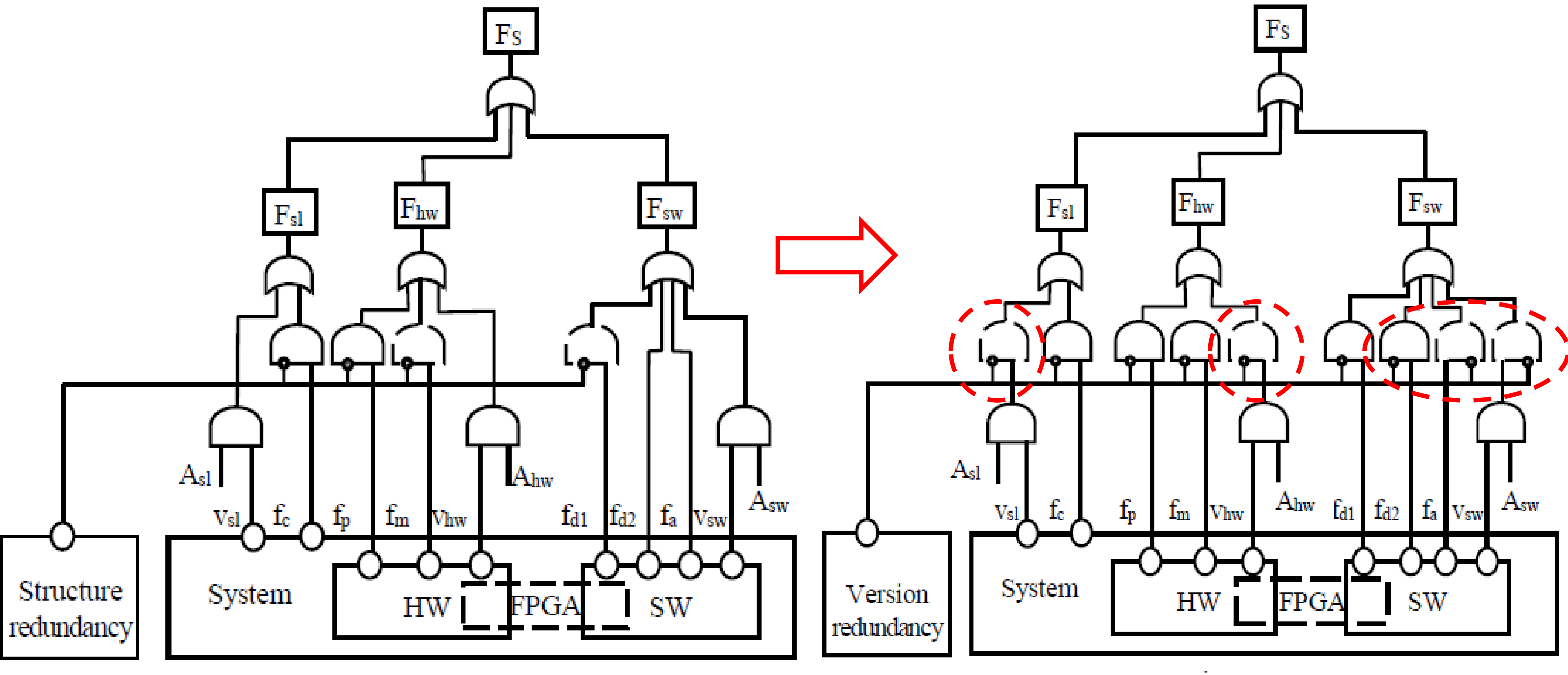




radiy

# Diversity Fundamentals: Structure vs Version Redundancy

## F/ATA - Structure redundancy　　F/ATA – Version&Structure redundancy



# Diversity Related Concepts: Formal Models of MVS

**One-version $W(1)$** and **multi-version $W(n)$** systems are defined by 4 and 6 variables:

$$\mathbf{W(1) = \{X, Y, Z, \Phi\},}$$
$$\mathbf{W(n) = \{X, Y, Z, \Phi, V, \Psi\} = \{W(1), V, \Psi\},}$$

where $X, Y, Z$ – sets of input signals, states and output signals correspondingly;
$\Phi = \{\varphi_i, i=1, ..., a\}$ – set of I&C functions (e.g. actuation functions of reactor trip system);
$V = \{v_j, j=1, ..., n\}$ – set of versions with output signals $Z_1, \ldots, Z_n$ (or signals $Z_{id}$, $d = 1, \ldots, n_i$;
$n_i$ – number of versions for function $\varphi_i$; $\forall \varphi_i \sim v_j = \{ v_{ij}, j = 1, ..., n_i\})$ ;
$\Psi = \{ \psi_s, s=1, ..., в \}$ – mapping $Z_i \rightarrow Z$.

In general:

$$\mathbf{W(n,m,l) = \{X, Y, Z, \Phi, V, \Psi, R, \Theta, C, Q\} = \{ W(n), R, \Theta, C, Q\} = \{ W(n,m), C, Q\}}$$

where $R = \{r_d, d=1, ..., m\}$ – set of version redundancy kinds, $\Theta$ - mapping: $R \rightarrow V$;
$C=\{c_q, q=1,...,l\}$ - set of redundant channels; $Q$ – mapping: $V \rightarrow C$.

# Diversity Related Concepts: Key Questions

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

  **How to assess** actual value of diversity?

  **How to ensure** required value of diversity?

- **Practical issues:**

  **How:**

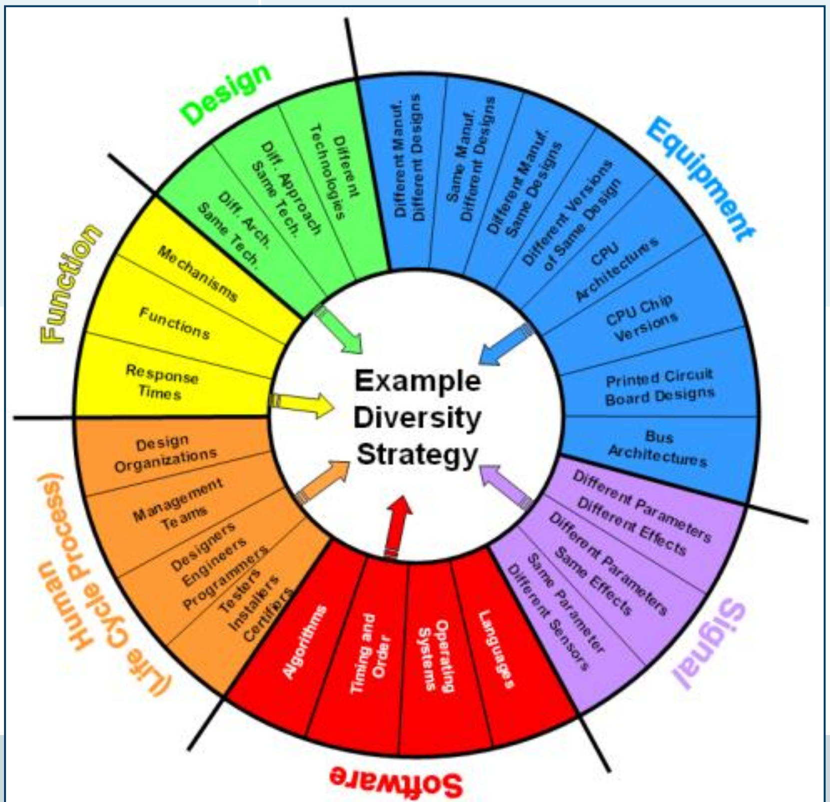
  to formulate (in general/detail) requirements to diversity application;

  to assess of system diversity value to meet strong standard requirements (reactor trip systems, aerospace control systems, railway signaling&blocking,…);

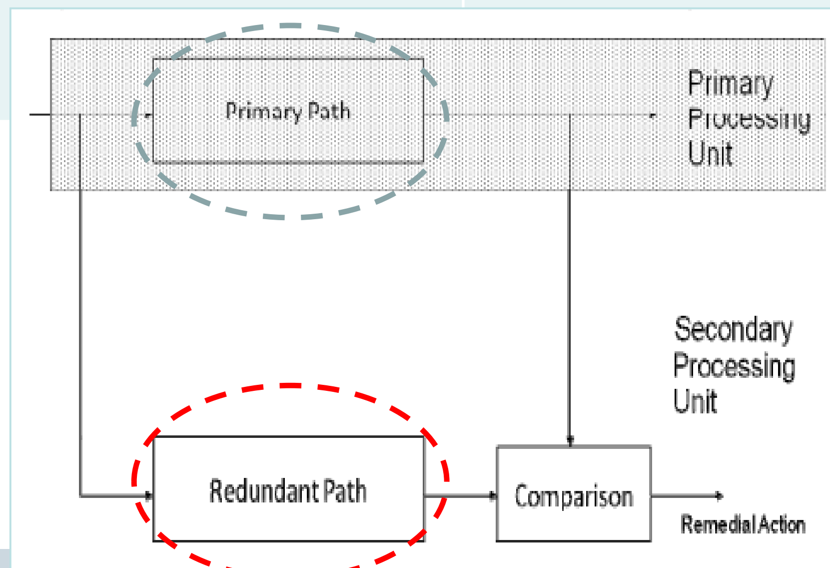
  to choice diversity types and volume by optimal (required safety / minimal cost) way?

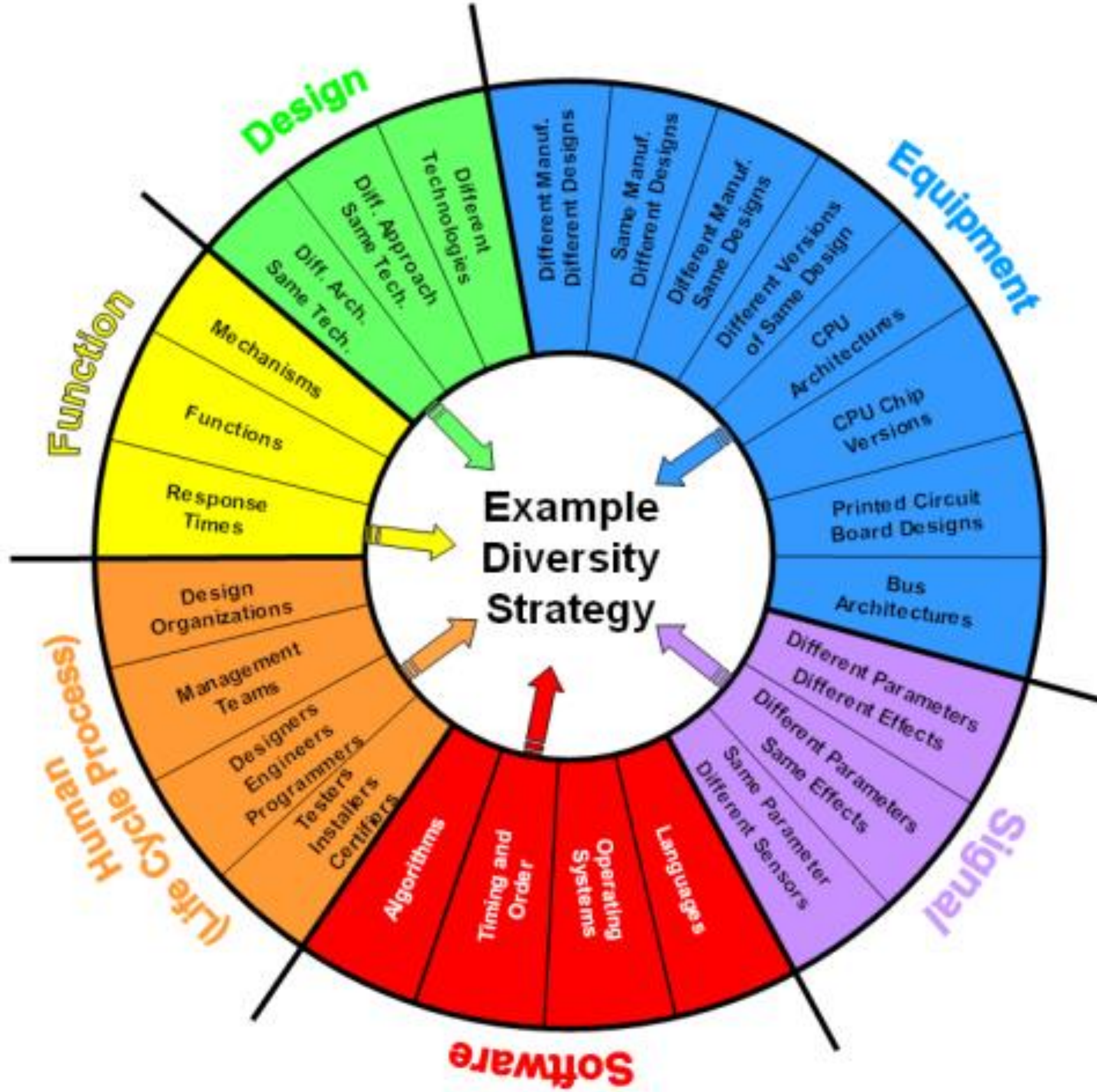
# Challenges: Uniqueness of MVSs, Classification of Diversity

| Aspect | Challenge | Question |
|---|---|---|
| 1. Uniqueness of multi-version systems | There are a lot of DA implementations *but*:<br>- MVSs are applied in NPPs (NUREG7007), aviation, railway, automotive (**IEC26262**) | ? |




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






## NUREG7007 diversity 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 |

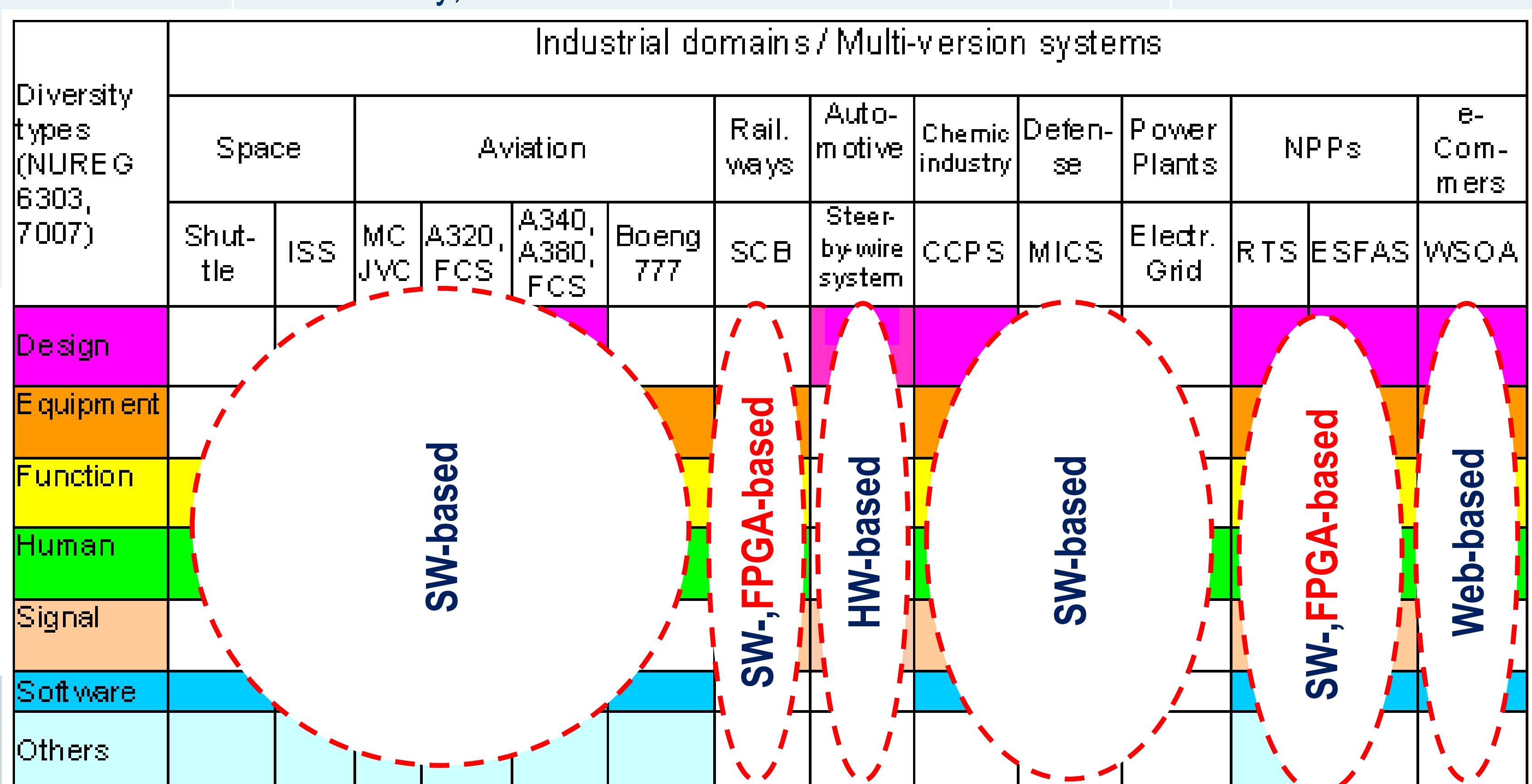
# Challenges: Uniqueness of MVSs/ Application

| Aspect | Challenge | Question |
|---|---|---|
| 1. Uniqueness of multi-version systems | There are a lot of DA implementations *but*:<br>- 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 | ■ | ■ | ■ | ■ | ■ | ■ | | | | | | ■ | | |

# Challenges: Uniqueness of MVSs/ Application

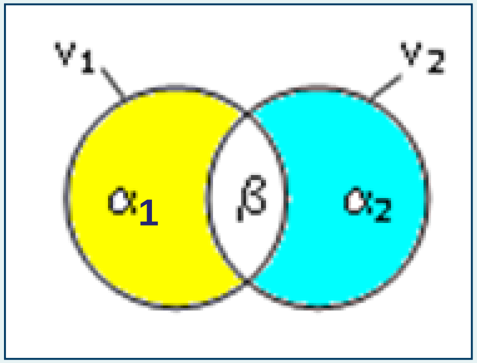
| Aspect | Challenge | Question |
|---|---|---|
| 1. Uniqueness of multi-version systems | There are a lot of DA implementations *but*:<br>- MVSs are applied in NPPs, aviation, railway,… in different way; | ? |



# Challenges: Uniqueness of MVSs/ Question

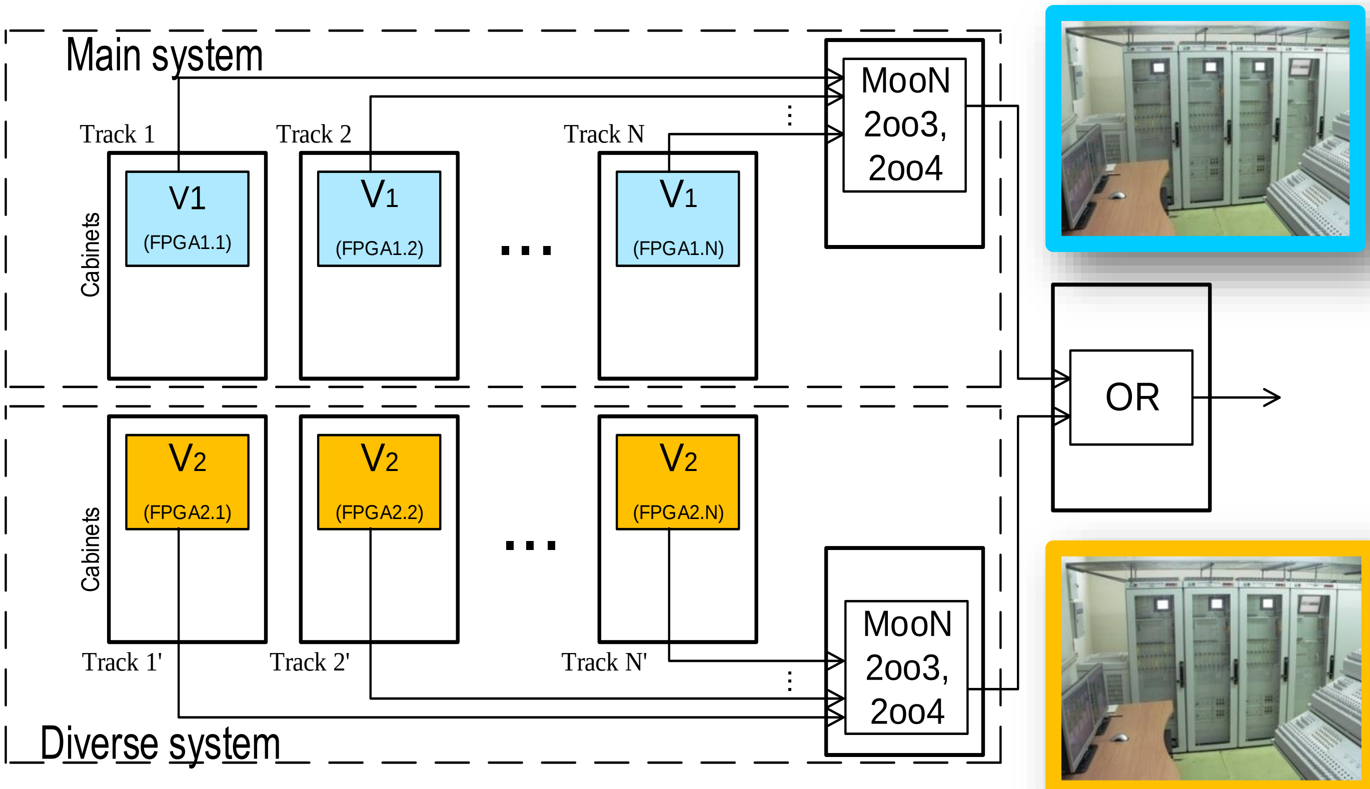
| Aspect | Challenge | Question |
|---|---|---|
| 1. Uniqueness of multi-version systems | There are a lot of DA implementations but:<br>- MVSs are applied in NPPs, aviation, railway,… **in different way;**<br>- **component failures occur rarely** (Radiy more 105 years experience);<br>- **use of statistical evaluation methods is limited**;<br>- **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?***<br><br>***Standards***<br>***IEC 60880***<br>***IEC61508***<br>***IEC 26262?*** |

# Challenges: New Technologies and Risks

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

# Diversity Related Industry Examples: NPP RTSs

## Structure of 2-Version Reactor Trip System Based on Radiy Platform




- The Radiy platform-based RTS design consists of two independent and diverse divisions:
  - FPGA1 / FPGA2;
  (or FPGA / MP);
  - other diversity types.
- Safety actuation by either division initiates reactor shutdown.
- Each division is composed of three (or four) separate channels.

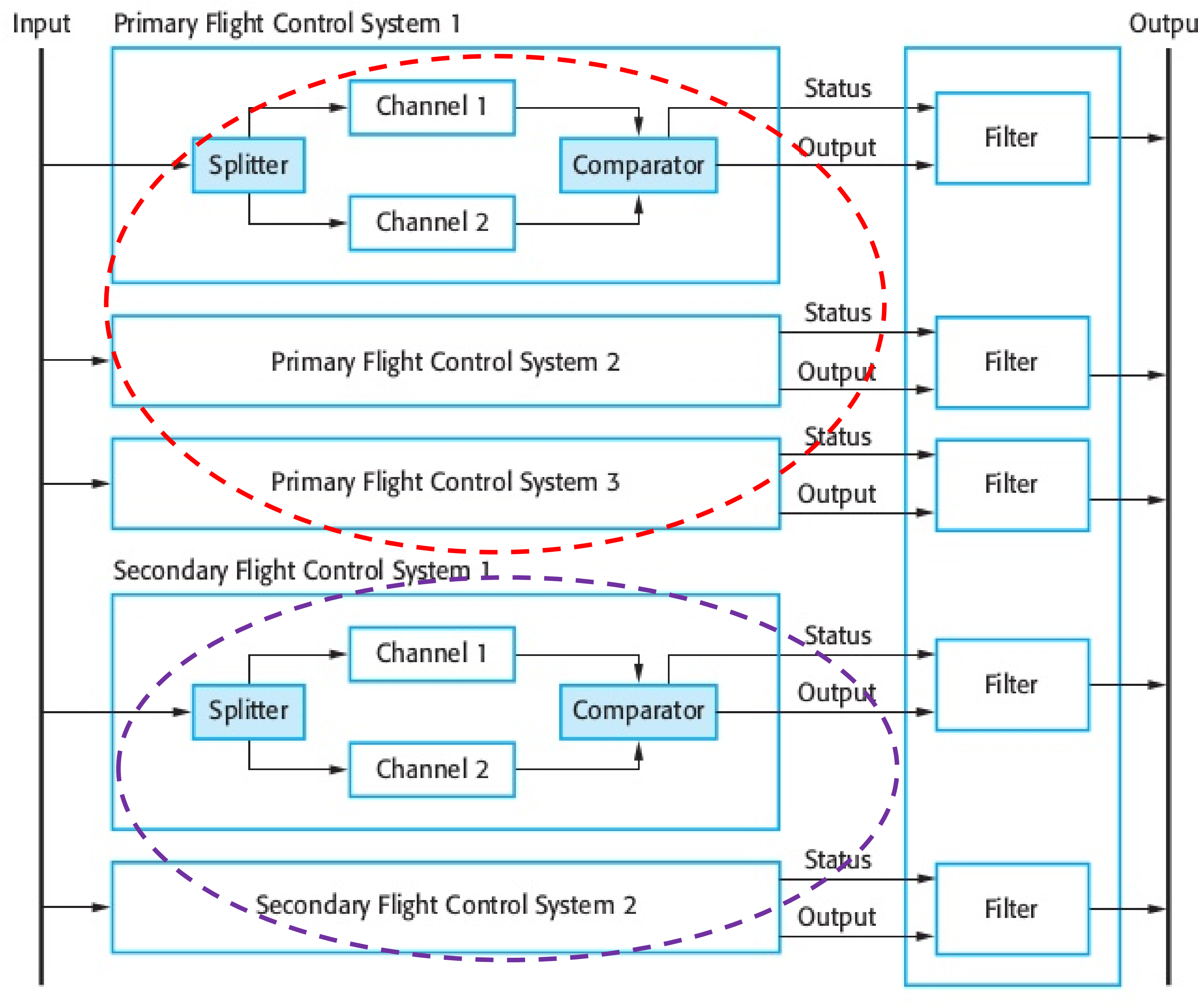
radiy
XAI

# Diversity Related Industry Examples: A340/A380 Control System

(I. Sommerville. Software Engineering, Addison-Wesley, 2011)

**A340,380 on-board control systems**

- 2 diverse OSs primary/secondary
- 2 diverse appl SW primary/secondary

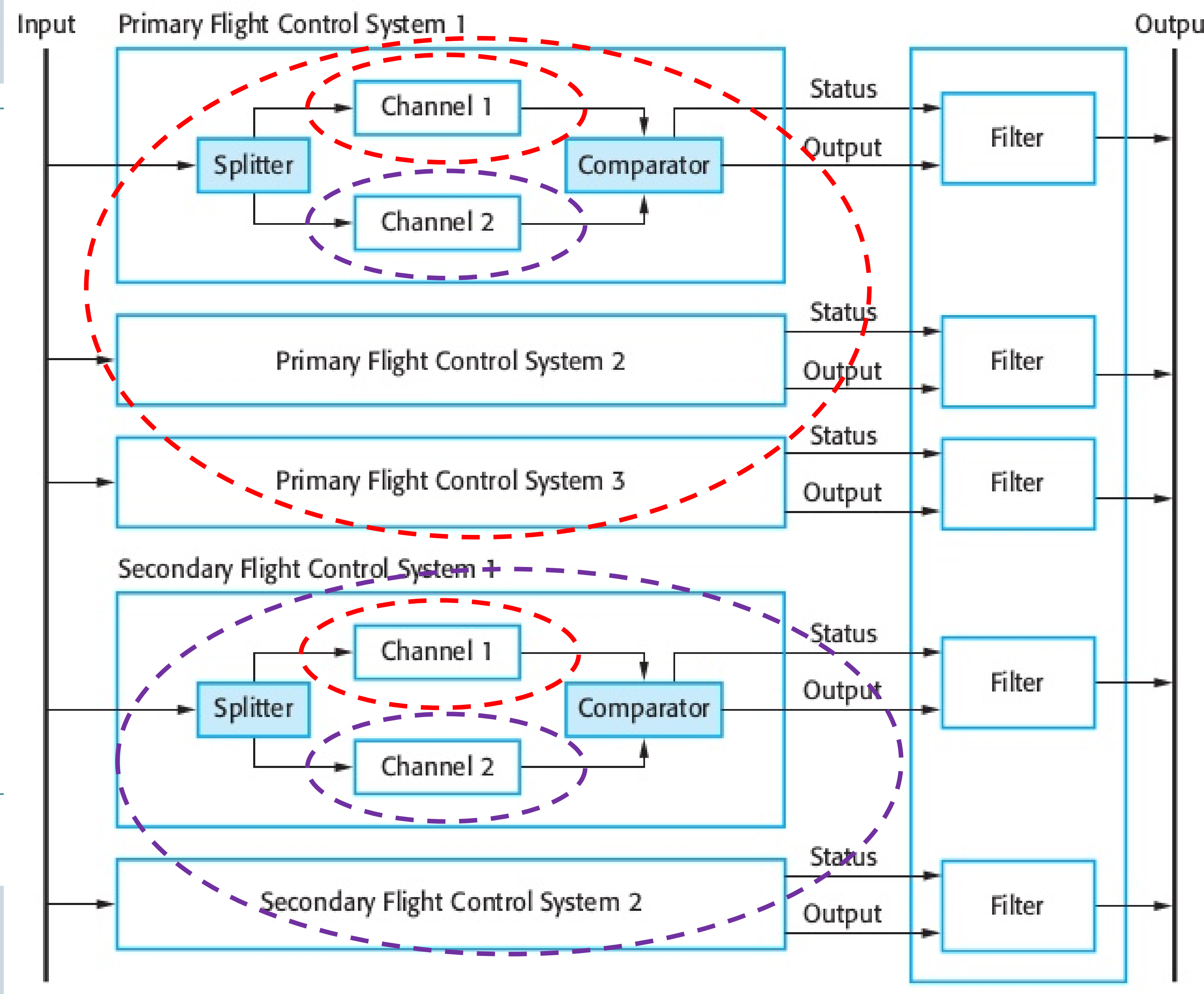


# Diversity Related Industry Examples: A340/A380 Control System

(I. Sommerville. Software Engineering, Addison-Wesley, 2011)

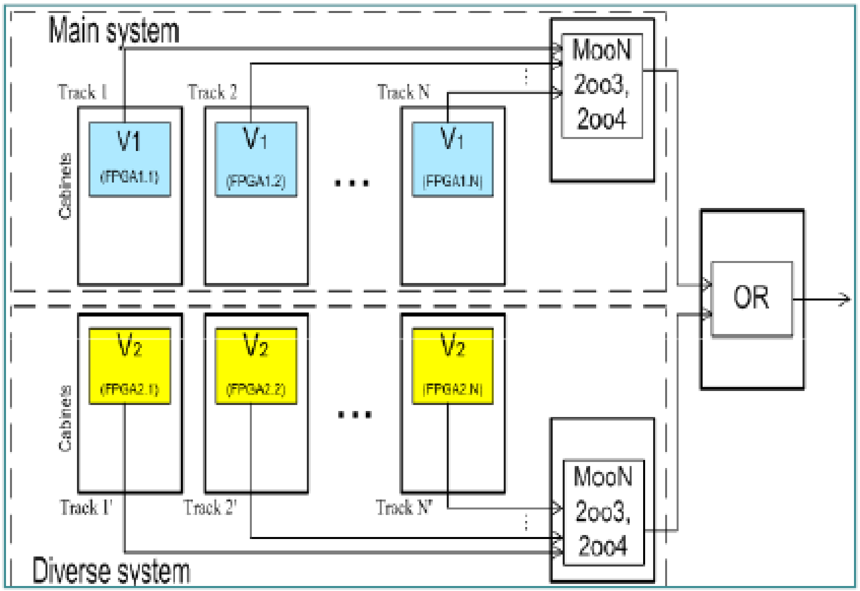
**A340,380 on-board control systems**

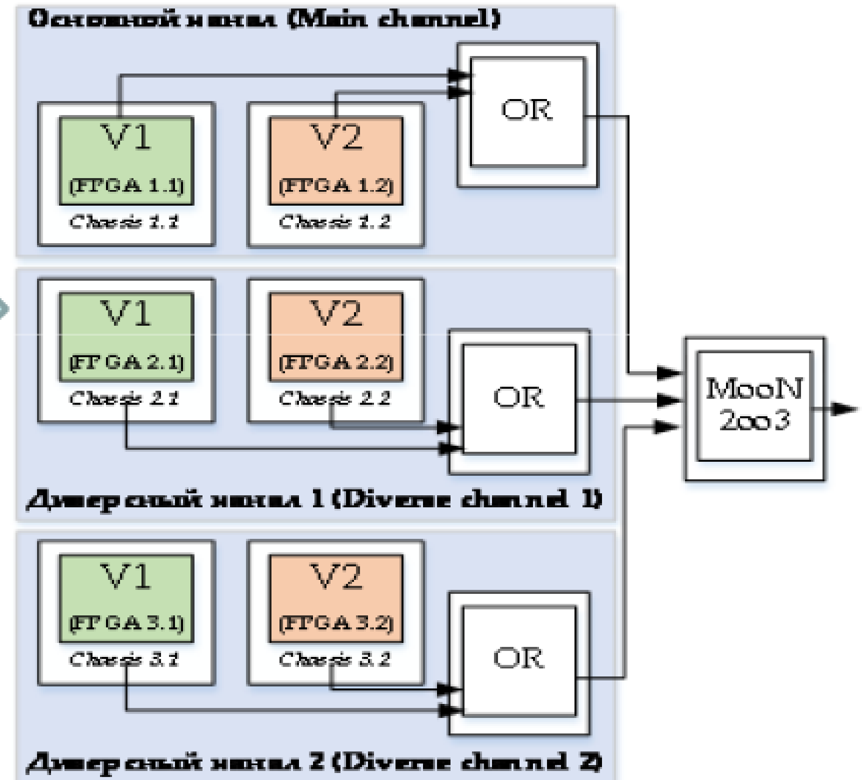
- 2 diverse OSs
  primary/secondary
- 2 diverse appl SW
  primary/secondary
- 2 diverse CPUs
  channel 1/2
- 2 diverse PCBs
  channel 1/2



# MVS Safety Assessment: Reactor Trip System/ Two structures

(V. Kharchenko, V Butenko, O Odarushchenko, E Odarushchenko. Markov's Modeling of NPP I&C Reliability and Safety: Optimization of Tool Selection, Second International Symposium on Stochastic Models in Reliability, Ber-Sheva, Israel, 2016; V. Kharchenko, V. Butenko, O. Odarushchenko, V. Sklyar. Multi-Fragmental Markov"s Modeling of a Reactor Trip System// Journal of Nuclear Engineering and Radiation Science 1 (3), Canada, 2015)

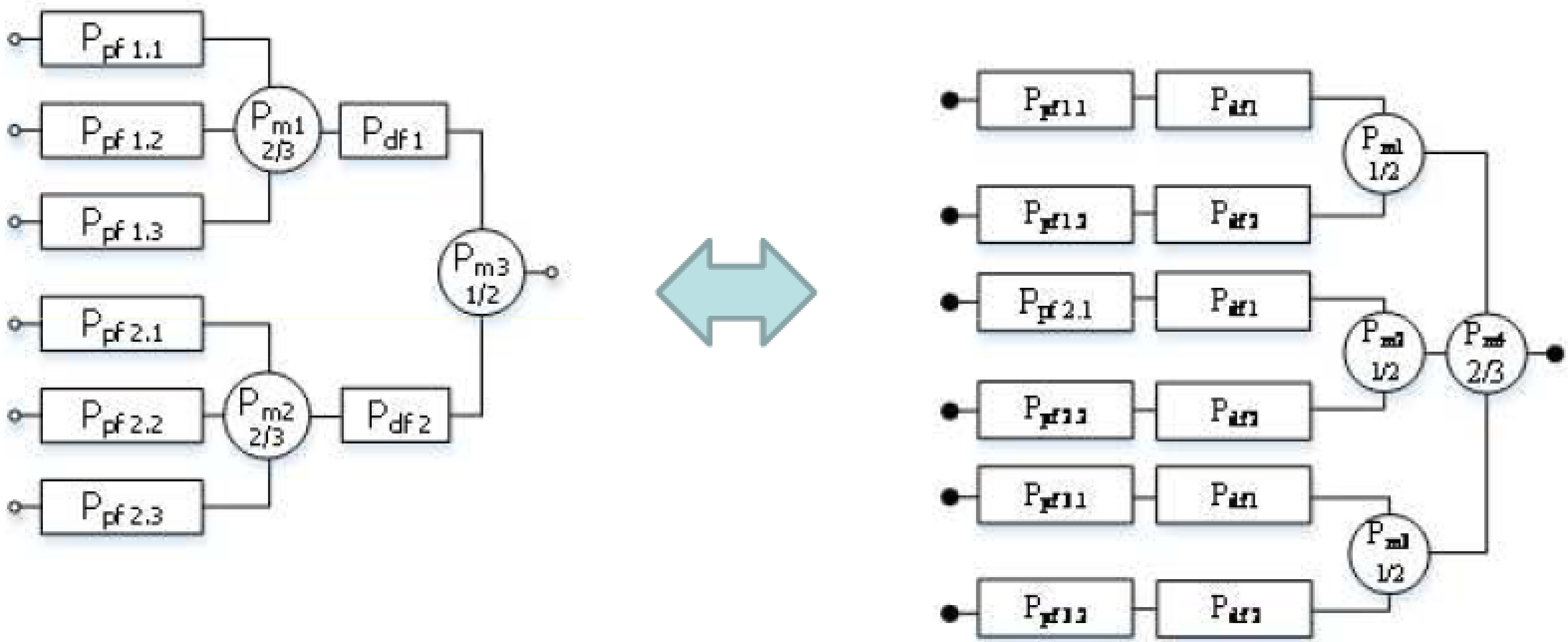



**What structure is more reliable?**

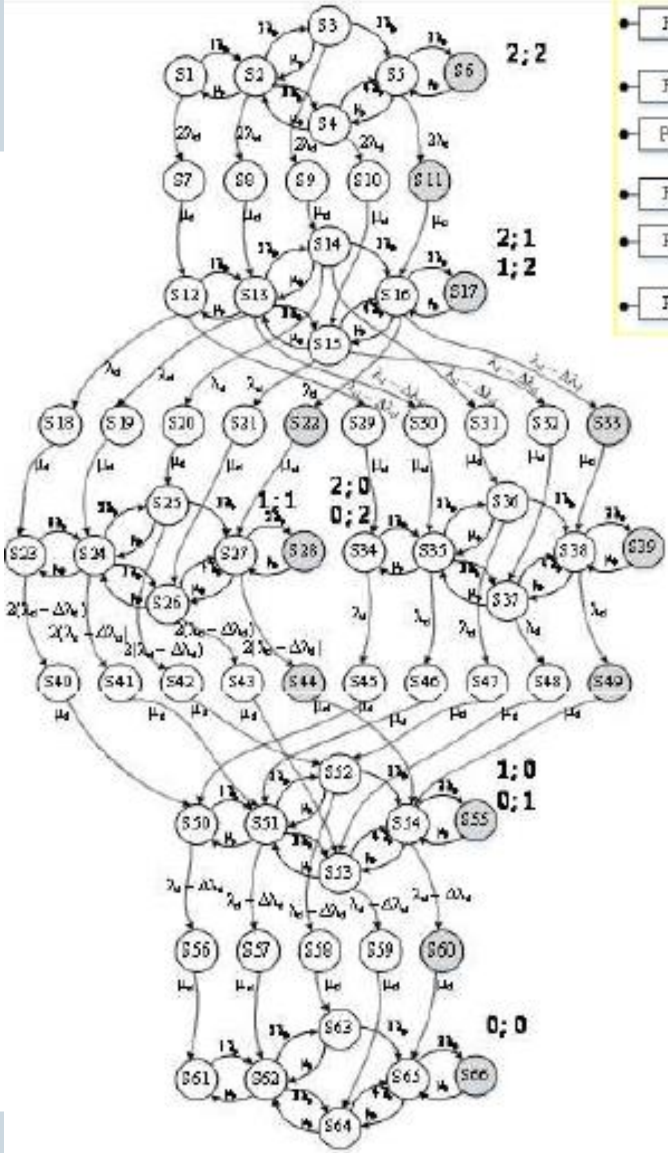
**What structure is more safe?**

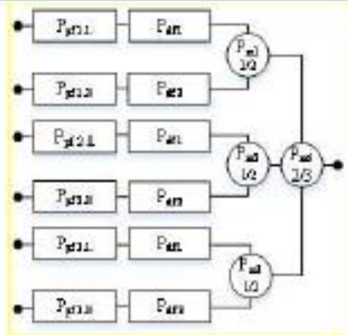
# MVS Safety Assessment: Reactor Trip System/ RBDs

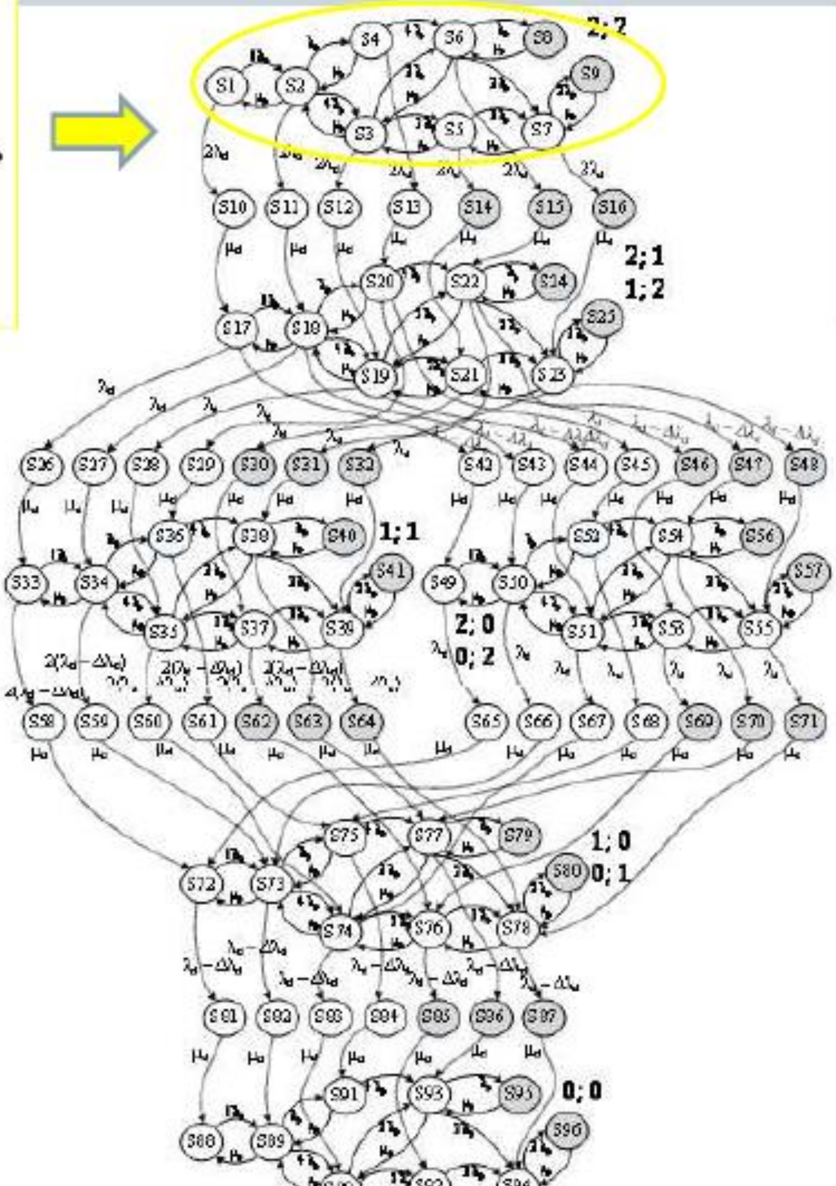



**What structure is more reliable?**
**What structure is more safe?**

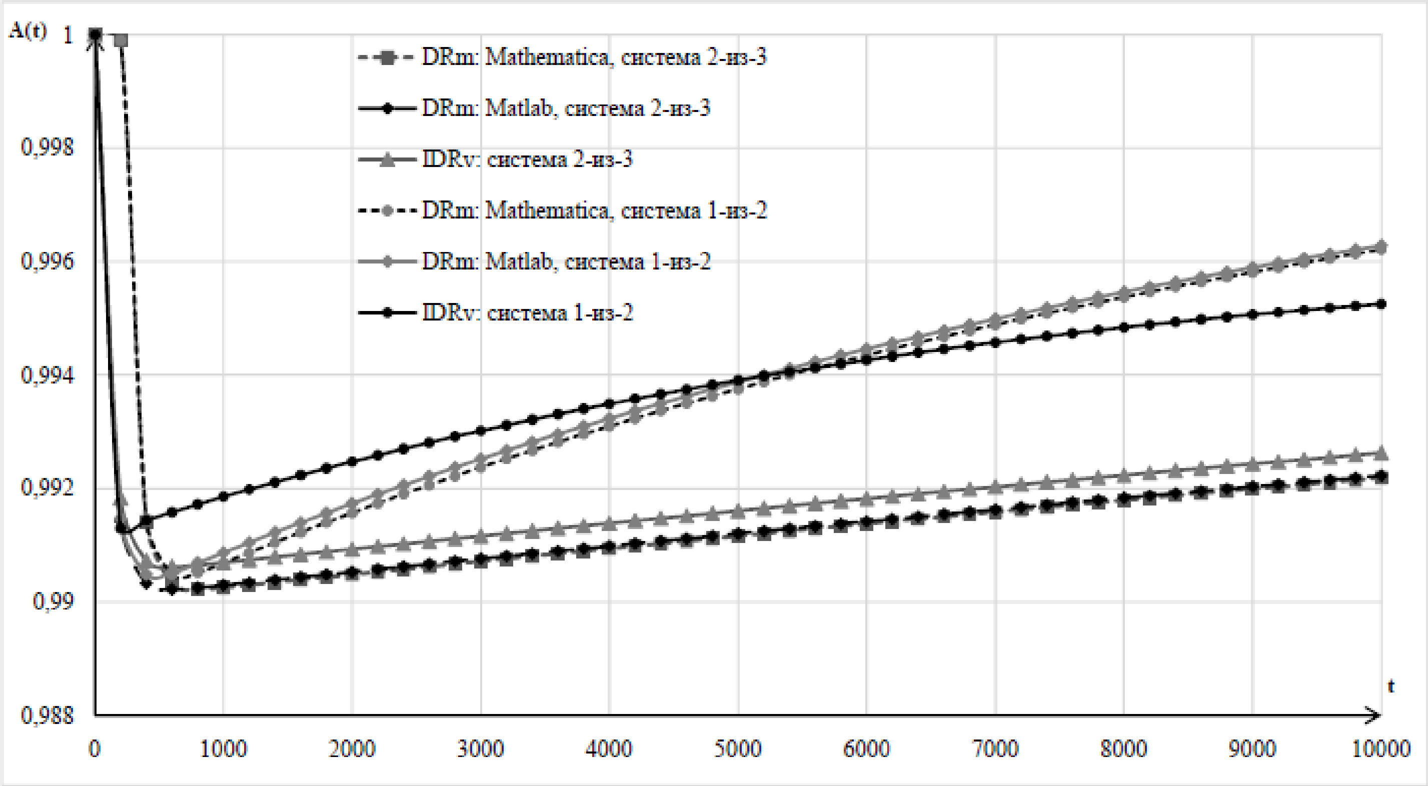
# MVS Safety Assessment: Reactor Trip System/ Markov's Graphs



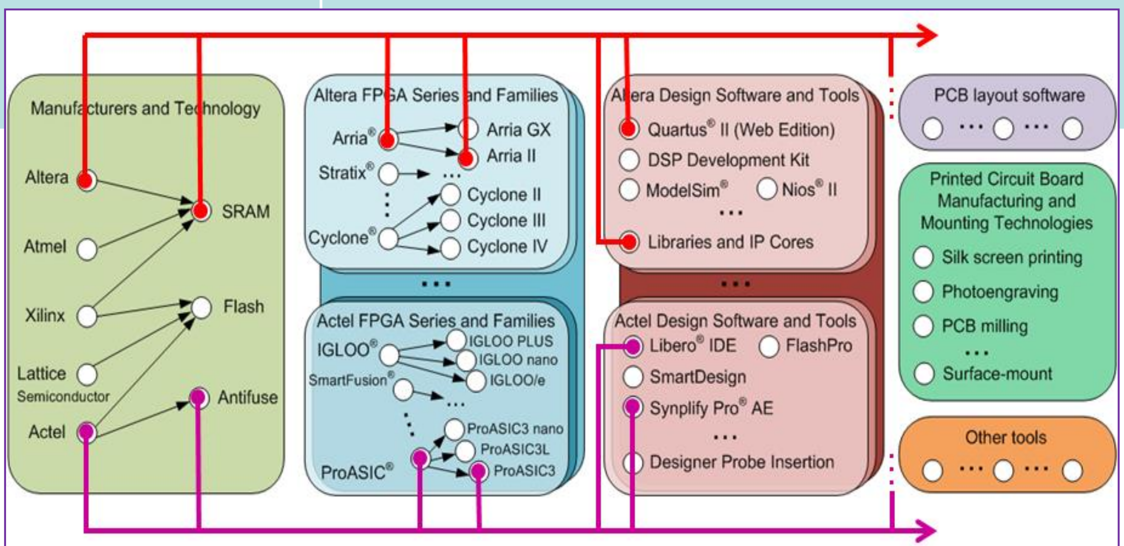


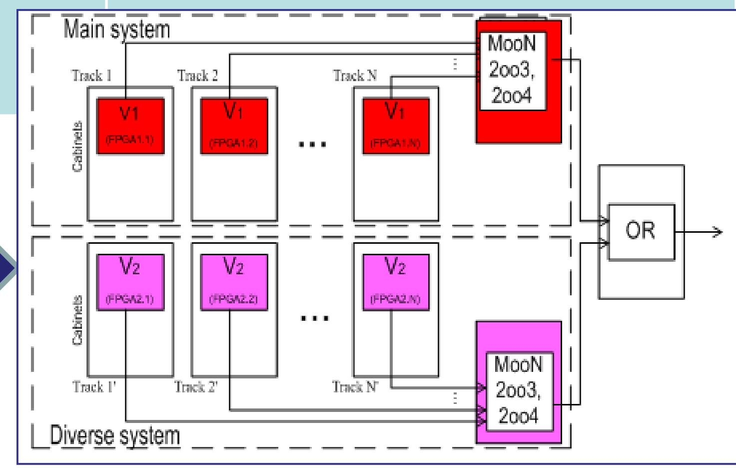
# MVS Safety Assessment: Reactor Trip System/ Simulation



# Challenges: MVS Safety Ensuring

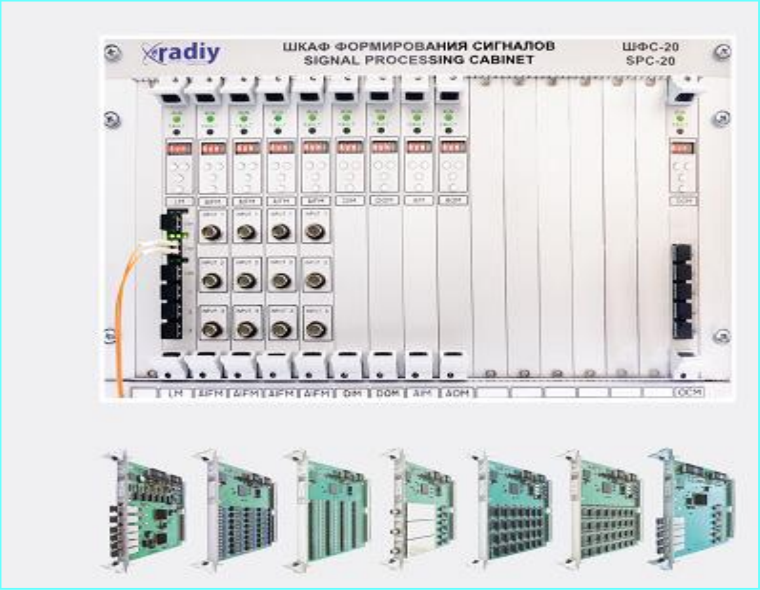
| Aspect | Challenge | Question |
|---|---|---|
| **4. CCF risk decreasing and MVS safety** | There is a problem of **decreasing number of common version faults (CVF)**. The CVF number (and probability of CCF) may be decreased using several types of diversity (**multi-diversity or "diversity of diversity"**). 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?*** |



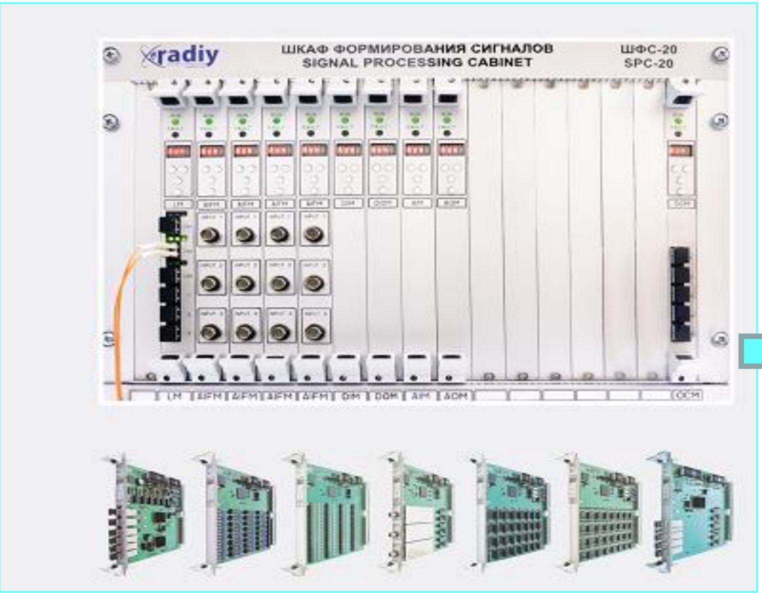
# Techniques of Diversity Assessment: MVPs for NPP I&Cs

## Radiy FPGA-based platform



# Techniques of Diversity Assessment: MVPs for NPP I&Cs

## Radiy FPGA-based platform

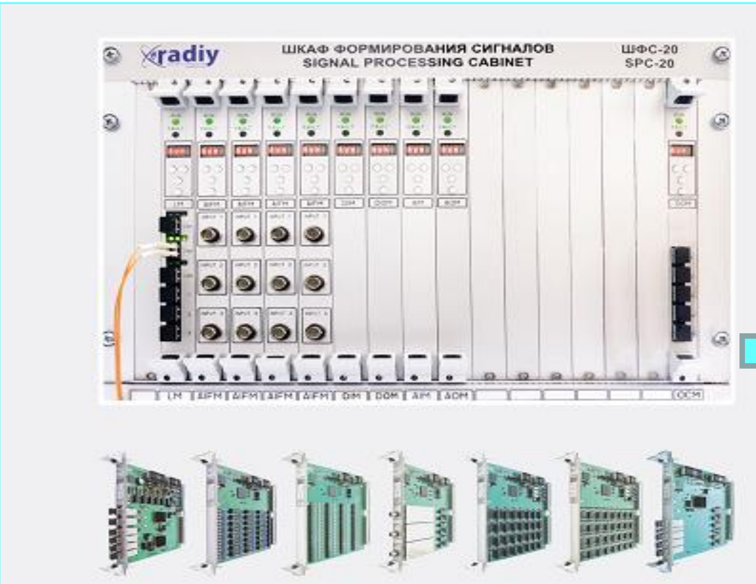



## Multi-version projects

| 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) |

# Techniques of Diversity Assessment: MVPs for NPP I&Cs

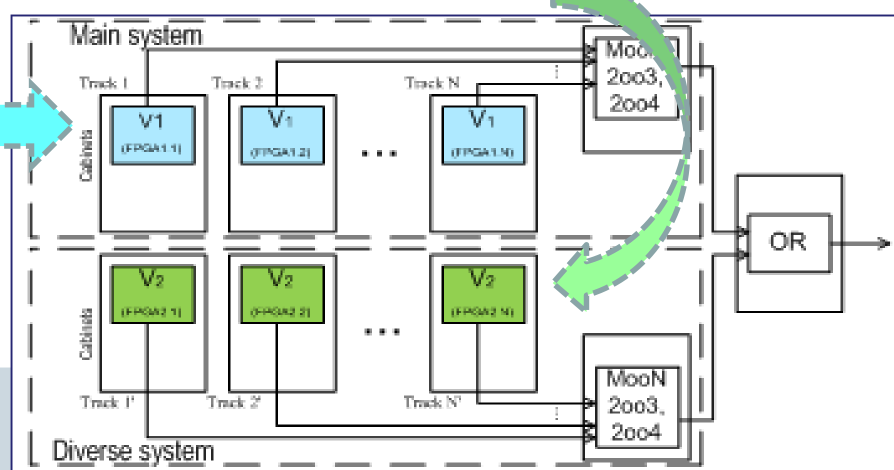
## Radiy FPGA-based platform




## 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) |

## 2-version Reactor trip system



# Techniques of Diversity Assessment: NUREG 7007

| 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 | | | |

# Techniques of Diversity Assessment: NUREG 7007

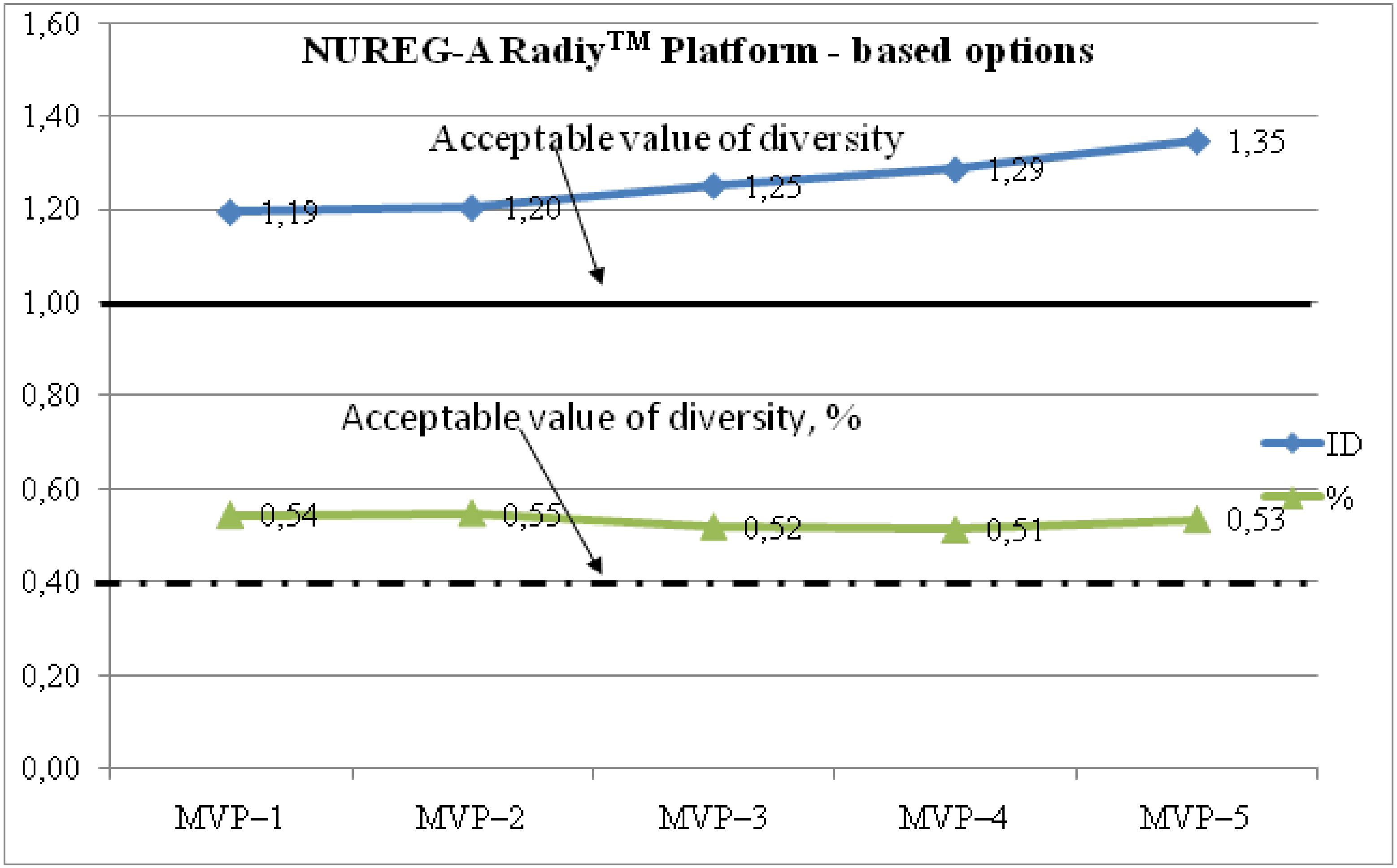
| | Attribute criteria | Rank | DCE WT | Category / Strategy name INT | INH | Score |
|---|---|---|---|---|---|---|
| DESIGN | Design | | | | | |
| | Different technologies | 1 | 0.500 | | | |
| | Different approaches within a technology | 2 | 0.333 | | | |
| | Different architectures | 3 | 0.167 | | | |
| | 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 | | | | | |

# Techniques of Diversity Assessment: NUREG 7007

| | 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

# Techniques of Diversity Assessment: NUREG 7007

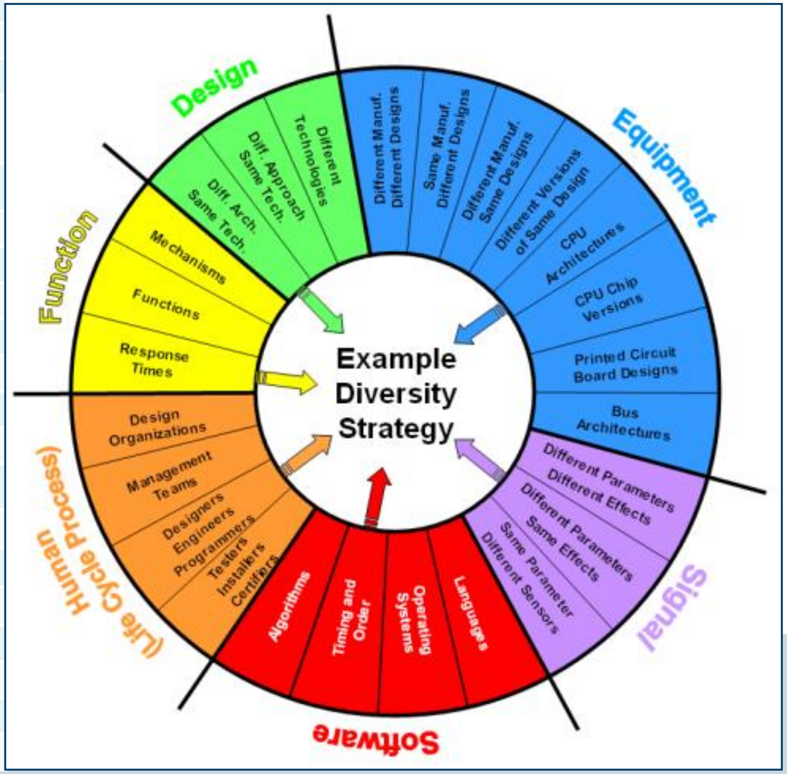


# Diversity for Security: Assurance and Assessment

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

| Diversity 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 different equipment designs | H |
| Same manufacturer of different equipment designs | HM |
| Different manufacturers of same equipment design (ED) | M |
| Same manufacturer of different versions of the same ED | 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 (UM) to implement safety function | H |
| Different function, control logic, or means of same UMs | 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 parameters sensed by different physical effect (PE) | H |
| Different reactor or process parameters sensed by the same PE | M |
| The same parameter sensed by a different redundant set of 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 |

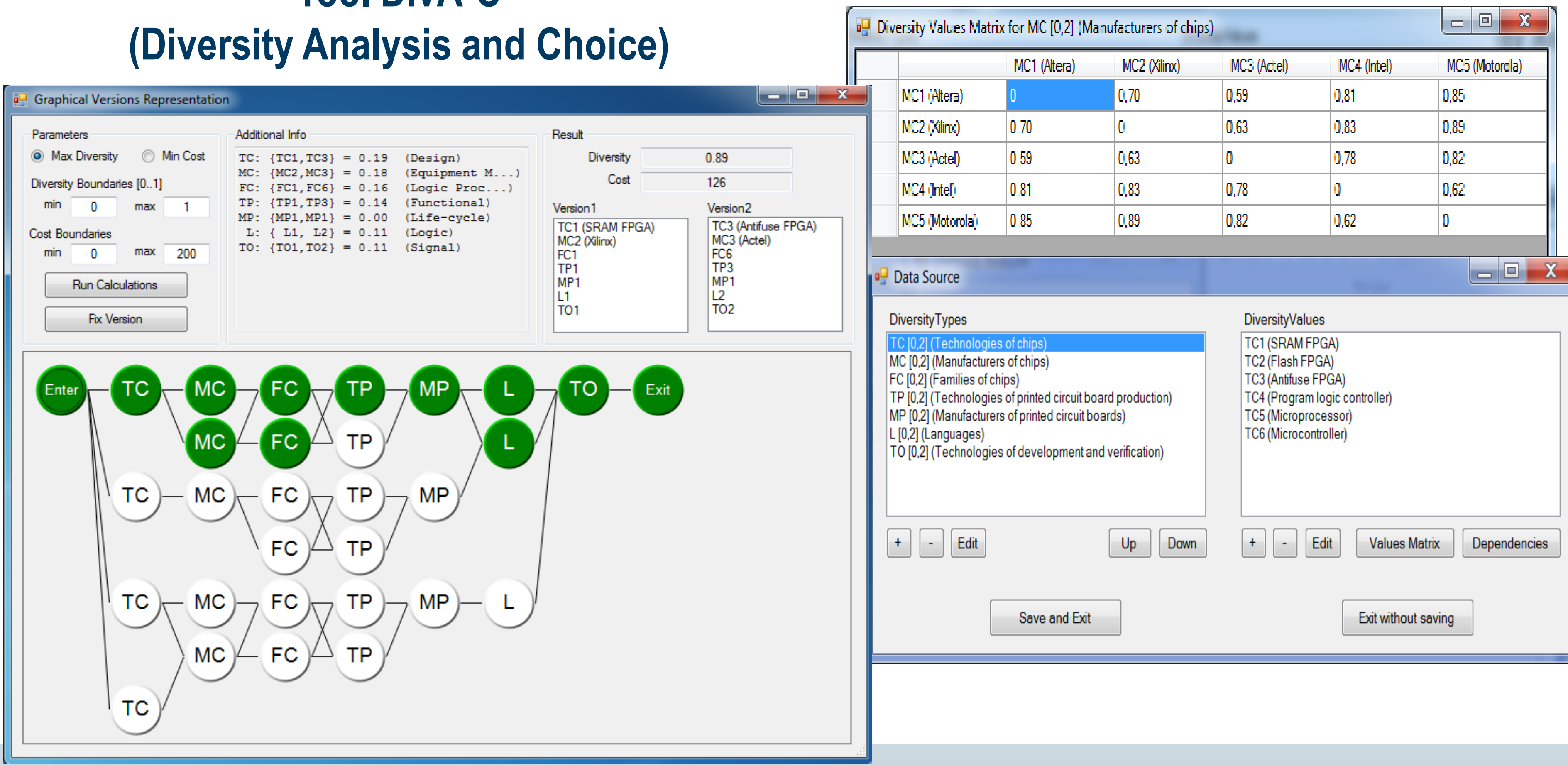
**H – high,**
**HM – high middle,**
**M – middle,**
**L – low**



# Choice of Diversity Types: Tool Support

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

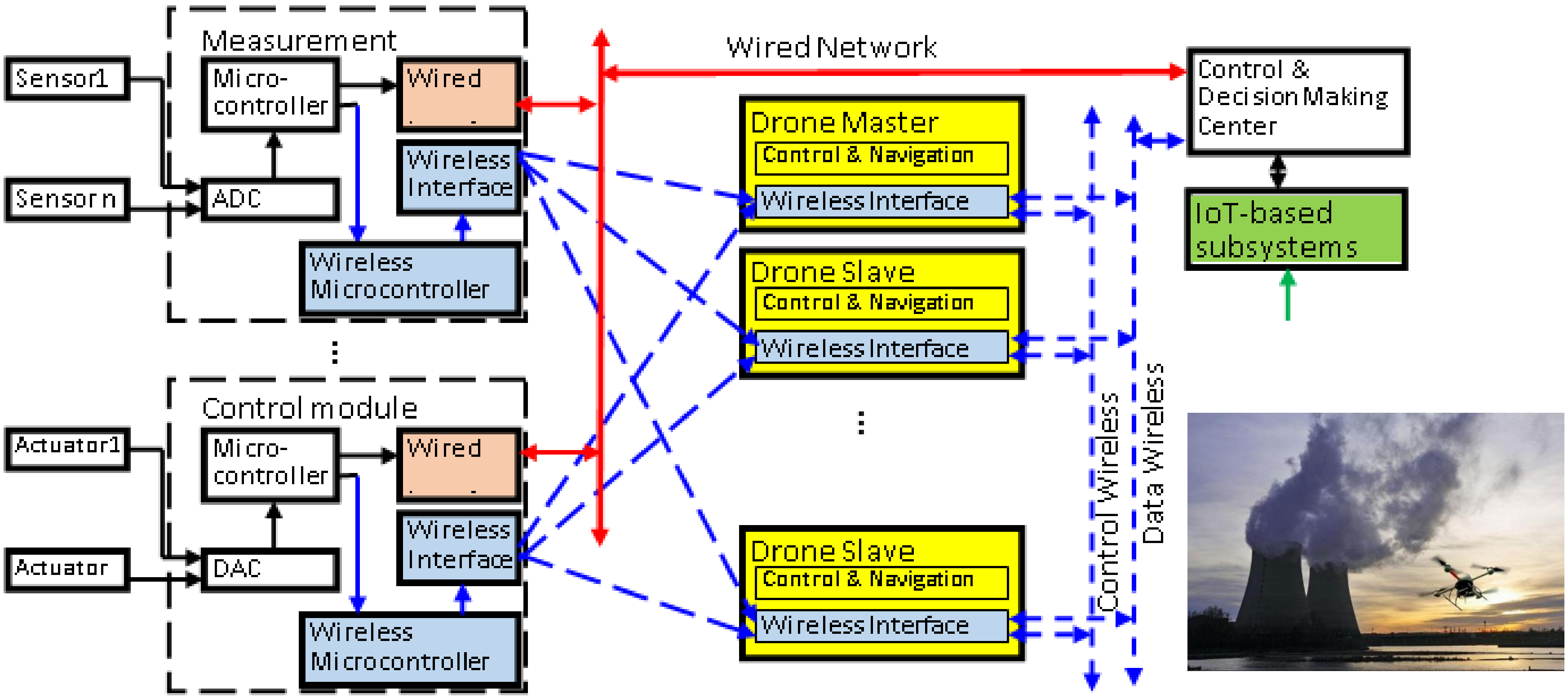
## Tool DivA-C
## (Diversity Analysis and Choice)



# Multi-Version Systems: Post Severe Accident Monitoring System

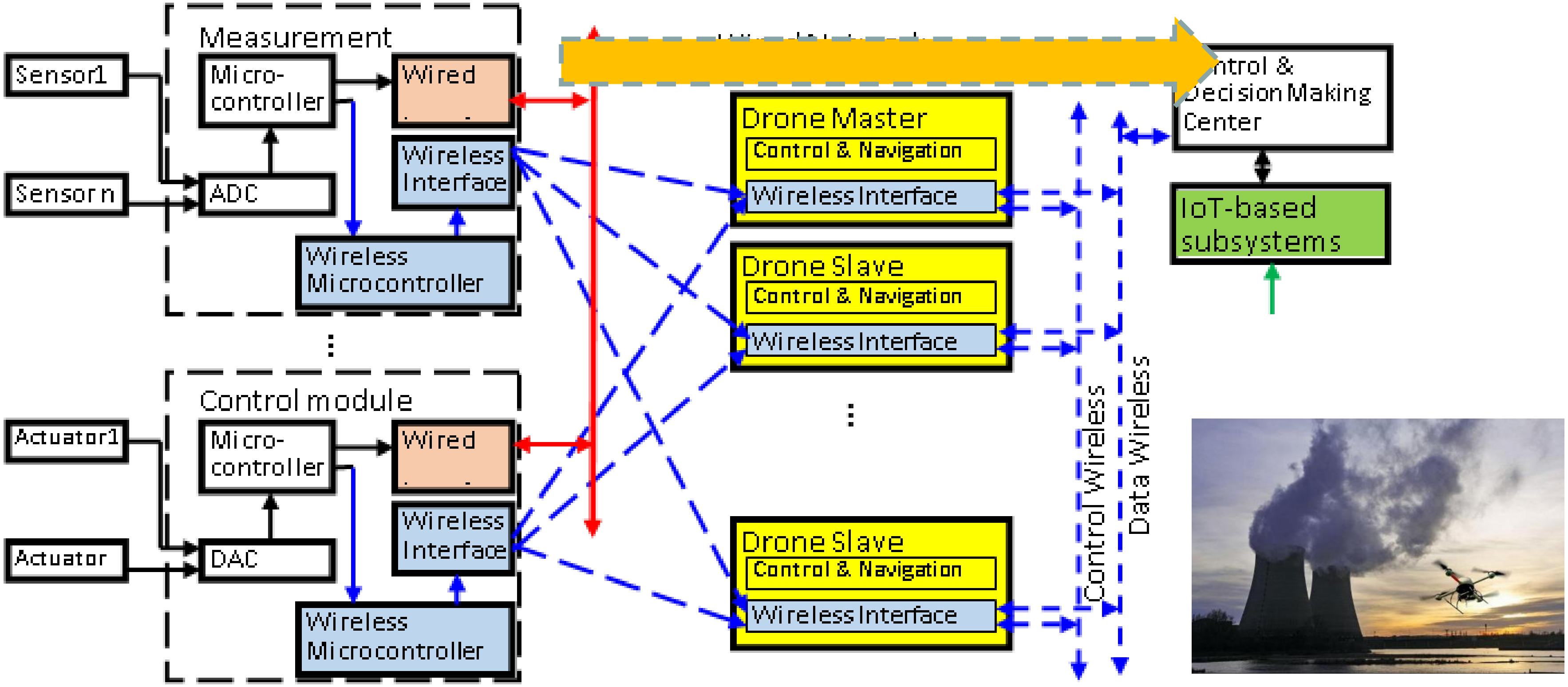
(V. Kharchenko, A. Sachenko, V. Kochan, V. Kharchenko et al. Mobile Post Emergency Monitoring System for NPPs. Proceedings of the 12th ICT in Education, Research and Industrial Applications: Integration, Harmonization and Knowledge Transfer, ICTERI-TheRMIT2016, Kyiv, Ukraine, 2016)

## Architecture of PSAMS



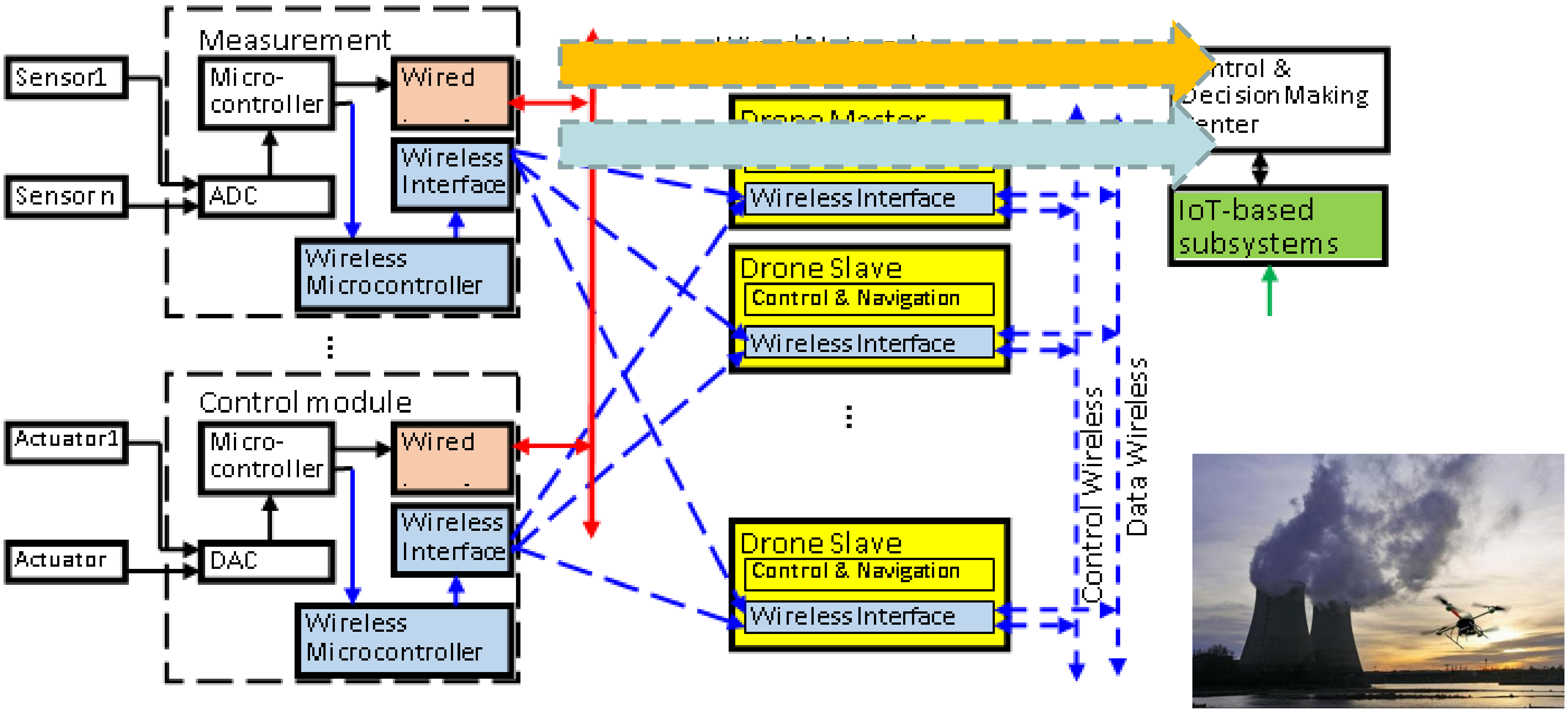
# Multi-Version Systems: Post Severe Accident Monitoring System

## Architecture of PSAMS: Wire-based instrumentation, control and communication



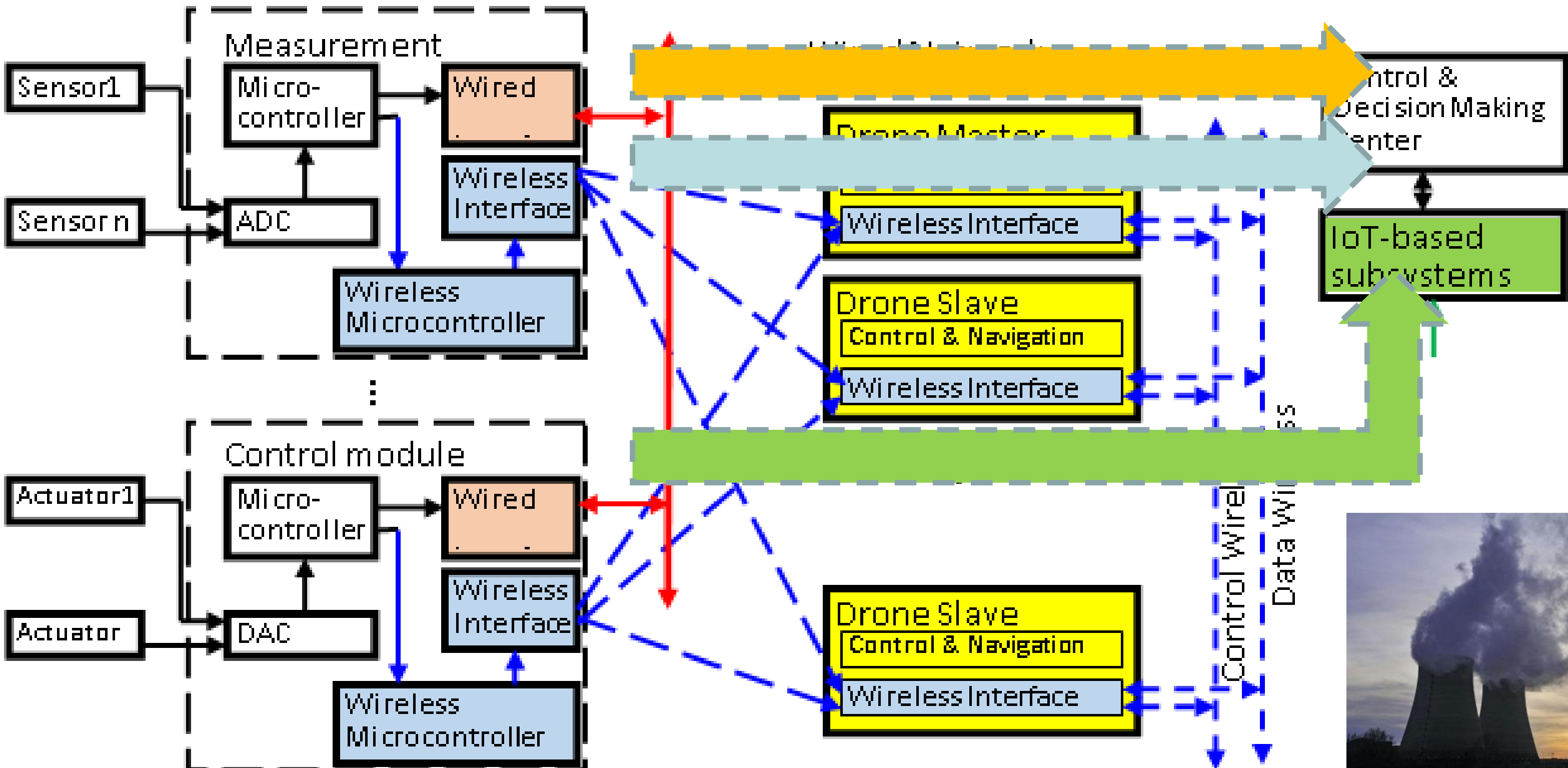
# Multi-Version Systems: Post Severe Accident Monitoring System

## Architecture of PSAMS: + Wireless/LiFi-based instrumentation, control and communication



# Multi-Version Systems: Post Severe Accident Monitoring System

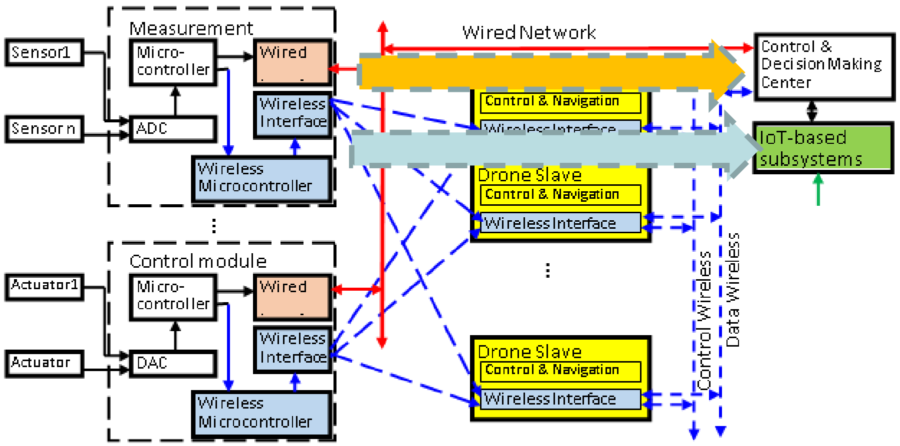
## Architecture of PSAMS: IoT-based instrumentation and communication

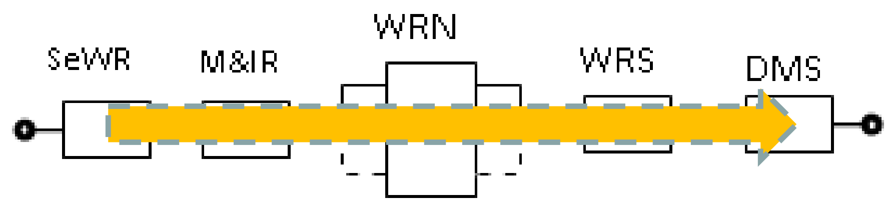



# Multi-Version Systems: Post Accident Monitoring System

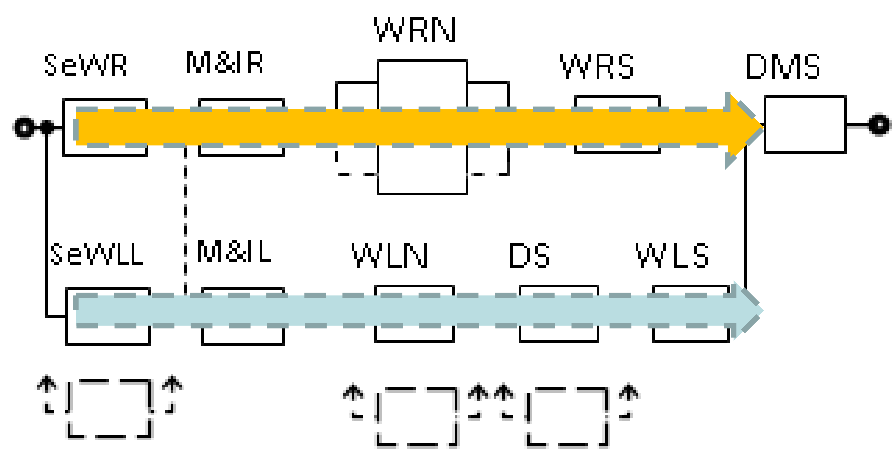
(V. Kharchenko, A. Sachenko, V. Kochan, H. Fesenko. Reliability and Survivability Models of Integrated Drone-Based Systems for Post Emergency Monitoring of NPPs. Proceedings of the IEEE Conference on Information and Digital Technologies, Rzeszow, Poland, 2016)

## RBD (Reliability Block Diagram) Based Reliability Assessment




a

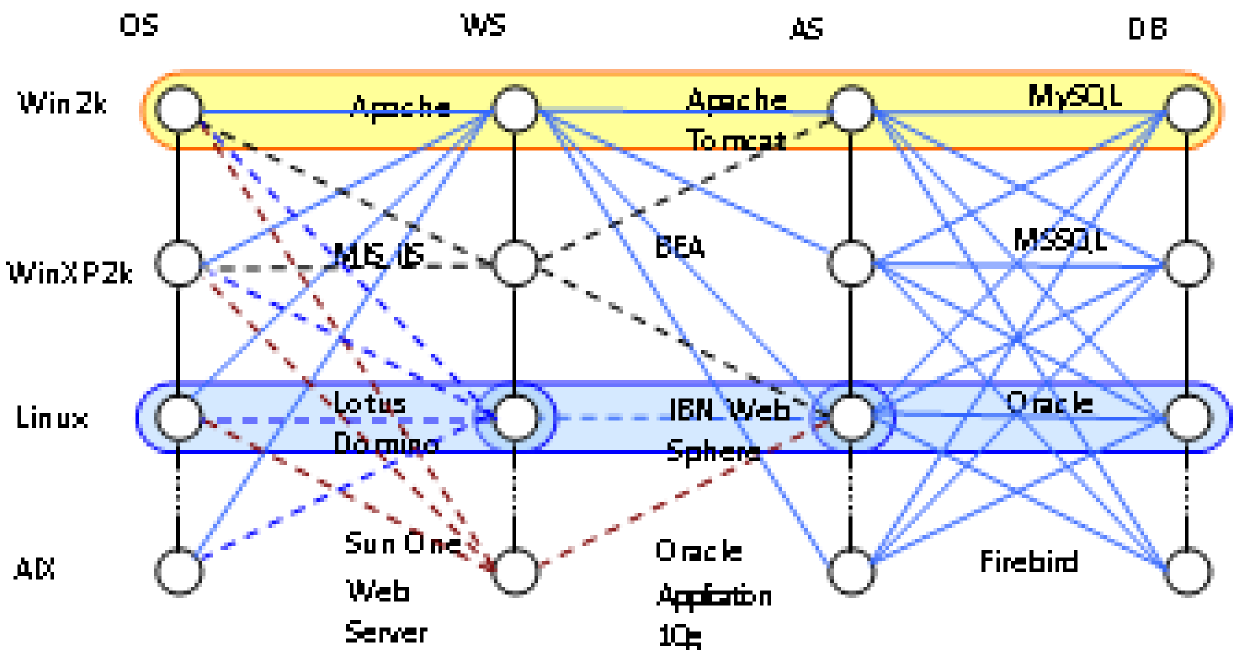



b

# Multi-Version Systems: Service-Oriented Architecture

(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)

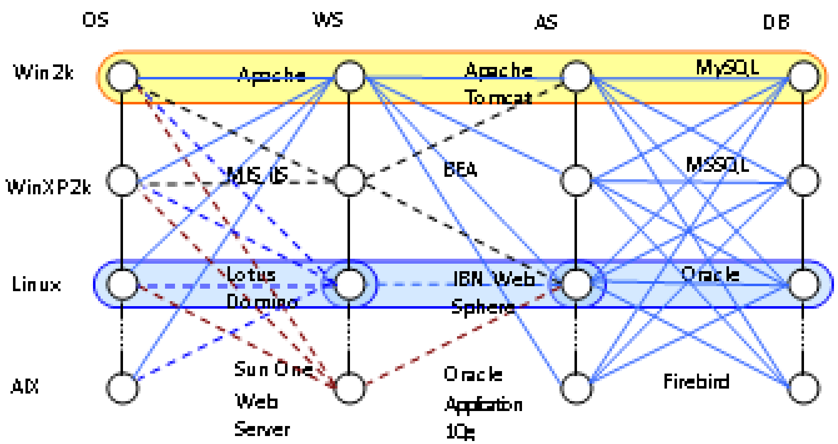
## Graph for version generation

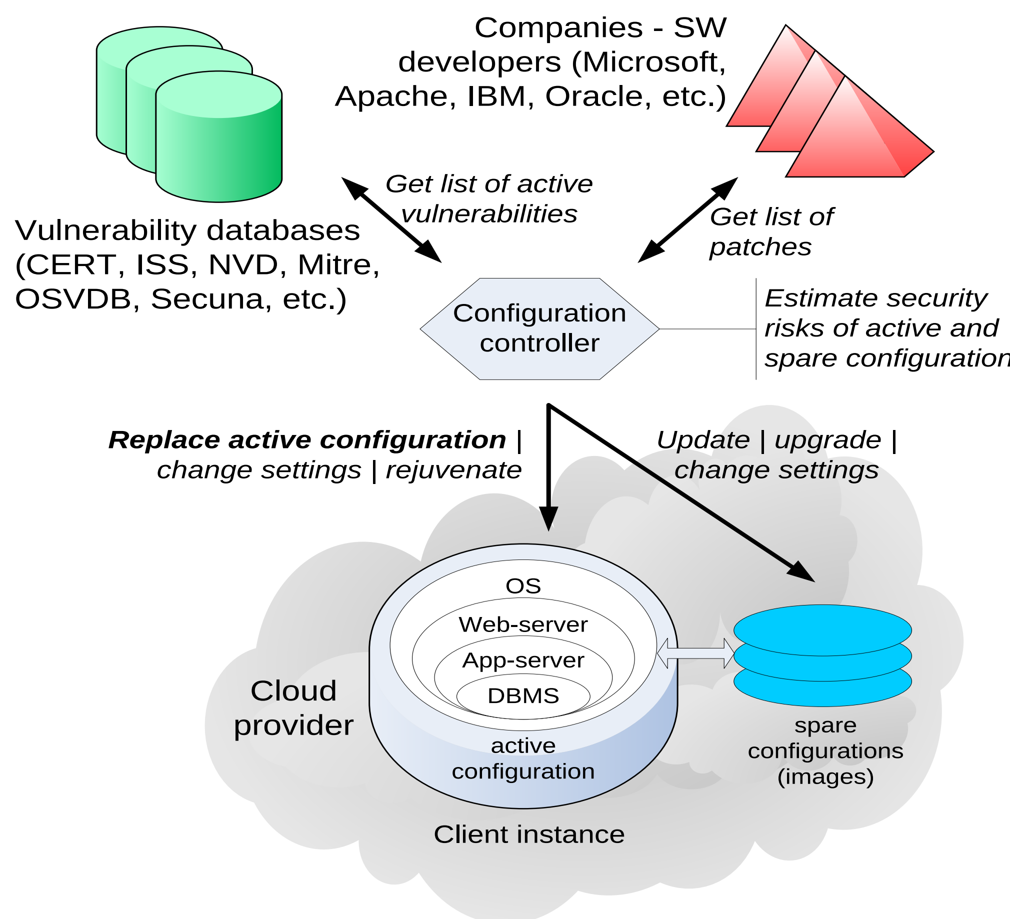



SOA = {OS, WS, AS, DB}
OS – operation system,
WS – web-server,
AS – application server,
DB – data base

# Multi-Version Systems: Service-Oriented Architecture

(A. Gorbenko, V. Kharchenko, O.Tarasyuk, A. Romanovsky. Intrusion-Avoiding Architecture Making Use of Diversity in the Cloud-Based Deployment  Environment, LNCS, Springer, 2011)

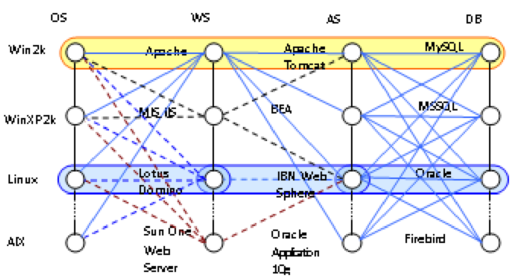


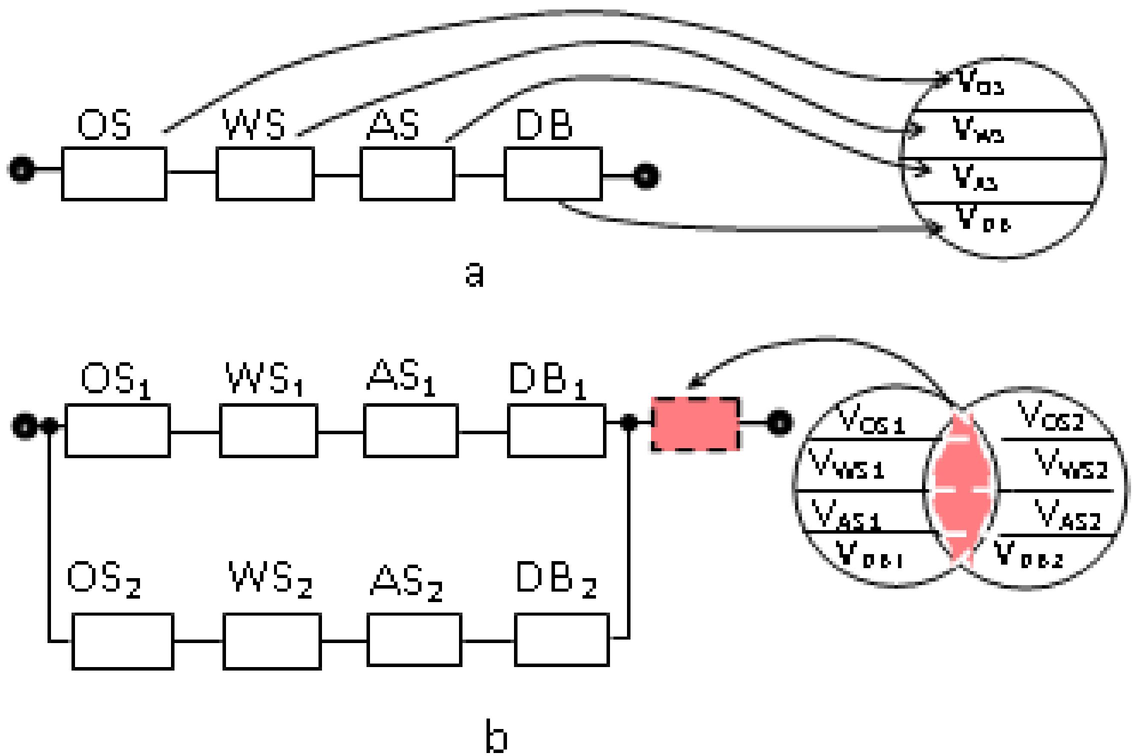



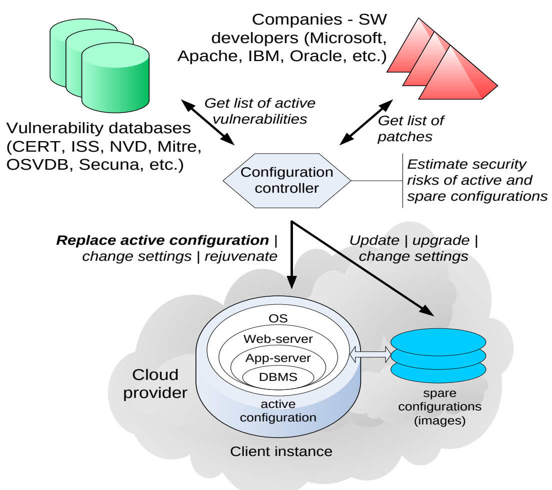

## Dynamically reconfigurable cloud-based intrusion tolerant SOA

# Multi-Version Systems: Service-Oriented Architecture

## SBD (Security Block Diagram) Based Security Assessment



# Outline

About our team and projects
Introduction. Green vs Safe IT
Green Computing. Key principles
Safe Computing. Principles and Industry Solutions
Conclusions

# Conclusions

**Green IT engineering as a part of sustainable and green engineering…**

Global challenges (mobile / IoT devices power consumption decreasing → cloud computing / data centers power consumption increasing)?

**Green IT system/SW life cycle and green gap analysis…**

Green life cycle model including utilization costs (for embedded systems, networks, clouds, IoT)

**Green IT engineering as solution for safety and energy critical applications…**

Dependable system (out of undependable components) can be "greener' due to special techniques (energy modulated computing, diverse clocking,…)

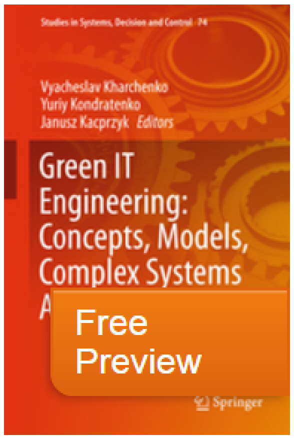
**Common cause/ fatal failure (cased by design faults, attacks on joint vulnerabilities) is key challenge for safety critical systems.**

Diversity decreases CCF risk but there is a problem of common version faults, costs, assessment of actual safety level of diversity considering rare stream of failures.

**Diversity of nature, culture, nations is very important for civilization sustainability**

# Springer Books on Green IT Engineering (vol.1,2)

Studies in Systems, Decision and Control






## Green IT Engineering: Concepts, Models, Complex Systems Architectures

Editors: **Kharchenko**, Vyacheslav, **Kondratenko**, Yuriy, **Kacprzyk**, Janusz (Eds.)

Studies in Systems, Decision and Control




## Green IT Engineering: Components, Networks and Systems Implementation

Editors: **Kharchenko**, Vyacheslav, **Kondratenko**, Yuriy, **Kacprzyk**, Janusz (Eds.)

Springer



xradiy

# Springer Books on Green IT Engineering (vol. 3)

**Green IT Engineering: Social, Business and Industrial Applications**",
**Volume 3**

in the book series "***Studies in Systems, Decision and Control***" (SSDC)

which will be published by Springer http://www.springer.com/series/13304) /

Editors Prof. Dr. Vyacheslav Kharchenko, Prof. Dr. Yuriy Kondratenko, Prof. Dr. Janusz Kacprzyk.

Springer

# Springer Books on Green IT Engineering (vol. 3)

**Key topics of the book, Volume 3:**
Green IT engineering in Social Applications (social networks, media, smart home, health systems,…);
Green IT engineering in Business Applications (information systems, banking IT, e-commerce,…);
Green IT engineering in Industrial Applications (aerospace, energy, transport,…).

Authors can consider different aspects of implementation to the social, business and industrial applications such subjects as:
- Development and implementation of Green logic, programmable components and systems;
- Measurement, integration and verification of energy-saving systems and networks;
- Greening of data centres and cloud-based IT-infrastructures;
- Development and implementation of green software;
- Ecological human-machine interface and systems;
- Implementation of complex energy-saving and safe systems;
- Development of adaptive green WiFi and mobile systems and networks;
- Assessment and implementation of energy saving IoT (Internet of Things) based systems;
- Lightweight cryptography and green aspects of embedded systems;
- Big data for green and greening of big data based systems;
- Green issues of Industry 4.0;
- Economical issues and university-industry cooperation in green IT engineering, etc.

**Important dates for Volume 3**
Acceptance of invitation and submission of abstracts – July 30, 2017
Notification about acceptance by editors – August 28, 2017
Submission of chapter (18-20 pages) – October 22, 2017
Notification about acceptance of chapter – December 4, 2017
Submission of camera ready – December 22, 2017

Springer

# Thank you very much!



National Aerospace University "KhAI", CSN Department, 17, Chkalov street, Kharkiv 61070,
RPC Radiy
Ukraine

e-mail:
v.kharchenko@csn.khai.edu