Application of Reliability Theory to Functional Safety of Computer Control Systems

Vladimir Sklyar

●

National Aerospace University "KhAI", Ukraine
Indian Institute of Technology Bombey, India
v.sklyar@csn.khai.edu

Abstract

Taxonomy for Dependability and Security has been updated to reflect all used attributes as well to refine orthogonal relations between attributes. Functional Safety is a part of Reliability that has dealt with Safety Functions and related dangerous failures. From this point of view, all the Reliability Theory methods, models and indicators may be applied for the Functional Safety domain without any essential change. The three main types of architecture of modern safety critical computer control systems are considered (Embedded Systems, Industrial Control Systems, and Internet of Things). Application of Reliability and Safety indicators to Industrial Control Systems of Nuclear Power Plants is given. Internet of Things has just started to be applied to safety critical systems during the last years. Research and Development program is proposed to study IoT Reliability and Functional Safety.

Keywords: functional safety, dependability, security, reliability theory, industrial control systems, embedded system, internet of things, research and development

I. Introduction

A goal of this paper is to analyze Reliability Theory applications for safety critical computer control systems (CCS).

Reliability Theory has been developed as an applied science in 50-s to decide a general problem to create reliable systems from unreliable components. To 80-s the main theoretical results have been obtained so since 80-s we have proven in use engineering practices to assure and assess reliability of control systems.

Since 80-s computer systems became too complex and too responsible to be described only with reliability, so new attributes like dependability, security, safety, and others have been implemented by researchers [1]. A joint committee on "Dependable Computing and Fault Tolerance" was formed by the Institute of Electrical and Electronics Engineers (IEEE) Computer Society (CS) and the International Federation of Information Processing (IFIP) Working Group (WG) 10.4 (http://www.dependability.org). A general terminology has been developed and presented in 2004 in the paper [2]. For safety critical control systems this concept should be refined to emphasis a background for requirements and compliance evaluation implementation.

Today we have a set of theoretical results implemented in industrial standards which define state-of-the-art for safety-critical applications in different domains, as following:

- Umbrella functional safety standard: IEC 61508, Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-related Systems
- Process industries: IEC 61511, Functional safety – Safety instrumented systems for the

process industry sector;

- Machinery IEC 62061, Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems;
- Nuclear: IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety;
- Automotive: ISO 26262, Road vehicles – Functional safety;
- Railway: EN 50129, Railway Industry Specific – System Safety in Electronic Systems;
- Medicine: IEC 62304, Medical Device Software;
- Avionic: DO-178C, Software Considerations in Airborne Systems and Equipment Certification;
- Space: NASA-STD 8719.13, Software Safety Standard.

Safety and security are important features for new developed industrial domain of Internet of Things (IoT). IoT is defined as an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react. IEEE started a project to develop standard for an Architectural Framework for the IoT (IEEE P2413) in 2014. At the same year the Joint Technical Committee on Information Technologies of International Electrotechnical Commission and International Standardization Organization (ISO/IEC JTC1) created the Working Group on Internet of Things (WG 10) to develop a new standard ISO/IEC 30141 "IoT Reference Architecture".

It is worth to mention, IEEE P2413 (Standard Project) "Standard for an Architectural Framework for the IoT" already discusses issues related to safety and security for critical domains. Since IoT Architecture is defined clearly, safety and security risks for critical applications will be analyzed on the standard base. At the same time typical reference architectures for safety-critical Embedded Systems (ES) and Industrial Control Systems (ICS) on the base of Programmable Logic Controllers (PLC) are well known and defined in the standards. These three types of architectures (ES, PLC-based ICS and IoT) are mainly used at the present time to implement safety-critical control systems.

This paper contains the following parts:

- Firstly, terminology attributes and taxonomy in Dependability and Security are discussed;
- Secondly, reference architectures for ES, ICS and IoT are presented;
- Thirdly, Reliability, Availability and Safety indicators are discussed in this paper to support engineering solutions in safety critical domains;
- After that, the main Research and Development (R&D) tasks are formulated for Functional Safety of IoT as for relatively new domain which request intensive investigation in safety and security critical applications.

II. Terminology and Taxonomy Discussion in Dependability and Security

Let's consider existing approaches to the state taxonomy of dependability.

Four of the attributes RAMS (Reliability, Availability, Maintainability, Safety) used to be considered as extensions for "classical" Reliability. The paper "Basic Concepts and Taxonomy of Dependable and Secure Computing" [2] launched in 2004 the new IEEE Transactions on Dependable and Secure Computing. It explains the complexity of dependability in relation with security of modern computer-based systems (see Figure 1).

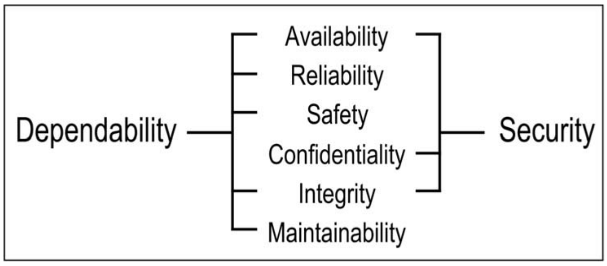

Figure 1: *Dependability and security attributes*
(as per "Basic Concepts and Taxonomy of Dependable and Secure Computing" [2])

In the [2], dependability is considered as an integrating concept including the following attributes:

- Availability is a readiness for correct service;
- Reliability is a continuity of correct service;
- Safety is an absence of catastrophic consequences for the user and the environment;
- Integrity is an absence of improper system alterations;
- Maintainability is an ability to undergo modifications and repairs.

Security is a composite of the attributes availability, integrity, and confidentiality. When addressing security, availability is considered for authorized actions as well as integrity is considered for a proper authorization. Confidentiality is a supplementary, in comparison with dependability, security attribute, which means the absence of unauthorized disclosure of information.

It is worth also to mention the paper "Reliability: Past, Present, Future" by Igor Ushakov [3], which lays the cornerstone of the e-journal "Reliability: Theory & Applications". The author discussed directions of Reliability Theory, which are still to be state-of the-art after a decade. Such directions, in fact, represent attributes, which can complement dependability, including the following:

- Effectiveness ("performability") relates to systems for which one is not able to formulate "all or nothing" type of failure criterion; effectiveness characterizes a system's ability to perform its main functions even with partial capacity;
- Survivability is a special property of a system to "withstand impacts"; in this case one assumes that the impacts are directed to the most critical components of the system;
- Safety is a special property of a system characterizing effective performance of its main predetermine functions without dangerous environmental consequences for people and nature;
- Security is sometimes considered as a part of reliability-survivability problem; indeed, many systems must not only operate reliably but also at the same time provide protection against non-sanctioned access.

After that publication, effectiveness and survivability were included in dependability and security attributes [4]. Author cannot guess was it done independently or dependently from the [3].

We need to mention two more essential attributes used for state-of-the-art CCSs.

Firstly, it is Quality of Services (QoS) which describes the overall performance of networks and is widely applicable for web-based application. In fact, it is some extension of the above mentioned Performability.

Secondly, we have Resilience which is an attribute close to Survivability [5]. In the know proceedings Resilience has never been integrated with Dependability and Security attributes.

Resilience is the ability of a system to cope with changes which usually lay in challenges to normal operation such as faults, cyber threats and others.

In the former Soviet Union, Dependability taxonomy was based on the government standards (as named "GOST") which are still remaining in force in many countries. The umbrella standard in

Dependability taxonomy is GOST 27.002-89 “Industrial product dependability. General concepts. Terms and definitions”.

The following definitions and taxonomy are stated in GOST 27.002-89. Dependability is the property to keep within the established values of the parameters under all the stated conditions within a stated period of time.

It includes the following four attributes:

- Reliability is continuity of the operation state during some time;
- Durability is continuity of operation with periodic maintenance and repairs until retirement time; it is highly related with long term operation.
- Maintainability is an ability to support operation state and to turn back to operation state after periodic maintenance and repairs.
- Storability is an ability to support all dependability attributes during storage.

A problem appears when somebody tries to harmonize dependability issues as (RAMS – Integrity) with (Reliability – Durability – Maintainability – Storability).

To make it consistent, let’s analyze dependency between all proposed Dependability and Security attributes. Taxonomy is refined to make it orthogonal (see Figure 2).

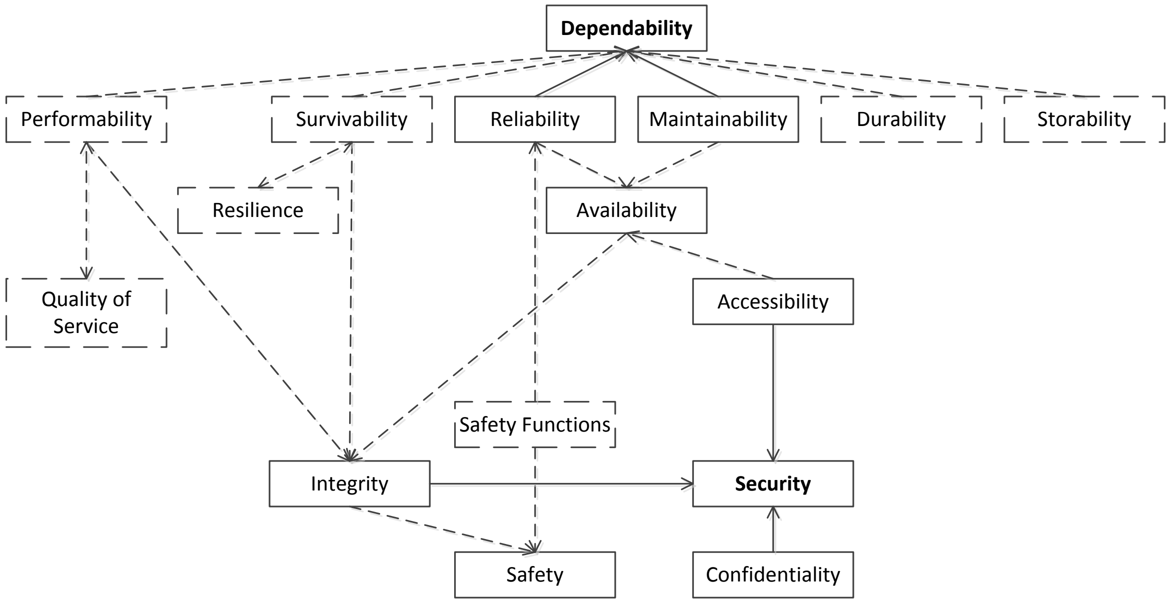

Figure 2: *Updated Dependability and Security Taxonomy*

Squares with a dotted border are used at Figure 2 to highlight new attributes versus traditionally used Dependability and Security attributes (see Figure 1) with regular borders. The same, dotted lines are used in Figure 2 to highlight new dependencies between attributes versus dependencies on Figure 1, which are highlighted with regular lines. Arrows on the lines show that attributes of the low level is included in attribute of high level. If such hierarchy is not established, then arrow has both side arrows (as, for example, between Performability and Quality of Service, between Survivability and Resilience).

Update of Dependability and Security taxonomy is supported with the following statements, which underline differences between Figure 2 and Figure 1.

1. Additional Dependability attributes are added to make taxonomy consistent with [2-4] and GOST 27.002-89. It is Performability, Survivability, Durability, and Storability. Added attributes are highlighted in Figure 2 with dotted borders.

2. Quality of Service is added as additional attribute related to Performance. Application domains of these attributes are a bit different, so established relations between them does not

indicate which attributes have the highest level. The same things are with a pair of Survivability and Resilience.

3. Availability is a combination of Reliability and Maintainability what is from equation A = MTTF / (MTTF + MTTR), where MTTF – Mean Time to Failure, MTTR – Mean Time to Restoration.

4 Accessibility is more appropriate term for safety domain the Availability. However Accessibility is a part of Availability, so such relation is established.

5. Safety takes a care mostly about the failures of Safety Functions (dangerous failure), which are intended to achieve or maintain a safe state of a system. So there is a relation between Reliability and Safety, and this relation is established via Safety Functions.

6. At the same, Safety includes both Safety Functions and Integrity, what is stated in the standards IEC 61508 as the confidence level (sometimes, probability) of a system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time.

7. Integrity consideration as a Safety attributes entails that Integrity shall be complimented with Performability, Survivability and Availability.

A proposed Dependability and Security taxonomy can be used for safety and security critical domains to highlight attributes which are essential for implementing one or the other CCS application [6,7].

III. Architecture of Computer Control Systems

Control Systems fundamentals lay in interaction with some processes of the real World via three the main parts which are sensors, controllers and actuators (see Figure 3). For modern CCSs not mandatory, but typically is a presence of Human-Machine Interface (HMI) with monitoring data transmission, processing and storage.

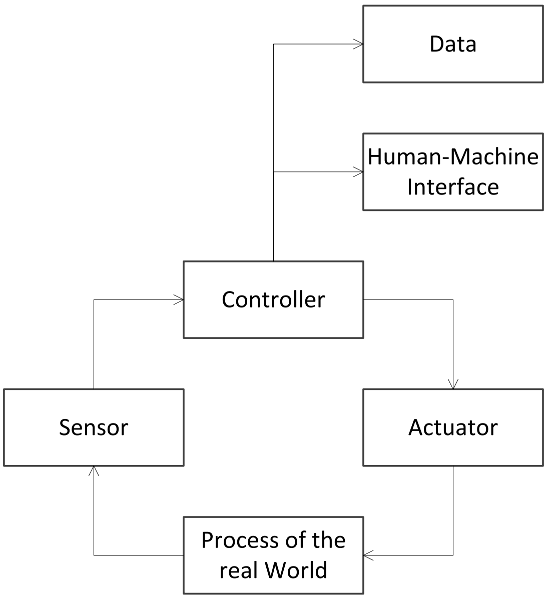

Figure 3: *Typical Architecture of Computer Control Systems*

For ES such architecture can be implanted on one chip or on one board.

ES applications are used in the presence in such domains as consumer electronics, control systems and industrial automation, bio-medical systems, field instrumentation, handheld computers, data communication, network information appliances, telecommunications, wireless communications, robotics and helicopters (drones), computer vision etc.

Typical programmable components of ES are Microcontroller Units (MCU), Digital Signal Processors (DSP), Field Programmable Gates Arrays (FPGA), Complex Programmable Logic Devices (CPLD), and Application Specific Integrated Circuits (ASIC).

ICS structure [8] includes a wide range of sensors and transmitters, PLCs, actuators, HMI workstations and data storages, combined with the networks (see Figure 4). Design parts for ICS include mechanical, electrical, firmware, hardware, and software.

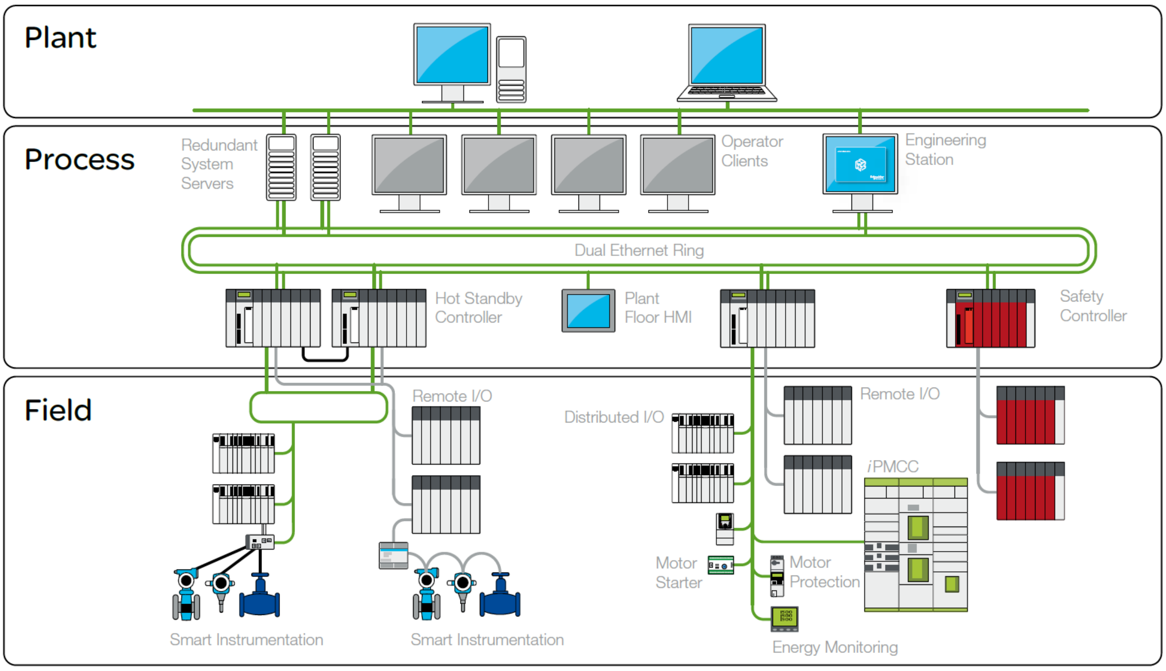

Figure 4: *Typical Architecture of Computer Control Systems (Source: Schneider Electric – Modicon Quantum PLC)*

Reference architecture of IoT [9,10] is presented as a set of layers with interfaces (see Figure 5). Each of the layers has its own architecture. Interfaces can use different communication protocols with different security measures.

Device Layer is directly responsible for control functions performance, including for that a set of sensors, on the board controllers and actuators (see Figure 3), which can have the same with ES structure. Digital control is usually restricted on this layer. All other layers are supplementary from the point of view of CCS. From this prospective the interfaces DL-NL and DL-AL are the most interfering for CCS Functional Safety.

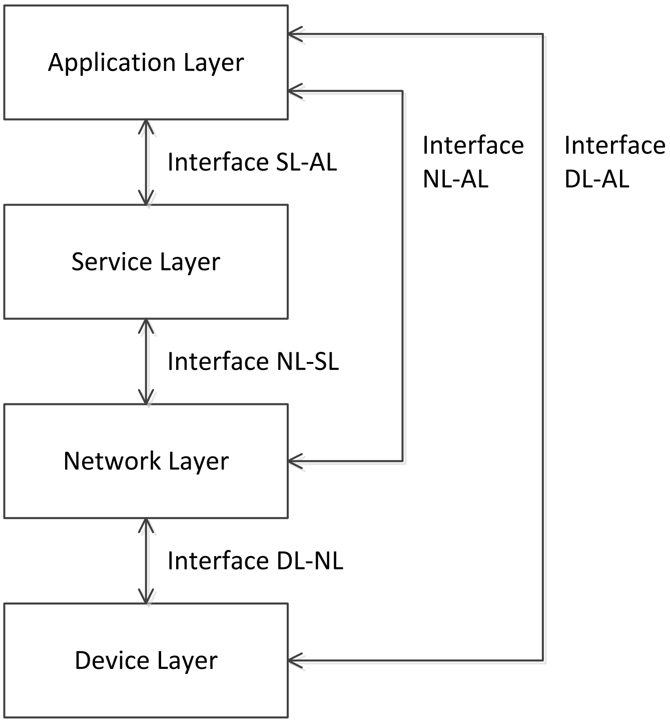

Figure 5: *Typical Architecture of IoT*

IV. Reliability, Availability and Safety Indicators: Fundamentals

Let's consider the statement of the standards series IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems" which discuss Safety Indicators. At the same time, let's try to compare these Safety indicators with well-known Reliability and Availability indicators.

The basic concept of Functional Safety assessment is dividing a common failure rate Λ (let us begin with the exponential distribution with a constant failure rate) into dangerous and safe failures as well as into detected and undetected failures. This is a main difference of Functional Safety from Reliability. From this point of view we have four failures sets (see Figure 6):

- Safe Detected failures with a failure rate λ_{Sd} – failures which put the equipment under control (EUC) to a safe state and are discovered by self-diagnostics;
- Safe Undetected failures with a failure rate λ_{Su} – failures which put the EUC to the a state and are not discovered by self-diagnostics;
- Dangerous Detected failures with a failure rate λ_{Dd} – failures which put the EUC to a potentially dangerous state and are discovered by self-diagnostics;
- Dangerous Undetected failures with a failure rate λ_{Du} – failures which put the EUC to a potentially dangerous state and are not discovered by self-diagnostics.

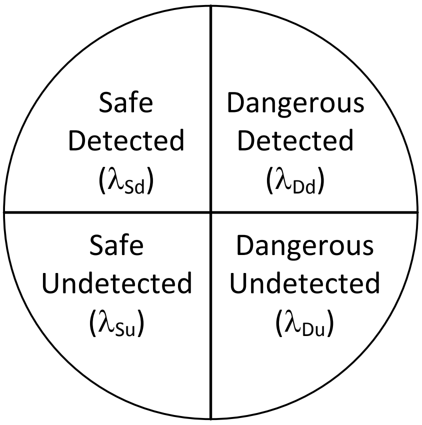
Safe Detected (λ_{Sd})
Dangerous Detected (λ_{Dd})
Safe Undetected (λ_{Su})
Dangerous Undetected (λ_{Du})

Figure 6: *Failures Theoretical-Set Model*

So, there are some obvious dependencies following from Figure 6:

- Common failure rate is $\Lambda = \lambda_{Sd} + \lambda_{Su} + \lambda_{Dd} + \lambda_{Du}$;
- Dangerous failure rate is $\lambda_D = \lambda_{Dd} + \lambda_{Du}$;
- Safe failure rate is $\lambda_S = \lambda_{Sd} + \lambda_{Su}$;
- Detected failure rate is $\lambda_d = \lambda_{Sd} + \lambda_{Dd}$;
- Undetected failure rate is $\lambda_u = \lambda_{Su} + \lambda_{Du}$.

Also a lot of relative metrics can be extracted from dependencies between sets cardinality and different failure rates values. The most important from these metrics are the following:

- Safe Failure Fraction (SFF) in accordance with IEC 61508 is SFF = $(\lambda_S + \lambda_{Dd}) / \Lambda$;
- Dangerous Failure Fraction (DFF) in accordance with IEC 61508 is DFF = 1 – SFF = λ_{Du} / Λ;
- Diagnostic Coverage (DC) for dangerous failures in accordance with IEC 61508 is $DC_D = \lambda_{Dd} / \lambda_D$;
- More widely used dependency for Diagnostic Coverage is DC = λ_D / Λ;
- Proof Test Coverage (PTC) should be calculated from the total failure rates for the using the formula PTC = $1 - \lambda_{DuaPT} / \lambda_{Du}$, where λ_{DuaPT} is λ_{Du} after Proof Test.

To move ahead with Safety indicators we need to introduce some definitions from the standards series IEC 61508.

Safety Function is a function to be implemented by a safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event; all the above indicators are usually calculated for specified Safety Functions; sometimes for ICS a term **Safety Instrumented Function (SIF)** is used as equal;

Safety Integrity is a probability of a safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time.

Safety Integrity Level (SIL) is a discrete level (one out of a possible four), corresponding to a range of safety integrity values, where SIL 4 has the highest level of safety integrity and SIL 1 has the lowest.

Mode of Operation is a way in which a safety function operates, which may be either

- Low Demand Mode: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year; or
- High Demand Mode: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year; or
- Continuous Mode: where the safety function retains the EUC in a safe state as part of

normal operation.

IEC 61508 states different Safety Indicators depending from the Mode of Operation.

For Low Demand Mode average probability of dangerous failure on demand (PFDavg) shall be calculated. PFDavg is mean unavailability of a safety-related system to perform the specified safety function when a demand occurs from the EUC.

The IEC 61508 states that only Dangerous Undetectable failures contribute to PFDavg, the last can be calculated as PFDavg(Du) = 1 – A(Du) = U(Du) = λ_{Du} / (λ_{Du} + μ_{Du}), where μ_{Du} is restoration rate of Dangerous Undetectable failures.

Also for Dangerous failures PFDavg(D) = 1 – A(D) = U(D) = λ_D / (λ_D + μ_D), where μ_{Du} is restoration rate for all the Dangerous failures.

For High Demand Mode and Continuous Mode average frequency of a dangerous failure per hour (PFH) shall be calculated. PFH is the average frequency of a dangerous failure of a safety related system to perform the specified safety function over a given period of time.

Usually PFH is defined as failure rate, so on the base of Dangerous Undetectable failures PFH(Du) = λ_{Du}, and on the base of all the Dangerous failures PFH(D) = $\lambda_{D.}$

Also the IEC 61508 states that PFH can be calculate as unavailability or as unreliability depending from a safety-related system application conditions.

So, the general conclusion is a typical Reliability Theory method, models and indicators can be directly applied for the Functional Safety domain.

V. Reliability, Availability and Safety Indicators: Application for Nuclear Domain

This section provides a case study for application of the above indicators for safety assessment of ICSs integrated on the base of safety PLC named RadICS designed by company Radiy (www.radiy.com).

The RadICS PLC is composed of a logic module (LM) and a number of varied I/O modules contained within a chassis. There is the following scope of available I/O modules for the RadICS PLC:

- Analog Input Module (AIM);
- Discrete Input Module (DIM);
- Analog Input Flux Module (AIFM);
- Analog Output Module (AOM);
- Discrete Output Module (DOM);
- Optical Communications Module (OCM).

The RadICS PLC performs the safety function defined in its application (ICS) layer logic, which will be specified by and possibly implemented by the end-user (Nuclear Power Plants). Diagnostics are executed at both the application and the platform level, and detected failures that are potentially unsafe are converted to safe events by opening the discrete outputs.

The target in the considered case was to determine SIL of the RadICS PLC as a platform for future applications for Nuclear Power Plants.

Reliability, Availability and Safety are investigated in special Failure Mode Effect and Diagnostic Analysis (FMEDA) Report. FMEDA is a modification of well-known FMEA technique. A difference lays in assessment of diagnostic coverage, which is an essential part of Functional Safety implementation. Also the FMEDA generates failure rates and the Safe Failure Fraction. The analysis assumed that the FSC will be used in de-energize–to–trip applications.

For hardware assessment only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis. Failures caused by external events, however should be considered as random failures. Examples of such failures are loss of power, physical abuse, or problems due to intermittent instrument air quality.

The first step to in FMEDA is to define the failure rate for fail safe detected, safe undetected, dangerous detected, and dangerous undetected failures. Electrical and mechanical component Reliability Handbooks with statistical data are used to define the failure rate of separated components. Criticality analysis is used to divide components failures between safe and dangerous. Diagnostic coverage analysis is used to divide components failures between detected and undetected.

Calculation of the above failure rates is a basic for calculation of application specific indicators depending of ICS hardware configuration. For example, typical single-channel Safety Function (SIF), based on a CANDU 6 reactor (http://www.candu.com/en/home/candureactors/default.aspx) heat transport high pressure trip parameter, consists of the following:

- 1 pressure sensor measuring one outlet header pressure (requires 1 AIM);
- 2 discrete outputs used to provide trip signals to the 2oo3 voting logic (using 1 DOM);

This trip system is modeled in two parts; the individual channel, and the inter-channel voting. The example configuration as used for the sensors and PLC comprising each individual channel of the 3-channel safety system is as follows:

- One LM uses no on-board discrete inputs or outputs;
- One AIM reads a typical pressure transmitter used in CANDU plants, with both off-scale low or high leading to trip;
- One DOM using a total of two discrete output channels (used to drive the 2oo3 inter-channel voter consisting of 6 solenoid valves).

Note that this SIF operates in a low demand mode; however the modeling is complicated by the 2 layers of logic solving. This requires modeling the real sensors and the PLC in one model operating in continuous demand mode. This determines a failure rate to be used in the inter-channel voting part of the model, which operates in a low demand mode.

To confirm that the PLC has met its requirement to consume less than 15% of the allowable PFDavg of SIL 2, the channel model is also examined in low demand mode.

The described approach allows to calculate the above indicators (SFF, DFF, DC, PTC) for specific applications.

As a result of the above case the RadICS PLC has been certified by exida LLC (exida.com) as a product complied with SIL3 requirements of IEC 61508 (http://www.exida.com/SAEL/rpc-radiy-fpga-based-safety-controller-fsc-radics). At the present some tens of applications are implemented on the base of RadICS PLC for Nuclear Power Plants in Europe and Americas. The mentioned applications demonstrate the specified level of Functional Safety.

VI. Discussion: a Proposed Research and Development (R&D) Program for IoT Reliability and Functional Safety

An updated taxonomy has been proposed in this paper for Dependability and Security. This taxonomy integrates all known attributes in safety and security critical domains. Relations between Safety and all other attributes are established.

Functional Safety is a part of Reliability that has dealt with Safety Functions and related dangerous failures. Safe failures do not affect Functional Safety features. From this point of view, all the Reliability Theory method, models and indicators may be applied for the Functional Safety domain without any essential change.

ES, ICS, and IoT Device Layer have been considered in Section III as three the main architectures used for CCSs. ES and ICS have a long references story for safety critical applications while IoT has only started to be applied during the last five years.

Taking into account the above, the following Research and Development (R&D) program is proposed to study IoT Reliability and Functional Safety:

- Task 1 "IoT Reference Architecture Development" with the following subtasks: Standards for safety critical applications. Standards for IoT. Case Study: Analysis of existing IoT platforms. Used programmable components and challenges in safety assessment. Layers of architecture. Communications between layers of architecture. Functions distributions between layers of architecture. Opportunities for isolation of safety from non-safety functions. Prospective of IoT based applications for safety critical domains;
- Task 2 "Safety and Reliability Models Development" with the following subtasks: New challenges for Reliability Theory from the IoT prospective. Application of Reliability, Availability and Safety indicators for IoT. Trade-in between Safety and Availability. Comparative risk analysis for IoT based applications versus PLC based applications. Safety assurance methods: redundancy, diversity, diagnostic, separation, qualification testing, etc.;
- Task 3 "Application of Reliability and Safety Assessment Methods for IoT" with the following subtasks: Overview of safety assessment methods and tools. Hazard Analysis. Fault Tree Analysis. Markov models. Failure Mode, Effect and Criticality Analysis;
- Task 4 "IoT Safety Life Cycle" with the following subtasks: Safety management. Safety Life Cycle structure. Verification & Validation methods. Software tools evaluation. Configuration management and change control;
- Task 5 "IoT Testing" with the following subtasks: Test coverage approach for IoT Safety Life Cycle. Review of technical specifications. Static code analysis. Unit and integration testing. Fault Insertion Testing. Validation testing with physical I/O. Environmental impact testing. Model-based testing (MBT). Formal verification;
- Task 6 "Computer Security of IoT" with the following subtasks: Vulnerabilities and treats for IoT. Case studies of existing malware. Recommendations for security management system: business protection, data protection, operation protection;
- Task 7 "Assurance Case for IoT" with the following subtasks: Assurance Case notation and methodology updating. Tools for Assurance Case building. Implementation of IoT Assurance Case methodology for licensing and certification framework;
- Task 8 "Energy consumption efficiency assessment for IoT" with the following subtasks: Energy consumption model for IoT. Energy consumption assessment tools. Energy consumption measurement experiment;
- Task 9 "Design and testing of a representative IoT based application" with the following subtasks: Choice of application. Choice of hardware-software platform and design technology stack. Model-based design methodology. Design implementation. Trial operation.

References

[1] Laprie, J.-C. (1985). Dependable Computing and Fault Tolerance: Concepts and Terminology. *Proceedings of the 15th IEEE International Symposium Fault-Tolerant Computing (FTCS-15).*

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

[3] Ushakov, I. (2006). Reliability: Past, Present, Future. *Reliability: Theory & Applications,* 1(1): 10-16.

[4] Trivedi, K., Kim, D.S., Roy, A. and Medhi, D. (2009). Dependability and Security Models. *Proceedings of the 7th International Workshop on the Design of Reliable Communication Networks.*

[5] Castet, J. and Saleh, J. (2006). Survivability and Resiliency of Spacecraft and Space-Based Networks: a Framework for Characterization and Analysis. *Proceedings of the Conference on Network Protocols (ICNP 2006).*

[6] Yastrebenetsky, M. and Kharchenko, V. (Edits) (2014). Nuclear Power Plant Instrumentation and Control Systems for Safety and Security, IGI Global, 2014.

[7] Sklyar, V. (2016). Safety-critical Certification of FPGA-based Platform against Requirements of U.S. Nuclear Regulatory Commission (NRC): Industrial Case Study. *Proceedings of the 12th International Conference on ICT in Education, Research and Industrial Applications (ICTERI 2016).*

[8] Andrashov, A., Bakhmach, I., Sklyar V., Kovalenko A. (2015). FPGA-based I&C applications in NPP's modernization projects: Case study. *Proceeding of the 9th International Conference on Nuclear Plant Instrumentation, Control & Human-Machine Interface Technologies (NPIC&HMIT 2015).*

[9] Top 10 IoT Technologies for 2017 and 2018. Technical Report G00296351, Gartner Inc., 2016.

[10] Sajid, A., Abbas, H., Saleem, K. (2016). Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges. *IEEE Access*, 4:1375-1384.