EU Project SafEUr – Competence Requirements for Functional Safety Managers

Andreas Riel, Ovi Bachmann, Klaudia Dussa-Zieger, Christian Kreiner, Richard Messnarz, Risto Nevalainen, Bernhard Sechser, Serge Tichkiewitch

Workshop 2:
Standards and Experiences with the Implementation of Functional Safety

25 June 2012
Bus accident in Switzerland on 13 March 2012

- Bus crashed into a tunnel side wall without any outside incident.
- 28 people died, 22 of them children.
- The bus driver had probably been distracted.

Reuters/Denis Balibouse
Bus accident in Switzerland on 13 March 2012

At excellent road and traffic conditions, such a terrible accident can also happen if

- there is an unwanted actuation of the electronic steering system,
- there is an unwanted actuation of an ESP system,
- there is an unwanted actuation of a torque vectoring system,
- and more.
Motivation and Focus

• Lack of trainings in Functional Safety System Development.

• Focus on
  – linking the theory expressed in standards with practice using case studies;
  – the system development aspect;
  – the Safety Standards IEC 61508, ISO 15504 (SPICE).
The SafEUr Consortium

- EMIRAcle – European Manufacturing and Innovation Research Association, a cluster leading excellence in Belgium and France
- Institute of Technical Informatics at Graz University of Technology in Austria
- ISCN GmbH, International Software Consulting Network, in Austria and Ireland
- Method Park Software AG in Germany
- SIBAC GmbH in Germany
- Spinet Oy in Finland
SafEUr Industry Partners

• SOQRATES Working Group on Functional Safety comprising more than 20 suppliers and leading engineering and research organisations from Austria and Germany, e.g. Continental, Giesecke & Devrient, KTM, ZF.

• All the SME Consortium Partners deliver Training and Consulting Services in Functional Safety to Industry.
SafEUr Key Project Data

- Project Type: Leonardo da Vinci Multilateral Project for Development of Innovation
- Total Budget: 482,732 EUR
- EU Funding: 362,049 EUR
- Project Start: 01/11/2011
- Project End: 31/10/2013
SafEUr Key Project Goals

• Definition of the competencies required to fulfill the role of a Safety Manager.
• Definition of a corresponding Training Program.
• Creation of E-Learning based Training Material in 4 languages (EN, FI, FR, GE).
• Creation of a Pool of Test Questions for Certification.
• Integration of the materials into the E-Learning and Examination Portals of the ECQA (www.ecqa.org), powered by ISCN.
• Delivery of free-of-charge Pilot Trainings in the participating EU countries.
• Dissemination and Marketing, development of an Exploitation Plan and Strategy
U1.E1: International Standards and Norms

- be able to relate contemporary functional safety standards to the relevant industry sectors;
- know the structure and content modules of the standards IEC 61508 and ISO 26262;
- know the relationship between functional safety standards, norms, and process compliance;
- know the relationship between functional safety standards, norms, and safety assessment and certification.
U1.E2: Product Life Cycle

- know the key phases and stakeholders of a typical product/system life cycle;
- know key safety-specific issues of the life cycle, such as safety case specification and supplier qualification;
- think in terms of processes and their associated activities, roles, documentation, etc.
- take into account organisational aspects, such as organisation structure and culture;
- relate functional safety aspects to risk management.
U1.E3: Terminology

- know key terms related to functional safety as they are used and defined in the standards;
- be able to deal with differences in terminology among the different standards.
U2.E1: Safety management on organisational and project level

- recognise the importance of and requirements in safety culture to achieve systematic, high level safety awareness and responsibility in the whole organisation;
- identify elements in organisational safety system management and assume the role of a safety manager;
- define requirements for project / product / system level safety management;
- establish the necessary safety and quality assurance for project / product / system level safety engineering work;
- create and develop necessary documentation for organisational and project / product / system level safety management.
U2.E2: Safety Requirements and Safety Case Definition

• identity main elements of a safety case, based on standards and related concepts;
• establish requirements for evidence collection to construct a full safety case;
• create necessary arguments and modular safety cases;
• explain a full safety case for organisational management and other stakeholders (customers, regulators, etc.);
• review safety cases developed by suppliers or third parties.
U2.E3: Overview of Required Engineering and V&V Methods

• select the right engineering and test approaches based on the provided method tables, the identified safety integrity level, and the product architecture;
• set up a V&V Plan which covers all necessary test phases, test levels, test methods, test metrics, and evidences of complete functional safety coverage and compliance;
• practically understand and implement safety related testing, such as fault injection testing, diagnostic coverage testing, equivalence class testing, load testing, branch coverage in testing, etc.
• draw up a compliance map demonstrating the use of qualified tools and qualified engineering methods as part of the safety plan.
U2.E4: Establishing and Maintaining a Safety Plan

- establish safety plans correctly;
- monitor and review the progress of the implementation of such plans;
- use safety plans as a tool for managing the function safety aspects of a development project.
U2.E5: Regulatory & Qualification Requirements

• act as a responsible person and facilitator in his/her organisation, to support required certification and/or qualification tasks with other parties;
• recognise and explain at least one certification and/or qualification scheme and its benefits;
• participate and coordinate necessary data collection and evidences for certification and/or qualification;
• review draft certification / qualification reports from independent parties;
• communicate with regulatory body / bodies to satisfy their information needs in qualification and licensing.
U3.E1: System Hazard Analysis and Safety Concept

• understand the key vocabulary words to carry out a hazard and risk analysis;
• describe the working environment and the item definition;
• understand the difference of functional and non-functional behaviour of the system;
• be able to moderate a hazard and risk analysis in a development department;
• be able to come to a correct assessment of the SIL or ASIL.
U3.E2: Integrating Safety in System Design & Test

• understand the difference between system requirements and system design;
• explain signal paths in systems and their influence on the system,
• show the allocation of subsystems to his systems requirements and system design;
• describe a state machine on system level and allocate time slots for the subsystems on the safety critical path for the identified system reaction time.
U3.E3: Integrating Safety in Hardware Design & Test

• explain the terms Failure, Fault, Error, together with Fault classes, Failure modes, and attributes of dependability (availability, reliability, safety, confidentiality, integrity, maintainability);
• select the right strategy from a set of basic dependability strategies;
• explain the basic terms of modelling hardware fault tolerance (hazard functions, MTTF, MTTR, MTBF, availability, maintainability) and select the right modelling strategy for hardware fault tolerance;
• calculate the reliability of series, parallel, and mixed systems, as well as apply this theory to N-redundant systems.
U4.E1: Integrating Safety in Software Design & Test

- explain Design Diversity strategies and select the right ones;
- explain Data Diversity strategies and select the right ones;
- explain and select the right fault tolerant software patterns (architectural, detection, error recovery, error mitigation, fault treatment) for a system to be designed;
- select the right adjudication concept;
- select the right Information Redundancy (codes).
U5.E1: Legal Aspects and Liabilities

• know the legal aspects of product liability (national and international);
• know the personal responsibility not to harm any human being by developing defective products;
• be able to estimate the residual risk of a product to be released;
• know which kind of information must be provided in order to satisfy legal aspects.
U6.E1: Integration of Reliability in Design to Enhance Functional Safety

• define the chain of the reliability in design and the needed actors to intervene in this chain;
• define the links between the top events and the elementary design parameters for a given problem;
• know the link between the modelling of the physical behaviour of the system and the modelling of the design parameters.
U6.E2: Safety in the Production, Operation and Maintenance

- know the different states proposed in the guide for the study of the start and stop modes of a production system;
- know how to build the specification for the safety control of a production system;
- know the limits of the guide for the study of start and stop modes.
Conclusion and Outlook

• SafEUr Trainings will be available from September 2012 as Classroom Trainings or Distance Trainings by E-Learning Facilities.
• SafEUr will be the only Program in Functional Safety to deliver a European Certificate.
• SafEUr links Theory in Standards with Practical Systems Engineering Competencies.
Acknowledgment

This presentation was developed within the international consortium “ECQA Certified Functional Safety Manager”:

- Graz University of Technology, Austria, www.tugraz.at
- International Software Consulting Network Ltd., Ireland, www.iscn.com
- Methodpark Software AG, Germany, www.methodpark.de
- Sibac GmbH, Germany, www.sibac.de
- Spinet Oy, Finland, www.spinet.fi

- The development was partly funded by the EU under: Leonardo da Vinci programme 518632-LLP-1-2011-1-AT-LEONARDO-LMP

This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Contact and Feedback

Andreas.Riel@grenoble-inp.fr
 rmess@iscn.com
 christian.kreiner@tugraz.at

Thank You!