Embedded – IC & Automation Fortronic

June 21st, 2012
Centro Congressi Milanofiori – Milan

Introduction to Functional Safety

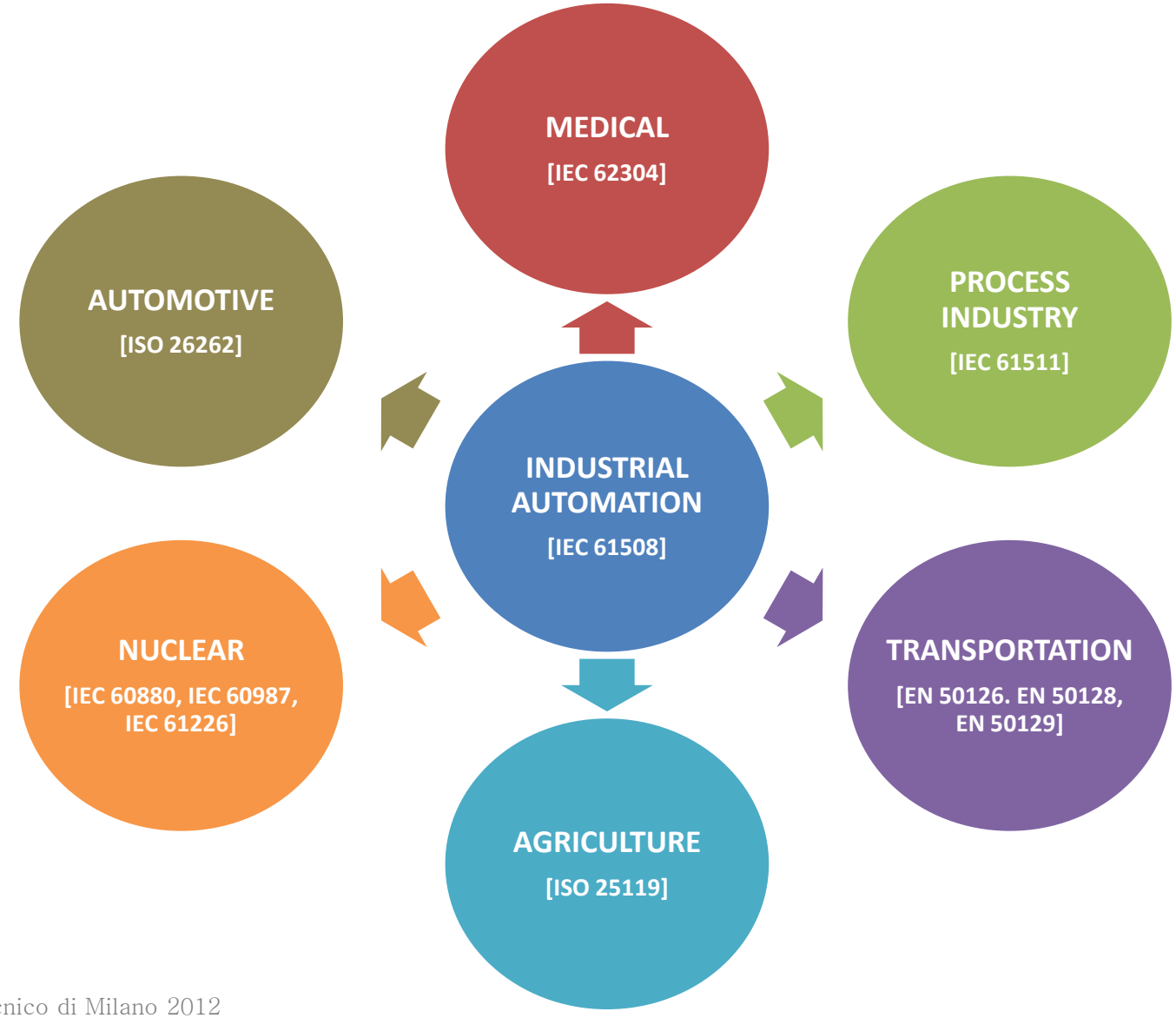
Enrico Silani
CEFRIEL – Politecnico di Milano

What is Functional Safety? What is Functional Safety about?

- **IEC 61508 Definition:**
  - **Safety** is the freedom from unacceptable *risk* of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment.
  - **Risk** is a combination of the probability of occurrence of *harm* and the severity of that harm.
  - **Functional Safety** is part of the overall safety that depends on a system or equipment operating correctly (i.e. perform a **safety function**) in response to its inputs.

- **Functional Safety** is thus about achieving "absence of unreasonable risk due to *hazards* (potential source of harm) caused by malfunctioning behavior of the electrical/electronic/programmable electronic (E/E/PE) systems".
- **Failures** are the main impairment to safety:
  - **Systematic Failures**: failure related in a deterministic way to a certain cause that can only be eliminated by a change of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.
  - **Random HW Failures**: failure that can occur unpredictably during the lifetime of a hardware element and that follow a probability distribution.

Functional Safety standards



IEC 61508 standard

- In general, Functional Safety Standards impose a *structured way* for the industry to proceed
- **IEC 61508** is a standard for the effectiveness of *safety system* in E/E/PE systems:
  - Originated in the process control industry
  - Basic Functional Safety standard that covers the complete *safety life cycle*
  - Derivatives later created for specific markets such as railways, automotive,…
- IEC 61508 is in use since 1998, amendments added since 2000
- New version (2010) now in FINAL status and mandatory for new developments
- Used in more than 60 countries

- The standard addresses:
  - Architectural & Functional aspects
  - Procedural aspects (including safety life cycle)
  - Faults avoidance and faults control
  - Systematic faults and HW random faults

- Rigorous documentation serves as evidence for complying to the safety standard

Safety Function vs Safety Integrity

- **Key Concepts** in IEC 61508 standard are **RISK** and **SAFETY FUNCTION**
  - **Risk** is a function of frequency (or likelihood) of the hazardous event and the event consequence severity
  - Risk is reduced to a *tolerable level* by applying **safety function**.
  - The **SIL** (Safety Integrity Level) is the measure of the "risk reduction level" of the Safety Function.

SAFETY FUNCTION	SAFETY INTEGRITY
Function, which is intended to achieve or maintain a *safe state* for the equipment under control (EUC) in respect to a specific hazardous event.	• Probability of a *safety-related system* satisfactorily performing the required safety function under all stated conditions within a stated period of time (*process safety time)* • Four Level of safety integrity (SIL 1 to 4) • Consider all causes of failures (random HW faults and systematic failures) which lead to an unsafe state

SAFETY-RELATED SYSTEM
Designated system that both: • Implements the required safety functions necessary to achieve and maintain a safe state for the EUC • Is intended to achieve, on its own or with other E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions

Fault avoidance and Fault Control

FAULT AVOIDANCE

- Systematic failures caused by faults originating **before** system installation
- For example specification and program faults, incomplete verification and validation, etc.
- Addressed by the **process** (off target)

FAULT CONTROL

- Systematic hardware errors (hard-errors) and random hardware errors (soft-errors) caused by faults originating **after** system installation
- For example broken hardware and a temporary bit-flip due to radiation
- Addressed by **diagnostics / techniques** (on target)

What are the main Functional Safety drivers?

- **Customer Requirements (*)**
  - Customers may demand functional safety evaluation before purchasing equipment
  - Customers may use it as a Technical Quality Specification (a single statement in their specification results in several requirements for the supplier)
  - NOTE: In some cases, Customers wants products with documented safety characteristics (including failure rates and failure mode data) not really “safety products”
- **Regulations (*)**
  - Some regulatory bodies require or encourage functional safety evaluation
- **Internal Requirements:**
  - Legal protection / Product Liability
  - Internal organization Safety & Reliability requirements
- **Market Acceptance**
  - Having a functional safety certification maintains a product’s competitiveness in the marketplace
- **Legislation**
  - Legislative requirements, such as some European Directives, require a functional safety evaluation
- **Insurance companies**
  - Insurers may require a FS evaluation before equipment is installed in the workplace, or may provide discounted premiums for using products evaluated for functional safety

(*) Buyers and Authorities in some cases sees FS as one Reference to reduce their uncertainties on complex systems

Forces and Trends?

- Certainly not all industrial products require certification… but more are requiring it.

  What is happening?

- Mechanical products evolving to electronic products
- Manually operated products evolving to automatic products
- Growth of software quantity and complexity
- More government regulations
- Software differentiates and defines their product to customers:
  - Less expensive than physical implementation
  - More features
  - More flexible and scalable
  - Sometimes the primary visible portion of the product

Certification and Safety Case

- What is Certification?
  - No legally binding definition
  - Typically: assessment by third party / independent assessment body (TÜV Sud, TÜV Nord, EXIDA, etc.) against certification criteria
  - Practically: document stating that an assessment report exists listing the certification criteria
  - The IEC 61508 does not require certified product for Functional Safety
- Different types of Certification:
  - **Functional Safety Management** certificate: confirms compliance of presented FS management system, products not included
  - **Type Approval** certificate: confirms compliance of the presented type or prototype
  - **Product** certificate: confirms compliance of the product as produced, includes surveillance of the production of the certified product
- How to obtain the Certification:
  - Compliance to the relevant standard required
  - **Safety Case** to argue compliance in a written form: i.e., customers present their case to an Assessor and "*prove*" their SIL claim

At which "level" Functional Safety can be implemented?

No Functional Safety at all

- All the functions of the product are QM related
- In some (most of the) cases, redundancy and/or diagnostic and/or failure analysis techniques and methods are considered during the development

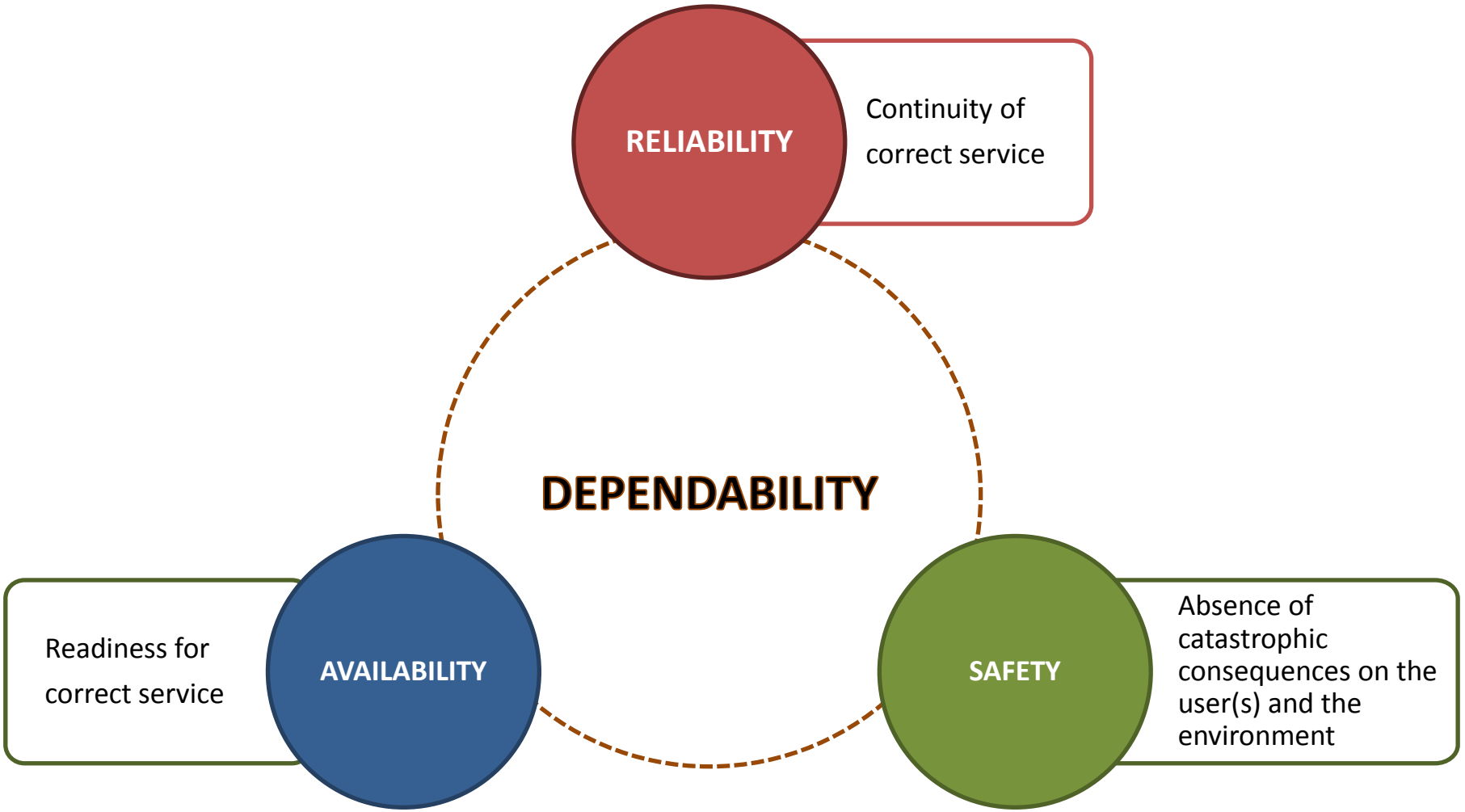
Functional Safety is needed and/or desired

- FS can be implemented at component (e.g., IC, SW operating systems) level only: detailed design techniques, failure analysis/data and documentation to help product development
- FS can also be implemented at product level: detailed design techniques, failure analysis/data and documentation showing using in system design
- Only technical reports (for concept and/or detailed phases) can be sufficient

Functional Safety is mandatory

- FS must be implemented at system level: risk based framework for process assessment, selection of SIL level, component selection, system failure analysis, system design and verification, tool qualification, …
- Technical Reports and Full certification

Safety vs Availability vs Reliability



Functional Safety of Electrical, Electronic and Programmable Electronic Systems

Training Course: An introduction to Functional Safety

con il patrocinio di

assodel
Associazione Nazionale
Fornitori Elettronica

Day 1 — 9:00 – 18:00

Introduction and General Requirements

Introduction Functional Safety
- Concept of functional safety
- Risk: tolerability and assessment

Introduction to ISO/IEC safety norms
- General structure of the standards
- Overview of IEC61508 and ISO26262 standard

General requirements
- Overview of the safety lifecycle
- Concept and Detailed implementation phases
- Hazard and risk analysis
- Definition od the Safety Integrity Level
- Definition and allocation of safety requirements

Hardware requirements
- System architecture requirements
- Failure Mode and Effect Analysis
- Failures
  - Random and systematic failure
  - Safe failure fraction
  - Common cause failures
- Hardware design requirements overview

Day 2 — 9:00 – 18:00

Hardware & Software Design

Software requirements
- The software lifecycle
- Software architecture requirements
- Languages and tools
- Failure
  - Systematic failures
  - Isolation and propagation
  - Criticality analysis
- Software design requirements overview

Techniques and methods
- Hardware design
  - Overview of design techniques
  - Reference tables
- Software design
  - Overview of design techniques
  - Reference tables

Date:

14-21 Settembre 2012

Costo: 1.500€

Sconto: 20% per le aziende associate a Assodel

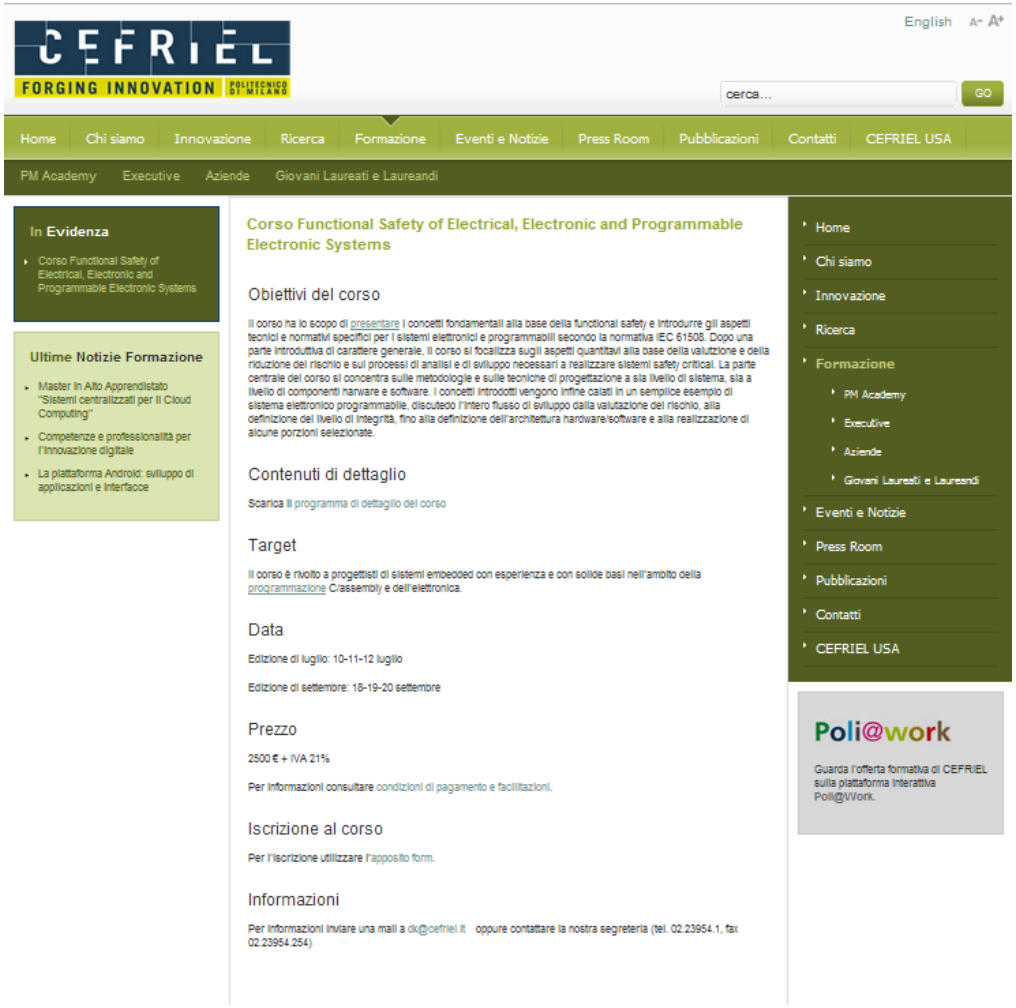
Sede:

CEFRIEL
Via R.Fucini 2, 20133
Milano
Tel. 02.23954.1

Info:

Web	**www.cefriel.it**
Mail	**dk@cefriel.it**
Tel.	**02.23954.1**

http://www.cefriel.it/index.php/it/formazione/2163-fs



CEFRIEL
FORGING INNOVATION
POLITECNICO DI MILANO

assodel
Associazione Nazionale
Fornitori Elettronica