IAEA Regional Workshop RER2010

Provision of diversity through the application of FPGA based systems

July 1 2015
Saint Petersburg, Russian Federation

Oszvald Glöckler

Sunport
Connecting Forward

www.sunport.ch

Sunport

Presentation Outline

- Introduction
- Description and Characteristics of Field-Programmable Gate Arrays
- Examples of FPGA applications in the NPP industry
- Categories of I&C System Diversity
- Diversity Strategies using FPGA Technology
- Common-Cause Failures (CCFs)
- Defence in Depth in I&C Systems Hierarchy
- Redundancy and Diversity Architectures
- Summary

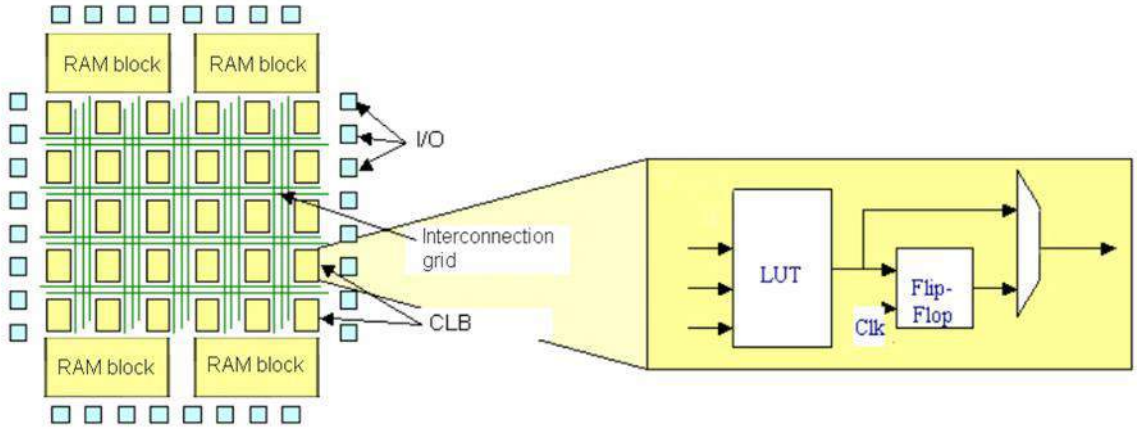
Sunport

Key Words

- Redundancy
- Diversity
- Independence
- Defence in Depth
- Common Cause Failure (CCF)
- Field-Programmable Gate Arrays (FPGAs)

Sunport

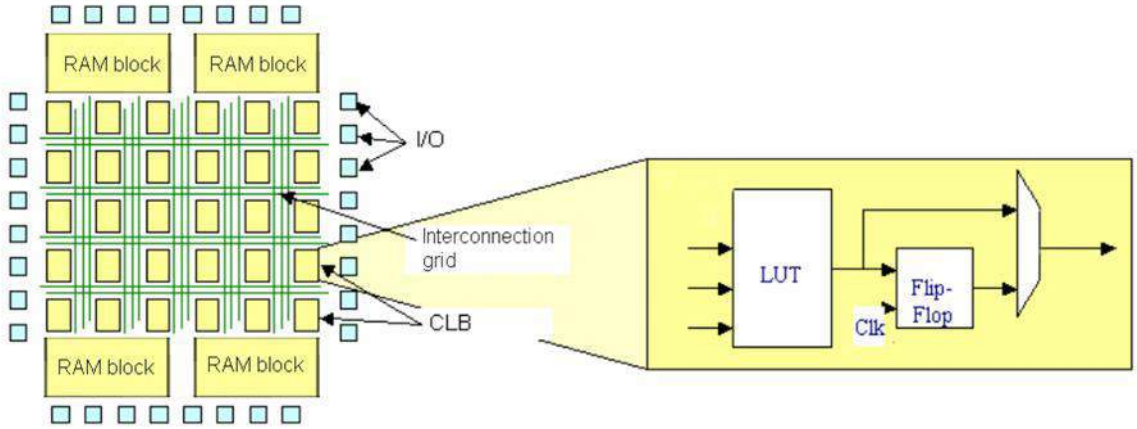
Common basic architecture of FPGAs



- FPGAs are programmable integrated circuits,
- designed to be configured by the user after chip manufacturing through the use of hardware description languages (HDL).

Sunport

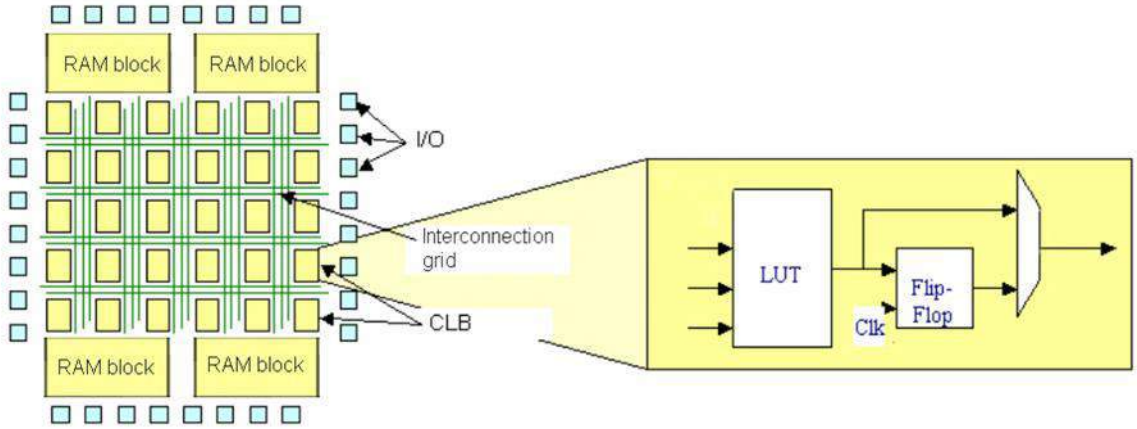
Common basic architecture of FPGAs (CLBs)



- A set of configurable logic blocks (CLBs) to implement any logic functions (AND, OR, XOR, NOT).
- In general, each CLB can be configured to implement an N-to-M Boolean function using simple logic gates, or using look-up table (LUT) to implement a logic function.
- The output of each CLB includes a flip-flop for synchronizing the data flow within the FPGA.

Sunport

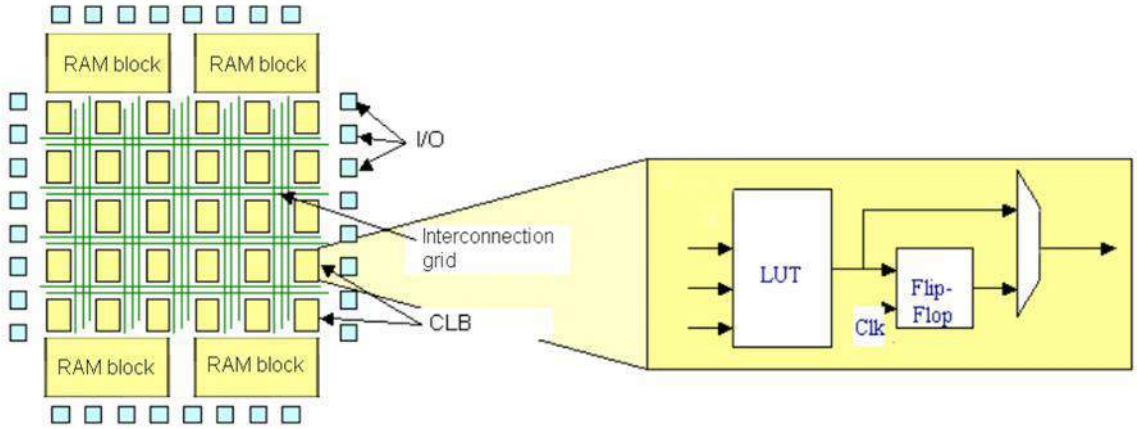
Common basic architecture of FPGAs (I/O Blocks)



- Set of programmable Input/Output (I/O) blocks: electrical interfaces.
- Can be configured as input or output, and is connected to one or more CLBs.
- Some I/O blocks can perform analogue-to-digital conversion.

Sunport

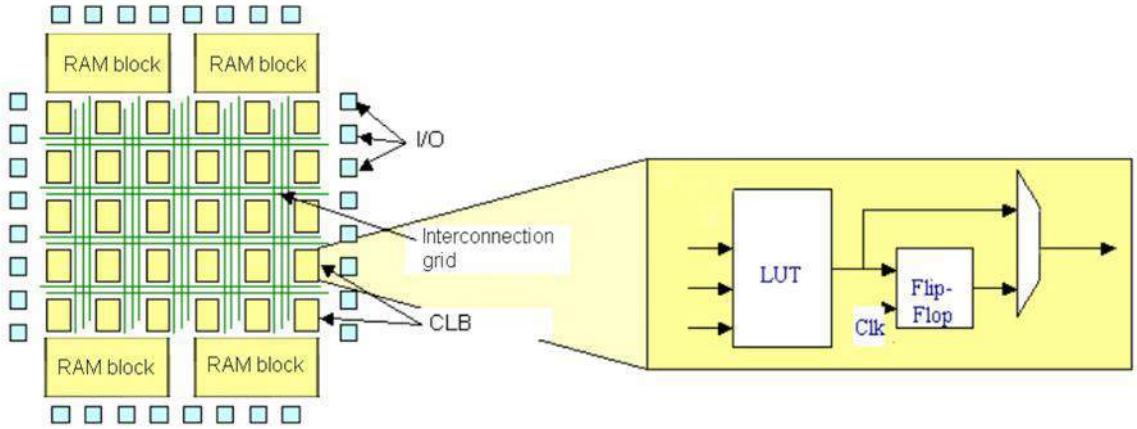
Common basic architecture of FPGAs (Grid)



- Interconnection grid: set of wires to be connected at intersecting points when the FPGA is configured to the desired application.
- They link inputs/outputs of various CLBs, as well as I/O blocks in configurations representing the desired applications.

Sunport

Common basic architecture of FPGAs (Memory & µP)



- Application dedicated data memory: non-volatile flash memory to reload applications in case of fast power restart or resistance to single-event upsets (SEUs).
- Microprocessors can be linked to CLBs through interconnection grid.

Sunport

The most common FPGA chips are:

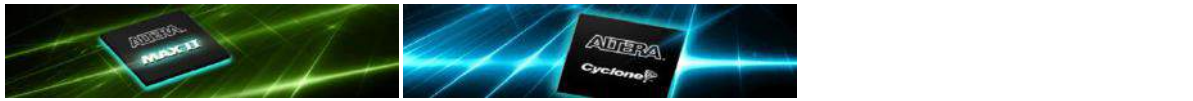
- EPROM / EEPROM / Flash based chips are re-writable types (they allow reprogramming of the FPGA) and non-volatile (no data or logic is lost in case of power loss);
- SRAM based chips are re-writable, but volatile;
- Anti-fuse based chips are non re-writable, non-volatile, and can only be programmed once.

EPROM: Erasable Programmable Read-Only Memory
EEPROM: Electrically Erasable Programmable Read-Only Memory
SRAM: Static Random-Access Memory

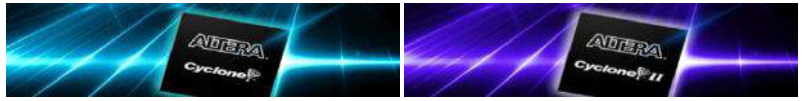
Sunport

FPGA chip manufacturers

Actel POWER MATTERS · ALTERA · ATMEL · Lattice Semiconductor Corporation · XILINX



CPLD (MAX) FPGA (Cyclone)



EMP EP1 EP2

- Various FPGA chips have a higher degree of uniqueness, compared to software-based designs
- They require specific development tools (vendor or proprietary) for application programming (e.g. Quartus II for Altera)
- It is not possible to develop a common malware which would affect all types of FPGA-based systems

Sunport

Altera devices

ACEX® 1K
APEX™ 20K
APEX 20KC
APEX 20KE
APEX II
Arria® GX
Arria II GX

Classic™
Configuration
Cyclone®
Cyclone II
Cyclone III
Cyclone IV
Cyclone V (GX, GT, E)
Excalibur™
FLEX®

HardCopy® II
HardCopy III
HardCopy IV (E and GX)
MAX®
MAX II
MAX IIG
MAX IIZ
MAX V
Mercury™

Stratix®
Stratix II
Stratix III (E and L)
Stratix IV (E, GX, GT)
Stratix V (GX, GS, GT, E)
Stratix GX
Stratix II GX

Sunport

Main points of FPGA Technology

- FPGAs are configurable integrated circuits (SW, logic elements);
- Can be used for the implementation of logic and a variety of math functions;
- Application functions are implemented via the use of Hardware Description Languages (HDL);
- Depending on the chip characteristics the configuration can be updated;
- FPGA based systems can include on-board microprocessors;
- FPGA technology constitutes the closest reconfigurable alternative to a pure hardware implementation.

Sunport

Main points of FPGA Technology (cont …)

- Implementation of safety functions without embedded application software or operating systems;
- Parallel execution of most control algorithms ensures short response time and deterministic behaviour;
- Simpler design process and software architecture allows reduction of development and V&V effort;
- Less vulnerability to obsolescence due to portability of HDL code between various FPGA-chips produced by different manufacturers;
- Suitability for reverse engineering of analog and digital equipment makes this technology very attractive for refurbishment applications;
- Natural cyber security resilience: the technology simply does not lend itself to virus attacks or external tampering.

Sunport

Cyber Security of FPGA technology

- There are no known viruses and malware designed to attack HDL coded configurations;
- Simple and structured design allows corresponding V&V processes to detect the presence of potential threats and malicious design more readily;
- No operating systems in which viruses could be introduced;
- Physical access to the FPGA chips strictly controlled by design: no physical access for modification while in on-line operating mode;
- Impossible to connect common storage media or communication devices that could infect the code.

Sunport

Examples of FPGA applications in the NPP industry

- Refurbishment of the Window Annunciation System, Embalse CANDU NPP, Argentina
- Signal Processing Unit, SDS2 PHT pump trip, Embalse CANDU NPP, Argentina
- Kozloduy Units 5 & 6, Bulgaria, Replacement of complete Engineered Safety Features Actuation Systems (ESFAS)
- All 4 NPP sites in Ukraine, 28 RTSs, 10 reactor power control and limitation systems, 18 ESFAS, and 4 nuclear and conventional island control were installed (2004-2015)

Sunport

Examples of FPGA applications in the NPP industry (cont…)

- Wolf Creek Plant, USA, Main Steam and Feedwater Isolation System Replacement
- BWRs and Advanced BWR, Japan, Start-up Range & Power Range Neutron Monitoring System, Radiation Monitoring Systems
- EDF 900 MW Series (34 units), France, obsolete electronic modules replaced in Rod Control System and Reactor In-Core Measurement systems (2009-2019)
- OPG, Canada: FPGA based emulators for obsolete PDP-11 computers used in fuel handling systems and DCC (Reactor Regulation Systems)
- Canada, China, USA, FPGAs are used in I&C systems of new reactor designs

Sunport

Six Categories of I&C System Diversity

1. Design diversity

- Different technologies, e.g. analog vs. digital, PLC vs. FPGA,
- Different approaches, incl. HW/SW, to solve the same problem,
- Different approaches/solutions using the same technology,
- Different architectures (arrangement and connection of components).

2. Equipment manufacturer diversity

- Different manufacturers (different or same designs),
- Same manufacturer / different designs,
- Different versions of the same design by the same manufacturer.

Note:

Diversity: Producing two or more systems of different nature for the same purpose (based on the same specification) to avoid CCF.

Sunport

Six Categories of I&C System Diversity (cont …)

3. Functional diversity

- Different underlying mechanisms in actuators (rod insertion vs. boron injection),
- Different purpose or function (normal rod control vs. reactor trip rod insertion),
- Different response time scale (secondary system may react if accident conditions persist for a time).

4. Human diversity / Life-cycle diversity

- Different design organizations,
- Different engineering management teams within the same company,
- Different designers, engineers, or programmers,
- Different testers, installers, or certification personnel.

Sunport

Six Categories of I&C System Diversity (cont …)

5. Signal diversity

- An events in the reactor manifests itself in different physical processes and variables (e.g. power increase, loss of coolant),
- A physical variable sensed by different types of sensors built on different physical effects (e.g. level measurements, temperature, flow),
- A physical variable sensed by different types of sensors, built on the same physical effects by different manufacturers (e.g. pressure measured by Rosemount, Bailey, Gould TXs),
- A physical variable sensed by a redundant set of identical sensors at various locations.

Sunport

Six Categories of I&C System Diversity (cont …)

6. Software diversity

- Different algorithms, logic, and program architecture,
- Different timing and order of execution,
- Different runtime environment, operating systems,
- Different computer languages.

Sunport

Additional Category of Digital System Diversity

Logic Processing Equipment Diversity

- Different logic processing CPU architecture (e.g. Intel 80X86 vs. Motorola 68000);
- Different logic processing CPU version in the same architecture (e.g. Intel 80386 vs. Intel 80486);
- Different component integration architecture (e.g. different printed circuit board designs)
- Different data-flow architecture (e.g. different bus structure, VME vs. Multibus II)

Sunport

Shutdown System 1 (SDS1) vs. Shutdown System 2 SDS2 systems in CANDU NPPs

- Different sets of sensors, detectors (ICFDs, ex-core ion chamber, flow and pressure TXs) for SDS1 and SDS2
- Different SDS computers and analog components (relays, comparators)
- Different cable routes, instrument rooms, and power supplies
- Different actuation systems (shut-off rods vs. gadolinium poison injection)

- Different design organizations (OPG vs. AECL)
- Different specifications and requirements (e.g. response time)
- Different maintenance teams

Sunport

Diversity Strategies using FPGA technology

- FPGA - PLC
- FPGAs based systems from different vendors
- FPGAs based systems from the same vendor with different hardware using different FPGA chips programmed with different design tools
- All six diversity categories as described in NUREG/CR-6303, can be implemented with FPGA-based systems either in combination or in lieu of CPU based I&C systems

Sunport

Diversity attribute	Type	Details
Design		
Different design solutions - same FPGA technology	ED Engineered Diversity	Two reactor trip systems (primary and diverse) based on different combinations of two digital technologies: (1) Primary system: FPGA and micro-processor; (2) Diverse system: FPGA-based only
Different architectures	ID Inherent Diversity	Inherent difference in system architectures due to technology diversity
Equipment Manufacturer		
Different manufacturers - different designs	ED	Primary and diverse systems are based on equipment of different manufacturers for which the control logic algorithms are implemented from the same specification

Sunport

Diversity attribute	Type	Details
Logic Processing Equipment		
Different logic processing architecture	ID	Primary system: Altera Cyclone FPGAs (safety related control logic) - TI MSP430 microcontrollers (communication, diagnostic and auxiliary functions) Diverse system: - Altera Cyclone FPGA to perform all functions
Different component integration architecture	ID	Inherent difference at the board level: Different circuit board designs for primary and diverse systems
Different data-flow architecture	ID	Different data exchange organization: - Between FPGA and microcontroller in the primary system - Between FPGA and FPGA in the diverse system

Sunport

Diversity attribute	Type	Details
Life-cycle		
Different management within the same company	ID	Separate design organizations to develop primary and diverse systems
Different design teams: designers, engineers, programmers	ID	Separated design teams for primary and diverse systems
Different implementation and validation teams: testers, installers, or certification personnel	ID	Separate V&V teams for primary and diverse systems

Sunport

Common-cause failures (CCFs)

IAEA / IEC definition:

Coincidental failure of two or more structures, systems or components that is caused by any latent deficiency from design or manufacturing, from operation or maintenance errors, and which is triggered by an event induced by natural phenomenon, plant process operation, or action caused by man or by any internal event in the I&C system.

Sunport

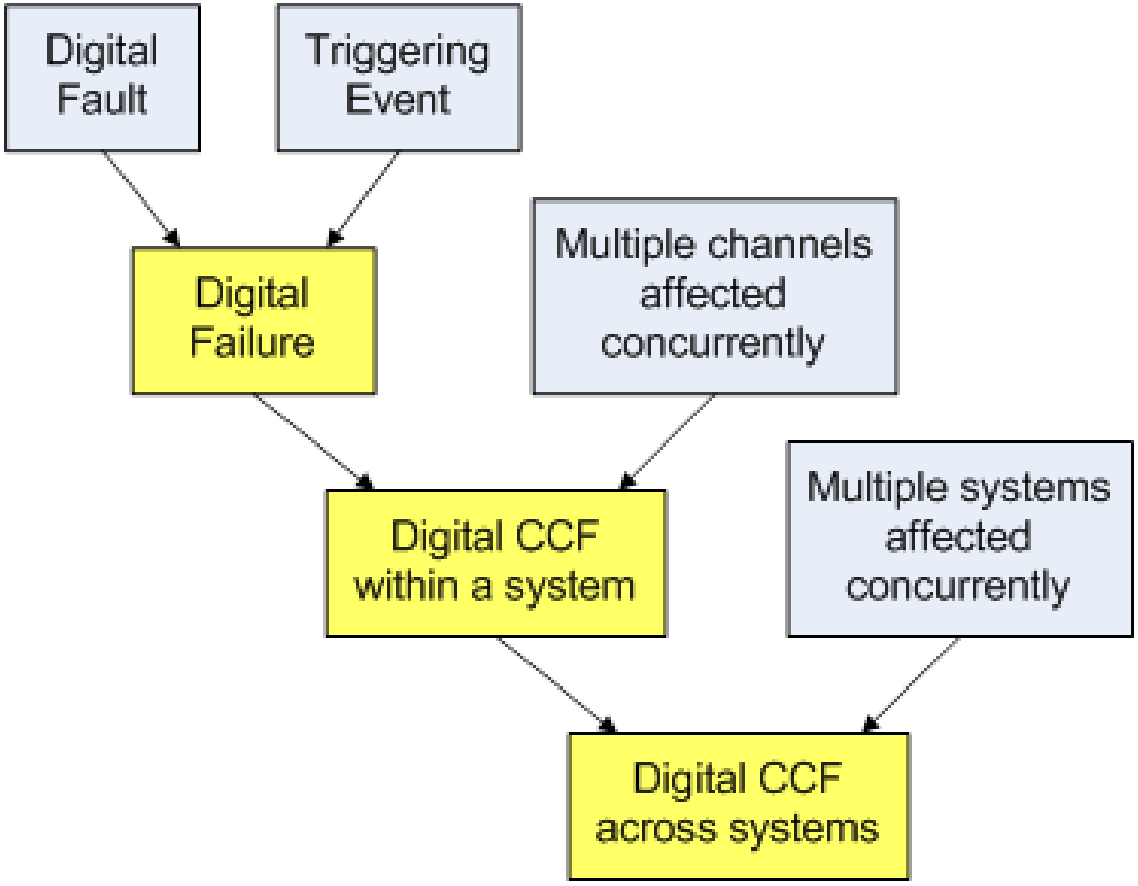
For a potentially unsafe CCF to occur, a number of conditions must be met:

- The system contains one or more latent faults (e.g. design flaw) that can cause functional failure;
- A triggering event, usually an unanticipated or untested operational condition, or an external effect, is present to activate the fault;
- Multiple channels are affected concurrently;
- The failures cause an unsafe plant condition, typically in the form of degradation or loss of a safety functions;
- To adversely affect multiple systems, those systems must share the same fault(s) and be susceptible to the same trigger concurrently.

Note: Common-mode failure (CMF) vs. Common-cause failure (CCF)
Concurrent events vs. causally related events

Sunport

Conditions required to create a digital CCF



Sunport

Potential sources of faults can occur in any of the following phases:

- Conceptual design
- Requirements specification
- Development process
- Manufacturing
- Installation and commissioning
- Post-installation modifications
- Maintenance and operation

Notes: fault / error / flaw → failure
V&V and QMS

Triggering mechanisms:

Human actions, Signal trajectory, External events, Temporal effects

Sunport

Defence in Depth in I&C Systems Hierarchy

Lines of Defence: Four independent I&C Systems

1. Control system — The control line of defence consists of non-safety equipment which routinely prevents reactor excursions toward unsafe regimes of operation, and is used for normal operation of the reactor.

2. RTS – The reactor trip line of defence consists of safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.

Note: prevention vs. mitigation
safety vs. non-safety systems

Sunport

Defence in Depth in I&C Systems Hierarchy (cont …)

Lines of Defence: Four independent I&C Systems

3. ESFAS – The ESFAS line of defence consists of safety equipment which removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (fuel cladding, reactor vessel, and containment).

4. Monitoring and indicators – The monitoring and indication line of defence consists of sensors, displays, data communication systems and manual controls required for operators to respond to reactor events (emergency response).

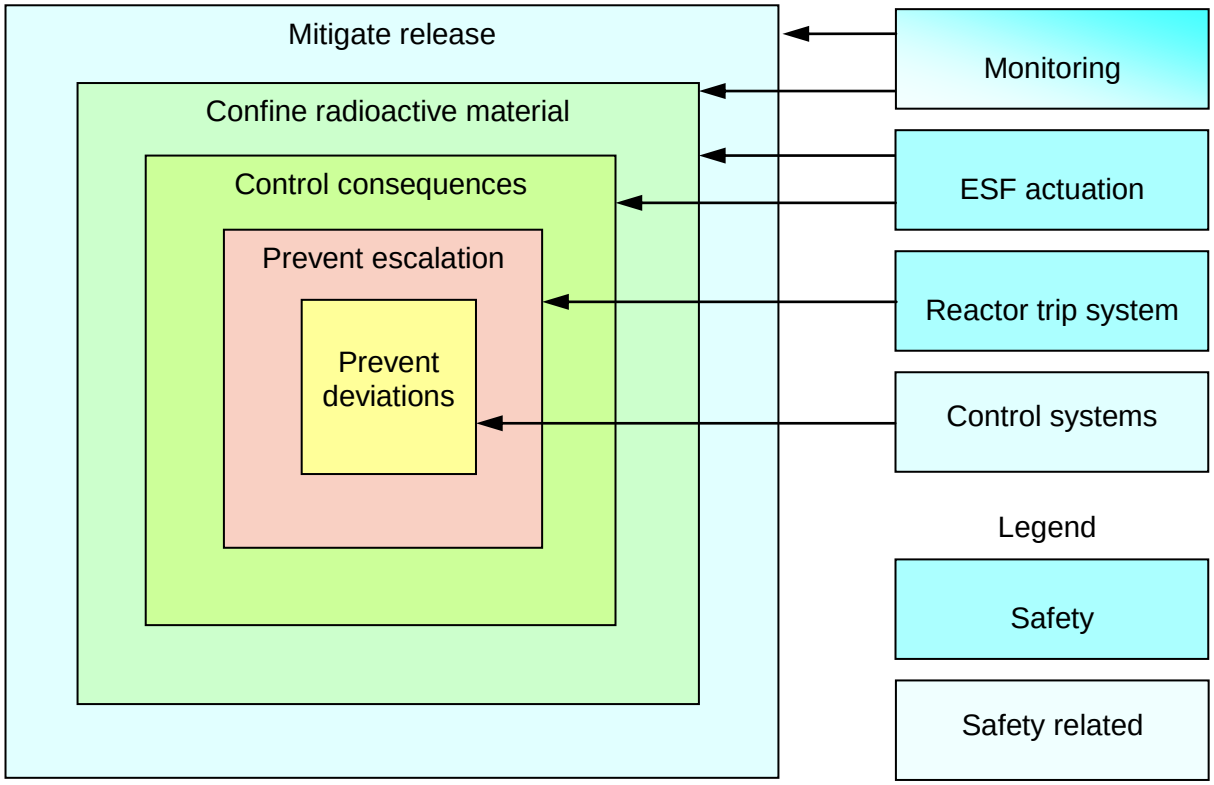
Note: prevention vs. mitigation
safety vs. non-safety systems

ESFAS: Engineered Safety Features Actuation System

Actuation of emergency core cooling, pressure relief valves, containment spray pumps, containment isolation valves, emergency generators

Sunport

Typical I&C system relationship to plant Defence in Depth



Sunport

Defence in Depth in I&C Systems

Independence between Lines of Defence (the four I&C Systems):

- Functional, design, human and operational diversity, and no data communication is applied to prevent CCFs of multiple Lines of Defence.

Independence of Sub-Systems within the same Line of Defence (an I&C System):

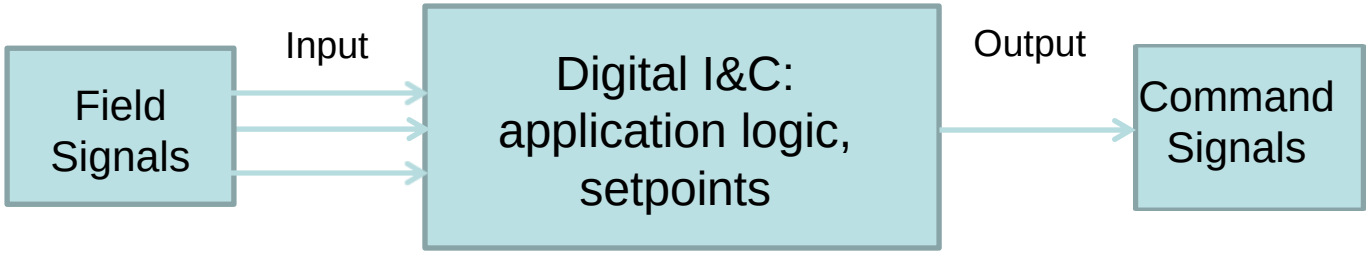
- Functional, human and operational diversity, and no data communication is applied to prevent CCFs of Sub-Systems within the same I&C System, in complement to lack of design diversity (same equipment used in the Sub-Systems).

Independence of redundant channels within the same Sub-System of an I&C System:

- Human and operational diversity is applied to prevent CCF in redundant channels, in complement to lack of design & functional diversity.

Sunport

Single-channel I&C system

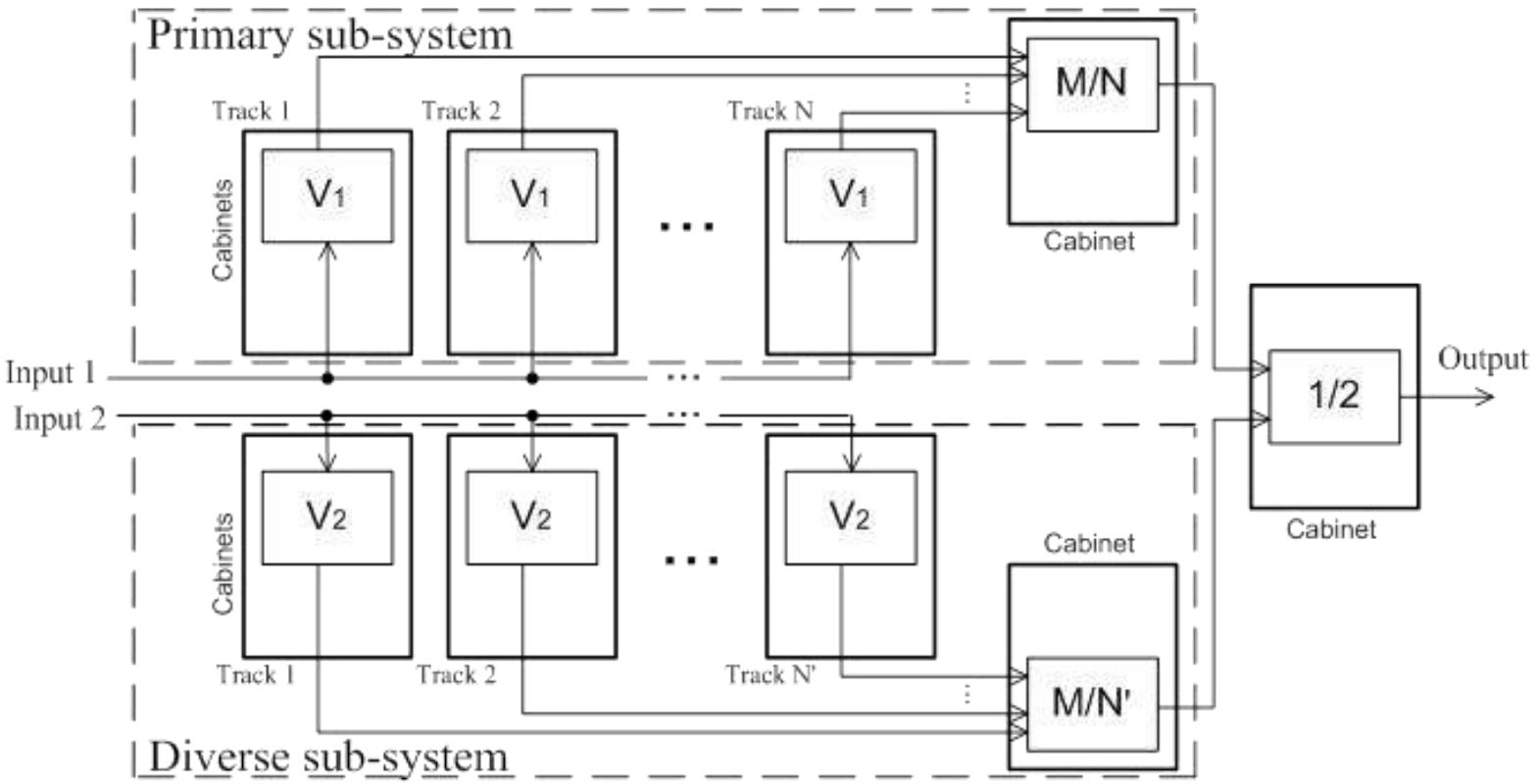


Susceptible to Single Failure (SF):

An occurrence which results in the loss of capability of a component to perform its intended safety functions.

Sunport

Possible solution for SF and CCF: diversity and redundancy



Sunport

Concern

Increased redundancy and diversity in I&C system architecture leads to increase in:

- Complexity,
- Communication,
- Maintenance tasks,
- Spare parts inventory,
- Space needed,
- Power consumption,
- Configuration management needs,
- Licensing burden.

Sunport

Summary

- FPGA-based systems are viable alternatives to microprocessor-based or analog hardware systems.
- The FPGA world is diverse enough to meet all D3 requirements for safety I&C systems.
- The described advantages make the FPGA-based technology an attractive option for modernization and new-built projects.