



ASSESSMENT OF MAJOR SYSTEMS I&C AND ELECTRICAL SYSTEMS

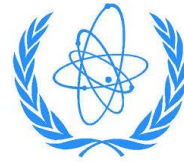
Joint ICTP-IAEA Essential Knowledge Workshop on Deterministic Safety
Assessment and Engineering Aspects Important to Safety

12–23 October 2015
Trieste, Italy

Ales KARASEK



I&C AND ELECTRICAL SYSTEMS INTRODUCTION




Ales Karasek

I&C Design Engineer
CEZ, NPP Dukovany

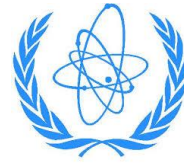
ales.karasek@cez.cz

<http://www.linkedin.com/in/karaseka>



- **10+ years in NPP I&C Engineering** (I&C upgrades, modification, operation support, preventive maintenance plans, cyber security,...)
- **CISSP** (January 2015)  Certified Information Systems Security Professional
- **IAEA I&C Safety Guide Working Group** (December 2011 – December 2012)
- **Digital I&C Cyber Security Program** (January 2010 – Present)
- **NPP Dukovany Plant Control I&C Systems Refurbishment** (January 2009 – Present)
- **NPP Dukovany Safety I&C Systems Refurbishment** (February 2002 – December 2009)

I&C AND ELECTRICAL SYSTEMS OVERVIEW



The **instrumentation and control (I&C)** system architecture, together with plant operations personnel, serves as the '**central nervous system**' of a nuclear power plant (NPP).

The **I&C system** architecture of a NPP provides the functionality to **control or limit plant conditions for normal or abnormal operation and to achieve a safe shutdown state** in response to adverse operational events (e.g., incidents or accidents).

I&C system can significantly **impact cost competitiveness** of the NPP (e.g. reliability and availability, enhanced power production, O&M costs).

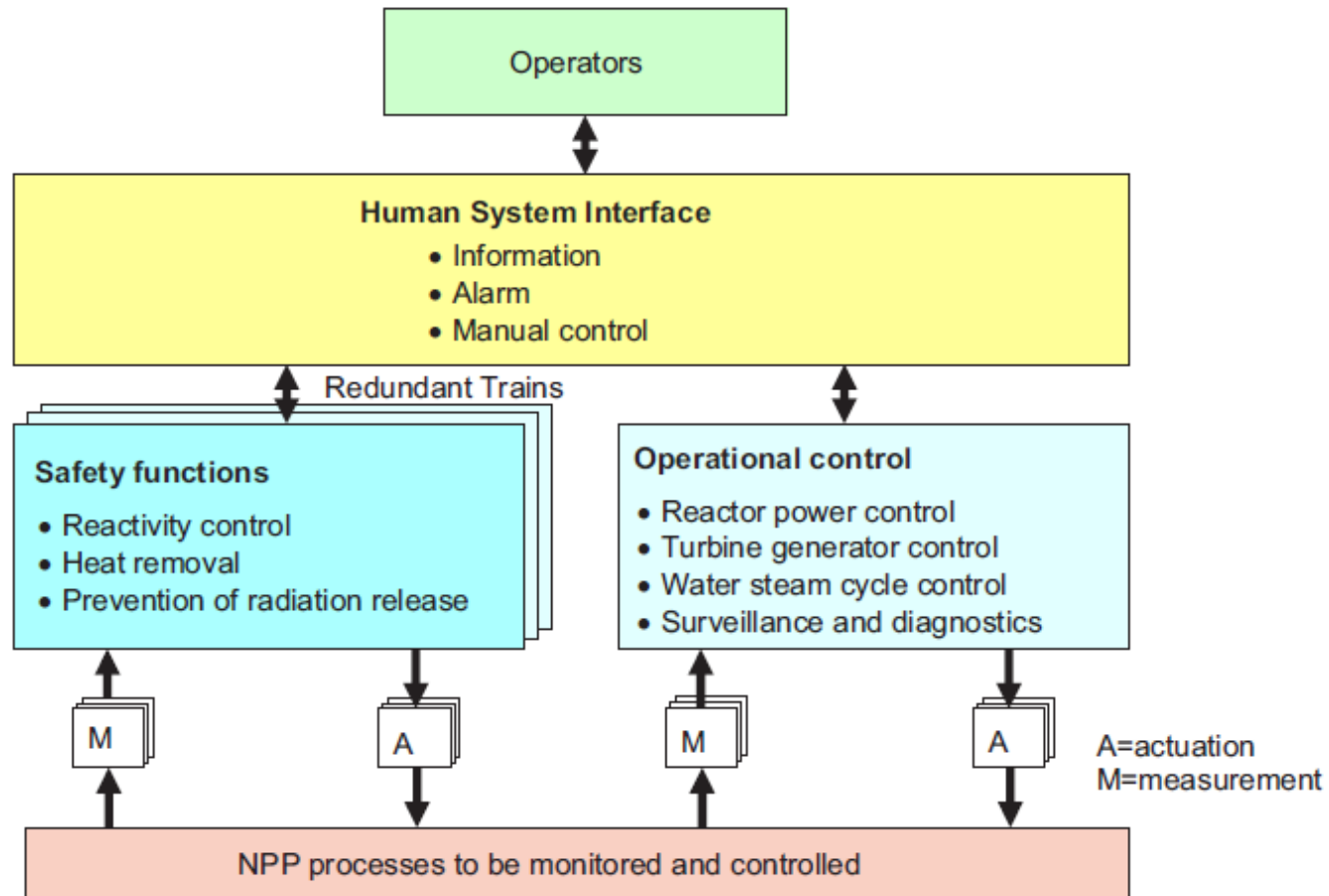
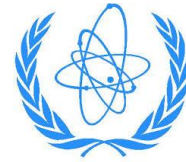
[IAEA NP-T-3.12]

Electrical systems that supply power to systems important to safety **are essential to the safety** of nuclear power plants.

[DS-430, 1.5]

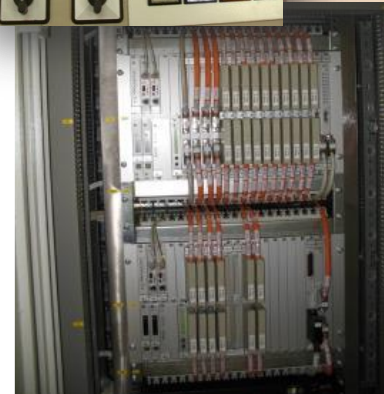
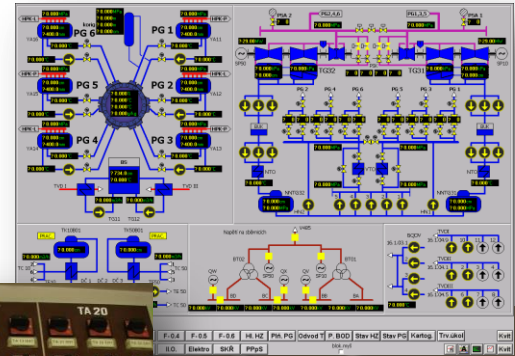
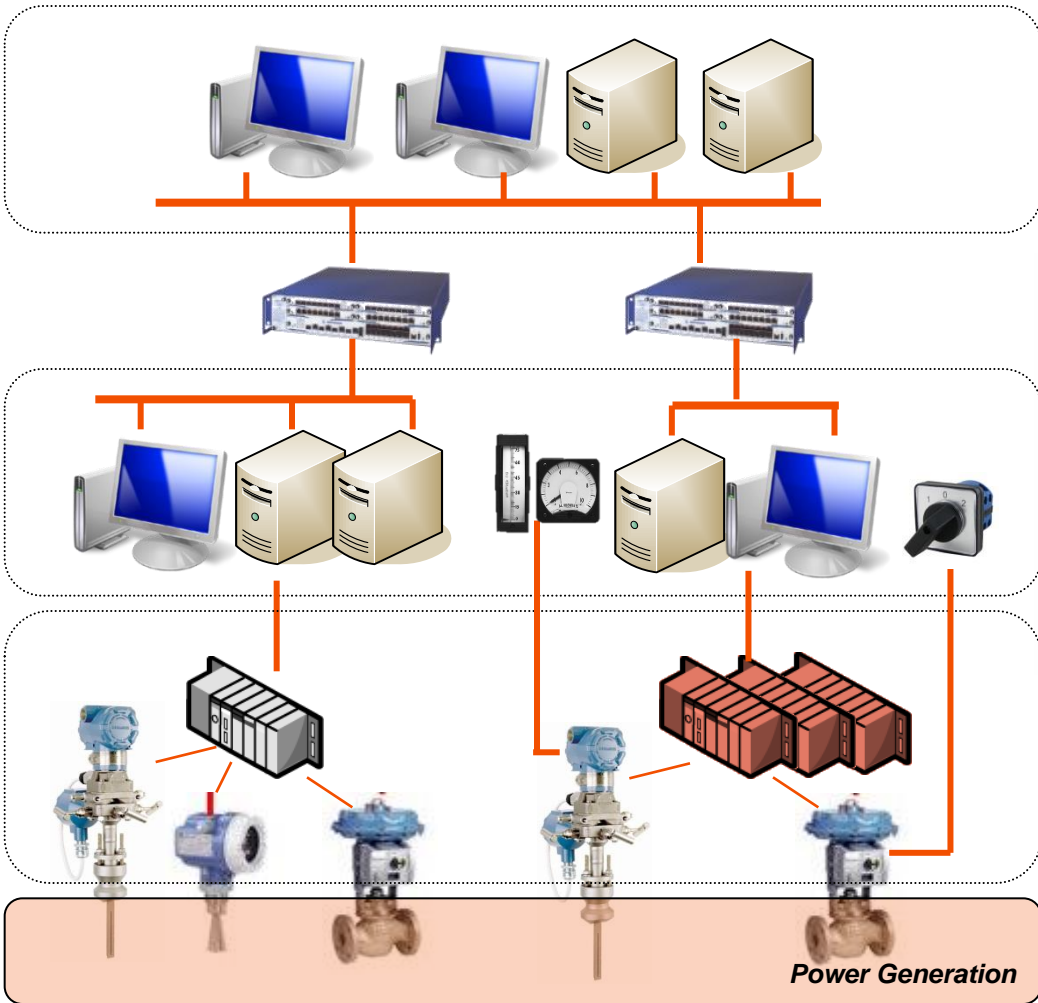
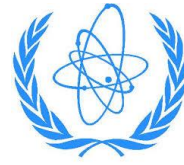
I&C AND ELECTRICAL SYSTEMS

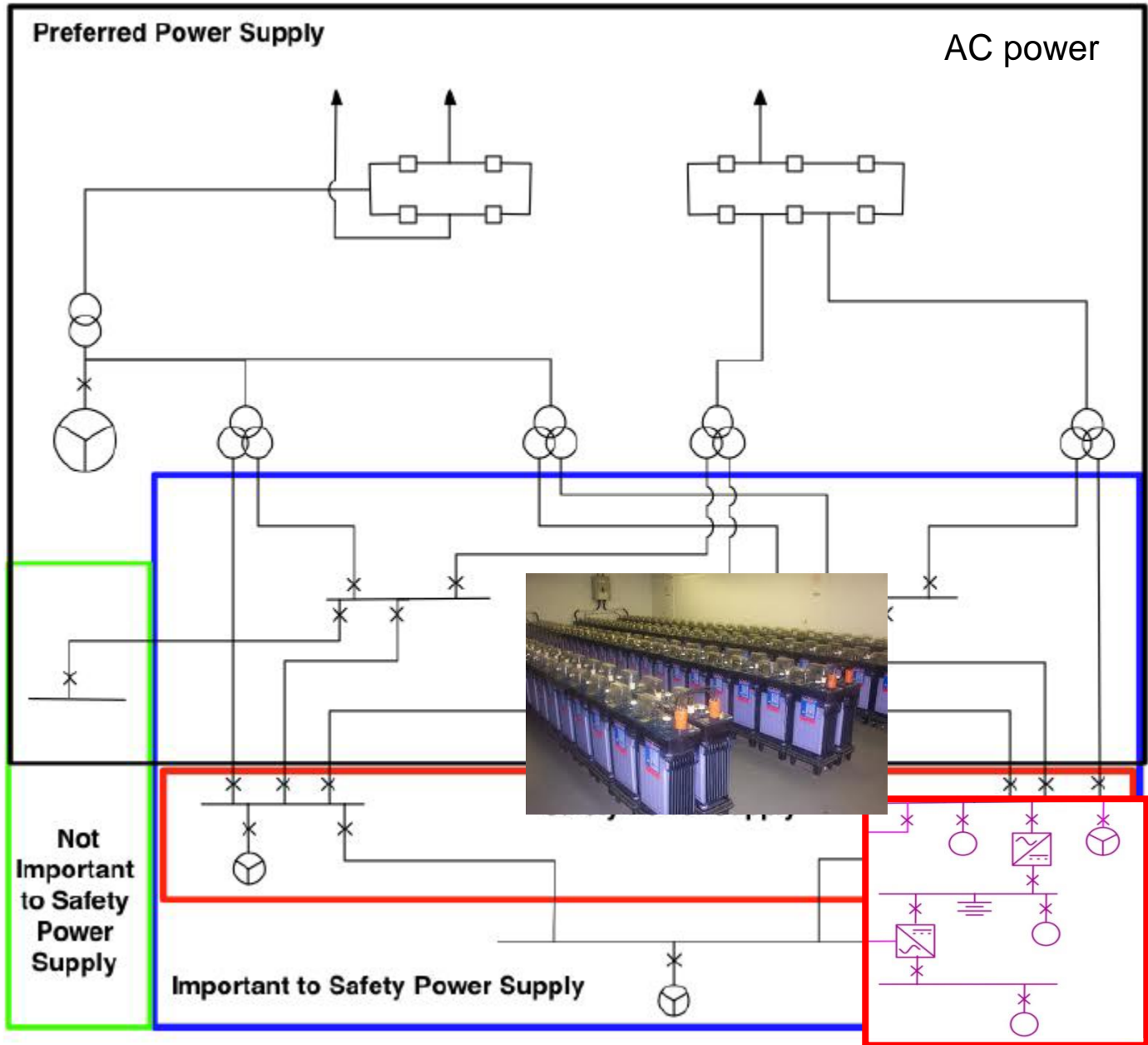
I&C OVERVIEW



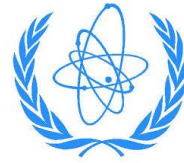
[IAEA NP-T-3.12]

I&C AND ELECTRICAL SYSTEMS ARCHITECTURE OVERVIEW





I&C AND ELECTRICAL SYSTEMS SAFETY CLASSIFICATION



SSR 2/1 Requirement 22: **All items** important to safety shall be **identified** and shall be **classified** on the basis of their function and their safety significance.

SSR 2/1 Requirement 23: The **reliability** of items important to safety shall be **commensurate with their safety significance**.

SSR 2/1 Requirement 62: Instrumentation and control systems for items important to safety at the nuclear power plant shall be **designed for high functional reliability** and periodic testability **commensurate with the safety function(s)** to be performed.

Power supplies for I&C systems ... should have classification, reliability provisions, qualification ... consistent with the reliability requirements of the I&C systems they serve.

[DS-431, 7.62]

Plant equipment

Items important to safety

Items not important to safety

Safety related items or systems

Safety systems

Protection system

Safety actuation system

Safety system support features

Initiation I&C for:
Reactor trip
Emergency core cooling
Decay heat removal
Confinement isolation
Containment spray
Containment heat removal

Actuation I&C for:
Reactor trip
Emergency core cooling
Decay heat removal
Confinement isolation
Containment spray
Containment heat removal

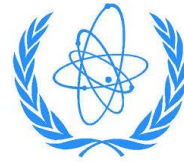
Emergency power supply
Control room habitability
Safety equipment heating and cooling

Reactor control systems
Specific plant control systems
Control room I&C
Fire detection and extinguishing I&C
Radiation monitoring
Emergency control centre I&C
Communication equipment
Fuel handling and storage I&C
I&C associated with the operation of the safety system
I&C for monitoring the state of the safety system
Access control systems.

National or international standard	Classification of the importance to safety			
IAEA NS-R-1	Systems Important to Safety			Systems Not Important to Safety
	Safety	Safety Related		
IEC 61226 Functions Systems	Systems Important to Safety			Unclassified
	Cat. A Class 1	Cat. B Class 2	Category C Class 3	
Canada	Category 1	Category 2	Category 3	Category 4
France N4	1E	2E	SH Important to Safety	Systems Not Important to Safety
European Utility Requirements	F1A (Auto.)	F1B (Auto. and Man.)	F2	Unclassified
Japan	PS1/MS1*	PS2/MS2	PS3/MS3	Non-nuclear Safety
Rep. of Korea	IC-1		IC-2	IC-3
Russian Federation	Class 2	Class 3		Class 4 (Systems Not Important to Safety)
Switzerland	Category A	Category B	Category C	Not important to safety
UK Functions Systems	Cat. A Class 1	Cat. B Class 2	Category C Class 3	Unclassified
USA and IEEE	Systems Important to Safety			Non-nuclear Safety
	Safety Related, Safety, or Class 1E	(No name assigned)		

I&C AND ELECTRICAL SYSTEMS

DEFENCE IN DEPTH

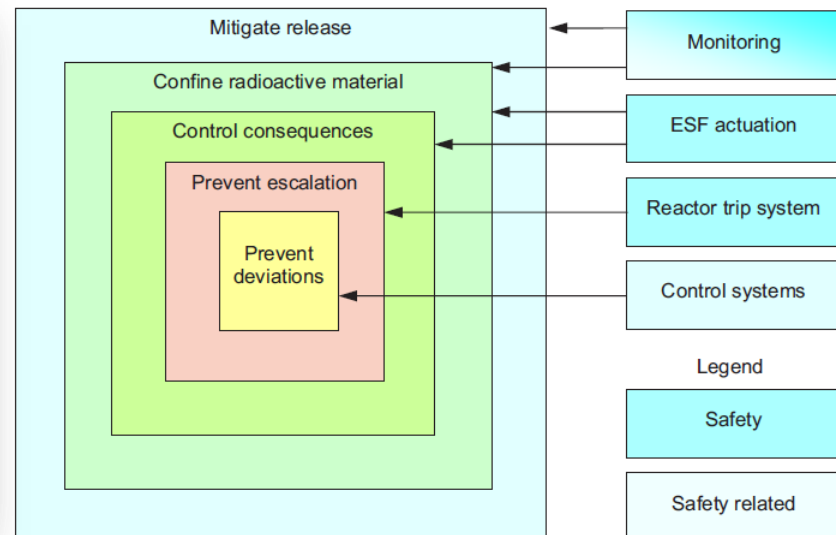


SSR 2/1 Requirement 7: The **design of a nuclear power plant shall incorporate defence in depth**. The levels of defence in depth shall be independent as far as is practicable.

The overall I&C architecture should define the defence-in-depth and diversity strategy to be implemented within the overall I&C. [DS-431, 4.9]



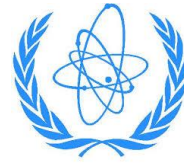
[Fort Bourtange, Netherlands]



[NP-T-3.12]

I&C AND ELECTRICAL SYSTEMS

DEFENCE IN DEPTH



Design Extension Conditions

DEC-A

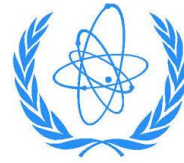
DEC-B

	Design Basis Events			Beyond Design Basis Accidents	
Normal Operation	Anticipated Operational Occurrence	Design Basis Accidents	Other Accidents Encompassed by the Design Basis Accidents	Beyond Design Basis Accidents that do not Result in Significant Core Damage	Severe Accidents (Significant Core Damage)

Levels of Defense in Depth	Associated Plant Conditions	Objective	Essential Means	
			Systems (Additive ¹)	Human Role ²
Level 1	Normal operation, with plant conditions remaining within normal operating limits	Prevention of abnormal operation and failures	Control systems ³ used to maintain plant within normal operating limits, associated indications, SPDS, and other surveillance features	Monitor and, if necessary, take control actions to maintain plant parameters within defined limits using normal operating procedures (NOPs ⁴); monitor plant safety status; monitor safety system availability; perform maintenance and surveillance tests per surveillance test procedures (STPs)
Level 2	Anticipated operational occurrences (AOOs), with plant conditions remaining within reactor trip limits	Control of abnormal operation and failures to avoid exceeding reactor trip limits	Limitation systems ⁵	Perform actions specified by abnormal operating procedures (AOPs ⁴); monitor and control plant parameters to within reactor trip limits; monitor critical safety functions; monitor safety system availability; perform manual shutdown if required
Level 3	Level 3.a Postulated single initiating events ⁶	Control of event to limit radiological releases and prevent escalation to core melt conditions	Reactor protection system, auxiliary supporting systems, post-accident monitoring instrumentation	Perform manual actions credited in the safety analysis and prescribed in emergency operating procedures (EOPs); monitor critical safety functions; select and implement manual safety and non-safety success paths as required per EOPs
	Level 3.b Postulated multiple failure events		Diverse manual and automatic actuation systems and associated indications, other safety features needed for postulated multiple failure events (risk reduction systems)	Perform manual actions to mitigate consequences of the event (e.g., actions credited in a Diversity and Defense in Depth or D3 analysis)

I&C AND ELECTRICAL SYSTEMS

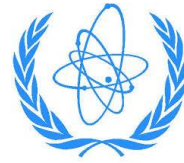
DEFENCE IN DEPTH



Levels of Defense in Depth	Associated Plant Conditions	Objective	Essential Means	
			Systems (Additive ¹)	Human Role ²
Level 4	Postulated core melt accidents (short and long term)	Control of accidents that result in core melt, to limit off-site releases	Additional safety features provided specifically to mitigate core melt accidents	Perform actions to mitigate consequences of core melt per Severe Accident Management (SAM) guidelines; perform post-accident monitoring for radioactivity releases
Level 5	-	Mitigation of radiological consequences of significant releases of radioactive material	Off-site emergency response Intervention levels	

I&C AND ELECTRICAL SYSTEMS

DEFENCE IN DEPTH



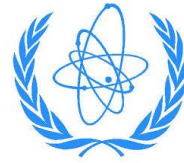
Level	Electrical System
Prevention of abnormal operation and failures	Robust and reliable grid , robust and reliable onsite power systems
Control of abnormal operation	Power supply transfer capability, house-load operation possibilities
Control of accidents within the design basis	Robust and reliable safety power systems (batteries) and onsite standby AC power supplies
Control of severe plant conditions	Robust and reliable alternate AC power supply
Mitigation of radiological consequences	Off-site emergency response

The electrical power systems are support systems necessary for all levels of defence in depth.

[DS-430, Annex I]

I&C AND ELECTRICAL SYSTEMS

DEFENCE IN DEPTH - SBO

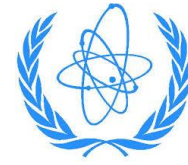


A station blackout (SBO): loss of the preferred power supply concurrent with a turbine trip and unavailability of the emergency AC power system.

The plant's capability to **maintain fundamental safety functions** and to remove decay heat from spent fuel should be analysed for the period that the plant **is in a blackout condition**.

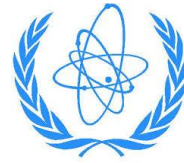
- Increasing the **capacity of batteries** to supply power to safety instrumentation and control equipment, and to other vital equipment;
- Use of **unit to unit connections**;
- Installing an **alternate AC power source** that is **diverse** in design and **protected** from elements that can degrade the normal and standby power sources.

I&C AND ELECTRICAL SYSTEMS DEFENCE IN DEPTH - SBO



I&C AND ELECTRICAL SYSTEMS

SIMPLICITY



Unnecessary **complexity should be avoided** in the design of I&C safety systems.

All features of I&C safety systems should be beneficial to their safety functions.

The intent of avoiding complexity is to keep the I&C system **as simple as possible** but still fully implement its safety requirements.

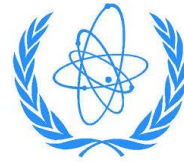
[DS-431, 6.2-6.5]

The use of software or complex multi-element logic modules might create difficulty in justification of reliability and sensitivity to common cause failures.

[DS-430, 5.92]

I&C AND ELECTRICAL SYSTEMS

SINGLE FAILURE CRITERION



SSR 2/1 Requirement 25: The **single failure criterion** shall be applied to each safety group incorporated in the plant design.

Each **safety group should perform all actions** required to respond to a PIE in the **presence** of the following:

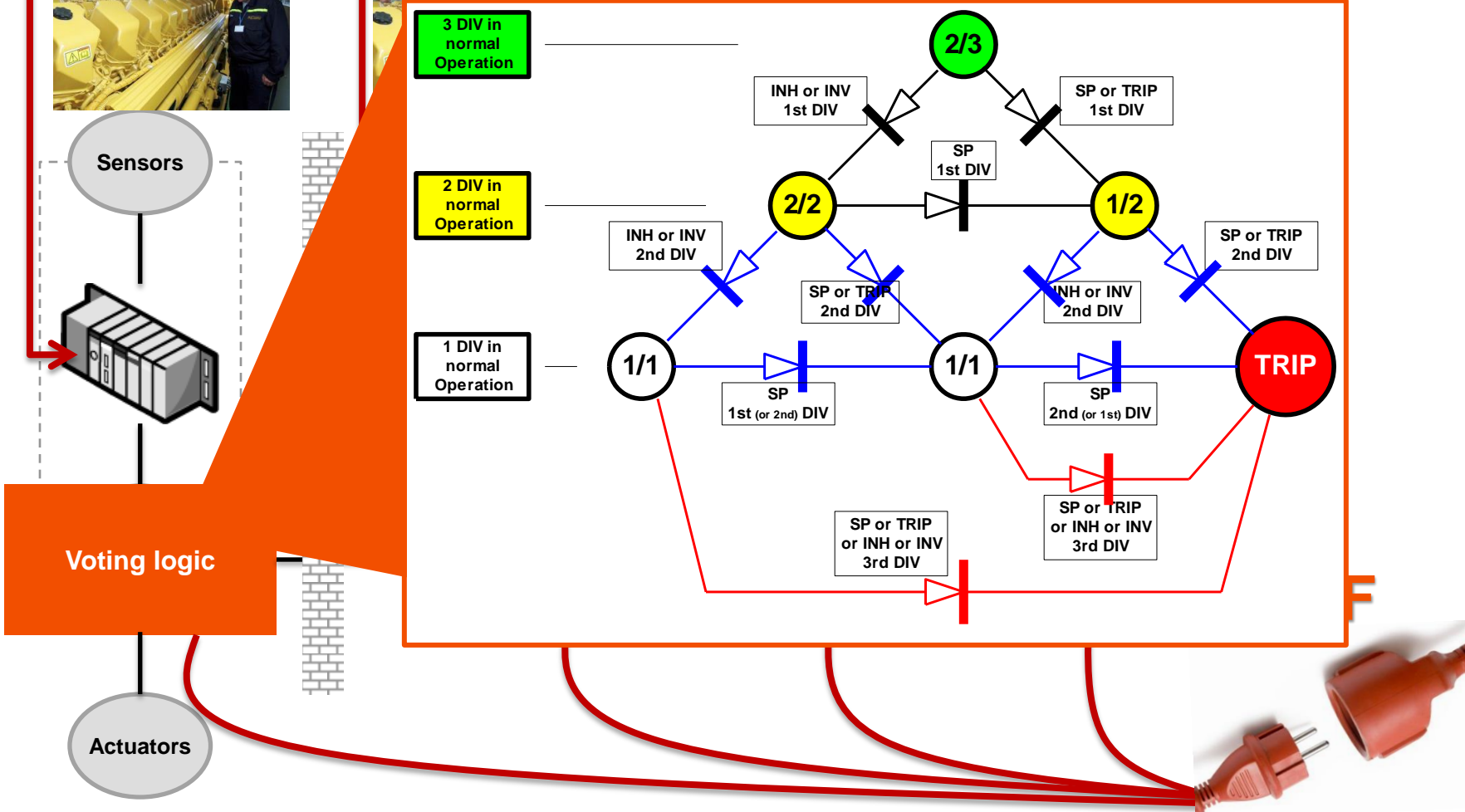
- **Any single detectable failure** within the safety system in combination with:
- All failures caused by the single failure,
- All failures and spurious system actions that cause, or are caused by, the design basis event requiring the safety group, and
- The removal from service or bypassing of divisions of safety system for testing or maintenance that is allowed by plant operating limits and conditions.

[DS-431, 6.13 9 / DS-430, 7.24]

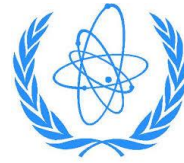
Normally concepts such as **redundancy**, **independence**, **testability**, continuous **monitoring**, environmental **qualification**, and **maintainability** are employed to achieve compliance with the single failure criterion.

[DS-431, 6.12]

I&C CENTRALIZATION REDUNDANCY



I&C AND ELECTRICAL SYSTEMS REDUNDANCY



I&C systems should be **redundant to the degree needed to** meet the I&C **reliability requirements** (including conformity with the single failure criterion).

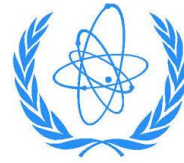
- Redundancy is not fully effective unless the redundant elements are also independent.
- Redundancy increases the reliability, but it also increases the probability of spurious operation.

[DS-431, 6.21, 6.22]

Electrical systems important to safety should be **redundant to the degree necessary to** meet design basis **reliability requirements**.

[DS-430, 5.15]

I&C AND ELECTRICAL SYSTEMS INDEPENDENCE



SSR 2/1 Requirement 21: **Interference between safety systems or between redundant elements of a system shall be prevented** by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate.

Physical separation

- Protects against common cause failure due to the effects of internal hazards. Internal hazards of concern include fire, missiles, steam jets, pipe whip, chemical explosions, flooding, and failure of adjacent equipment;

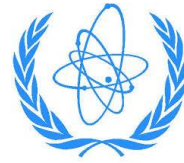
[DS-431, 6.31 / DS-430, 5.32]

Electrical isolation

- Electrical isolation is used to prevent electrical failures in one system from affecting connected systems, or redundant elements within a system.

[DS-431, 6.39 / DS-430, 5.38]

I&C AND ELECTRICAL SYSTEMS INDEPENDENCE

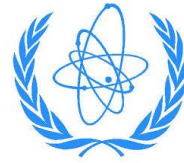


Functional independence and independence of communication

- Functional independence is a condition that exists when successful completion of a system's required functions is not dependent upon any behaviour including failures and normal operation of another system, or upon any signals, data, or information derived from the other system.
- Inputs from I&C systems of lower safety classification should not adversely affect the ability of safety systems to perform their safety functions.
- The communication of data between safety systems and systems of a lower safety classification should be designed so that no credible failures in the lower class systems will prevent any connected safety system from accomplishing its safety functions.
- The communications of data between redundant elements of a safety group should be designed so that no credible failures in the sending element will prevent the connected elements from meeting their requirements.

[DS-431, 6.45-6.52]

I&C AND ELECTRICAL SYSTEMS INDEPENDENCE



Physical separation should be provided between:

- Cables classified as safety and cables of a lower safety classification;
- Cables belonging to different safety divisions; and
- Cables of different voltage classes.

Physical separation should be provided between cables in the following voltage classes:

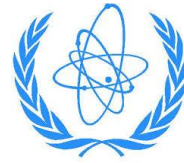
- Instrumentation and control cables;
- Low voltage power cables (1 kV or less);
- Medium voltage power cables (20 kV or less); and
- High voltage power cables (greater than 20 kV)

[DS-430 5.128-5.130]



I&C AND ELECTRICAL SYSTEMS

COMMON CAUSE FAILURE



SSR 2/1 Requirement 24: **The design** of equipment **shall take due account of the potential for common cause failures** of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.

Common cause failure (CCF): Failure of **two or more** structures, **systems** or components **due to a single event** or cause.

[DS-431]

CCF might happen because of human errors, errors in the development or manufacturing process, failure propagation between systems or components, or inadequate specification, qualification for, or protection against, internal or external hazards etc.

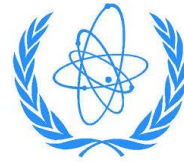
[DS-431, 4.27]

Because of the complexity of software-based systems and associated inability to execute exhaustive testing, there is an increased concern that the potential for latent systematic faults is greater.

[IAEA NP-T-3.12]

I&C AND ELECTRICAL SYSTEMS

COMMON CAUSE FAILURE



Although the terms **common mode** and **common cause** are sometimes used interchangeably, they have different meanings.

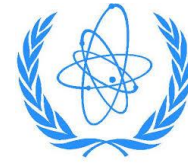
Mode = manner in which a component fails.

Cause = event or condition that produces the failure.

Cause produces degradation and, ultimately, failure in one or another mode.



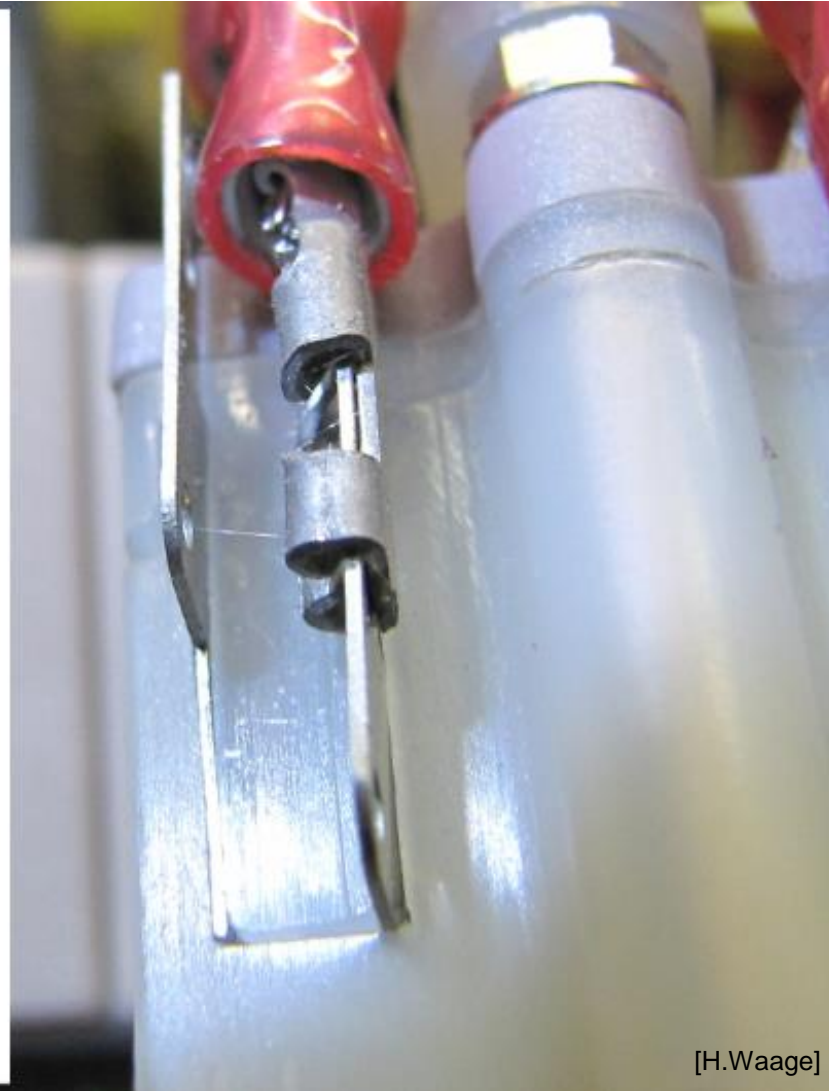
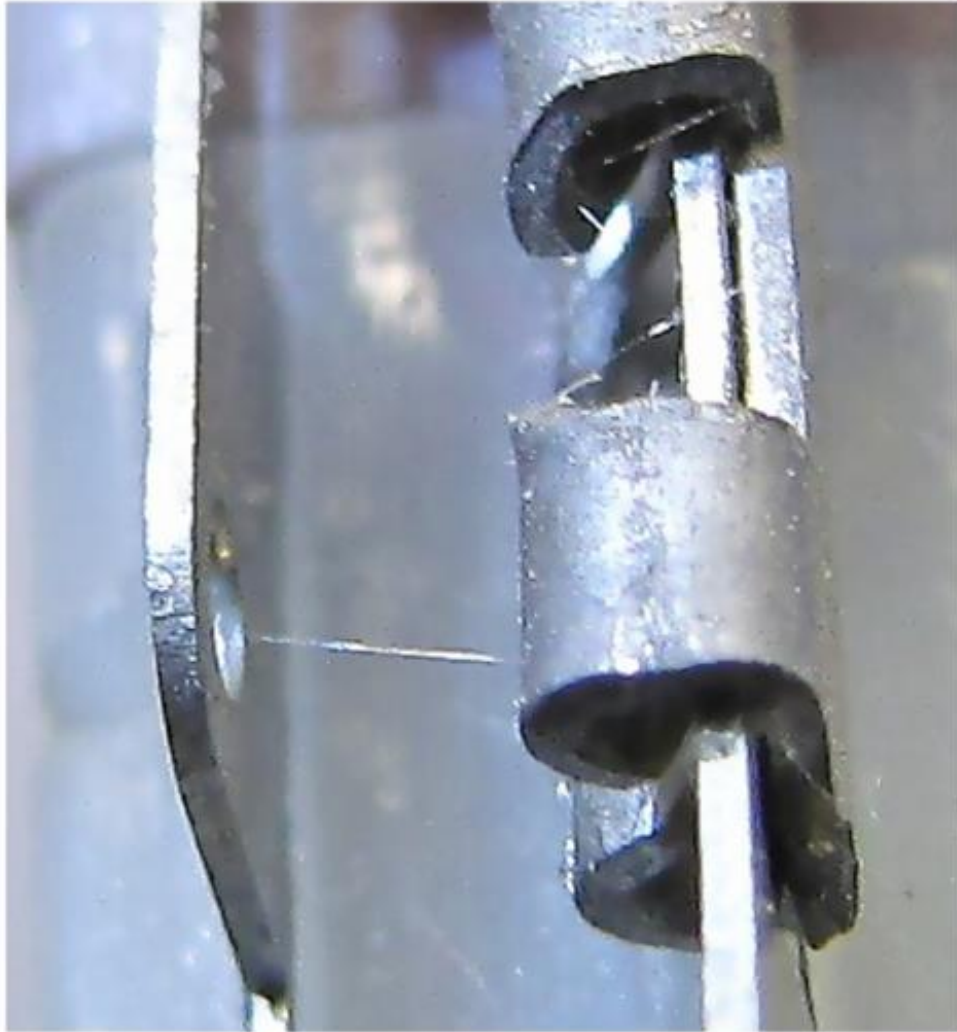
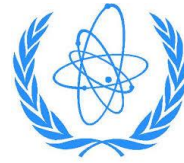
I&C AND ELECTRICAL SYSTEMS COMMON CAUSE FAILURE



[www.telegraph.co.uk]

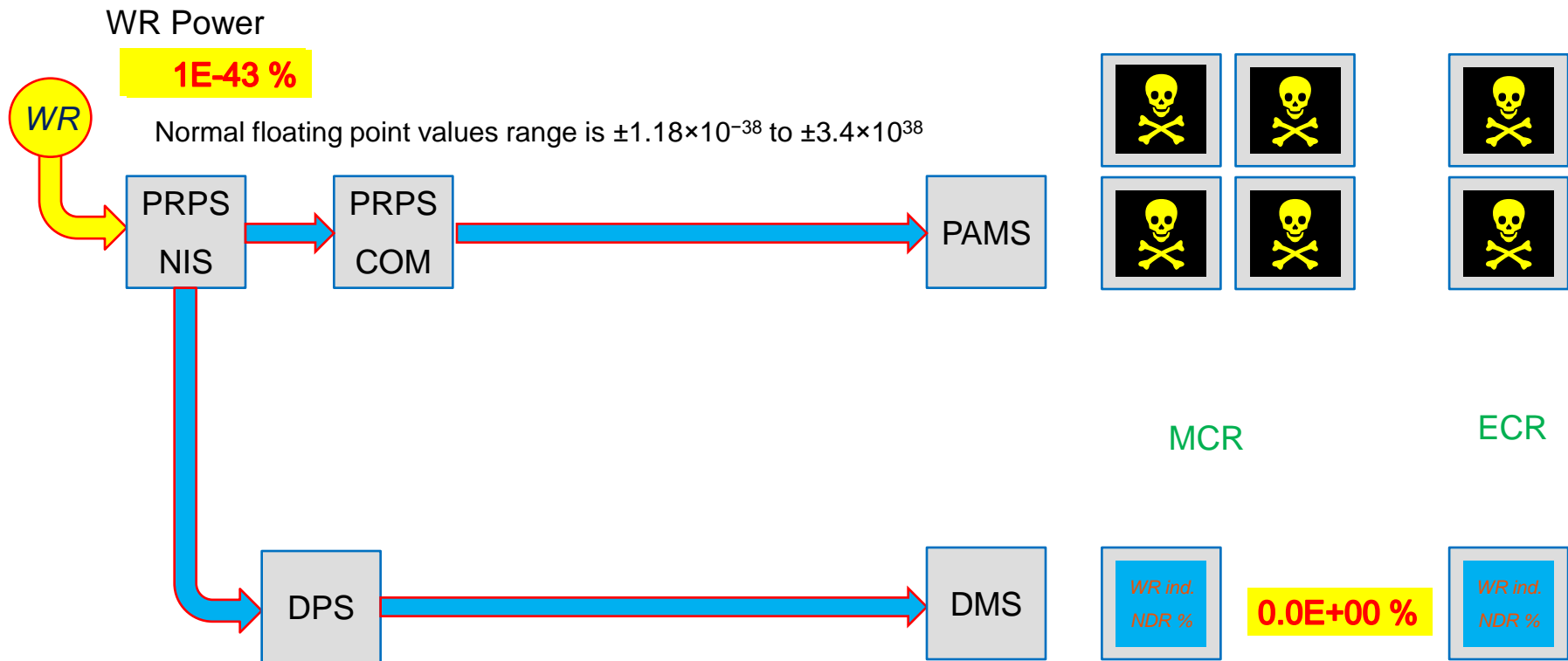
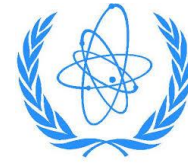
[<http://web.ard.de/>]

I&C AND ELECTRICAL SYSTEMS COMMON CAUSE FAILURE



[H.Waage]

I&C AND ELECTRICAL SYSTEMS COMMON CAUSE FAILURE

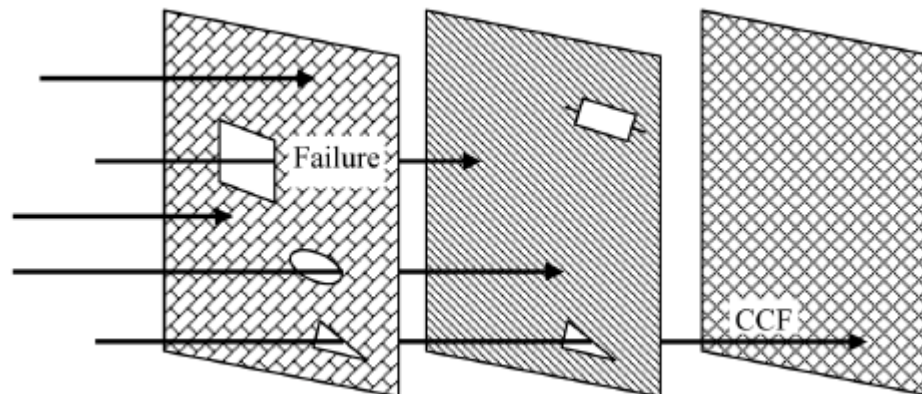
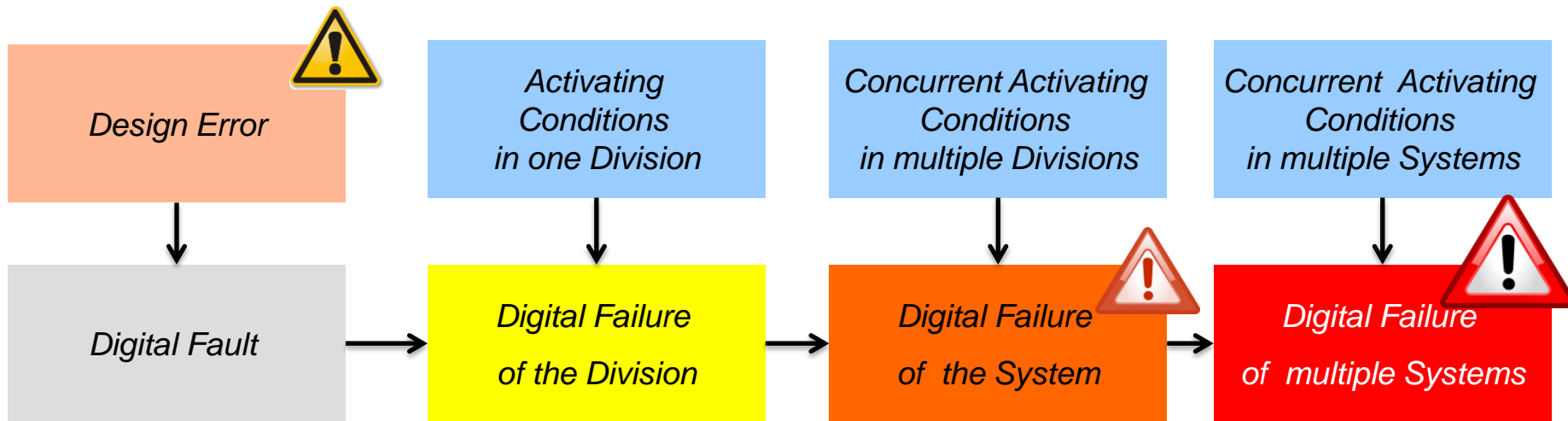
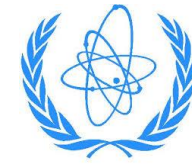


NIS – Nuclear Instrumentation System
 COM – Communication System
 WR – Wide Range
 PAMS – Post Accident Monitoring System

NDR – Numerical Digital Readout
 MCR – Main Control Room
 ECR – Emergency Control Room
 DMS – Diverse Monitoring System

[H.Waage]

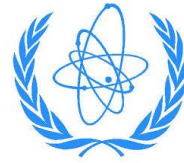
I&C AND ELECTRICAL SYSTEMS COMMON CAUSE FAILURE



[EPRI 1019182, 2010]

I&C AND ELECTRICAL SYSTEMS

COMMON CAUSE FAILURE



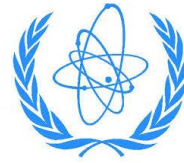
How to reduce CCF vulnerability:

- Independence (physical separation, electrical isolation, functional independence)
- Diversity (...)
- Qualification (internal and external hazards)

- Fault avoidance (high quality development process)
- Fault detection and removal (verification and validation, product testing and simulation, design reviews and analyses, operational experience)
- Fault tolerance (fail-safe design preventing the propagation of failures)

I&C AND ELECTRICAL SYSTEMS

COMMON CAUSE FAILURE

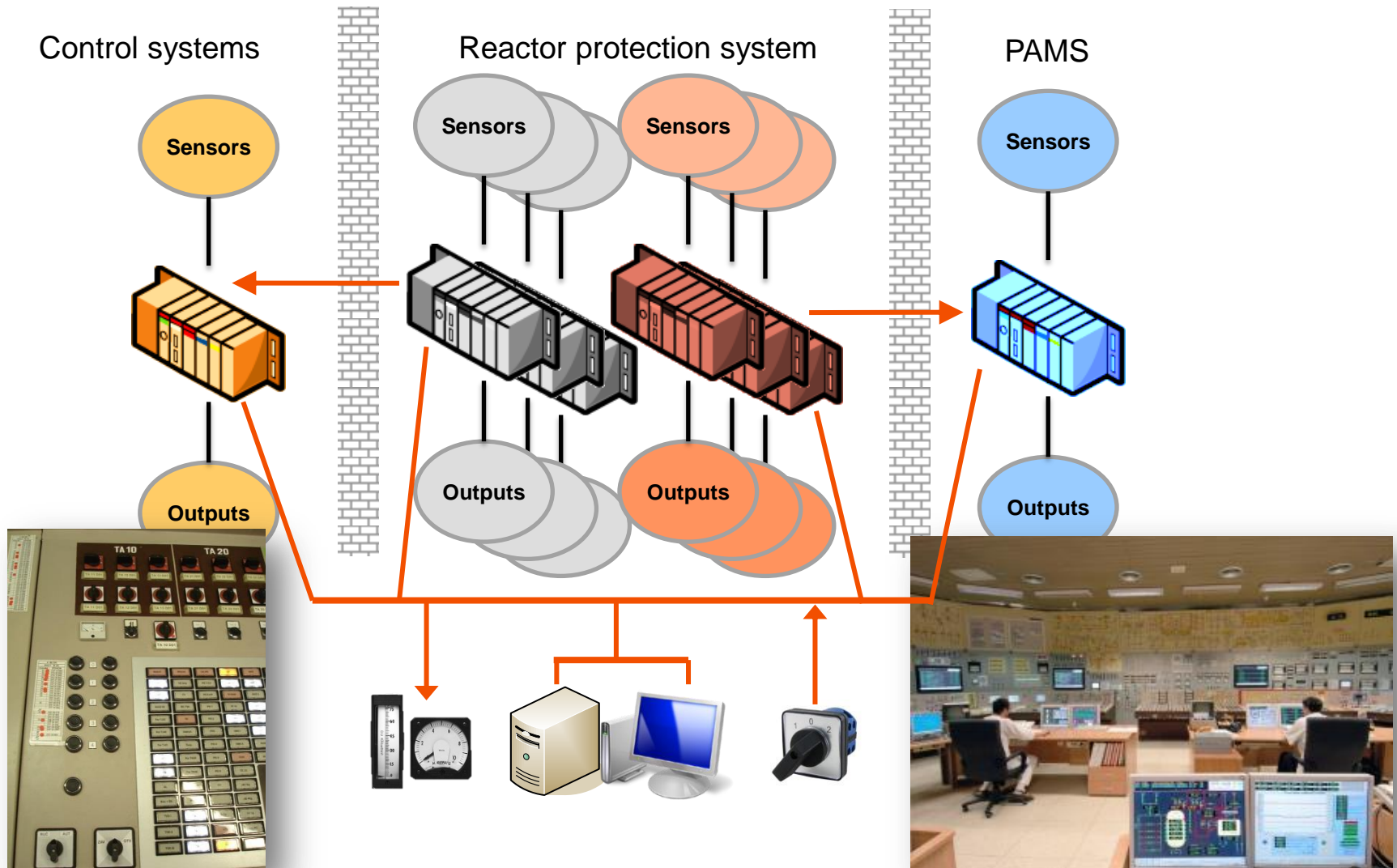
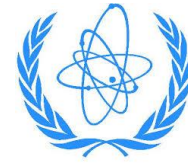


Where diversity is provided to cope with the potential for CCF, the use of more than one type of diversity should be considered.

- **Functional diversity:** achieved by systems that take different actions to achieve the same safety intent;
- **Signal diversity:** achieved by systems in which a safety action may be initiated based upon the value of different plant parameters;
- **Design diversity:** achieved by using different design approaches to solve the same or a similar problem;
- **Equipment diversity:** achieved by hardware that employs different technology (e.g., analogue vs. digital, solid-state vs. electromagnetic, computer-based vs. FPGA-based);
- **Human diversity:** achieved by using different design personnel;
- **Logic diversity** (including software diversity): achieved by using different programs using, for example, different programmers, languages, methods, or tools.

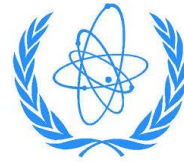
[DS-431, 6.61-6.62]

I&C AND ELECTRICAL SYSTEMS COMMON CAUSE FAILURE



I&C AND ELECTRICAL SYSTEMS

COMMON CAUSE FAILURE



Diversity in power sources is usually inherent in the architectural design of the power system.

Typically safety power system loads can be supplied from:

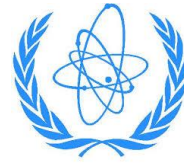
- The **off-site power** system, via the preferred power supply;
- The **main generator**, which is the normal power source and in-house load scenarios will supply power;
- The **standby power source**, which will supply the safety power systems on loss of off-site power;
- **Alternate AC power** source during station blackout conditions.

DC loads can be supplied from **batteries** or from any of the above sources.

[DS-430, 5.54-5.56]

I&C AND ELECTRICAL SYSTEMS

FAIL-SAFE DESIGN



SSR 2/1 Requirement 26: The concept of **fail-safe design shall be incorporated**, as appropriate, **into the design of systems** and components important to safety.

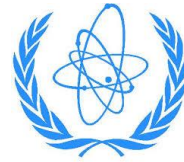
Loss of power to any I&C component or **failure** of an I&C component in any of its known and documented failure modes should **place the system in a predetermined condition** that has been demonstrated to be acceptable for nuclear safety.

Failures of I&C or electrical components **should be detectable** by periodic testing, self-diagnostics or self-revealed by alarm or anomalous indication.

The failure modes that might result from **systematic errors in the design** or operation of hardware or software **are essentially unpredictable**. Disciplined development process, the concept of defence in depth, application of diversity are tools for reducing the number of such errors, and coping with the effects of such errors that remain.

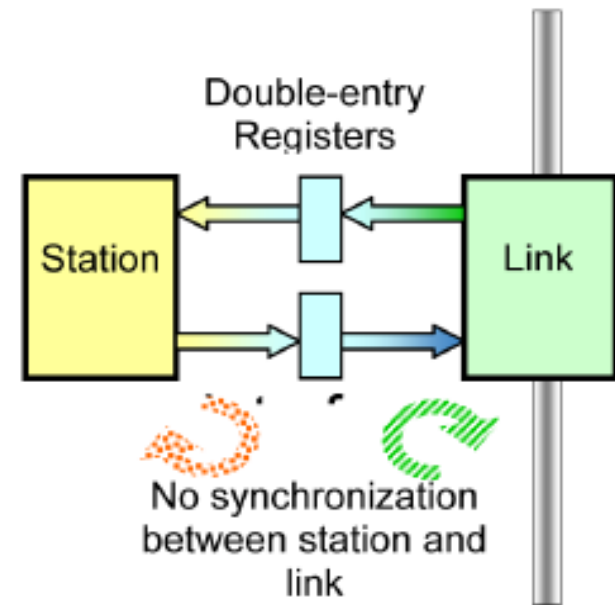
[DS-431, 6.69-6.78 / DS-430, 5.77]

I&C AND ELECTRICAL SYSTEMS FAIL-SAFE DESIGN



Possible methods:

- Independence,
- Data validation,
- Data buffering,
- Go to a safe condition when de-energized,
- One-directional communication links,
- Avoiding central communication hub/router.



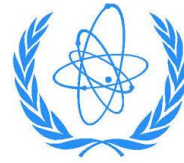
[EPRI 1019182, 2010]

Failures of the fail-safe design features themselves should be considered.

[DS-431, 7.98-7.103, DS-431, 6.71]

I&C AND ELECTRICAL SYSTEMS

FAIL-SAFE DESIGN



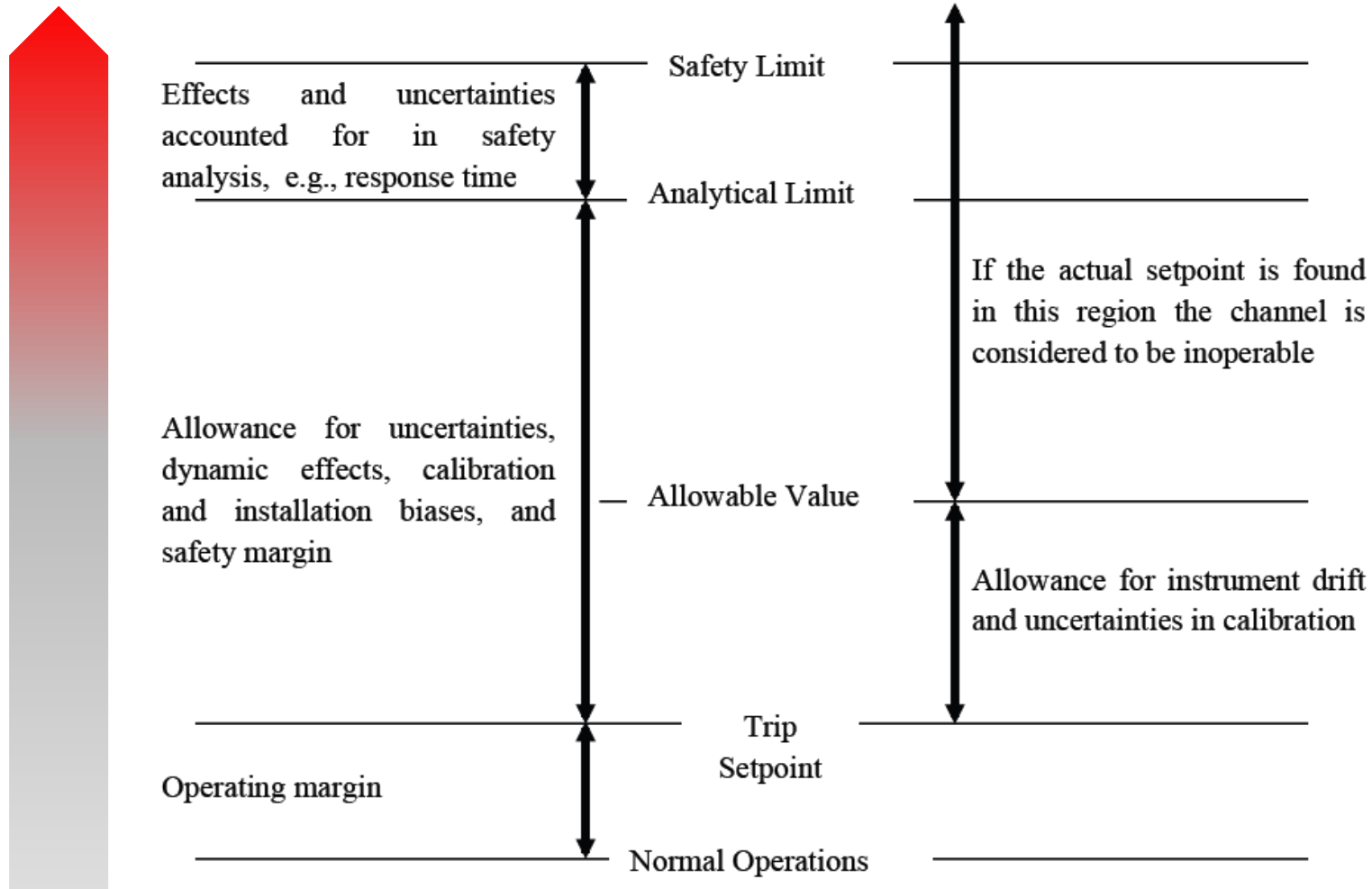
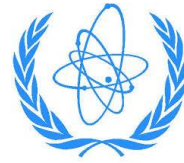
The **electrical protection scheme** should prevent failures from disabling safety functions to below an acceptable level.

Protective relays should be used for the prompt removal from service of any element of a power system when abnormal conditions occur such that operating equipment might degrade or fail.

Selective tripping of breakers should be used to minimize the impact of fault conditions.

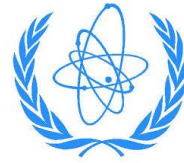
[DS-430, 5.79-5.82]

I&C AND ELECTRICAL SYSTEMS SETPOINTS



[DS-431]

I&C AND ELECTRICAL SYSTEMS QUALIFICATION



SSR 2/1 Requirement 30: A **qualification program** for items important to safety **shall be implemented** to verify that items important to safety at a nuclear power plant are capable of **performing their intended functions when necessary**, and in the prevailing **environmental conditions, throughout their design life**, with due account taken of plant conditions during maintenance and testing.

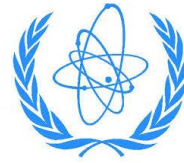
The qualification programs should address all topics affecting the suitability of each system or component for its intended functions, including:

- Suitability and correctness of functions and performance,
- Environmental qualification,
- Qualification for the effects of internal and external hazards (including seismic qualification), and
- Electromagnetic qualification.

[DS-431, 6.85 / DS-430, 5.170]

I&C AND ELECTRICAL SYSTEMS

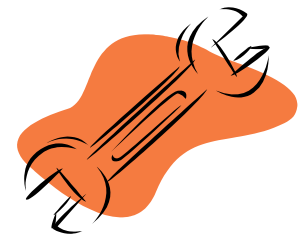
TESTABILITY AND MAINTAINABILITY



SSR 2/1 Requirement 29:

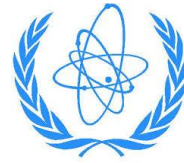
Items important to safety for a nuclear power plant **shall be designed to be** calibrated, **tested, maintained**, repaired or replaced, inspected and monitored as required to ensure their capability of performing their functions and to maintain their integrity in all conditions specified in their design basis.

Provisions for calibration, **testing, maintenance**, repair, replacement or inspection of items important to safety during shutdown shall be included in the design so that such tasks can be performed with **no significant reduction in the reliability** of performance of the safety functions.



I&C AND ELECTRICAL SYSTEMS

TESTABILITY AND MAINTAINABILITY



All systems important to safety should include provisions for **testing**.

[DS-431, 6.165 / DS-430, 5.240]

Arrangements for testing include, procedures, test interfaces, installed test equipment, and built in test facilities.

[DS-431, 6.178 / DS-430, 5.242]

The **scope and frequency** of testing and calibration should be justified as consistent with functional and availability (reliability) requirements.

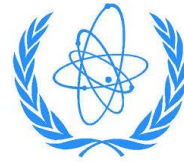
[DS-431, 6.186]

Arrangements for testing should neither **compromise the independence** of safety systems nor introduce the **potential for common cause failures**.

[DS-431, 6.177]

I&C AND ELECTRICAL SYSTEMS

TESTABILITY AND MAINTAINABILITY



Testing and calibration of safety system equipment should be **possible in all modes** of normal operations, including power operation, while retaining the capability of the safety systems to accomplish their safety functions.

[DS-431, 6.167 / DS-430, 5.243]

Where the ability to test a safety system or component during power operation is not provided:

- The reliability of the functions affected should be shown to be acceptable,
- The accuracy and stability of the untested components should be acceptable,
- Consideration should be given to providing means for comparing measurements of untested instrument channels with other devices,
- The capability to test the untested components during shutdown should be provided.

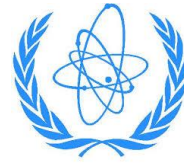
[DS-431, 6.169]

Typically the justification will demonstrate that the **overlapping tests** provide complete coverage, that reliability of the equipment is acceptable given the longer test interval, and that any components not tested on-line will be tested during plant shutdown.

[DS-431, 6.165]

I&C AND ELECTRICAL SYSTEMS

TESTABILITY AND MAINTAINABILITY



The design should ensure that systems cannot unknowingly be left in a test or maintenance configuration.

[DS-431, 6.203]

A consistent, coherent, and easily understood **method of naming and identifying** all system components and for use as descriptive titles for the HMI should be determined and followed throughout the design, installation and operation phases of the plant.

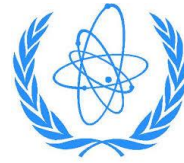
[DS-431, 6.216 / DS-430, 5.273]

Clear identification of components reduces the likelihood of inadvertently performing maintenance, tests, repair or calibration on an incorrect channel.

[DS-431, 6.222 // DS-430, 5.277]

I&C AND ELECTRICAL SYSTEMS

TESTABILITY AND MAINTAINABILITY



Adequate quantities of **spare parts** and components should be available for operation and maintenance (e.g. based on I&C design, component reliability and future availability of replacement components and vendor support).

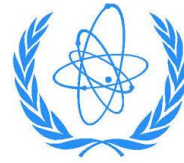
[DS-431, 2.166]

Spare parts issues:

- Availability (vendor long term support, obsolescence handling, market survey, ...);
- Storage conditions (sensitive electronic components);
- Maintenance (periodic testing of certain electronic equipment may be needed);
- Qualification (spare parts repairs, new internal components...);
- Configuration management (identification, links do documentation and configuration).



I&C AND ELECTRICAL SYSTEMS SUPPORT SYSTEMS



Power supplies for I&C systems, regardless of type (e.g., electrical, pneumatic, hydraulic), should have classification, reliability provisions, qualification, isolation, testability, maintainability, and indication of removal from service, consistent with the reliability requirements of the I&C systems they serve.

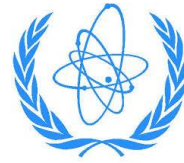
[DS-431, 7.62]

Auxiliary supporting features of the safety system shall meet all requirements for the safety system.

Other auxiliary features not isolated from the safety system that perform a function that is not required for the safety systems to accomplish their safety functions, shall not degrade the safety systems.

[IEEE 603]

I&C AND ELECTRICAL SYSTEMS MANAGEMENT SYSTEM AND DESIGN PROCESS



SSR 2/1 Requirement 2:

The design organization shall establish and implement a **management system** for ensuring that **all safety requirements** established for the design of the plant are considered and **implemented in all phases of the design process** and that they are met in the final design.

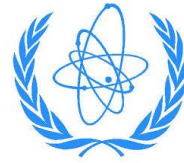
Management systems include the organizational structure, organizational culture, policies, resources and processes for developing an I&C system that meets safety requirements.

Management systems define **quality assurance activities** and integrate them with activities to assure safety, health, environment, security, and economic objectives are met.

Demonstration that the final product is fit for its purpose depends greatly on the use of a **high-quality development process**.

[DS-431, 2.6, 2.7, 2.15]

I&C AND ELECTRICAL SYSTEMS DESIGN PROCESS



SSR 2/1, requirement 62: Instrumentation and control systems for items important to safety at the nuclear power plant **shall be designed for high functional reliability** and periodic testability commensurate with the safety functions to be performed.

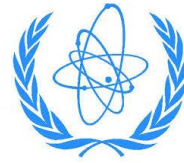
Basic design principles for high reliability:

- Defense in depth (overall I&C architecture)
- Strict development process (fault avoidance)
- Thorough V&V and testing (fault detection and removal)
- Design simplicity (deterministic and predictable behavior)
- Fault tolerance and failures propagation prevention (fail-safe design, diversity, redundancy and independence)

In the design of I&C systems, examples of features used to provide functional reliability include: the ability to tolerate random failure, independence of equipment and systems, redundancy, diversity, tolerance of common cause failures, testability and maintainability, fail-safe design, and selection of high quality equipment.

[DS-431, 6.9]

I&C AND ELECTRICAL SYSTEMS DIGITAL SYSTEMS



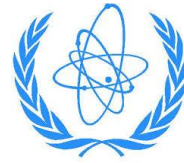
I SSR 2/1, requirement 63: f a system **important to safety** at the nuclear power plant is dependent upon **computer based equipment**, appropriate **standards and practices for the development and testing** of computer hardware and software shall be established and implemented **throughout the service life of the system**, and in **particular throughout the software development cycle**. The entire development shall be subject to a quality management system.'

The basic, and most important, defense against CCF due to software is to produce software of the highest quality, i.e. as error free as possible.

[IEC 60880]

I&C AND ELECTRICAL SYSTEMS

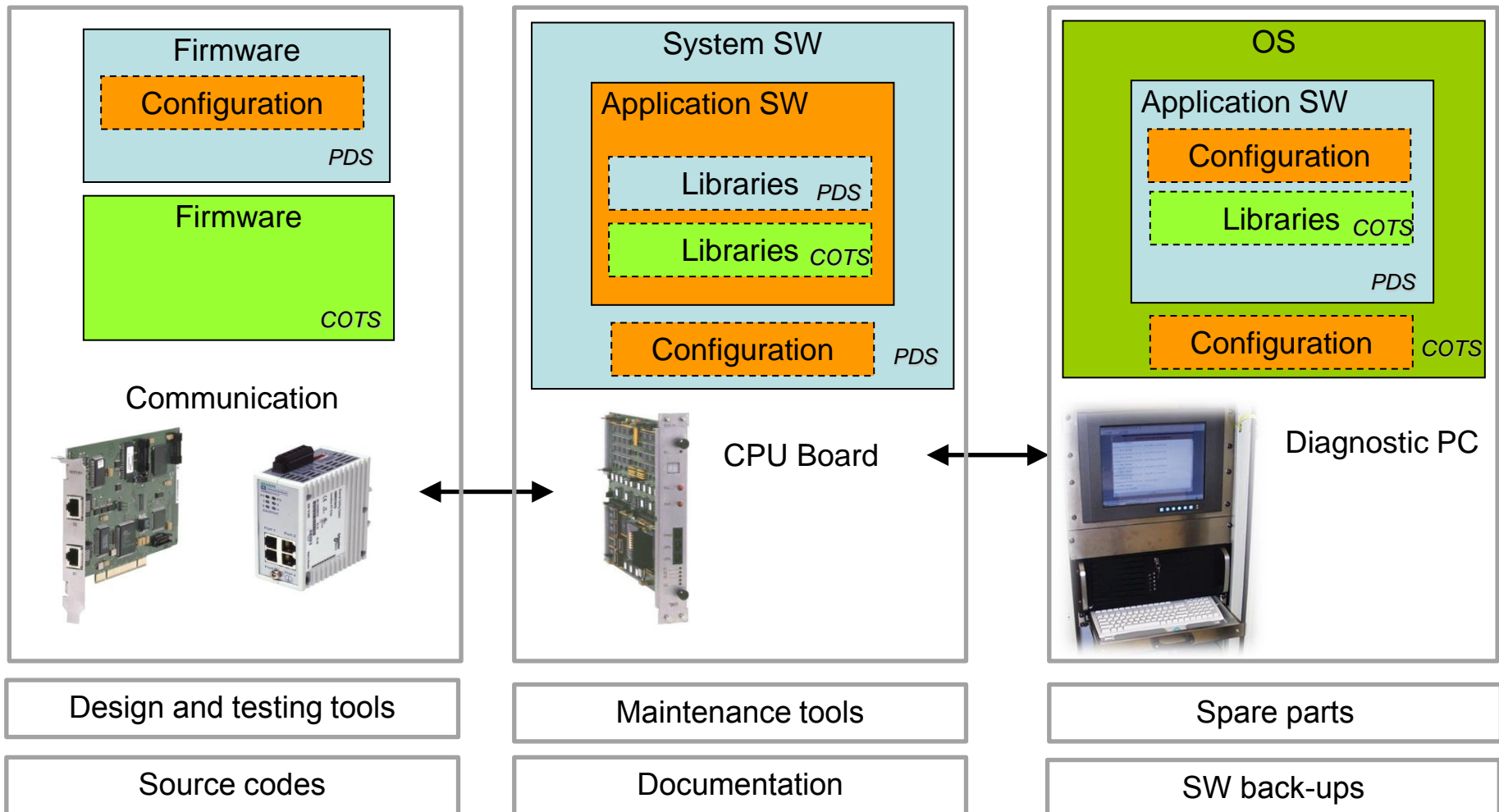
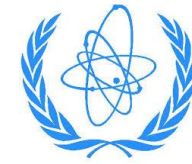
DIGITAL SYSTEMS



Characteristics (pros)	Cons
Complex functions and HMI	Hidden vulnerabilities, difficult testing
Flexibility (configuration, modification)	Cyber security, configuration management
Easy to reuse (faster, cheaper development)	CCF
Improved diagnostic (self-tests), maintenance	Complexity, hidden vulnerabilities, difficult testing
Discrete signals, timing	Sampling, unpredicted transients
Small form factor (low physical size and low cabling needs)	Specific environmental conditions (specific HW)
Data storage, analytical tools, maintenance and design tools	Complexity, tools qualification, cyber security

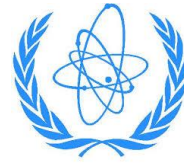
I&C AND ELECTRICAL SYSTEMS

DIGITAL SYSTEMS



I&C AND ELECTRICAL SYSTEMS

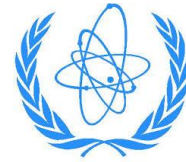
DIGITAL SYSTEMS



	SW based	FPGA
Development process	Well defined and controlled life cycle	Well defined and controlled life cycle
Tools	Use of complex tools	Use of complex tools
Predeveloped items qualification	Tools, libraries, general purpose operating systems, ...	Tools, SW or HW IP cores
Complexity	Higher (use of operating systems), all functions in one SW	Lower (no operating system needed), ability to segregate functions
Processing	Sequential	Parallel
Design	Fail-safe, deterministic	Fail-safe, deterministic

Very often FPGA (basic controllers, regulators,...) are combined with SW based components (HMI, diagnostic and additional functions,...) in digital I&C systems.

I&C AND ELECTRICAL SYSTEMS DESIGN PROCESS



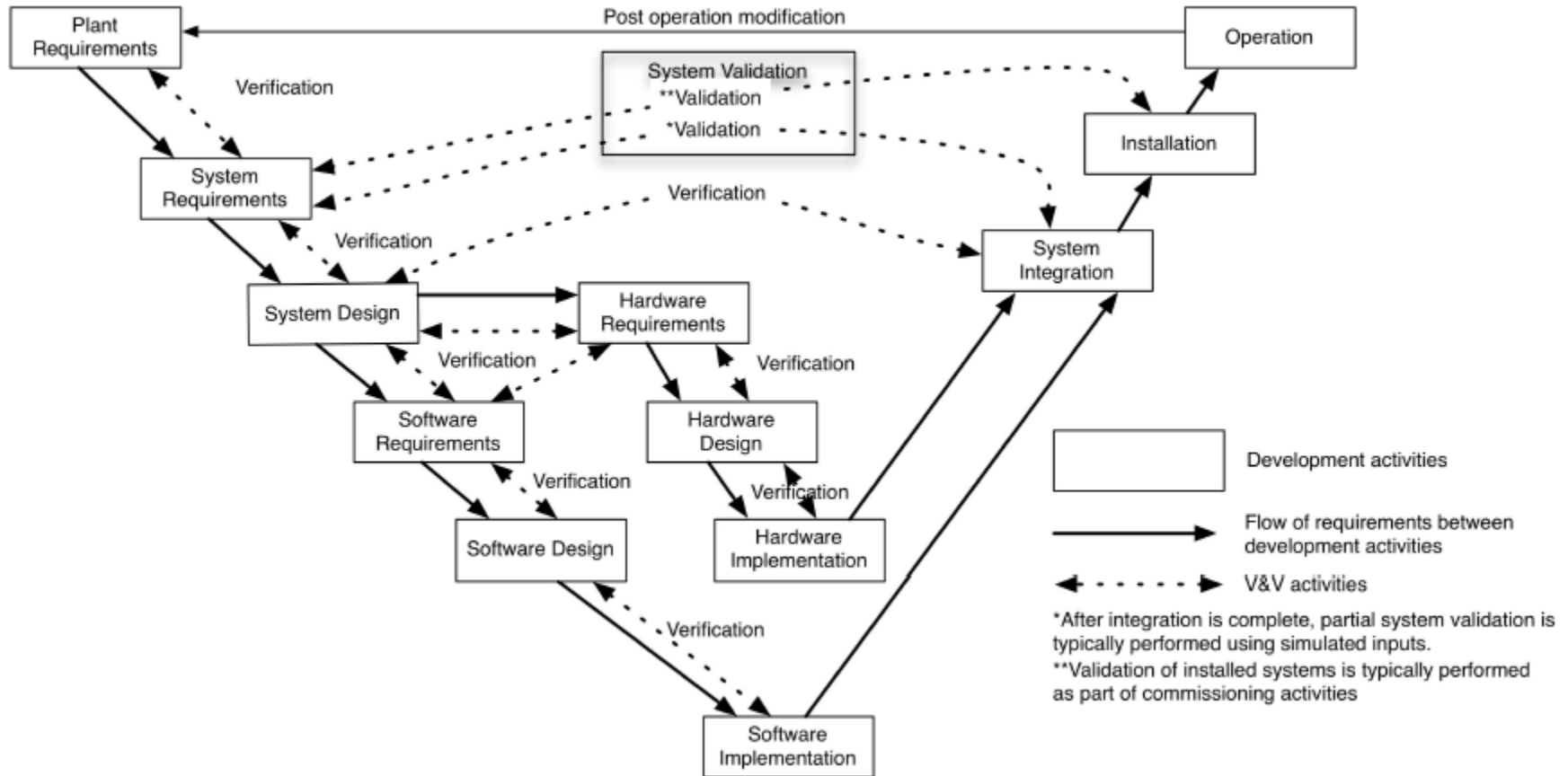
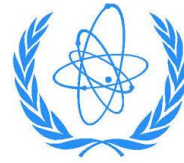
A well-documented development process also produces evidence that can allow independent reviewers and regulators to gain confidence in the final product.

[DS-431, 2.17]



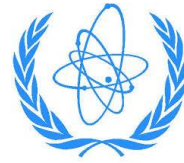
© Scott Adams, Inc./Dist. by UFS, Inc.

I&C AND ELECTRICAL SYSTEMS DESIGN PROCESS



[DS-431]

I&C AND ELECTRICAL SYSTEMS DESIGN PROCESS

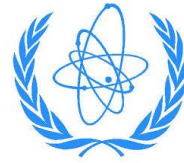


Before initiation of any technical activity, a plan describing the inputs, products, and processes, of that activity and the relationship of the activity with other activities should be prepared and approved in accordance with the management system.

[DS-431, 2.28]



I&C AND ELECTRICAL SYSTEMS DESIGN PROCESS



Experience in the operation of highly reliable digital systems in various industry sectors has shown that **specification faults** are an important, and sometimes a **dominant source of digital failure**.

Two main human causes may be identified at the root of most specification errors:

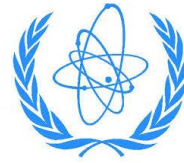
- Inadequate expression,
- insufficient understanding.

The most severe specification faults (i.e., those that could directly lead to a system failure) may be classified into three main types:

- incompleteness,
- Incorrectness,
- ambiguity.

[EPRI 1019182, 2010]

I&C AND ELECTRICAL SYSTEMS DESIGN PROCESS



Unnecessary **complexity should be avoided** in the design of I&C safety systems.

All features of I&C safety systems should be beneficial to their safety functions.

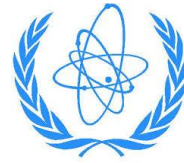
The intent of avoiding complexity is to keep the **I&C system as simple as possible** but still fully implement its safety requirements.

[DS-431, 6.2-6.5]

Simple and predictable: designed-in defensive measure to reduce the likelihood of encountering an fault activating condition is to have the digital system or component follow a deterministic, repetitive routine in very stable and restricted conditions, so that tests and verification can be performed to reach a high level of behavioral coverage, and that untested and / or never-encountered conditions during normal operation (under permanent influence factors) are extremely unlikely.

[EPRI 1019182, 2010]

I&C AND ELECTRICAL SYSTEMS DESIGN PROCESS



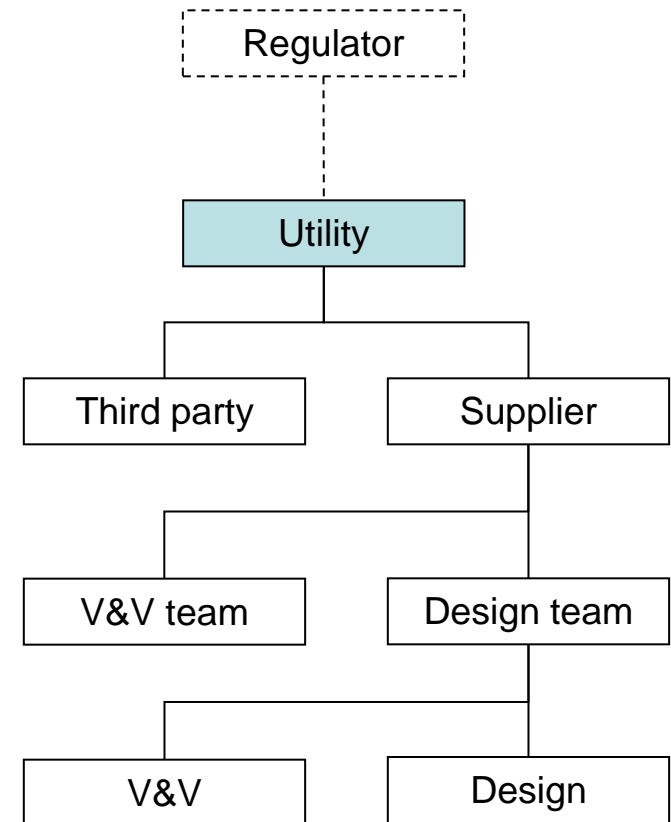
Verification and validation should be carried out by teams, individuals, or groups that are independent of the designers and developers.

The amount and type of independence of the V&V should be suitable for the safety class of the system or component involved.

[DS-431, 2.72-2.74]

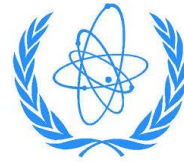
General levels of independence:

- Third party
- Independent unit within supplier's organization
- Independent personnel within design team



]

I&C AND ELECTRICAL SYSTEMS DESIGN PROCESS



System validation should be performed for each individual I&C system and the integrated set of I&C systems.

[DS-431, 2.134]

The software subject to system validation should be identical to the software that will be used in operation.

[DS-431, 2.138]

System validation should demonstrate that the system **meets all requirements** under all possible interface and load conditions.

[DS-431, 2.139]

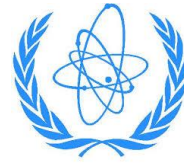
The system operation manuals and appropriate parts of the maintenance manuals should be validated as far as possible, during system validation.

[DS-431, 2.145]

Verification and validation activities should be **documented and recorded**.

[DS-431, 2.77]

I&C AND ELECTRICAL SYSTEMS DESIGN PROCESS



Equipment receipt inspection, pre-commissioning, or commissioning tests should verify that the system has not suffered damage during transportation.

[DS-431, 2.151]

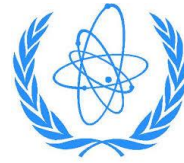
Modes of operation and interactions between I&C systems and the plant that could not be readily tested during system validation should be tested during commissioning.

Commissioning should give particular attention to verification of external **system interfaces** and to the confirmation of correct performance with the interfacing equipment.

During the commissioning period all I&C systems should be operated for an extended time under operating, testing and maintenance conditions that are as representative of the in-service conditions as possible.

[DS-431, 2.156-2.158]

I&C AND ELECTRICAL SYSTEMS DESIGN PROCESS



Adequate documentation will facilitate operation, surveillance, troubleshooting, maintenance, future modification or modernization of the system, as well as training of plant and technical support staff.

[DS-431, 2.93]

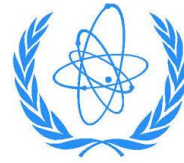
Before the systems are declared operable, relevant life cycle planned activities should be completed, **traceability should be established** from requirements to installed systems and their build and design documentation should be complete and reflect the as-built configuration.

[DS-431, 2.160]



I&C AND ELECTRICAL SYSTEMS

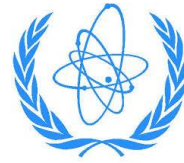
HUMAN FACTORS ENGINEERING



System development should implement requirements developed by the **Human Factors Engineering (HFE)**:

- The identification of **operating personnel roles and responsibilities** and other staffing requirements;
- **Safety classification** of the elements of the Human Machine Interface (HMI);
- The identification of **information needs** including considerations for defining a subset of **indications and controls** required to address accident and post accident conditions;
- The identification of control needs, **automatic and manual control functionality** and allocation of controls to **suitable locations**;
- **Task process, time constraints**, flow of operating personnel and information identified by analyses (i.e. task analysis); and
- Insights resulting from **consideration of human error**.

I&C AND ELECTRICAL SYSTEMS CYBER SECURITY



SSR 2/1 Requirement 39:

Unauthorized access to, or interference with, items important to safety, including computer hardware and software, **shall be prevented**.

All nuclear facilities with digital systems should therefore have digital I&C architectures designed to **prevent** and limit the **consequences of cyber compromise**.

[IAEA NSS17]

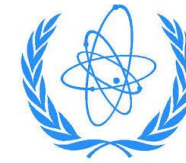
The objective of security is to protect software and data so that unauthorized persons and systems cannot read or modify them and so that authorized persons and systems are not denied access to them.

[IEC 60880]



I&C AND ELECTRICAL SYSTEMS

CYBER SECURITY



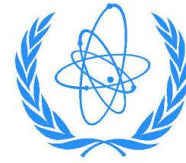
	IT	I&C
Performance	Non real-time Enough resources for additional SW	Real-time Limited resources
Availability	Low (rebooting and outages acceptable)	High (rebooting and outages planned)
Risk requirements	Confidentiality and data integrity	Human and process safety, fault-tolerant
Operation	Standard systems and automated tools, compatible security solutions available	Customized or specific systems and tools, security solutions must be tested
Changes	Fast, often automated	Slow, strict life cycle, testing
Support	Often more sources	Often via single vendor
Life time	approx. 3-5 years	approx. 10-20 years
Equipment	Standard IT, often uniform	Often mix of IT and specific proprietary equipment and networks
Access to components	Usually easy	Often isolated or remote

[IAEA NSS17]

confidentiality - integrity - availability

I&C AND ELECTRICAL SYSTEMS

CYBER SECURITY

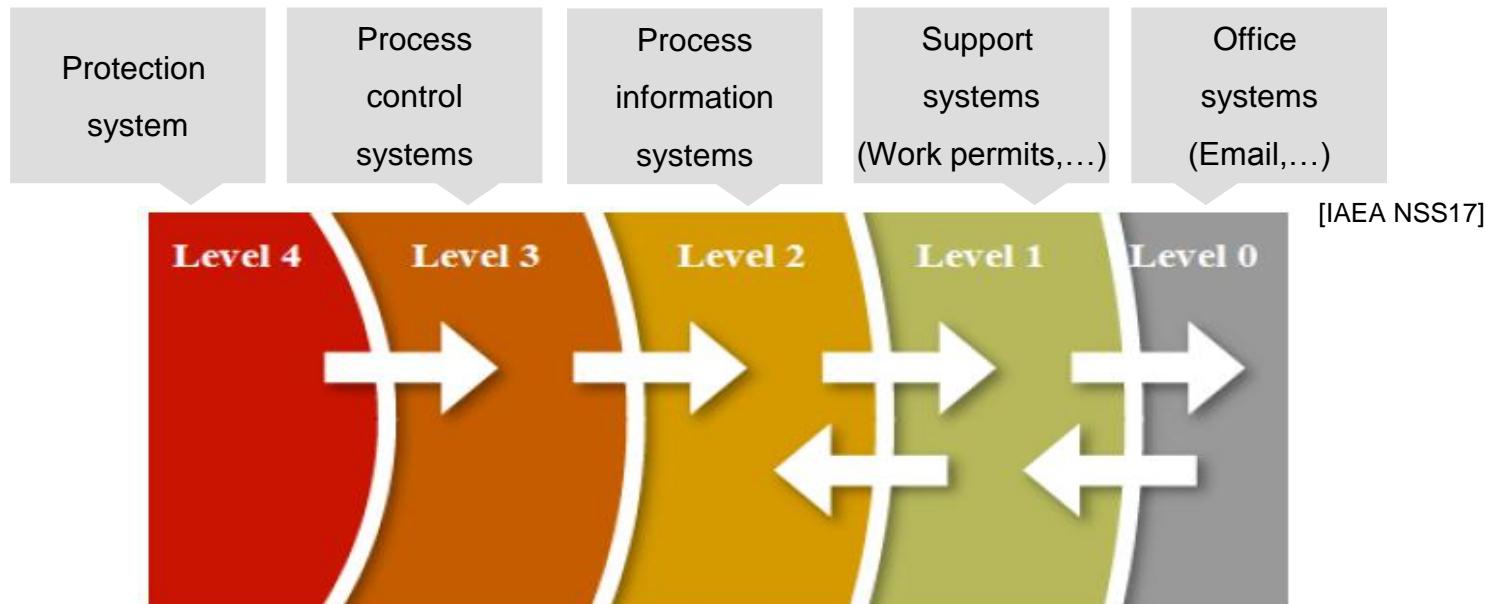


Protection requirements should reflect the **concept of multiple layers** (defense in depth concept).

[IAEA NSS17]

The security of computer systems should be based on a **graded approach**: categorize computer systems into **zones**, where graded protective principles are applied

[IAEA NSS17]

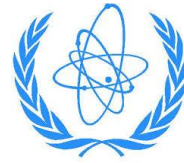


[IAEA NSS17]

[NRC RG 5.71]

I&C AND ELECTRICAL SYSTEMS

CYBER SECURITY



Myths:

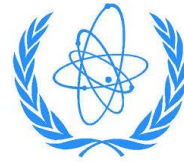
- “My system is Isolated”: check remote service access, maintenance and diagnostic access, removable media access...
- “I have only one-way links”: check communication initiation principles, system level communication (TCP handshakes), ...
- “I have firewall or antivirus, so I am 100% secure”: there is no silver bullet solutions, zero-day vulnerabilities, misconfiguration, other attack vectors,...
- “Security by obscurity - it is specific and proprietary system immune to viruses”: check use of COTS and IT technology, industrial well known or accessible standards, ...



[NPIC-HMIT 2009, Piètre-Cambacédès]

I&C AND ELECTRICAL SYSTEMS

CYBER SECURITY



SSR 2/1 Requirement 8:

Safety measures, nuclear security measures and arrangements for the State system of accounting for, and control of, nuclear material for a nuclear power plant shall be designed and implemented in an integrated manner so that they **do not compromise one another**.

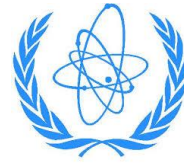
Neither the operation nor failure of any computer security feature should **adversely affect the ability** of a system **to perform its safety function**.

If computer security features are implemented in the Human Machine Interface, they should not **adversely affect the operator's ability to maintain the safety** of the plant.

Where practical, security measures that do not also provide a safety benefit, should be **implemented in devices that are separate from I&C systems**.

[DS-431, 7.107-7.110]

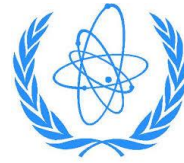
I&C AND ELECTRICAL SYSTEMS DESIGN BASIS



General description:

- System description (objective of the system, architecture and design description, human factor considerations, operational aspects)
- Specific requirements, industrial codes and standards
- System safety classification
- System functions
- System reliability
- System qualification
- System security
- System identification
- Support (auxiliary) systems

I&C AND ELECTRICAL SYSTEMS DESIGN BASIS

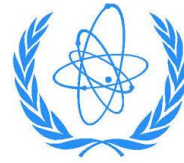


Information about system functions:

- The plant operational states in which the system is required;
- The various plant configurations for which each I&C system is to be operational;
- The functional requirements for each plant state, each plant operational mode and during extended shutdown (for electrical system voltage and frequency ranges including transient ranges);
- The safety significance of each required I&C function (i.e. safety classification);
- The postulated initiating events (PIE) to which the system is to respond;
- The system role in the defence-in-depth concept of the overall architecture;
- The variables, or combination of variables, to be monitored;
- The control functions required, including identification of actions that are to be performed automatically, manually, or both and the location for the controls;
- The required ranges, rates of change, accuracy, capacity and loads, quantization of digital representations, calculation precision, and required response times for each I&C safety function.

[DS-431, section 3 / DS-430, section 4]

I&C AND ELECTRICAL SYSTEMS DESIGN BASIS

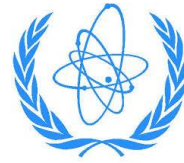


Information of the level of reliability and availability:

- The requirements for independence;
- The requirements for periodic testing, self-diagnostics, and maintenance;
- The qualitative or quantitative reliability and availability goals (probabilistic criteria and deterministic criteria);
- The fail-safe characteristics and characteristics needed to provide appropriate tolerance for random and common cause failures required for the system.

[DS-431, section 3]

I&C AND ELECTRICAL SYSTEMS DESIGN BASIS

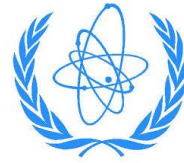


Information regarding to equipment qualification:

- The design criteria including identification of standards with which the systems should comply;
- The plant conditions with the potential to functionally degrade the performance of systems and the provisions to be made to retain the necessary capability;
- The range of internal and external hazards (including natural phenomena) under which the system is required to perform functions important to safety;
- The range of plant environmental conditions under which the system is required to perform functions important to safety;
- The limitations on materials to be used;
- The constraints imposed by the physical plant design and layout, with those on equipment location, cable access and power sources;
- The physical location of and interfaces between equipment.

[DS-431, section 3]

I&C AND ELECTRICAL SYSTEMS DESIGN BASIS

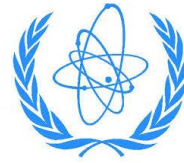


Information of the level of security (based on Identification of critical digital assets and vulnerability assessments):

- The security and operational constraints that are to be observed in the design;
- The security measures to be implemented (access control, computer security,...).

[DS-431, section 3]

I&C AND ELECTRICAL SYSTEMS DESIGN BASIS



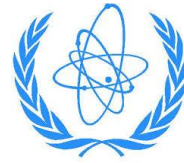
Additional information for the safety systems:

- The limiting values of parameters required to actuate safety systems;
- Variables and states that are to be displayed so that the operators can confirm the operation of protective system functions;
- The justification for any safety actions that are not automatically initiated (including: the occasions, incidents, time durations and plant conditions for which manual control is allowed; the range of environmental conditions of the operators' environment when they are expected to take manual action during plant operational states and accident conditions; necessary information will be displayed in appropriate locations; necessary support the operator actions).
- The conditions under which bypass / interlock of I&C safety functions are to be permitted;
- The requirements for diverse functions to mitigate the consequences of common cause failure.

[DS-431, section 3]

I&C AND ELECTRICAL SYSTEMS

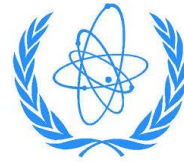
REFERENCES



- **[SSR 2/1]: “Safety of Nuclear Power Plants: Design”, IAEA Specific Safety Requirements, 2012**
- **[DS-431]: “Design of Instrumentation and Control Systems for Nuclear Power Plants”, IAEA Safety Guide, 2012**
- **[DS-430]: “Design of Electrical Power Systems for Nuclear Power Plants”, IAEA Safety Guide, 2012**
- [IAEA Safety Glossary, 2007]: “IAEA safety glossary : terminology used in nuclear safety and radiation protection”, IAEA, 2007
- [IAEA NP-T-3.12]: “Core knowledge on instrumentation and control systems in nuclear power plants.”, IAEA Nuclear Energy Series, 2011
- [IAEA GS-G-4.1]: “Format and Content of the Safety Analysis Report for Nuclear Power Plants.”, IAEA Safety Standard Series, 2004
- [IAEA NSS17]: “Computer security at nuclear facilities”, IAEA Nuclear Security Series No. 17, 2011
- [EPRI 1019182, 2010]: “Protecting Against Digital Common-Cause Failure: Combining Defensive Measures and Diversity Attributes”, EPRI, Palo Alto, CA: 2010. 1019182
- [EPRI 1016731, 2008]: “Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems”, EPRI, Palo Alto, CA: 2008. 1016731
- [EPRI 3002000502, 2013]: “Preventive Maintenance Practices for Digital Instrumentation and Control Systems.”, EPRI, Palo Alto, CA: 2013. 3002000502
- [EPRI 3002002953]: “Principles and Approaches for Developing Overall Instrumentation and Control Architecture that Support Acceptance in Multiple International Environments”, EPRI, , Palo Alto, CA: 2014. 3002002953

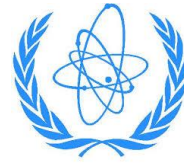
I&C AND ELECTRICAL SYSTEMS

REFERENCES



- [NRC RG 5.71]: U.S. NUCLEAR REGULATORY COMMISSION, REGULATORY GUIDE 5.71, 2010
- [IEC 60880]: “Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions”, IEC, 2006
- [IEC 62138]: Nuclear power plants - Instrumentation and control important for safety - Software aspects for computer-based systems performing category B or C functions “, IEC, 2004
- [IEC 61513]: “Nuclear power plants - Instrumentation and control important to safety - General requirements for systems”, IEC, 2011
- [IEC 62340]: “Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF) “, IEC, 2007
- [IEC 60987]: “Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems “, IEC, 2007
- [IEC 62566]: “Nuclear power plants - Instrumentation and control important to safety - Development of HDL-programmed integrated circuits for systems performing category A functions “, IEC, 2012
- [IEC 61226]: “Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions”, IEC, 2009
- [IEEE 603]: “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations”, IEEE, 2009
- IEC Glossary: <http://std.iec.ch>

I&C AND ELECTRICAL SYSTEMS REFERENCES



- [NPIC-HMIT 2009, Yastrebenetsky]: “OPERATING RELIABILITY OF WWER NPP DIGITAL I&C SYSTEMS”, Mikhail Yastrebenetsky & Alexander Siora, Ukraine, 2009
- [NPIC-HMIT 2009, Piètre-Cambacédès]: “DECONSTRUCTION OF SOME INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY MYTHS”, Ludovic Piètre-Cambacédès and Pascal Sitbon, France, 2009
- [WENRA]: “Safety Reference Levels for Existing Reactors”, Western European Nuclear Regulators’ Association , 2014
- [H.Waage]: “CCF in TEMELIN NPP Digital Systems”, EPRI Central Europe Equipment Reliability Workshop, 2015