NUCLEAR
REGULATORY AUTHORITY
OF THE SLOVAK REPUBLIC

Legal requirements for I&C system of the Slovak Republic

12th International Workshop on the Application of FPGAs in NPPS

Content

NPP in the Slovak Republic

Legislation

I&C system requirements

I&C systems for Mochovce 3 and 4

Use the FPGA

NPP in the Slovak Republic

NUCLEAR REGULATORY AUTHORITY OF THE SLOVAK REPUBLIC

Bohunice NPPs

Construction	UNIT 1,2 – V1		UNIT 3,4 – V2	
Start of construction	1972		1976	
Operation (Commissionong date)	1978	1980	1984	1985
Modernisation	1992-2000		2002-2008	
Power upgrade			2009-2013	
End of operation	2006	2008	2044*-2045*	

Basic Overwiev UNIT 3,4

- Location: western Slovakia near to Trnava
- Two units **VVER 440/V-213 PWR**
- Net capacity: 2 x 471 MWe
- Gross capacity: 2 x **505 MWe**
- Fuel type: Enriched uranium 4,87%

Bohunice NPPs - panorama

Mochovce NPPs

Construction	UNIT 1,2 – EMO12		UNIT 3,4 – MO34
Start of construction	1982		1987
Construction according original BD			
interruption	1992		
suspension	4 years		2002-2008
Power upgrade	1996		2008
Operation	1998	2000	2020*-2022*

Basic Overwiev UNIT 1,2

- Location southern Slovakia, near the town Nitra
- Two units **VVER 440/V-213 PWR**
- Net capacity: 2 x 436 MWe
- Gross capacity: 2 x 470 MWe
- Fuel type: Enriched uranium 4,87%

Mochovce NPPs - panorama

Legislation

NRA National legislation

IAEA Safety Guidelines and Recommendations

STN/IEC/EN Normative Documents

Safety Guidelines Elaborated and Accepted in the EU

Other Normative Documents

Legislation

- The Act No. **541/2004 Coll.** on Peaceful Use of Nuclear Energy (Atomic Law) and on Amendment and Modification of Certain Acts is the main document.
- Regulation of NRA SR No. **430/2011 Coll**. on nuclear safety requirements.
- Regulation of NRA SR No. **431/2011 Coll.** On a quality management system.
- Regulation of NRA SR No. **58/2006 Coll.** Laying Down Details on the Scope, Contents, and Manner of Maintaining, Documentation of Nuclear Facilities Necessary for Individual Decisions.
- Regulation of NRA SR No. **33/2012 Coll.** on the regular, comprehensive and systematic evaluation of the nuclear safety of nuclear equipment.

Regulation of NRA SR No. 430/2011 Coll. on nuclear safety requirements

Section 3 Categorisation of classified equipment into safety classes

- Classified equipment must be identified and then subsequently categorized, based on their functions and importance for nuclear safety, into safety classes I to IV. (specification are in Anex 1)
- Classified equipment of instrumentation and control system (I&C) are identified and subsequently categorized also according to relevant technical standards.
- Classification methods for classified equipment must be primarily based on deterministic methods.

Regulation of NRA SR No. 430/2011 Coll. on nuclear safety requirements

L) Safety systems and control systems

- Safety systems must be designed with the **highest achievable functional reliability, backup and independence of individual channels so that a single failure**

  a) **does not cause** the system to **lose its protective function**

  b) **does not reduce the number of independent measurement** and information channels of these systems **to one**

- Safety systems must **permit periodic functional tests of independent information channels during normal operation** and testing of their common circuits when the nuclear facility is shut down. This **common circuits** must be designed so their **possible failures lead** at most **to shutdown** of the nuclear facility, and **not to loss of protective function**
- Safety systems must be designed so that **system of protection cannot be rendered ineffective by an incorrect action**, **but must not restrict correct action**
- Safety systems must be designed so that **the effect of conditions** during normal operation, abnormal operation and during DBA **on backup channels do not cause it to lose functionality**, otherwise its reliability based on different principle must be proven
- **If a control system or safety system is dependent on the reliability of a computer system**, **specific quality** criteria and procedures must be established and applied to the development, delivery and testing of computer system **HW and especially SW** during the useful life of the control system and the safety system
- **The level of required reliability of the computer system must be in line with its safety importance**. **The reliability level must be achieved though a comprehensive strategy**, using complementary facilities in each phase of development of the process, taking account of an effective analysis and test methods, as well as verification and validation strategies in order to confirm the project requirements.

Regulation of NRA SR No. 430/2011 Coll. on nuclear safety requirements

- Computer system software **verification and validation** must be provided by that is **independent** of the supplier
- **An analysis of failure states and failure consequences must be performed** for safety systems in order to detect vulnerability of the system in case of component failures and suitability of design strategy for failure detection or for moderation of their consequences shall be assessed.
- **The level of reliability proposed in the safety analysis for computer-based systems must include a specified level of conservatism**, balancing the complexity of the technology used and the difficulty of the safety analyses.
- The process of **development** of safety or control computer **must be documented and checked, and must enable backtracking** including its testing and commissioning and also design changes to these systems.
- A **computer system** for a safety system or control system effecting nuclear safety must be **qualified**.
- Safety system based on computer systems must meet the following conditions:
  - **high quality** of hardware and software used shall be required
  - the entire **development process** including inspection, testing, commissioning and design changes to the design **must be systematically documented** and reviewed
  - **if system reliability cannot be proven with the high degree of confidence, protection functionality diversity must be ensured**
- If it is not possible to demonstrate the existence of a sufficient quantity of data from the operational activities of identical systems used in similar cases, the conservative level of reliability proposed in the safety analysis for the computer system must be adopted.
- **Safety systems and control systems must be separate** so that a **control system failure does not influence safety**. If this it is not possible, functionally necessary and purposeful connections between safety and control systems must be restricted to the extend that safety functionality is not influenced.

Regulation of NRA SR No. 430/2011 Coll. on nuclear safety requirements

- Safety systems and control systems must have built-in **automated safety actions** so that **no human intervention is required for a justified period** of time from the occurrence of an event and information must be available on automated safety actions so that their effect can be monitored.
- A safety system must be designed so that **project parameters are not exceeded even during a control system malfunction**. Safety system activities must take precedence over control system activities and human activities, with the option of activating the safety system manually
- A **computer-based safety system must have its reliability confirmed by specialists that are independent** of its designer and supplier; if the required system integrity cannot be proved with the expected level of reliability, other means must be used to ensure safety functions are met.
- A safety system must be designed to **recognize postulated trigger events and activate systems** for the alleviation of their consequences
- Control systems must be designed to provide required signals on important operating parameters and processes exceeding or falling below allowable limits.
- Control systems must be equipped with devices for monitoring, measuring, registering and controlling values and systems that are important for nuclear safety during normal and abnormal operation
- Control systems must continuously, at regular intervals, or as required record parameters that are important for nuclear safety according to safety analyses.
- Indicators, signals and controllers must be designed and distributed so that employees constantly have sufficient information on operation, and can intervene promptly if needed
- Measuring instruments, indicators, signals and recording devices must be designed so that in the case of an incident they provide

  a) information on the current state of affairs,

  b) basic information on the progress of events and records thereof,

  c) data allowing for the characterization of the spread of radioactive substances and ionizing radiation into the workplace and the environment.

Regulation of NRA SR No. 431/2011 Coll. On a quality management system

Section 6 Quality assurance requirements for classified equipment

- Quality assurance requirements for classified equipment shall be specified in **quality plans**
- are valid from their approval until the end of the life of qualified equipment

Section 8 Quality requirements for classified equipment

- **Classified equipment must be qualified** for their required functionality and presumed effects of their surroundings for conditions considered in their design, including earthquake resistance, during their commissioning, operation, decommissioning, storage pool closure and during breakdowns. **The qualification method shall correspond to the safety class of the classified facilities.**
- The meeting of quality requirements for classified equipment shall be documented in **accompanying technical documentation.**
- Pursuant to Section 10(1)(f) of the Act, a permit holder shall notify the Authority of the date **post-installation tests** at least ten days in advance.

Section 9 Quality Management System Changes Control

Safety Systems

RTS – Reactor Trip System,

DRTS – Diverse Reactor Trip System,

EXCORE – Neutron flux measurement,

RTB – Reactor Trip Breaker,

SMS – Seismic Monitoring System,

These systems constitute the Reactor Protection System (**RPS**).

ESFAS – Engineered Safety Features Actuation System.

Safety Related Systems

RRCS – Reactor Rod Control System,
RLS – Reactor Limitation System,
PAMS – Post Accident Monitoring System,
SAMS – Severe Accident Monitoring System,
INCORE – Reactor measurements,
PICS – Process Information and Control System,
SICS – Safety Information and Control System,
SAS – Safety Automation System, (part od PCS),
I.O. operational diagnostic for LBB (MS-A, MS-B, MS-C).

Systems not important to Safety

- **RCS** – Reactor Control System.
- **System of the main reactor building normal operation control:**
  - **PAS** – Proces Automation System,
  - **PCS** – Process Control System,
  - **TCS** – Turbine Control System.
- **CHDIS** – Chemical Monitoring System.
- **Remaining part of I.O: operational diagnostic :**
  - **MS –** Monitoring System (MS-D to MS-N).
- ...

Monitoring system

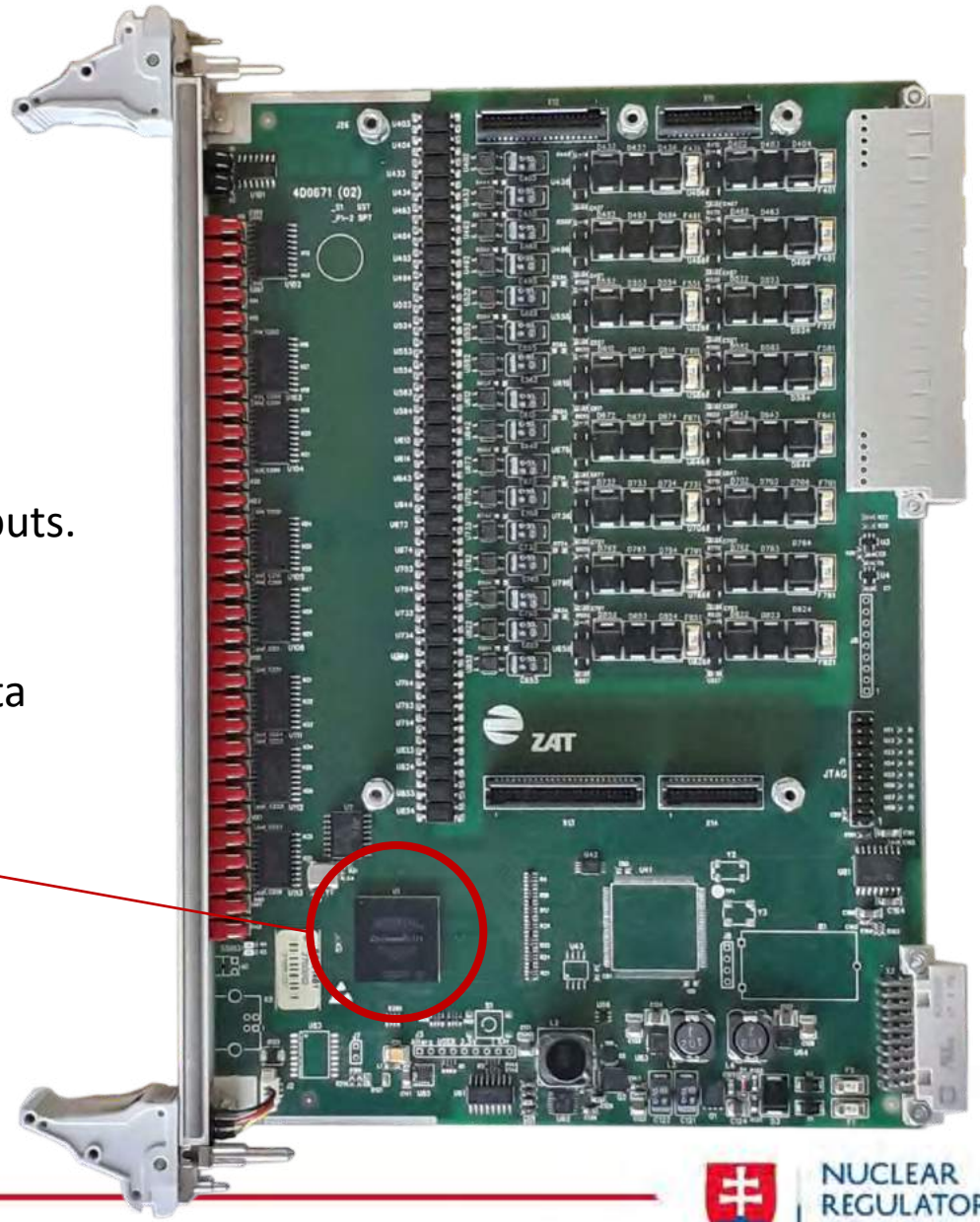
MS - A	• Leak monitoring in I.O. based on humidity measurement
MS - B	• Leak monitoring in I.O. based on ultrasonic measurement
MS - C	• Leak monitoring in I.O. based on activity measurement
MS - D	• Loose part monitoring system
MS - E	• Vibration monitoring system
MS - F	• System for monitoring of non-specified loads of NPP's components
MS - H	• System for monitoring of RCPs
MS - S	• Neutron noise monitoring system (in-core and ex-core)
MS - R	• System for monitoring the RPV inclination
MS - N	• Supervising system of diagnostics

FPGA

- Only in RRCS (SC III).
- Company ZAT.
- Components BC0014B1 (SandRA Z100).

- **Binary I/O Board** - 16 binary inputs, 16 binary outputs.

- FPGA on the binary I/O board processes data from binary inputs and on processor boards, receives data from processor boards.



NUCLEAR
REGULATORY AUTHORITY
OF THE SLOVAK REPUBLIC

lenka.riganova@ujd.gov.sk

Thank you for your attention