ATOMPROEKT
Enterprise
of State Corporation Rosatom

Hanhikivi–1 NPP
FUEL HANDLING SYSTEMS LICENSING DOCUMENTATION
at the example of Refueling machine

Helsinki, 18th of May 2017

Speakers:
Aleksandr Kutuzov
Aleksandr Brunov

ATOMPROEKT
Enterprise
of State Corporation Rosatom

PRESENTATION CONTENT

- SAFETY ENGINEERING PLAN FOR FUEL HANDLING (SEP-FH)
- FUNCTIONAL SAFETY DESIGN & ARCHITECTURE (FSDA)
- SYSTEM REQUIREMENT SPECIFICATION (SRS)
- SYSTEM DESCRIPTION (SD)
- SYSTEM REQUIREMENT EVALUATION (SRE)

ATOMPROEKT
Enterprise
of State Corporation Rosatom

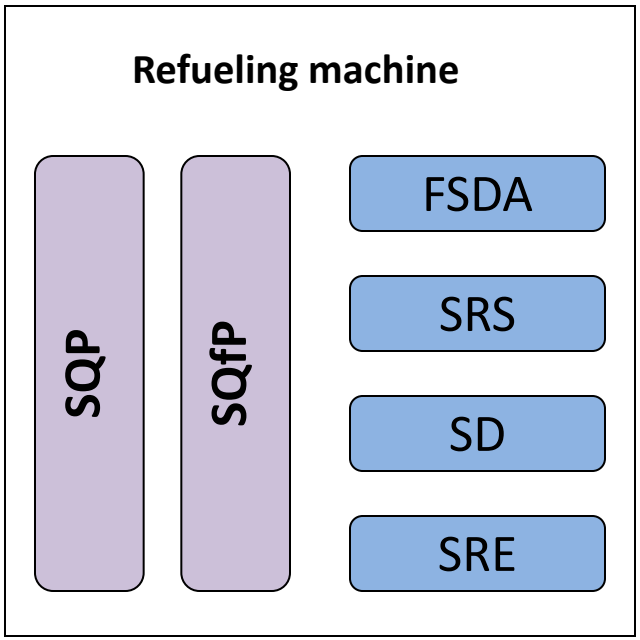
SEP-FH targets

Safety Engineering Plan for Fuel Handling has been prepared to expand plant SEP and SEQP to cover fuel handling systems. SEP-FHs targets are to:

- define the list of licensing documents for fuel handling;
- define the list of parent documents, requirements and standards applicable for each document;
- define the tasks for each document;
- describe the principles of documents developing;
- describe the methodology for nuclear risk analysis and functional safety design.

Fuel handling systems documentation structure (Refueling machine example)

Safety Engineering Plan for Fuel Handling (SEP-FH)



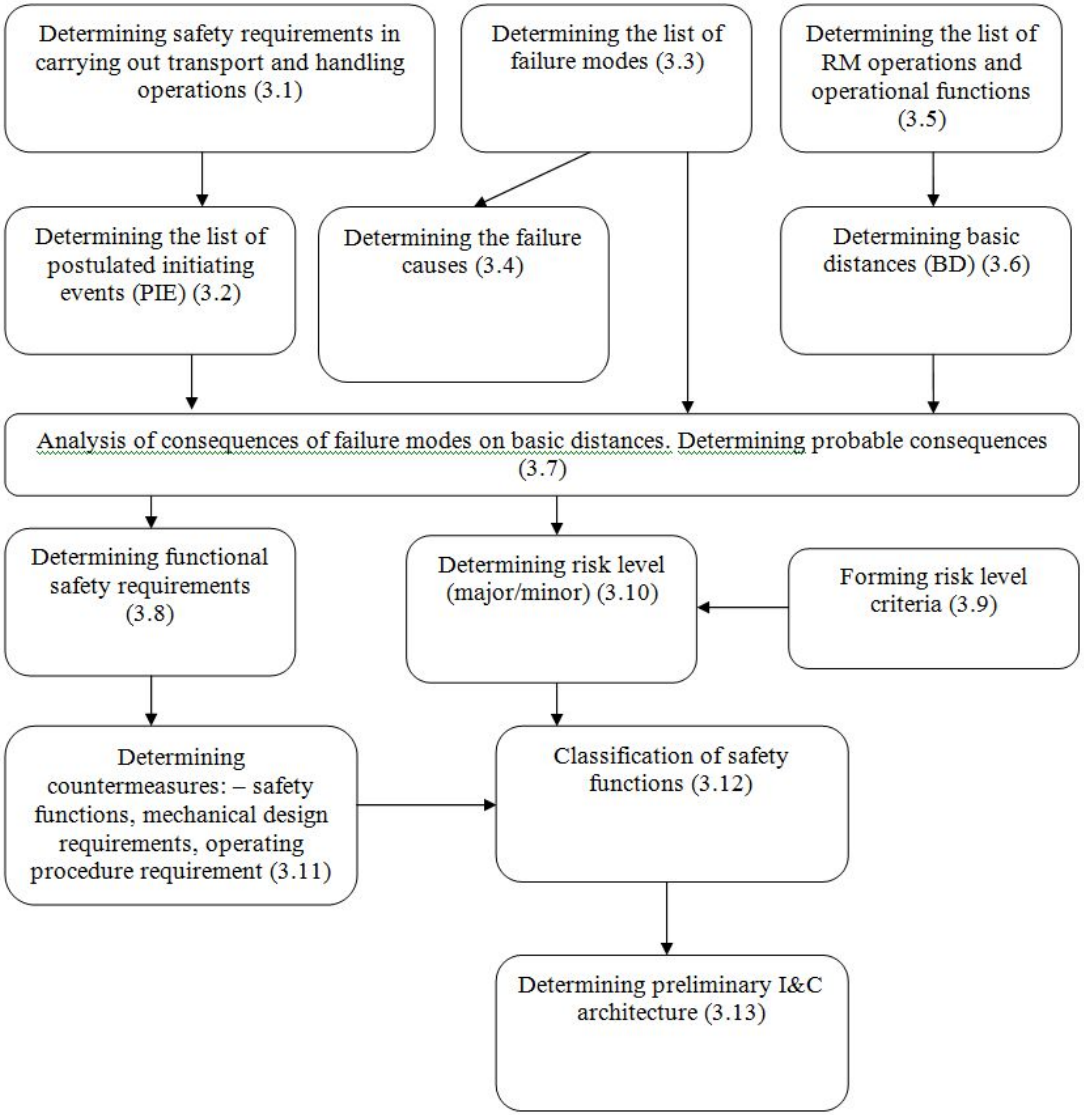
- Electrical Bridge Polar Crane l/c 360(205)/60/5/5+10t;

-Trestle Crane l/c 360(140)/60+10t;

- …

SEP-FH

Methodology of risk analysis and functional design



Example: SEP-FH define the risk-analysis method for FSDA. The examples of each stage are presented below in FSDA section.

ATOMPROEKT
Enterprise
of State Corporation Rosatom

PRESENTATION CONTENTS

- SAFETY ENGINEERING PLAN FOR FUEL HANDLING (SEP-FH)
- FUNCTIONAL SAFETY DESIGN & ARCHITECTURE (FSDA)
- SYSTEM REQUIREMENT SPECIFICATION (SRS)
- SYSTEM DESCRIPTION (SD)
- SYSTEM REQUIREMENT EVALUATION (SRE)

Mainly based on referent NPP data

FSDA-RM

Requirements from SEP-FH to FSDA on Refueling Machine (examples):

REQ ID	Description	Target document	Covers
ADLAS_FSDA-RM_QP-1.1-2_001	FSDA-RM shall follow the risk-analysis method described in SEP-FH	FSDA-RM	
ADLAS_FSDA-RM_QP-1.1-2_002	FSDA-RM shall define the list of countermeasures to reduce potential risks	FSDA-RM	
ADLAS_FSDA-RM_QP-1.1-2_003	FSDA-RM shall define the list of safety functions	FSDA-RM	
ADLAS_FSDA-RM_QP-1.1-2_004	FSDA-RM shall describe the preliminary I&C architecture	FSDA-RM	

ATOMPROEKT
Enterprise of State Corporation Rosatom

Main safety requirements for refueling machine

Main safety requirements for RM are based on YVL and EPC requirements for fuel handling at the NPP. The reference NPP experience is utilized as well.

See the next page

Requirement No.	Main safety requirement	Source
PSR-001	Design of the refueling machine shall ensure subcriticality under normal operation conditions and in case of possible accident	YVL-D.3-4.5-433 YVL-E.11-5.1-504 YVL-D.3-3.2-306 (b) REQ-C1-1142 REQ-C1-1684 REQ-C1-1179
PSR-002	Design of the refueling machine shall provide cooling of fuel assemblies during transportation	YVL-E.11-5.1-504 REQ-C1-1142 REQ-C1-1684
PSR-003	Design of the refueling machine shall ensure minimum probability of fuel damage (localization of radioactive substances)	YVL-E.11-5.1-504 YVL-E.11-1-106 YVL-D.3-3.2-306 (a) REQ-C1-1142 REQ-C1-1684
PSR-004	Design of the refueling machine shall ensure the required level of radiation protection (activity localization)	YVL-E.11-5.1-504 REQ-C1-1142 REQ-C1-1684
PSR-005	Design of the refueling machine shall ensure minimum probability of damage to CPS AR	Requirement of the General Designer

ATOMPROEKT
Enterprise of State Corporation Rosatom

Determining the list of Postulated Initiated Events (PIE)

List of postulated initiating events (hereinafter referred to as PIE) is a list of undesirable finite events while performing transport and handling operations by the refueling machine. Occurrence of these events actually means the disturbance of main safety requirements specified.

FA – Fuel Assembly

#PIE	Description	Base
PIE#01	FA falling	PSR-003
PIE#02	FA bending	PSR-003
PIE#03	FA compression	PSR-003
PIE#04	FA stretching	PSR-003
PIE#05	FA lateral impact	PSR-003
PIE#06	FA twisting	PSR-003
PIE#07	Inadmissible upper position of FA	PSR-002 PSR-004
PIE#08	Absorbing Rod bending	PSR-005
PIE#09	Absorbing Rod stretching	PSR-005
PIE#010	Falling of main mast into reactor (R), spent fuel pool (SFP), refueling well (RW)	PSR-003
PIE#011	Falling of Absorbing Rod into reactor (R), spent fuel pool (SFP), refueling well (RW)	PSR-003 PSR-005
PIE#012	Erroneous location of Absorbing Rod in the reactor with violation of refueling scheme requirements	PSR-001

ATOMPROEKT
Enterprise of State Corporation Rosatom

Determining the list of failure modes

Symbol	Name	Note
External failure modes (outside the reactor building)		
F001	Interruption in power supply	
F002	Seismic impact (Safe Shutdown Earthquake)	
	Aircraft crash	
	Air shock wave	
	... List according to YVL B.1	

External failure modes (inside the reactor building)		
F003	Collision	
F004	Inflammations and fires	
	Flooding caused by damage to equipment or pipes	
	Impacts of missiles	
	Explosions	
	Excessive strain	
	Malicious damage	

The document determines the full list of possible failure modes, which can occur during the RM operation. A detailed analysis of all possible deviations in the operation of refueling equipment mechanisms is carried out to determine the list of failure modes. Failure modes are divided to External (outside the reactor building), External (from RM point of view) and Internal (see the next slide)

ATOMPROEKT
Enterprise of State Corporation Rosatom

Determining the list of failure modes

Internal failure modes

All possible kinds of disturbances in operation of RM mechanisms and devices, regardless of their possible impact on safety of transport and handling operations with nuclear fuel are considered as internal failure modes of the refueling machine.

See the next page

- Destruction of the RM mechanisms and assemblies
- Failure modes associated with bridge travel
- Failure modes associated with trolley transfer
- Failure modes associated with travel of FA gripper
- Failure modes associated with the main mast sweep
- Failure modes associated with lock travel
- Failure modes associated with Control Rod gripper travel
- Failure modes associated with travel of FA lift-off mechanism
- Failure modes associated with placing Control Rods in the reactor

ATOMPROEKT
Enterprise of State Corporation Rosatom

Determining the list of failure modes

Internal failure modes		
Failure modes associated with bridge travel		
F030	Spurious actuation of bridge drive	
F031	Bridge transfer at speed exceeding the allowable speed	** for this transfer section
F032	Bridge positioning error without entering the area of inadmissible transfers	*** Boundaries of admissible transfer areas are determined by sensors.
F033	Bridge positioning error with entering the area of inadmissible transfers	

See the next page

ATOMPROEKT
Enterprise of State Corporation Rosatom

Determining the failure causes

Failure mode	Failure cause
F030 Spurious actuation of bridge drive	FC901 Unauthorized activation of power supply after loss of power supply
	FC001 Operator's error which results in untimely task for bridge travel
	FC201 Failure of remote control panel resulting in untimely generation of task for bridge travel
	FC301 Failure of control subsystem resulting in untimely generation of command for bridge travel
	FC401 Failure of actuator control subsystem resulting in untimely actuation of bridge travel

The preliminary list of failure causes has been identified. In the next phase requirement YVL-E.11-604 for FMEA will be prepared in more detail for component level by the equipment supplier (YVL-E.11-605).

FSDA-RM

Determining basic distances

Basic distances

Moving direction

- Horizontal
- Vertical
- Rotation

RM location

- Reactor, Fuel Pool, Refueling well
- Transport corridor

Speed ranges

- Operational speed
- Low speed

RM operations

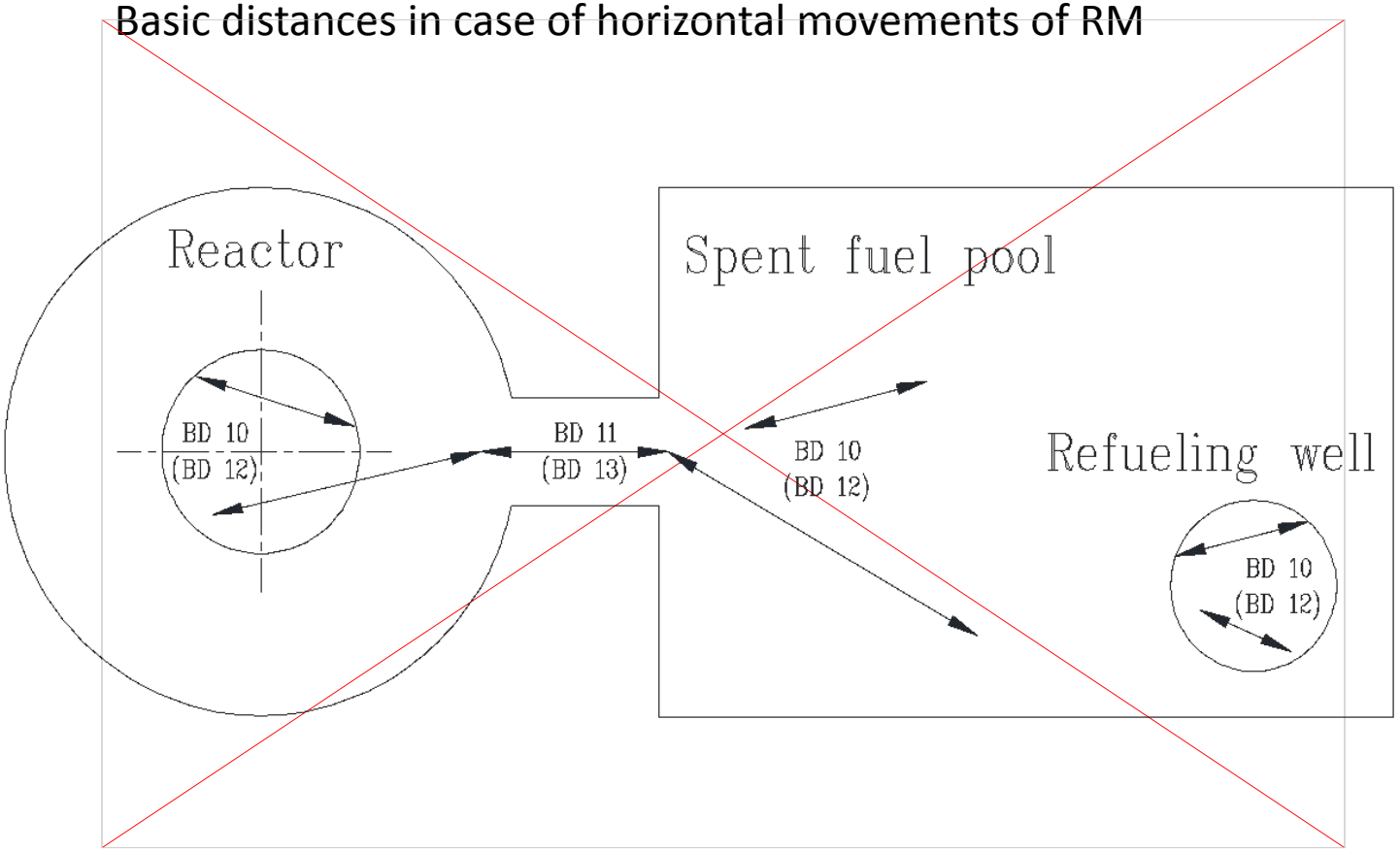
- Installation
- Extraction
- Transfer

Causes and conditions of PIE occurrence can significantly differ for various stages of transport and handling operations and even when performing a single process operation. Therefore, the essential stage of activity is allocation of specific areas of the nuclear fuel handling process, so-called basic distances, where causes and conditions of safety requirement violations remain invariable (causes and conditions of PIE occurrence).

ATOMPROEKT
Enterprise of State Corporation Rosatom

Determining basic distances

Basic distances in case of horizontal movements of RM



BD 10 – RM with FA or absorbing rod of the control and protection system (CPS AR)
(BD12) – RM without FA, CPS AR

ATOMPROEKT
Enterprise
of State Corporation Rosatom

Determining basic distances

Basic distances in case of vertical movements for the FA transfer operations.

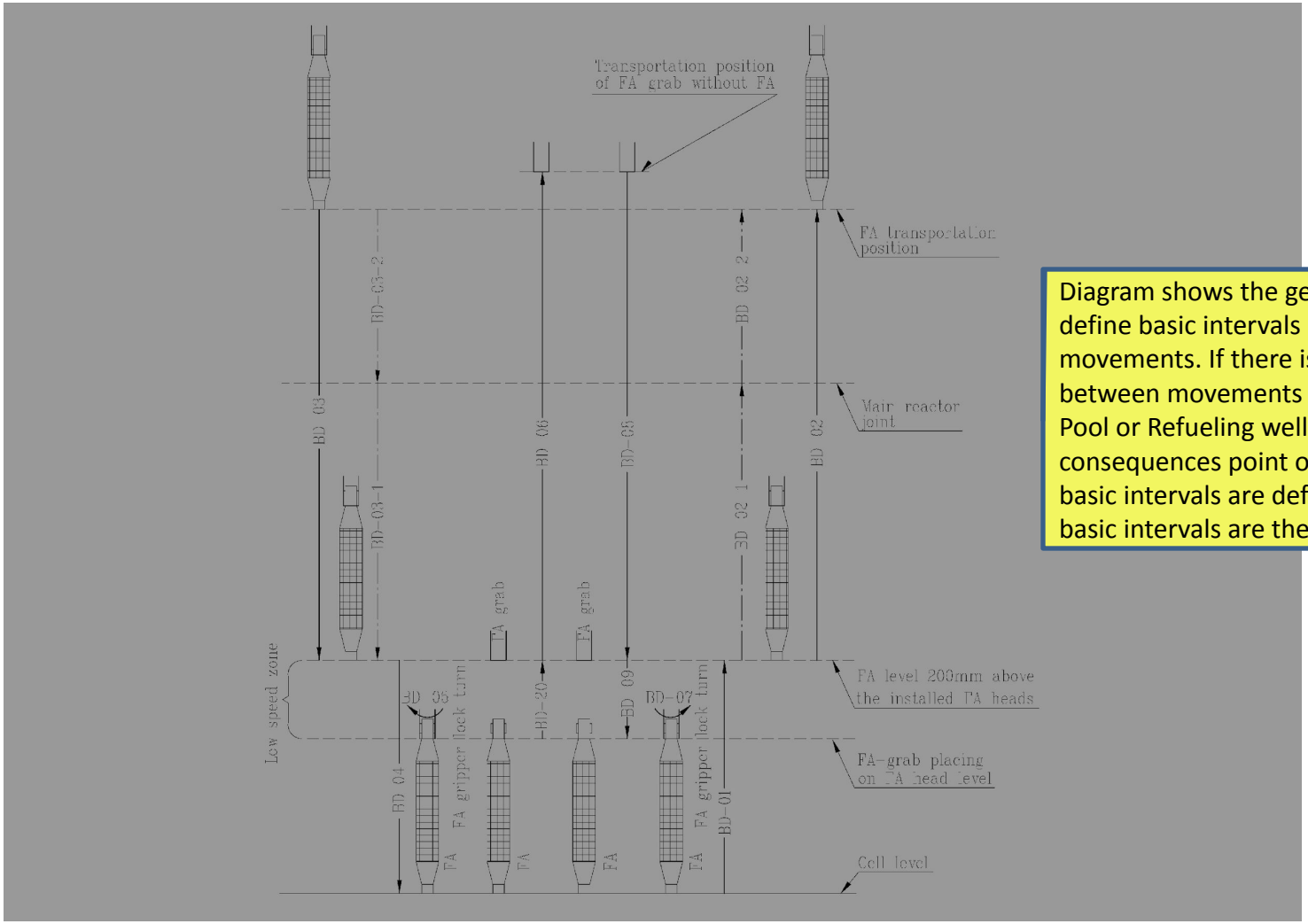
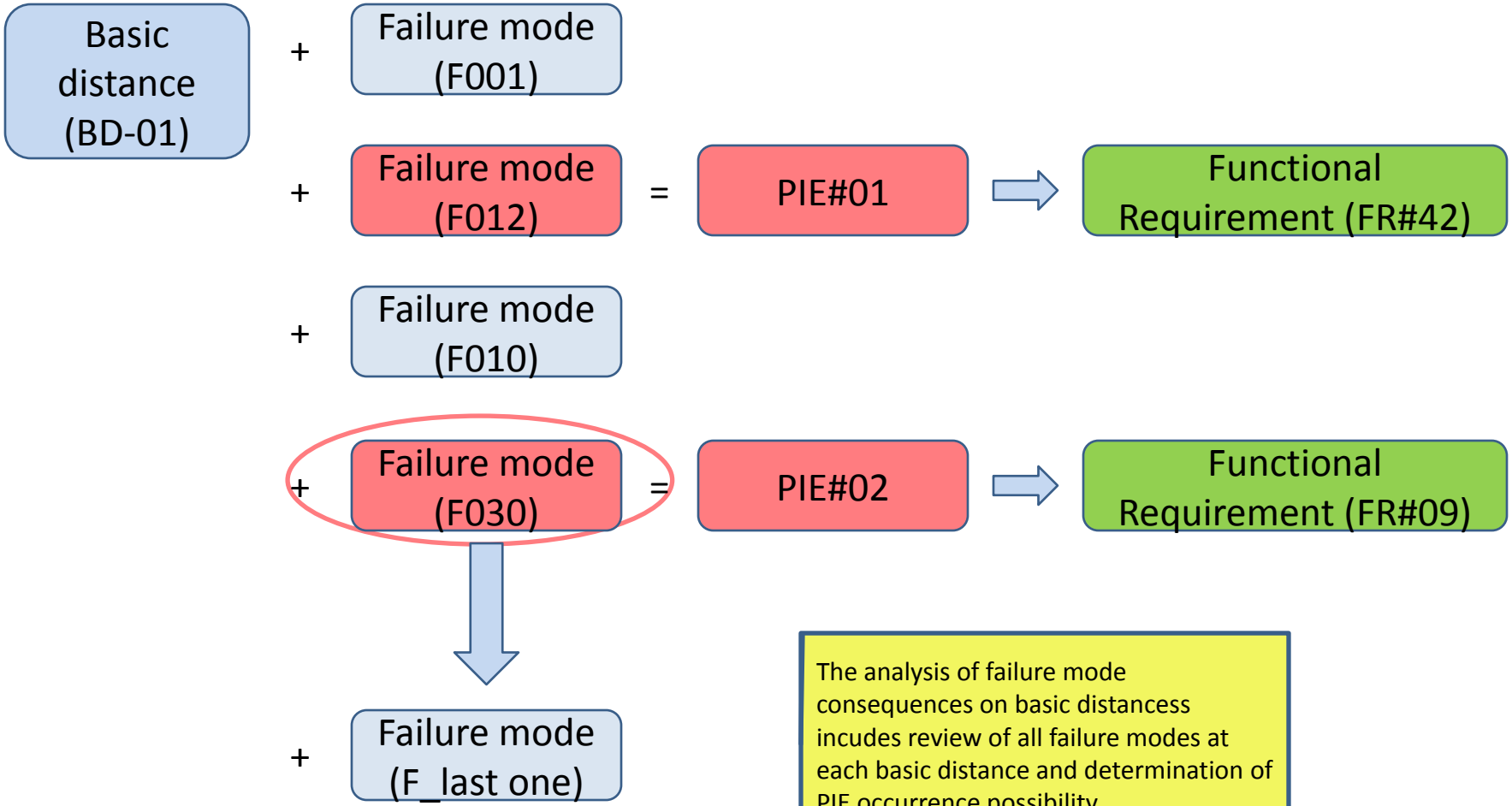


Diagram shows the general approach to define basic intervals in case of vertical movements. If there is a difference between movements in Reactor and Fuel Pool or Refueling well (from consequences point of view), special basic intervals are defined. Otherwise basic intervals are the same.

ATOMPROEKT
Enterprise of State Corporation Rosatom

Analysis of failure mode consequence on basic interval. Identification of safety requirements



The analysis of failure mode consequences on basic distancess incudes review of all failure modes at each basic distance and determination of PIE occurrence possibility.

ATOMPROEKT
Enterprise of State Corporation Rosatom

Nuclear hazards severity

RISK

MAJOR

- leads to release of active substances due to failure of FE cladding;
- leads to subcriticality disturbance.

MINOR

- minor damage FA without loss of of the fuel cladding integrity;
- damage of Control Rod;
- damage of RM mechanisms;

NO RISK

- no countermeasure for refueling machine is needed, some other SSC prevent the risk.
  Example: mispositioning of control rod in the reactor - subcriticality is ensured by boron injection

In this document the risks are divided into major and minor risks on the basis of severity of the nuclear consequences. «No risk» is used when safety is ensured without RM participation. Risk level is a defining criterion in further selection of counter-measures, classification of safety functions and selection of the way of their implementation.
At this preliminary stage of analysis conservative approach is used. Each risk which couldn't be classified as Minor without calculations was classified as Major. The results will be updated at the stage of Manufacturer detailed analysis.

ATOMPROEKT
Enterprise of State Corporation Rosatom

Definition of countermeasures

A counter-measure is considered to be main if there are no other counter-measures capable to prevent the occurrence of PIE in case of the this counter measure failure. Other counter-measures are preventive.

Functional Requirement (FR#42)

Countermeasures

Main countermeasures:

- Mechanical design requirement
- Safety I&C functions
- Operating procedure requirement

Preventive countermeasures:

- Mechanical design requirement
- Safety I&C functions
- Operating procedure requirement

ATOMPROEKT
Enterprise
of State Corporation Rosatom

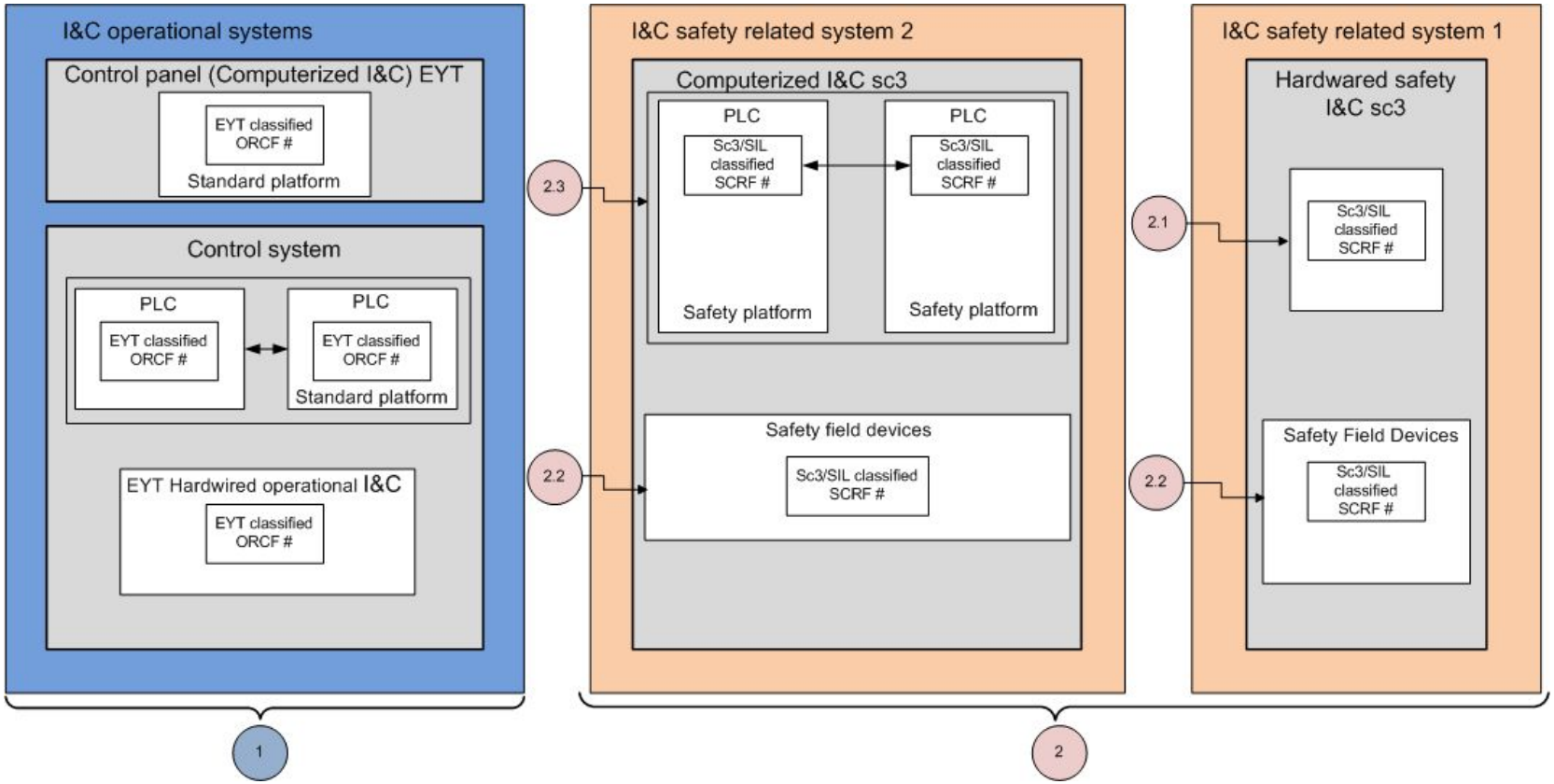
Risk analysis example

9.1.5.7 Refueling machine. Functional Safety Design and Architecture (FSDA).

Appendix 1 – Risk analysis table

ATOMPROEKT
Enterprise of State Corporation Rosatom

Preliminary I&C safety architecture



Preliminary safety architecture shows the implementation of RM functions. Functions are attributed to blocks on diagram in accordance with the following principle:
Operational functions – 1, Safety functions – 2.
In case there is strict requirement to implement the safety function:
- if there is no software – 2.1;
- if the function is activated by component with its own software (safety field device) – 2.2;
- If the function is activated by Programmable logic controller (PLC) – 2.3;
-Operational functions follow the same principle.

ATOMPROEKT
Enterprise
of State Corporation Rosatom

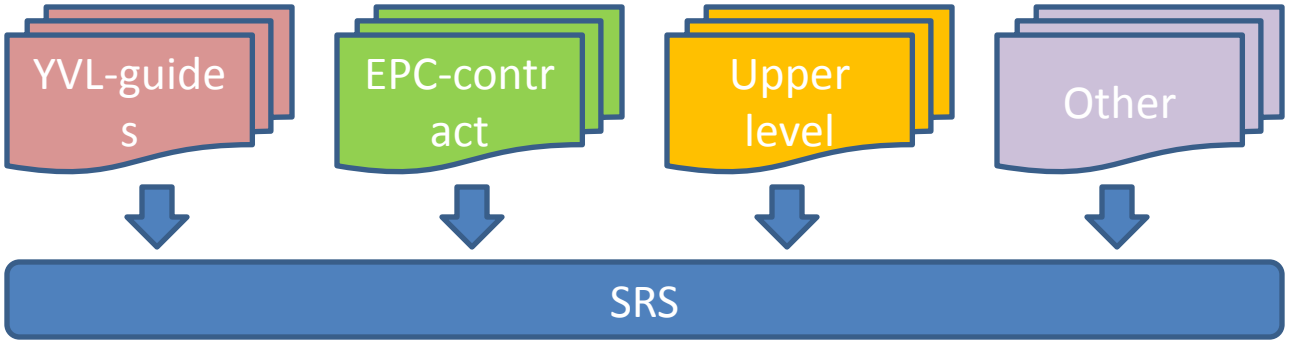
PRESENTATION CONTENTS

- SAFETY ENGINEERING PLAN FOR FUEL HANDLING (SEP-FH)
- FUNCTIONAL SAFETY DESIGN & ARCHITECTURE (FSDA)
- **SYSTEM REQUIREMENT SPECIFICATION (SRS)**
- SYSTEM DESCRIPTION (SD)
- SYSTEM REQUIREMENT EVALUATION (SRE)

ATOMPROEKT
Enterprise of State Corporation Rosatom

System Requirement Specification

The purpose of this document is to present all the requirements related to the Refueling Machine (RM) from YVL-guides, EPC-contract, Upper level documents and other sources.
Moreover, this document elaborates further requirements and provides traceability of the requirements.



According to YVL E.11-5.1-517 safety functions that have been identified on the basis of the hoisting device unit's risk analysis (FSDA) shall be focused on the hoisting device unit's subsystems as functional requirements (SRS).

Example:

3.1.8 Requirements for radiation safety

#	Req ID	Description	Covers
1.	ADLAS-SRS_FCA10-YVL-005	Refueling machine shall be designed to allow decontamination operations.	YVL-D.4-4.4-436 YVL-B.1-4.1-408 YVL-E.11-5.1-537 REQ-B8-960 REQ-B8-961 REQ-B8-1343 REQ-C5-187 REQ-C5-2776 REQ-C7-873

ATOMPROEKT
Enterprise
of State Corporation Rosatom

PRESENTATION CONTENTS

- SAFETY ENGINEERING PLAN FOR FUEL HANDLING (SEP-FH)
- FUNCTIONAL SAFETY DESIGN & ARCHITECTURE (FSDA)
- SYSTEM REQUIREMENT SPECIFICATION (SRS)
- **SYSTEM DESCRIPTION (SD)**
- SYSTEM REQUIREMENT EVALUATION (SRE)

Mostly based on the reference NPP data

ATOMPROEKT
Enterprise
of State Corporation Rosatom

Contents

9.1.5 Transportation and Handling Equipment of the Fuel Handling System
9.1.5.7. REFUELING MACHINE

Structure is based on KAA pilot

System description

General information

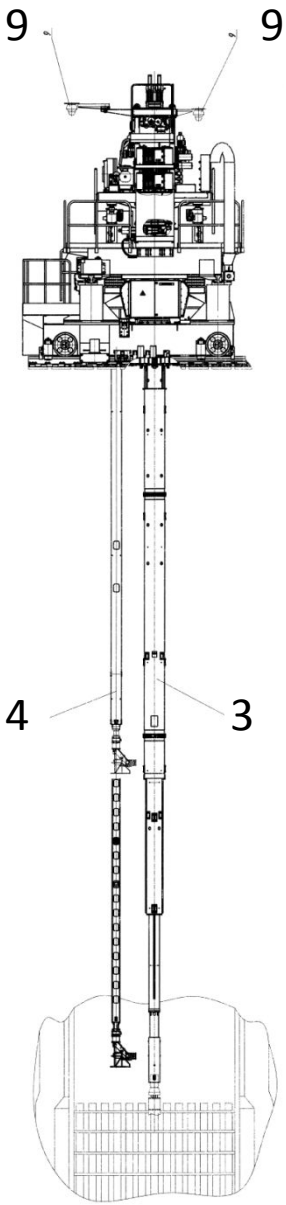
The RM is designed for :

- fresh and spent fuel handling;
- handling of absorbing rods of the control and protection system (hereinafter CPS AR);
- monitoring of FA tightness;
- monitoring of FA and CPS AR reloading using video control system;
- tools handling:
    - CPS AR cask;
    - device for FA installation level monitoring;
    - FA seats inspection device;
    - FA inspection device;
    - device for lifting of dropped FA and leak-tight bottle.

System description

ATOMPROEKT
Enterprise of State Corporation Rosatom

RM frontal view



Description of RM components

The refueling machine (RM) consists of a bridge (1) located in the central hall at the elevation of +31,200, a trolley (2) on which the main operating components of the machine are installed: the main mast (3) and TV arm (4).

Power to electrical equipment located on RM are supplied trough the local cabinet (7) and cable chain (5)

"Seismic terminal" for seismic clamps on the bridge is located outside the rail track (8).

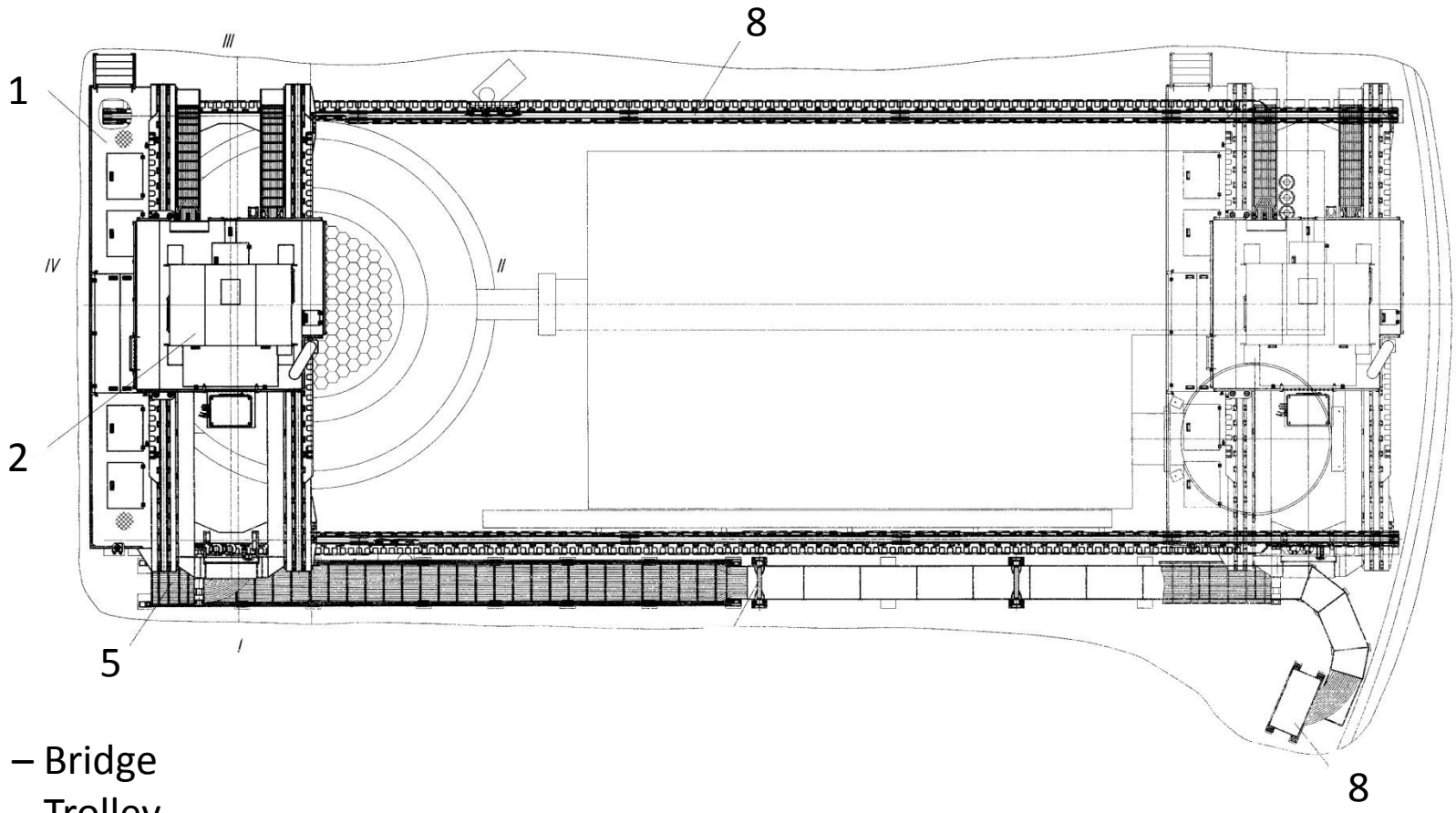
The RM is controlled from a stationary remote control room located outside the reactor building containment. The control and monitoring equipment is located in the control room.

3 – Main mast
4 – TV arm
9 – TV cameras

System description

ATOMPROEKT
Enterprise of State Corporation Rosatom

RM top view

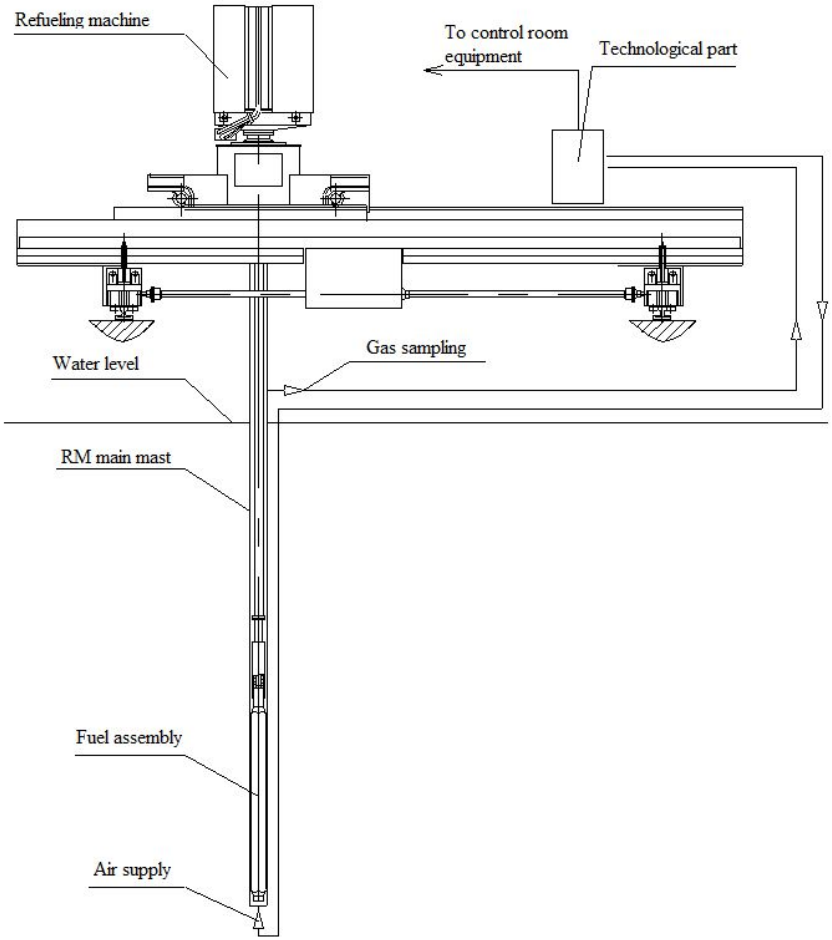


1 – Bridge
2 – Trolley
5 – Cable chain
7 – RM local cabinet
8 – Rail track

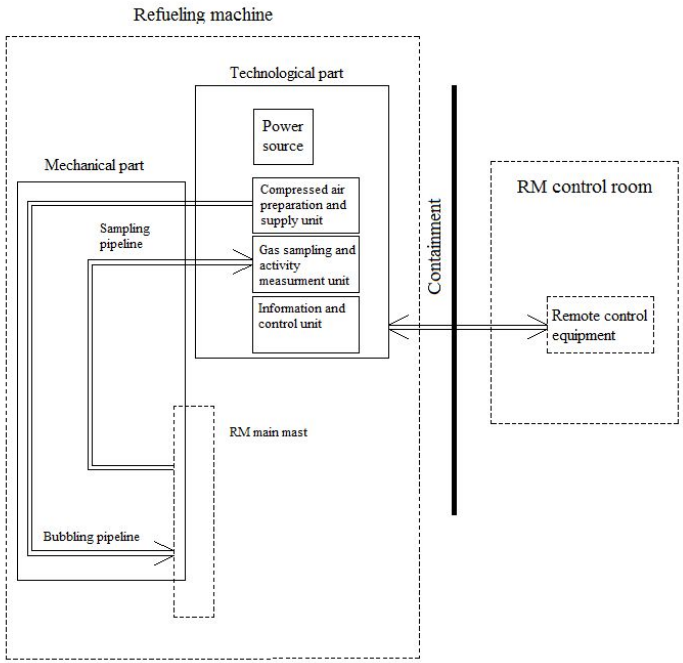
System description

ATOMPROEKT
Enterprise
of State Corporation Rosatom

Fuel cladding integrity monitoring system (RM CIMS)



Schematic diagram of the RM CIMS



Structural diagram of the RM CIMS

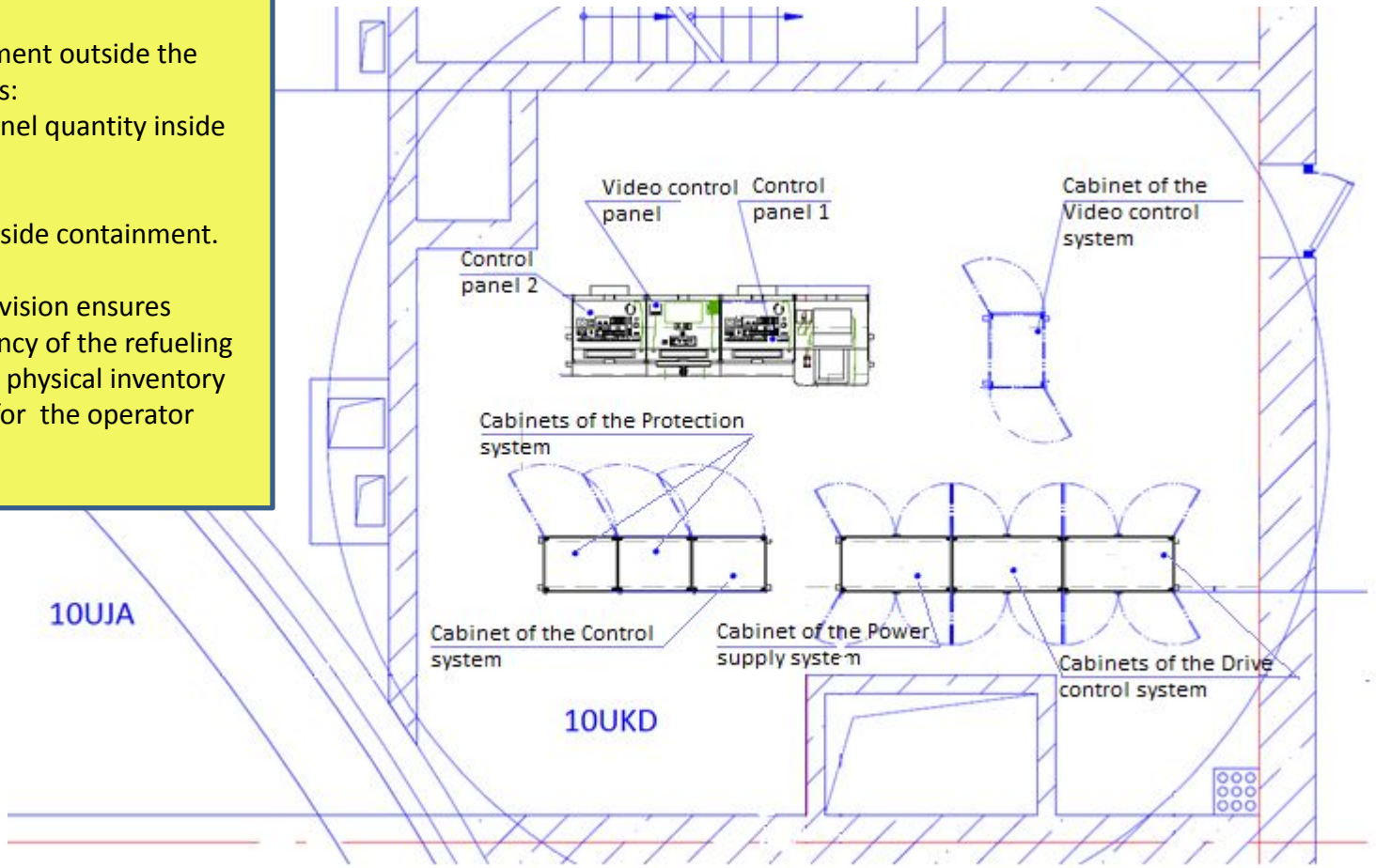
System description

ATOMPROEKT
Enterprise of State Corporation Rosatom

RM control room location (based on referent NPP)

Control room placement outside the containment reasons:
- limitation of personnel quantity inside the containment;
- more economical;
- shortage of place inside containment.

Remote video supervision ensures entirety and sufficiency of the refueling process control and physical inventory of the nuclear fuel for the operator



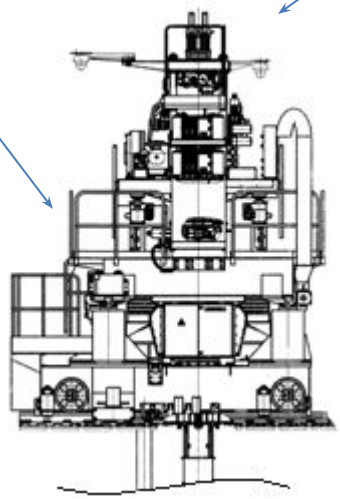
RM control room is located in free access area in the Safety building 10UKD.

ATOMPROEKT
Enterprise of State Corporation Rosatom

3.2 Interfaces with other systems

Spent fuel pool water level

Gamma background level above the Spent fuel pool (Automated monitoring system of radiation situation in the premises and at the site)



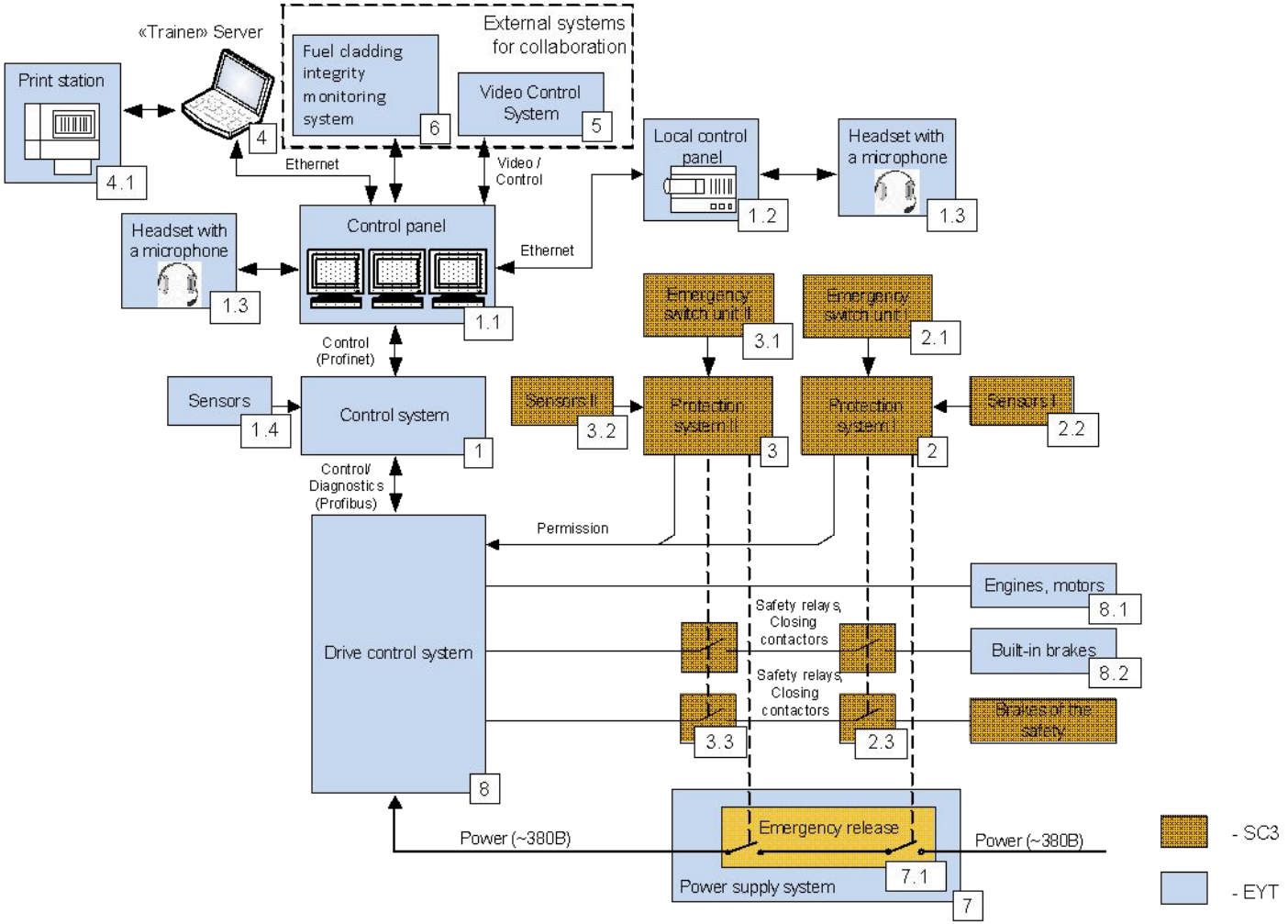
Neutron flux density: “STOP” signal from Neutron flux monitoring system

Signal from seismic sensors of the industrial ant seismic protection system

Signal from the instrumentation and control system of safety systems

System description

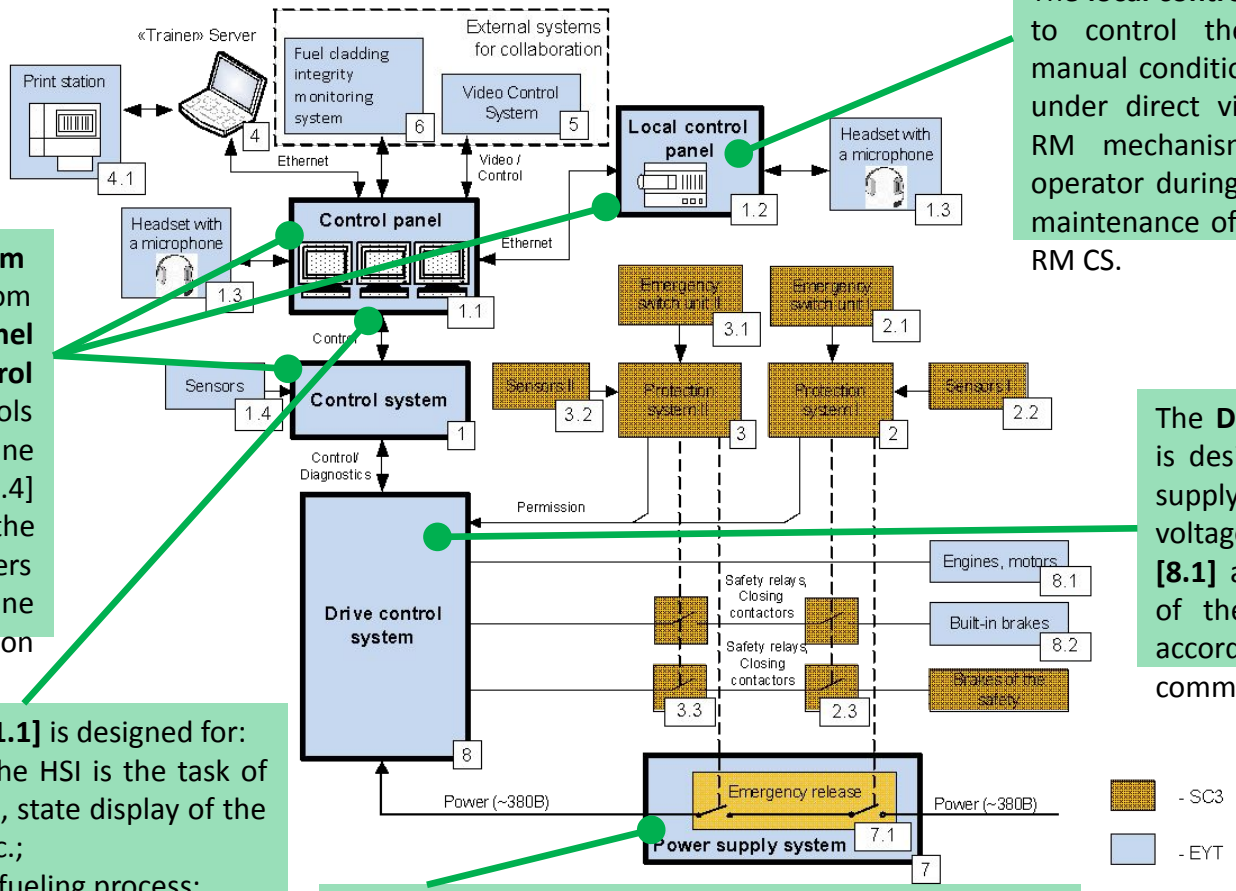
I&C conceptual structure



System description

ATOMPROEKT
Enterprise of State Corporation Rosatom

I&C systems of the RM is designed to control the movement of the RM and ensure continuous monitoring of the RM parameters during the refueling in the normal operation mode at the stopped power unit.



The **Control system [1]** receives task from **Local Control Panel [1.2]** and **Control Panel [1.1]**. It controls Refueling machine using sensors [1.4] measuring the different parameters of Refueling Machine like speed, position and load.

The **local control panel [1.2]** is designed to control the RM mechanisms in manual conditions from the central hall under direct visual supervision of the RM mechanism movements by the operator during the commissioning and maintenance of the RM jointly with the RM CS.

The **Drive Control System [8]** is designed to provide power supply and removal of supply voltages of electric **motors [8.1]** and **brake devices [8.2]** of the drive of the RM in accordance with accepted commands.

The **Control Panel [1.1]** is designed for:
- arrangement of the HSI is the task of the operation mode, state display of the RM mechanisms, etc.;
- recording of the refueling process;
- generation and **printing** of documents by the results of work **[4] [4.1]**

The **Power Supply System [7]** is designed to receive initial power supply of the 400 V three-phase voltage, 50 Hz, using two inputs from the 0.4 kV auxiliary switchgear and its conversion, distribution, controlled power supply for the RM CSs and the refueling machine electrical equipment.

System description

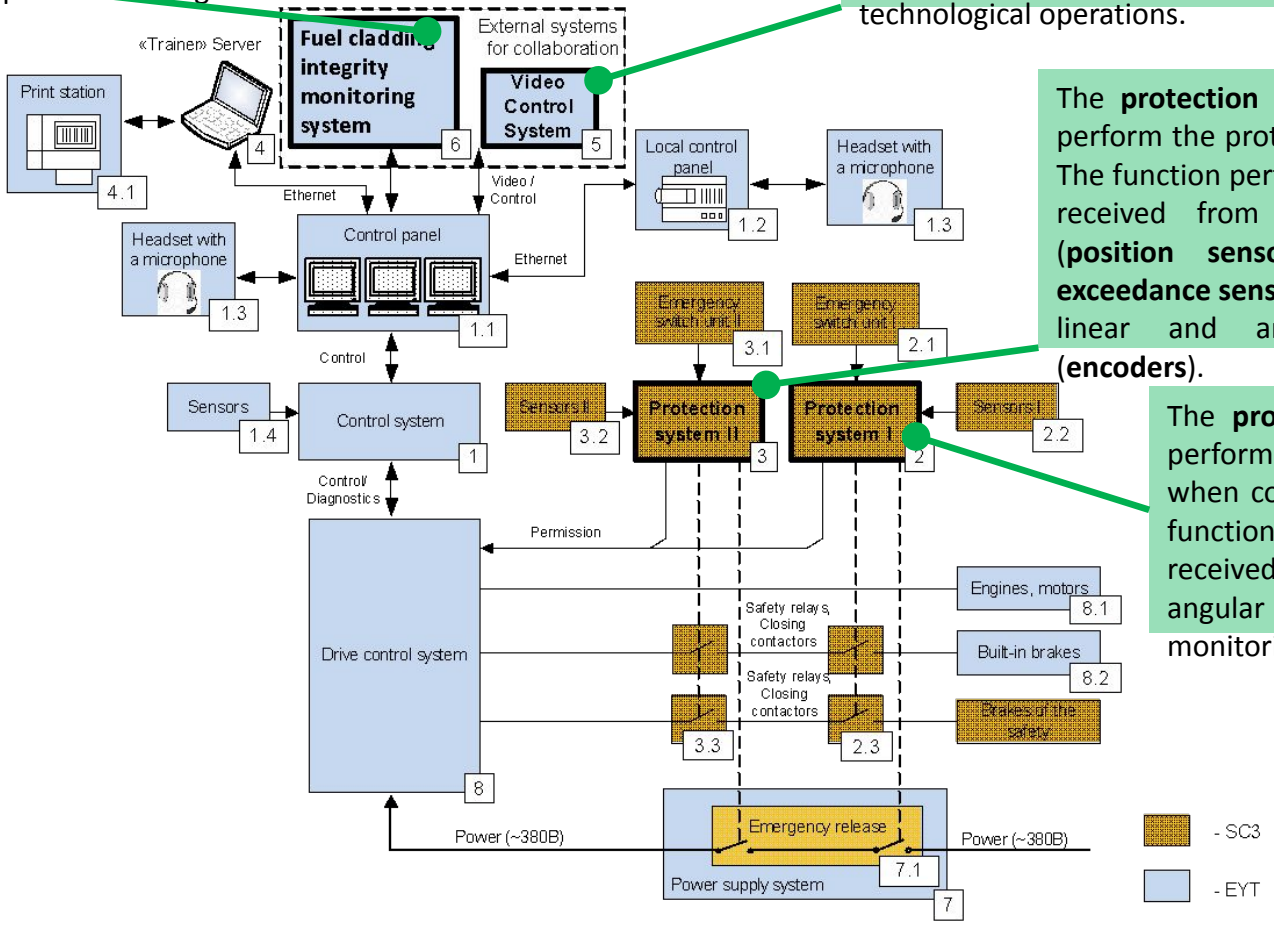
ATOMPROEKT
Enterprise of State Corporation Rosatom

The **Fuel cladding integrity monitoring system [6]** is designed to detect on-line FA with leaky FE at the shutdown reactor after the FAs are lifted from the core to transportation position in response to gaseous fission products released by FA into the water filling the inner space of working shaft.

The **video control system [5]** is designed to realize remote video observation while performing the process of FA reloading and physical inventory of the nuclear fuel, as well as to provide working area video control of the RM as whole in central hall during the technological operations.

The **protection system II [3]** is designed to perform the protection and interlock function. The function performance is based on the data received from its own discrete sensors (**position sensors** and **maximum force exceedance sensors**), force control sensors and linear and angular movement sensors (**encoders**).

The **protection system I [2]** is designed to perform the protection and interlock function, when controlling the RM. Performance of the functions takes into account the information received from its own sensors of linear and angular movements (**encoders**) and force monitoring sensors (**strain gage sensors**).



System description

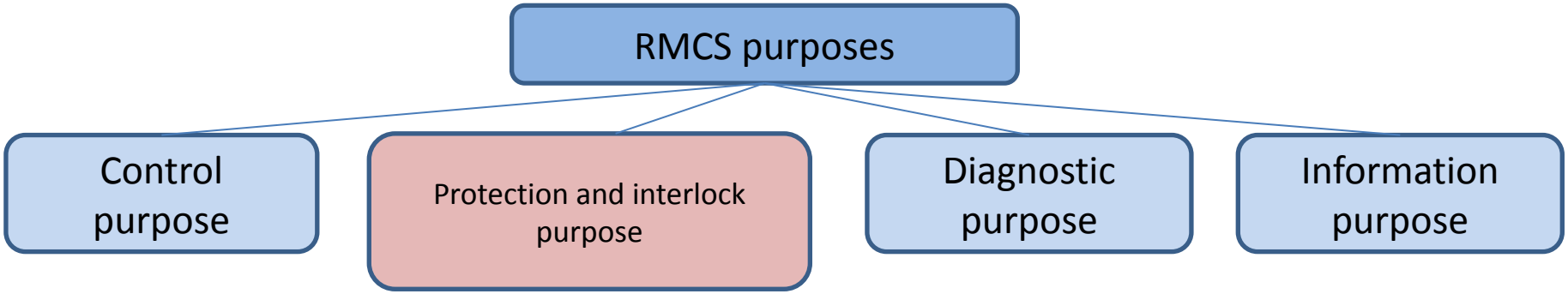
Composition of RM systems with preliminary safety classification.

RM systems are composed of the following components given in table:

#	RM systems	RM systems equipment	Safety class
		I&C	
1	Control system	Cabinet of the Control system	EYT
		Control panel 1	
		Control panel 2	
		Local control panel	
2	Protection system I	Cabinet of the Protection system I	SC3
3	Protection system II	Cabinet of the Protection system II	SC3
4	«Trainer» Server, Printer station	Laptop	EYT
		Printer	
5	VCS (Video control system)	Cabinet of the Video control system	EYT
		Video control panel	
6	Fuel cladding integrity monitoring system (RM CIMS)	Remote control equipment (Laptop)	EYT
		Technological part of the RM CIMS	
		Electrical	
7	Power supply system	Cabinet of the Power supply system	EYT (Emergency release - SC3)
8	Drive control system	Cabinet of the Drive control system I	EYT
		Cabinet of the Drive control system II	EYT

ATOMPROEKT
Enterprise of State Corporation Rosatom

3.6.2 RMCS purposes:



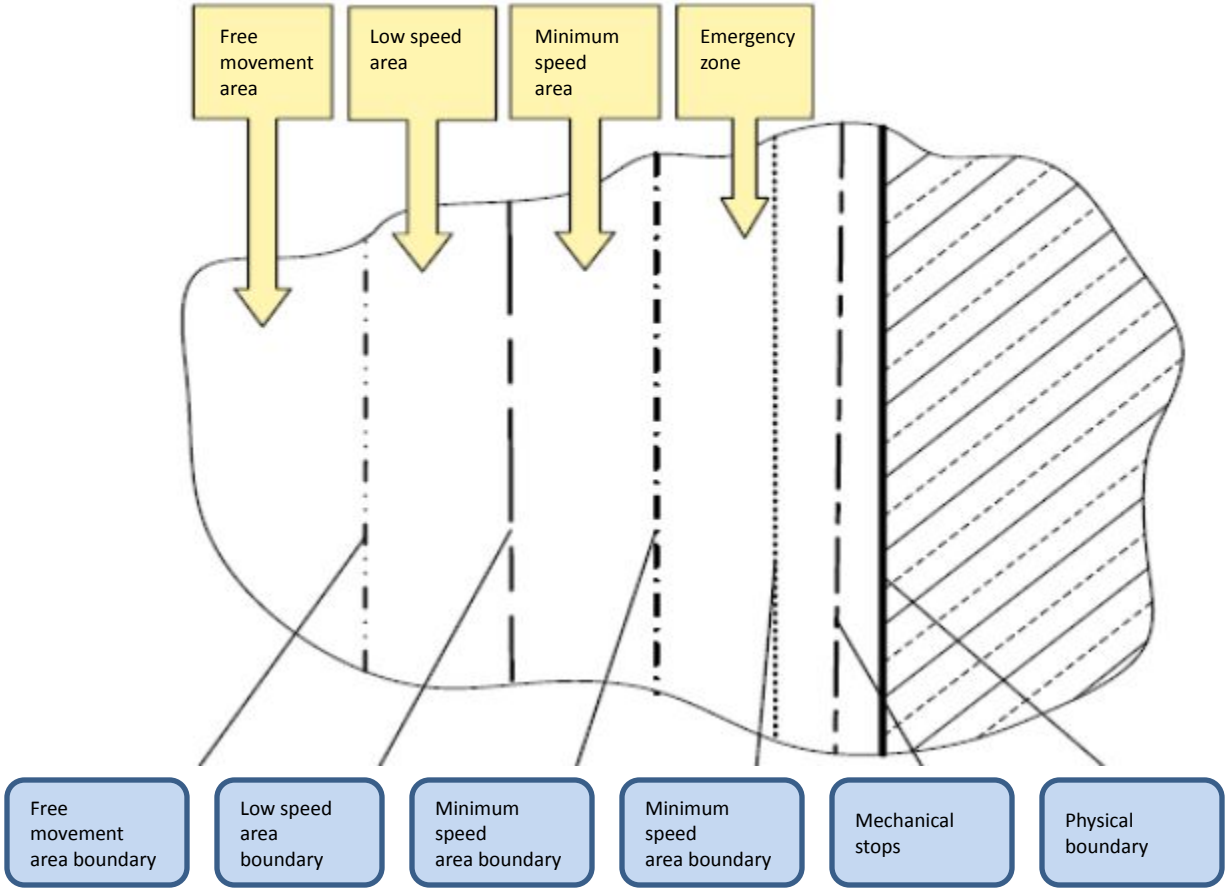
System description

RMCS control conditions

Control conditions	Interlocks	Description	Operator location	Example
Automatic (automatic cyclic) – (AC);	on	Cycle according to pre-developed refueling program	Remote control room	Usual refueling
Semi-automatic 1	on	Operation from the list	Remote control room	Abnormal operation
Semi-automatic 2	on	Cycle from the list	Remote control room	Usual refueling
Manual with interlocks	on	1 mechanism moving	Remote control room / Local control panel	Abnormal operation
Manual without interlocks	Partly off	-1 mechanism moving ; - minimum speed; - pre-defined set of interlocks;	Remote control room / Local control panel	- if it is required to complete a current operation under abnormal situations and in case of impossibility to control the RM under the other conditions; - during adjustment and alignment of the mechanisms.

System description

Permissible horizontal movement area of RM mechanisms



ATOMPROEKT
Enterprise
of State Corporation Rosatom

PRESENTATION CONTENTS

- SAFETY ENGINEERING PLAN FOR FUEL HANDLING (SEP-FH)
- FUNCTIONAL SAFETY DESIGN & ARCHITECTURE (FSDA)
- SYSTEM REQUIREMENT SPECIFICATION (SRS)
- SYSTEM DESCRIPTION (SD)
- **SYSTEM REQUIREMENT EVALUATION (SRE)**

ATOMPROEKT
Enterprise
of State Corporation Rosatom

System Requirement Evaluation

This document includes the list of requirements developed in the System requirement specification document for RM and references to the System description document where performance of the given requirements is shown. Moreover, this document includes the information on properties and the status of requirements and system description. The document is developed in accordance with the KAA pilot.

Example:

	A	C	D	E	G	H	I	J	K	L	M	Q	R	S	T	U	AA	AB	AC	AD
1	ADLAS_ID	Object Text	Req_revision	Requirement_status	SD_ID	SD_revision	SD_reference	V&V_planning	Fulfilment_as_designed_document_reference	Fulfilment_as_designed_document_revision	Fulfilment_as_designed_document_status	Requirement_Fin	Comments	Setting_document_revision	Status_of_setting_document	Designer_conformity_statement	Allocation_document	Allocated_requirement_text	Parent ID	Parent ID_revision
																			YVL-D.4-4.4-436	2013-11-15
																			YVL-B.1-4.1-408	2013-11-15
																			YVL-E.11-5.1-537	2013-11-15
																			REQ-B8-960	5.0
					FH1.B.P0				FH1.B.P0								FH1.B.P0		REQ-B8-961	5.0
					00.1.0901				00.1.0901								00.1.0901		REQ-B8-1343	5.0
	ADLAS-				05.07&&		9		05.07&&								05.07&&		REQ-C5-187	7.0
	SRS_FCA1	The system shall be designed to			&&.061.H		Material		&&.061.H								&&.061.H		REQ-C5-2776	7.0
17	0-YVL-005	allow decontamination operations on its equipment.	1.0	Valid	E.0001	1	s	Document review	E.0001	1	Valid			1	Valid	Conformity	E.0001		REQ-C7-873	8.0

ATOMPROEKT
Enterprise
of State Corporation Rosatom

Thank you for attention

ATOMPROEKT
Enterprise
of State Corporation Rosatom

Thank you for attention

ATOMPROEKT
Enterprise
of State Corporation Rosatom

Thank you for attention