

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

Helsinki, 18th of May 2017

Speakers: Aleksandr Kutuzov Aleksandr Brunov



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)



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-<u>FH</u>)

. . .



- Electrical Bridge Polar Crane I/c 360(205)/60/5/5+10t;
- -Trestle Crane I/c 360(140)/60+10t;





PRESENTATION CONTENTS

SAFETY ENGINEERING PLAN FOR FUEL HANDLING (SEP-FH)

Mainly based on referent NPP data

FUNCTIONAL SAFETY DESIGN & ARCHITECTURE (FSDA)

SYSTEM REQUIREMENT SPECIFICATION (SRS)

SYSTEM DESCRIPTION (SD)

SYSTEM REQUIREMENT EVALUATION (SRE)





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	

FSDA-RM



Main safety requirements for refueling machine

	Requirement No.	Main safety requirement	Source
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.	PSR-001	Design of the refueling machine shall ensure <u>subcriticality</u> 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-C1-1684
	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
See the next page	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



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		PSR-002			
	Inadmissible upper position of FA	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	PSR-003			
	(R), spent fuel pool (SFP), refueling well (RW)	PSR-005			
PIE#012	Erroneous location of Absorbing Rod in the reactor with violation of refueling scheme requirements	PSR-001			

FSDA-RM





Determining the list of failure modes

Symbol	Name	Note
	External failure modes (outside the reactor	r 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							
9	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)





FSDA-RM

Determining the list of failure modes

6	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								
F033	Bridge positioning error with entering the area of inadmissible transfers	areas are determined by sensors.								

See the next page



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

FSDA-RM

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).



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).



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



Determining basic distances

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

FSDA-RM







- leads to subcriticality disturbance.

- 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.





Risk analysis example

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

Appendix 1 – Risk analysis table



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.



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)



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

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



PRESENTATION CONTENTS

SAFETY ENGINEERING PLAN FOR FUEL HANDLING (SEP-FH)

FUNCTIONAL SAFETY DESIGN & ARCHITECTURE (FSDA)

SYSTEM REQUIREMENT SPECIFICATION (SRS)

Mostly based on the reference NPP data

SYSTEM DESCRIPTION (SD)

SYSTEM REQUIREMENT EVALUATION (SRE)



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

Structure is based on KAA pilot





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.



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





8 – Rail track



Fuel cladding integrity monitoring system (RM CIMS)





Structural diagram of the RM CIMS

Schematic diagram of the RM CIMS



RM control room location (based on referent NPP)



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



3.2 Interfaces with other systems

Spent fuel pool water level

Neutron flux density: "STOP" signal from Neutron flux monitoring system

System description

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

Signal from seismic sensors of the industrial ant seismic protection system

Signal from the instrumentation and control system of safety systems

ATOMPROEKT Enterprise of State Corporation Rosatom

System description

I&C conceptual structure



2.2

8.1

8.2

SC3

- EYT



[1.2]

using

Refueling

measuring

and load.

and

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 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.



Print station

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.

technological operations. External systems Fuel claddin... «Trainer» Server for collaboration integrity Video monitoring Control system System Local control Headset with a microphone panel Video / 4.1 Ethernet Control 000 1.3 Control panel Headset with a microphone Ethernet Emergency Energency search and Switch unit 2.1 3.1 Control (encoders). Sensors Sensors Protection Protection Sensors I Control system system I 2.2 system li 3.2 Control/ Diagnostics Permission Engines, motors Safety relays. 8.1 Closing contactors Built-in brakes Drive control system Safety relay 8.2 Closing Brakes of the contactors satety 3.3 2.3 8 Emergency release - SC3 Power (~380B) Power (~380B)

7.1

Power supply system

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.

- FYT

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**).



Composition of RM systems with preliminary safety classification.

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

#	RM systems	RM systems	Safety class				
		equipment					
		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					
		Printer	EYT				
5	VCS (Video control system)	Cabinet of the Video control system	EYT				
		Video control panel					
6	Fuel cladding integrity monitoring system	Remote control equipment (Laptop)					
	(RM CIMS)	Technological part of the RM CIMS					
			EYT				
		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				





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. 				



Permissible horizontal movement area of RM mechanisms





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)



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	Н	1	J	K	L	M	Q	R	S	Т	U	AA	AB	AC	AD	Ē
	ADLAS_ID	Object Text	Req_revis	Requirement_	SD_ID	SD_revisi	SD_refer	V&V_planni	Fulfilmen	Fulfilmen	Fulfilmen	Requirem	Comment	Setting_d	Status_of	Designer	Allocation	Allocated	Parent ID	Parent	
			ION	status		011	ence	"6	gned doc	gned doc	gned doc	cm_rm	3	revision	document	ity state	_uocume	ment tex		ID_ICVISION	
									ument re	ument re	ument st					ment		t			
									ference	vision	atus										
1																					
							1										1		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-88-960	5.0	
					FH1.B.PO				FH1.B.PO								FH1.B.PO		REQ-88-961	5.0	
					00.1.0901				00.1.0901								00.1.0901		REQ-B8-1343	5.0	
	ADLAS-	The system shall be designed to			05.07&&		9		05.07&&								05.07&&		REQ-C5-187	7.0	
	SRS_FCA1	allow decontamination			&&.061.H		Material	Document	&&.061.H							Conformi	&&.061.H		REQ-C5-2776	7.0	
17	0-YVL-005	operations on its equipment.	1.0	Valid	E.0001	1	s	review	E.0001	1	Valid			1	Valid	ty	E.0001		REQ-C7-873	8.0	



Thank you for attention



Thank you for attention



Thank you for attention