Assuring Shutdown Safety at Krško NPP

Ivo Žarković, Marin Ivanjko, Silvio Bratić
Nuclear Power Plant Krško
Vrbina 12, 8270 Krško, Slovenia
ivo.zarkovic@nek.si; marin.ivanjko@nek.si; silvio.bratic@nek.si

ABSTRACT

Nuclear power plant operating experience has shown that PWRs are susceptible to a variety of events during shutdown conditions. While these events have caused no harm to the public, nor posed an undue risk, they do illustrate that careful attention to outage management and shutdown operation is necessary to maintain adequate defence-in-depth for safety functions.

Many activities including generic communications, site visits, workshops, studies and surveys conducted by the Institute of Nuclear Power Operations (INPO), the Electric Power Research Institute (EPRI), and the World Association of Nuclear Operators (WANO), have heightened the awareness of shutdown concerns. This awareness is a prerequisite to enhancing shutdown safety.

The scope of activities that each utility undertakes during a normal refuelling outage is large and diverse. Besides refuelling, activities associated with preventive and corrective maintenance, modifications, surveillance testing, in-service inspection, and the administrative activities that support these tasks make outage planning and control a significant challenge. The coordination of these activities with the objective to manage risk and maintain key safety functions is essential and goes beyond compliance with technical specifications requirements during shutdown. In addition, while the scope of activities for an unplanned or forced outage is far less than that of a refuelling outage, the same awareness of vulnerabilities during shutdown conditions is required to safely conduct these outages.

The critical outage safety functions at Krško NPP are reactivity control, decay heat removal, reactor coolant inventory control, electrical power availability, spent fuel pit cooling, support systems availability and containment integrity. Those functions provide baseline for creating the outage plan. Activities planned for the upcoming outage contain Outage Risk Assessment and Management (ORAM) codes which serve as input data for Krško NPP Outage deterministic and PSA evaluation using software tool PARAGON. Results of the calculations are Core Damage Frequency, Core Damage Probability and the status of the equipment required to fulfil critical safety functions during shutdown.

As an example, preparation and execution of Krško NPP 2019 and 2021 outages are shown as well as how is the monitoring of the critical safety functions being performed during outage execution.

Keywords: *shutdown safety, outage, planning, equipment protection*

1. INTRODUCTION

The scope of activities that each utility undertakes during a normal refuelling outage is large and diverse. Besides refuelling, activities associated with preventive and corrective maintenance, modifications, surveillance testing, in-service inspection, and the administrative activities that support these tasks make outage planning and control a significant challenge. The coordination of these activities with the objective to manage risk and maintain key safety functions is essential and goes beyond compliance with technical specifications requirements during shutdown. In addition, while the scope of activities for an unplanned or forced outage is far less than that of a refuelling outage, the same awareness of vulnerabilities during shutdown conditions is required to safely conduct these outages.

Nuclear power plant operating experience has shown that PWRs are susceptible to a variety of events during shutdown conditions. While these events have caused no harm to the public, nor posed an undue risk, they do illustrate that careful attention to outage management and shutdown operation is necessary to maintain adequate defence-in-depth for safety functions.

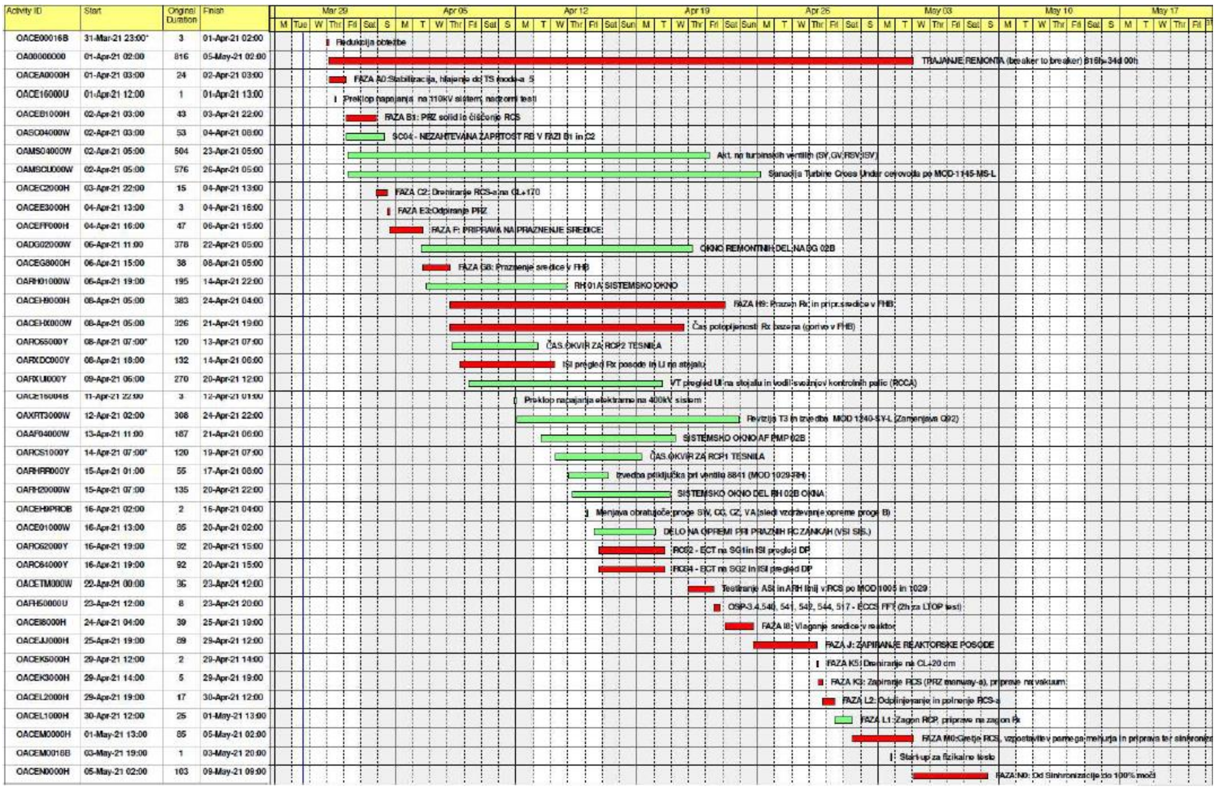
Outage periods involve many plant organizations and individuals working together and, as such, require high levels of coordination. Careful preparation and execution according to a well-developed plan are necessary for nuclear, radiological, and industrial safety, as well as efficient achievement of goals. Indeed, outages require the focus, expertise, and level of detail of major construction projects.

Outage goals and objectives reflect the industry’s high standards for safety and reliability. Nuclear safety, radiological performance, human performance, industrial safety, equipment performance, outage cost, and outage duration are all important aspects of outage performance. Aggressive goals in these areas are attainable when outages are planned carefully and managed well.

2. OUTAGE PLANNING

Effective outage planning and control is the primary means of enhancing safety during shutdown. Managing risk and maintaining safety functions during a multitude of outage activities requires a clear understanding of the utility safety philosophy, appropriate involvement of organizational levels, planning, coordination, communication, and the awareness of plant status by the personnel involved in those activities. The focus of outage safety in the past has often been on systems or components that were out of service for maintenance or repair during the outage. Outage safety can be improved by focusing on the availability of systems that provide and support key safety functions as well as on measures that can reduce both the likelihood and consequences of adverse events.

Nuclear power plant outages must be managed, planned and executed carefully so that nuclear safety is maintained during shutdown periods. Industry experience has shown that plants are vulnerable to events that can challenge shutdown safety if barriers are not robust. The amount of time that systems are out of service for modification or maintenance is a direct factor in the potential for losses of essential services and reduces the ability of operators to mitigate the consequences of events. Systems that affect key safety functions are kept available for shutdown safety to the maximum extent possible. Contingencies are in place when shutdown risk exceeds established thresholds. In addition, special controls of high-risk evolutions are provided.



Activity ID	Start	Original Duration	Finish
OACE00016B	31-Mar-21 23:00*	3	01-Apr-21 02:00
OA00000000	01-Apr-21 02:00	816	05-May-21 02:00
OACEA0000H	01-Apr-21 03:00	24	02-Apr-21 03:00
OACE16000U	01-Apr-21 12:00	1	01-Apr-21 13:00
OACEB1000H	02-Apr-21 03:00	43	03-Apr-21 22:00
OASC04000W	02-Apr-21 03:00	53	04-Apr-21 08:00
OAMS04000W	02-Apr-21 05:00	504	23-Apr-21 05:00
OAMSCU000W	02-Apr-21 05:00	576	26-Apr-21 05:00
OACEC2000H	03-Apr-21 22:00	15	04-Apr-21 13:00
OACEE3000H	04-Apr-21 13:00	3	04-Apr-21 16:00
OACEFF000H	04-Apr-21 16:00	47	06-Apr-21 15:00
OADG02000W	06-Apr-21 11:00	378	22-Apr-21 05:00
OACEG8000H	06-Apr-21 15:00	38	08-Apr-21 05:00
OARH01000W	06-Apr-21 19:00	195	14-Apr-21 22:00
OACEH9000H	08-Apr-21 05:00	383	24-Apr-21 04:00
OACEHX000W	08-Apr-21 05:00	326	21-Apr-21 19:00
OARC65000Y	08-Apr-21 07:00*	120	13-Apr-21 07:00
OARXDC000Y	08-Apr-21 18:00	132	14-Apr-21 06:00
OARXUI000Y	09-Apr-21 06:00	270	20-Apr-21 12:00
OACE16004B	11-Apr-21 22:00	3	12-Apr-21 01:00
OAXRT3000W	12-Apr-21 02:00	308	24-Apr-21 22:00
OAAF04000W	13-Apr-21 11:00	187	21-Apr-21 06:00
OARCS1000Y	14-Apr-21 07:00*	120	19-Apr-21 07:00
OARHRR000Y	15-Apr-21 01:00	55	17-Apr-21 08:00
OARH20000W	15-Apr-21 07:00	135	20-Apr-21 22:00
OACEH9PROB	16-Apr-21 02:00	2	16-Apr-21 04:00
OACE01000W	16-Apr-21 13:00	85	20-Apr-21 02:00
OARC62000Y	16-Apr-21 19:00	92	20-Apr-21 15:00
OARC64000Y	16-Apr-21 19:00	92	20-Apr-21 15:00
OACETM000W	22-Apr-21 00:00	36	23-Apr-21 12:00
OAFH50000U	23-Apr-21 12:00	8	23-Apr-21 20:00
OACEI8000H	24-Apr-21 04:00	39	25-Apr-21 19:00
OACEJJ000H	25-Apr-21 19:00	89	29-Apr-21 12:00
OACEK5000H	29-Apr-21 12:00	2	29-Apr-21 14:00
OACEK3000H	29-Apr-21 14:00	5	29-Apr-21 19:00
OACEL2000H	29-Apr-21 19:00	17	30-Apr-21 12:00
OACEL1000H	30-Apr-21 12:00	25	01-May-21 13:00
OACEM0000H	01-May-21 13:00	85	05-May-21 02:00
OACEM0016B	03-May-21 19:00	1	03-May-21 20:00
OACEN0000H	05-May-21 02:00	103	09-May-21 09:00

Figure 1 – Krško NPP outage plan with main phases and driving activities

3. SHUTDOWN SAFETY

Five key safety functions have been defined that are to be maintained throughout shutdown operations. These safety functions are decay heat removal, inventory control, electrical power availability, reactivity control, and containment. Systems, subsystems, support systems, and sometimes additional temporary systems must be available to provide these key safety functions and ensure shutdown safety. The required systems to maintain the key safety functions are defined and the minimum requirements established, along with a graduated approach to maintaining defence-in-depth for each key safety function.

In Krško Nuclear Power Plant we have expanded those five safety functions and defined seven. Those are:

1. Reactivity Control – REC
2. Decay Heat Removal – DHR
3. Reactor Coolant System Inventory Control – INV
4. Electrical Power Availability – ELE
5. Spent Fuel Pit Cooling - SFP
6. Support Systems Availability – SUP
7. Containment Closure – CNT

3.1 Reactivity Control (REC)

Reactivity control, as it relates to shutdown safety, includes maintaining sufficient shutdown margin in the reactor coolant system and spent fuel pool, as well as proper planning and control of all fuel-handling, reactivity control testing and start-up activities.

Boron dilution, during shutdown conditions, reduces reactivity shutdown margin. Boron dilution events are of concern because of the potential for unexpected reactor criticality. In such cases, criticality can occur even with the rods fully inserted into the core. Gradual decreases in boron concentration are difficult to detect, because detection relies on reactor coolant system sampling, on-line analysers and monitoring source range detector counts. It is necessary to identify potential boron dilution paths for each planned shutdown configuration and provide appropriate administrative controls for flow paths that may cause boron dilution. In Krško NPP it is Technical Specification requirement to isolate dilution paths – LCO-3.1.2.7. Source range detectors must be maintained frequently during shutdown conditions when fuel is in the core, particularly during activities that could result in boron dilution. Redundant boration paths are established to respond to a boron dilution event.

The reactor coolant system water temperature can decrease below the minimum value used to analyse reactor and fuel pool shutdown margin. Cold water adds positive reactivity, thereby decreasing the shutdown margin. This applies to both the core and the spent fuel pool.

3.2 Decay Heat Removal (DHR)

Decay heat removal (DHR) capability is required during shutdown conditions to maintain reactor coolant system (RCS) temperature and pressure and spent fuel pool (SFP) temperature below specified limits, whether fuel remains in the reactor vessel or is off-loaded to the SFP. Maintaining DHR is a key safety function that depends on associated DHR systems, backup systems, and alternate methods of heat removal. Providing defense-in-depth for DHR, commensurate with the plant conditions identified in the outage schedule, is an integral part of the shutdown protection plan and is vital to shutdown safety. Since unplanned emergent conditions require schedule changes, maintaining sufficient defense-in-depth becomes more challenging because the availability of DHR-related support functions is not guaranteed.

A loss of DHR is a significant contributor to potential core damage. The probability of the core being uncovered by the loss of inventory from boiling increases substantially when DHR is lost, especially early in the outage and prior to core off load when the decay heat load is high. During these times of elevated risk, it is prudent to avoid scheduling electrical bus work, switchyard work, and first-time activities until later in the outage when risk is lower.

On several occasions, DHR capability was lost or reduced because personnel did not fully understand the effects of changes to the outage work scope and implementing procedures. Although station personnel were aware that DHR systems and components were important for cooling fuel in the reactor vessel and in the SFP, outage work was sometimes perceived to be nonintrusive, not related to, or not affecting DHR. In most cases, the work being performed was not perceived as complex, difficult, or needing additional focus; thus, additional controls or oversight was not provided. In some cases, work was allowed on protected equipment trains. In others, systems were considered available to support the DHR function even though lengthy actions would be needed to make the system operational to provide the required cooling function. At some stations, SFP cooling consists of a single train of cooling capability. These designs are much more vulnerable to losses of cooling than dual-train designs.

3.3 Reactor Coolant System Inventory Control (INV)

Reactor vessel inventory control is important because of its effect on DHR. Inadequate inventory control can lead to vortexing in DHR systems, especially during reduced inventory conditions. Lower inventory also reduces the time to boil, making losses of DHR more consequential. For example, within 48 hours following shutdown from a high-power operating history, a loss of DHR at midloop operation could result in boiling in the core in about 10 minutes. Analyses of shutdown configurations show that, for one PWR, the highest contribution to core damage frequency during shutdown is when RCS water level is at the reactor vessel flange. In several recent events, there was inadequate sensitivity to operations that had the potential to drain the reactor vessel and challenge core cooling. In some cases, reactor vessel water level was maintained lower than necessary, reducing the safety margin for core cooling. Equipment problems and insufficient planning for contingencies have often expanded the time in reduced inventory.

3.4 Electrical Power Availability (ELE)

Electrical power is a fundamental element of shutdown nuclear safety because of the many safety and support systems that require it. Power sources must be protected from an inadvertent loss through sufficient defense-in-depth. Outages always have periods when equipment is not available and unusual electrical line-ups exist. Maintenance activities performed during these periods increase the likelihood of an electrical perturbation and resultant system degradation. The safety significance of the loss of electrical power depends on the equipment affected. The loss could range from complete loss of all AC power to the loss of a DC bus or an instrument bus. The loss of electrical power sometimes initiates a loss of other safety functions, such as DHR. Electrical power availability while a plant is shut down has been challenged on a few occasions because of human error during breaker and switching manipulations in the switchyard.

3.5 Spent Fuel Pit Cooling (SFP)

Sufficient cooling is needed for the spent fuel pool, particularly when fuel with a high heat load is present. The running spent fuel pool cooling system is protected when fuel off-load begins and when the time to reach 100 degrees Centigrade in the spent fuel pool is less than 72 hours, to prevent potential adverse impacts of outage activities. The outage schedule should ensure that spent fuel pool cooling is sufficient and defence-in-depth is commensurate with the risk associated with the loss of spent fuel pool cooling. The availability of fuel handling building ventilation and spent fuel pool cooling support systems must be managed carefully during offload periods. Similarly, to DHR considerations for the reactor, procedures are established for response to a loss of spent fuel pool cooling and for cooling restoration, mitigation contingencies, radiation monitoring and HVAC changes.

3.6 Support Systems Availability (SUP)

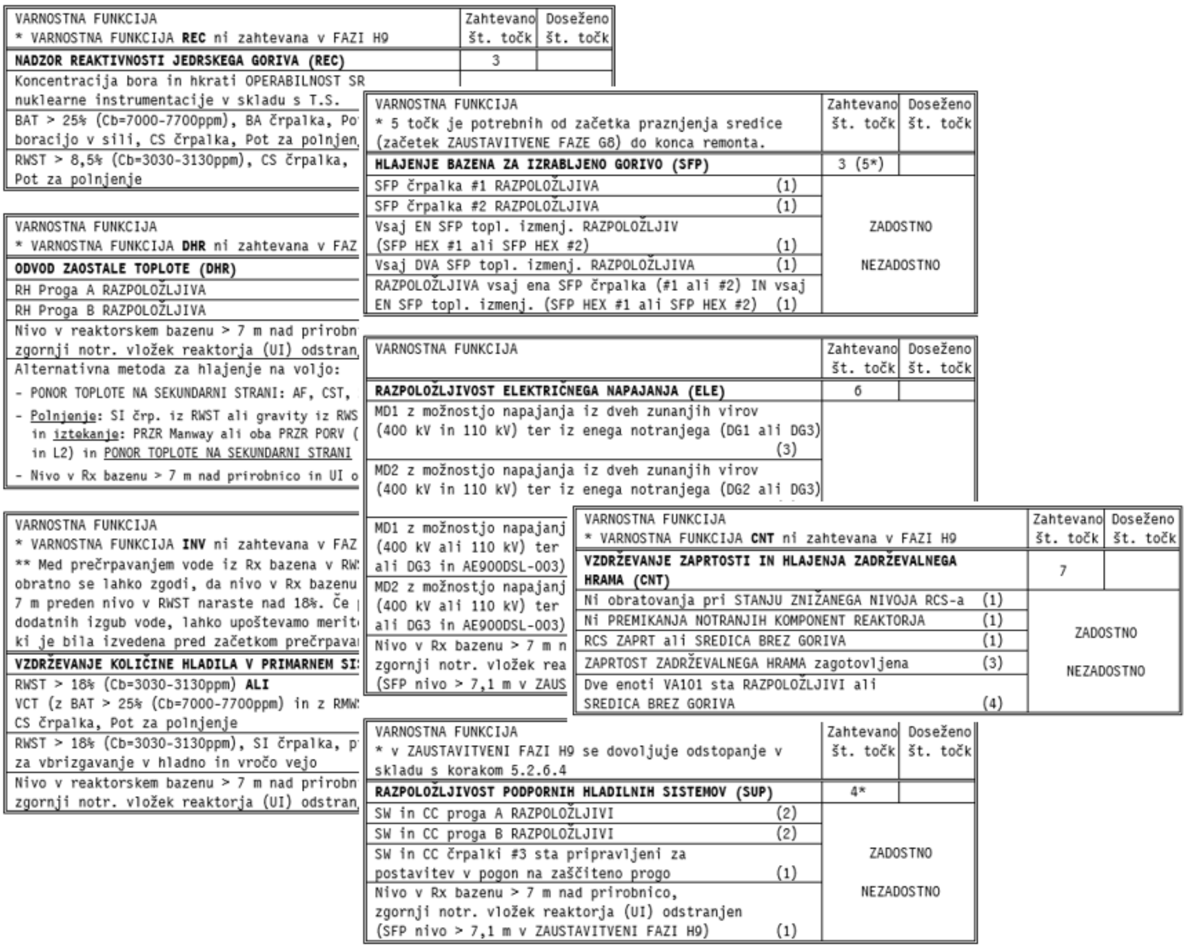
Cooling water for Decay Heat Removal and Spent Fuel Pit Cooling functions must be provided during all shutdown phases. That means that essential service water system and component cooling system must operate all the time during the outage. Main Control Room ventilation must also be operable during outage to provide habitable conditions for the operators.

3.7 Containment Closure (CNT)

Containment closure is needed to prevent the release of radioactive material. It must be achievable in sufficient time to prevent a radiological release if the reactor coolant boils. Containment closure involves using a qualified covering to either close or cover containment hatches and other penetrations that communicate with the containment atmosphere. The time needed to establish a barrier to a potential radiological release must be less than the time to boil the reactor coolant.

3.8 Shutdown safety functions availability

Adherence to the above-mentioned shutdown safety functions are assessed during shift turnover, when shutdown state changes and before major systems or components are removed from service. Shift Foreman and Shift Technical Advisor do the assessment using the Appendix 6.2 of procedure ADP-1.3.030 "Varnost v zaustavitvi". In the appendix you check required demands for each shutdown function then add up all the points and compare summarized points with the required points. If the sum is equal or larger than the required points, function is satisfied. If the sum is less then the required number, the function is degraded. Shutdown Safety Committee has to be called and contingency plan to restore the availability of the function must be made.



VARNOSTNA FUNKCIJA * VARNOSTNA FUNKCIJA **REC** ni zahtevana v FAZI H9	Zahtevano št. točk	Doseženo št. točk
NADZOR REAKTIVNOSTI JEDRSKEGA GORIVA (REC)	3	
Koncentracija bora in hkrati OPERABILNOST SR nuklearne instrumentacije v skladu s T.S.		
BAT > 25% (Cb=7000-7700ppm), BA črpalka, Po boracijo v sili, CS črpalka, Pot za polnjen		
RWST > 8,5% (Cb=3030-3130ppm), CS črpalka, Pot za polnjenje		

VARNOSTNA FUNKCIJA * VARNOSTNA FUNKCIJA **DHR** ni zahtevana v FAZ
ODVOD ZAOSTALE TOPLOTE (DHR)
RH Proga A RAZPOLOŽLJIVA
RH Proga B RAZPOLOŽLJIVA
Nivo v reaktorskem bazenu > 7 m nad prirobn zgornji notr. vložek reaktorja (UI) odstran
Alternativna metoda za hlajenje na voljo: - PONOR TOPLOTE NA SEKUNDARNI STRANI: AF, CST, - Polnjenje: SI črp. iz RWST ali gravity iz RWS in iztekanje: PRZR Manway ali oba PRZR PORV (in L2) in PONOR TOPLOTE NA SEKUNDARNI STRANI - Nivo v Rx bazenu > 7 m nad prirobnico in UI o

VARNOSTNA FUNKCIJA * VARNOSTNA FUNKCIJA **INV** ni zahtevana v FAZ ** Med prečrpavanjem vode iz Rx bazena v RW obratno se lahko zgodi, da nivo v Rx bazenu 7 m preden nivo v RWST naraste nad 18%. Če dodatnih izgub vode, lahko upoštevamo merit ki je bila izvedena pred začetkom prečrpava
VZDRŽEVANJE KOLIČINE HLADILA V PRIMARNEM SI
RWST > 18% (Cb=3030-3130ppm) **ALI** VCT (z BAT > 25% (Cb=7000-7700ppm) in z RMW CS črpalka, Pot za polnjenje
RWST > 18% (Cb=3030-3130ppm), SI črpalka, p za vbrizgavanje v hladno in vročo vejo
Nivo v reaktorskem bazenu > 7 m nad prirobn zgornji notr. vložek reaktorja (UI) odstran

VARNOSTNA FUNKCIJA * 5 točk je potrebnih od začetka praznjenja sredice (začetek ZAUSTAVITVENE FAZE G8) do konca remonta.	Zahtevano št. točk	Doseženo št. točk
HLAJENJE BAZENA ZA IZRABLJENO GORIVO (SFP)	3 (5*)	
SFP črpalka #1 RAZPOLOŽLJIVA (1)	ZADOSTNO NEZADOSTNO	
SFP črpalka #2 RAZPOLOŽLJIVA (1)		
Vsaj EN SFP topl. izmenj. RAZPOLOŽLJIV (SFP HEX #1 ali SFP HEX #2) (1)		
Vsaj DVA SFP topl. izmenj. RAZPOLOŽLJIVA (1)		
RAZPOLOŽLJIVA vsaj ena SFP črpalka (#1 ali #2) IN vsaj EN SFP topl. izmenj. (SFP HEX #1 ali SFP HEX #2) (1)		

VARNOSTNA FUNKCIJA	Zahtevano št. točk	Doseženo št. točk
RAZPOLOŽLJIVOST ELEKTRIČNEGA NAPAJANJA (ELE)	6	
MD1 z možnostjo napajanja iz dveh zunanjih virov (400 kV in 110 kV) ter iz enega notranjega (DG1 ali DG3) (3)		
MD2 z možnostjo napajanja iz dveh zunanjih virov (400 kV in 110 kV) ter iz enega notranjega (DG2 ali DG3)		
MD1 z možnostjo napajanj (400 kV ali 110 kV) ter ali DG3 in AE900DSL-003)		
MD2 z možnostjo napajanj (400 kV ali 110 kV) ter ali DG3 in AE900DSL-003)		
Nivo v Rx bazenu > 7 m n zgornji notr. vložek rea (SFP nivo > 7,1 m v ZAUS		

VARNOSTNA FUNKCIJA * VARNOSTNA FUNKCIJA **CNT** ni zahtevana v FAZI H9	Zahtevano št. točk	Doseženo št. točk
VZDRŽEVANJE ZAPRTOSTI IN HLAJENJA ZADRŽEVALNEGA HRAMA (CNT)	7	
Ni obratovanja pri STANJU ZNIŽANEGA NIVOJA RCS-a (1)	ZADOSTNO NEZADOSTNO	
Ni PREMIKANJA NOTRANJIH KOMPONENT REAKTORJA (1)		
RCS ZAPRT ali SREDICA BREZ GORIVA (1)		
ZAPRTOST ZADRŽEVALNEGA HRAMA zagotovljena (3)		
Dve enoti VA101 sta RAZPOLOŽLJIVI ali SREDICA BREZ GORIVA (4)		

VARNOSTNA FUNKCIJA * v ZAUSTAVITVENI FAZI H9 se dovoljuje odstopanje v skladu s korakom 5.2.6.4	Zahtevano št. točk	Doseženo št. točk
RAZPOLOŽLJIVOST PODPORNIH HLADILNIH SISTEMOV (SUP)	4*	
SW in CC proga A RAZPOLOŽLJIVI (2)	ZADOSTNO NEZADOSTNO	
SW in CC proga B RAZPOLOŽLJIVI (2)		
SW in CC črpalki #3 sta pripravljeni za postavitev v pogon na zaščiteno progo (1)		
Nivo v Rx bazenu > 7 m nad prirobnico, zgornji notr. vložek reaktorja (UI) odstranjen (SFP nivo > 7,1 m v ZAUSTAVITVENI FAZI H9) (1)		

Figure 2 - ADP-1.3.030, Appendix 6.2: Shutdown Safety Functions adherence

4. SHUTDOWN SAFETY IMPLEMENTATION

4.1 Phases

Outage in Krško Nuclear Power Plant is divided in phases which are defined by specific plant equipment status and inventory of the reactor coolant system. Those phases are:

Shutting down

Powering Up

1	RCS closed and solid
2	RCS closed and draining to CL+170 cm, SG U-tubes full
2*	RCS closed, SG U-tubes empty
3	RCS opened, level CL+170 cm; SG U-tubes full
4	RCS opened and draining to CL+20 cm; U-tubes empty, SG nozzle dams in place
4*	RCS opened; U-tubes empty, SG nozzle dams in place
5	Reactor Vessel Head in place, RCS opened, SG nozzle dams in place
6	Reactor Vessel Head removing/is removed, Upper Internals not removed
7	Reactor Cavity flooded, Upper Internals removed, refuelling not in process
8	Reactor Cavity flooded, refuelling in process
9	No fuel in the reactor

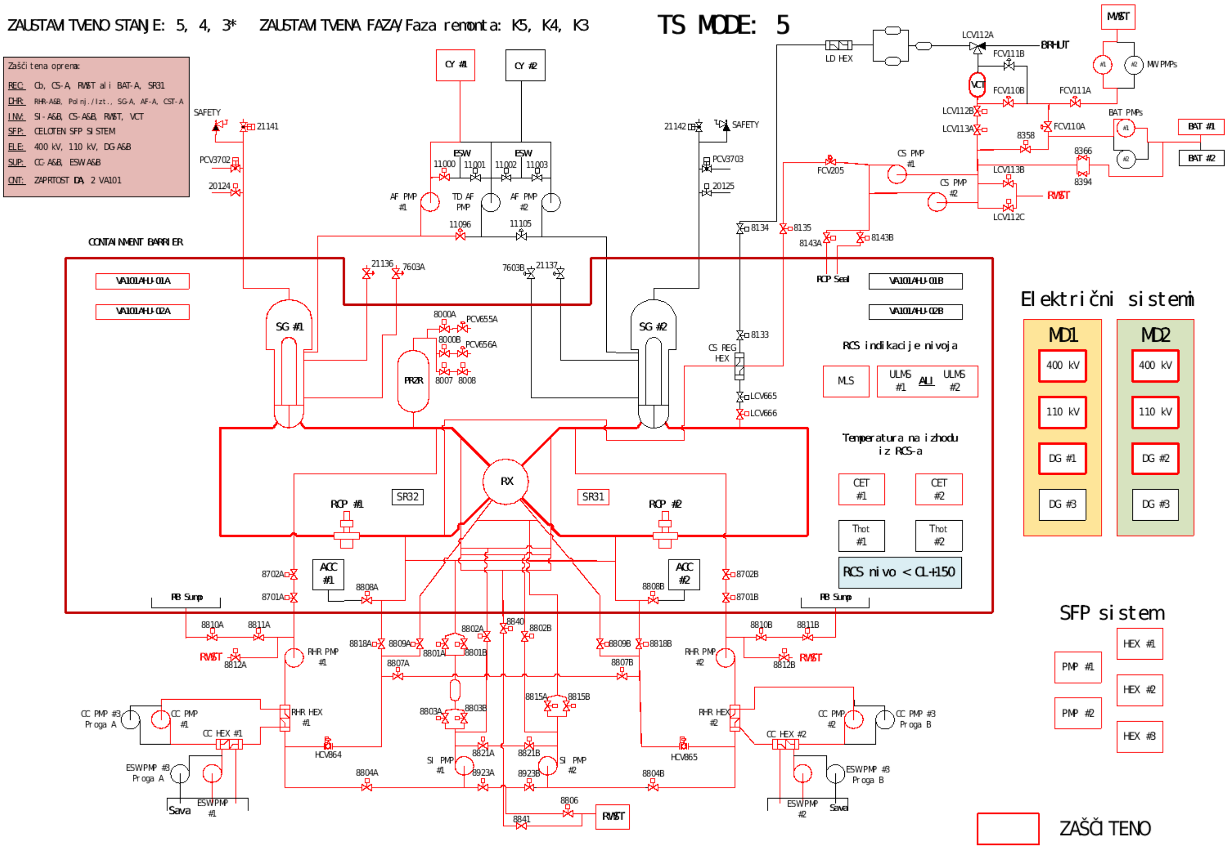
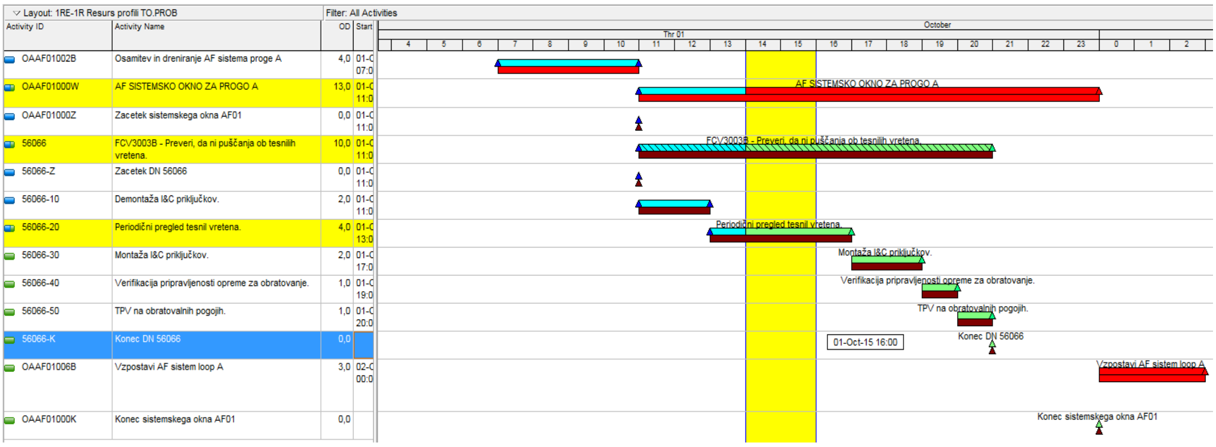


Figure 3 - Protected equipment diagram for the shutdown phase K5

4.2 System windows

Outage plan is divided into system windows. System windows are created based on Shutdown Safety requirements for each shutdown phase. Every work order in system window is assigned with ORAM code which is then used for PARAGON calculation to determine if by working on the asset we degrade shutdown safety function needed for that phase.



Layout: 1RE-1R Resurs profili TO.PROB | Filter: All Activities

Activity ID	Activity Name	OD	Start
OAAF01002B	Osamitev in dreniranje AF sistema proge A	4,0	01-C 07:0
OAAF01000W	AF SISTEMSKO OKNO ZA PROGO A	13,0	01-C 11:0
OAAF01000Z	Zacetek sistemskega okna AF01	0,0	01-C 11:0
56066	FCV3003B - Preveri, da ni puščanja ob tesnilih vretena.	10,0	01-C 11:0
56066-Z	Zacetek DN 56066	0,0	01-C 11:0
56066-10	Demontaža I&C priključkov.	2,0	01-C 11:0
56066-20	Periodični pregled tesnil vretena.	4,0	01-C 13:0
56066-30	Montaža I&C priključkov.	2,0	01-C 17:0
56066-40	Verifikacija pripravljenosti opreme za obratovanje.	1,0	01-C 19:0
56066-50	TPV na obratovalnih pogojih.	1,0	01-C 20:0
56066-K	Konec DN 56066	0,0	
OAAF01006B	Vzpostavi AF sistem loop A	3,0	02-C 00:0
OAAF01000K	Konec sistemskega okna AF01	0,0	

Figure 4 - Example of an outage system window

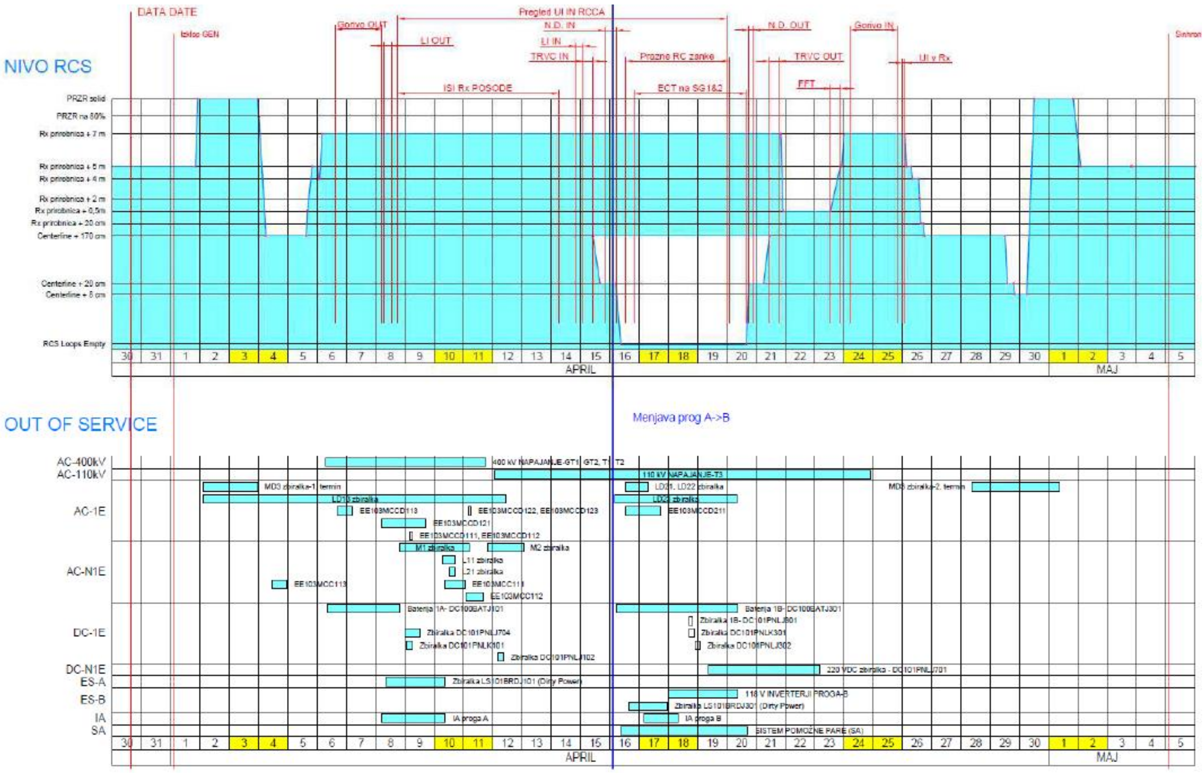


Figure 5 - Reactor Coolant System inventory and Out-of-Service Systems during outage

4.3 Risk identification – PARAGON

A systematic method of risk identification is applied to outage work activities. Risk is evaluated based on probability and consequence as it relates to shutdown safety. As a result of this analysis, a determination is made on the level of shutdown safety risk planning required and additional oversight needed for the work activity. Risk analysis should include the potential to extend time in an elevated nuclear safety risk condition, the potential of the work to impact a critical component function and whether the work could result in an unrecoverable action that would not be discovered until a system or component is needed.

A graded approach to shutdown safety risk planning is applied based on the assessment of risk. Shutdown safety risk management plans are developed to reduce or mitigate risk when defences are reduced to predefined levels in the shutdown risk programme. These plans, which contain contingency and compensatory measures, are required for high-risk evolutions and when the loss of a single component could impair a safety function significantly.

To identify potential risks during outage, Krško Nuclear Power Plant is using computation tool PARAGON to calculate CDF during outage activities. System windows, work orders and clearances are all assigned with the ORAM code to determine which system or subsystem will be taken out-of-service. PARAGON then calculates availability of the systems needed to assure shutdown safety for the particular state. If the required system is not available when needed, the program highlights whole phase in red. Wrongly placed work orders or clearances must then be checked, find the reason why they were placed there and solve the situation either by changing the scope of the activity or by finding appropriate system window.

Red status for the Spent Fuel Pit Cooling function, shown on the Figure 6, occurred in outage 2021 because of the planned preventive maintenance work on Component Cooling “P” isolation valve. Spent Fuel Pit cooling flow from CC system was terminated to ensure work can be done on the “P” isolation valve. Spent Fuel Pit temperature was closely monitored and in case it has risen above set value, contingency action would be performed. As a contingency action, mobile Spent Fuel Pit heat exchanger was connected to the system and was ready to be placed in service before Time to Boil value.

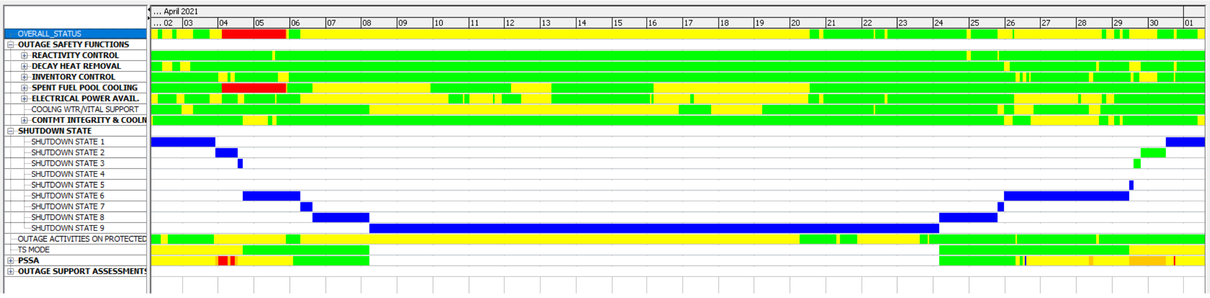


Figure 6 - PARAGON calculation (red highlights the phase where there has been an activity that degrades the SD Safety function)

Figure 7 and Figure 8 show comparison of annual Core Damage Frequency and Outage 2021 Core Damage Frequency. Core Damage Frequency of Outage 2021 was 2.7x10^{-7} which is lower that the target Core Damage Frequency of 3x10^{-5}.

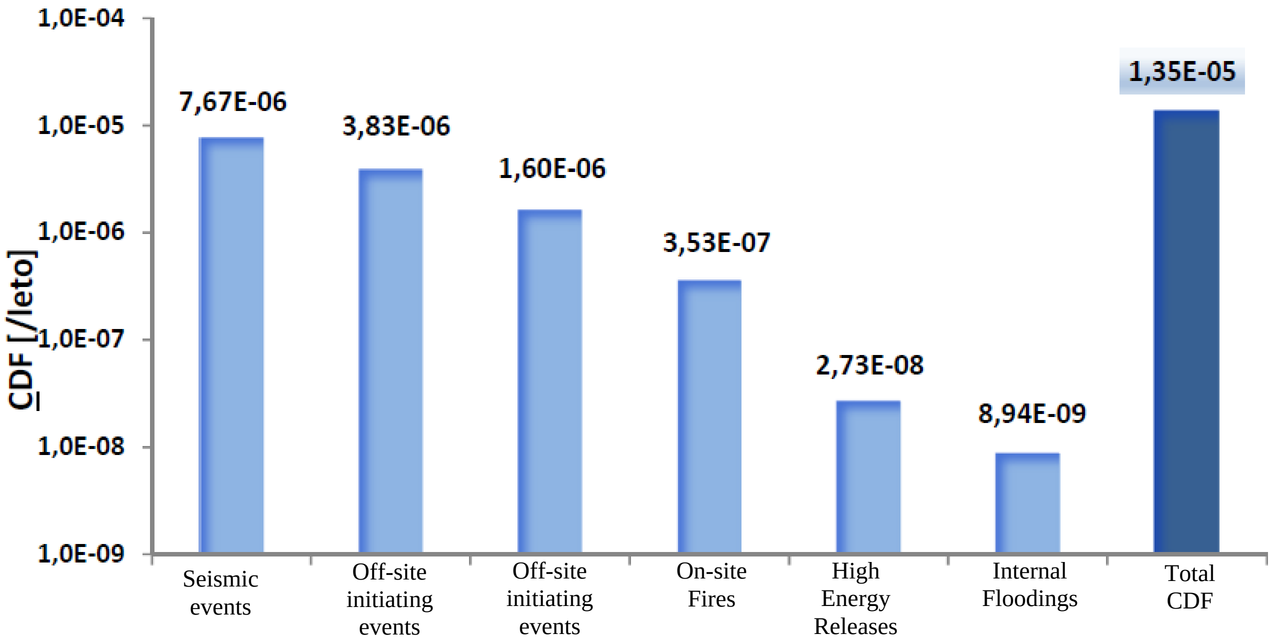
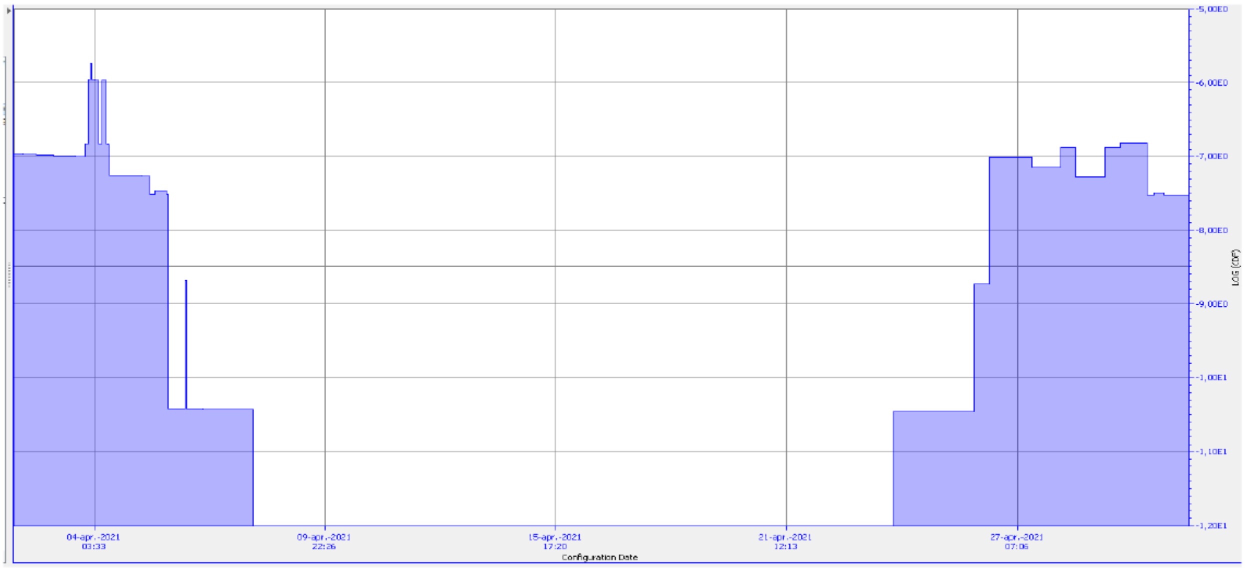


Figure 7 – 2021 annual Core Damage Frequency



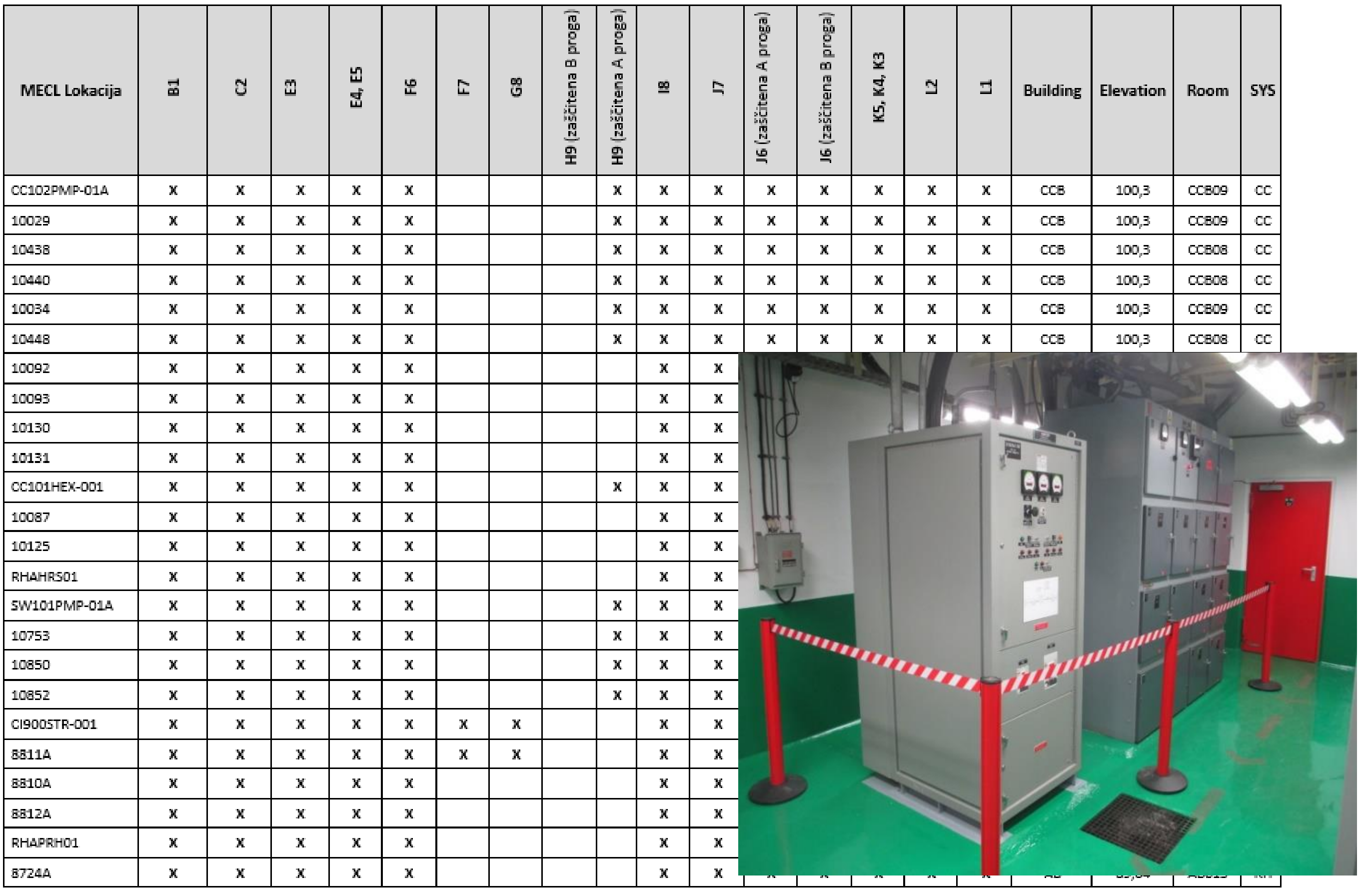
Outage CDP (SD state 1 to SD state 1)= Average_CDF * SD1toSD1_duration = 3.94e-8 * 707= 2.79e-5

Figure 8 – Outage 2021 Core Damage Frequency

4.4 Protected Equipment

NEK procedure ADP-1.3.031, defines protected equipment as equipment required to comply with shutdown safety functions requirements. By definition, any work on the protected equipment, that could jeopardize its availability, is prohibited. The Shift Supervisor is responsible for keeping protected equipment operable and assessing shutdown safety function availability when needed. In the case of shutdown function degradation, he has to notify the Production Manager and Operations Superintendent. Both of them are part of Shutdown Safety Committee, which is responsible for analysing the situation, approving the schedule change and deciding on contingency plans, if needed.

Areas containing only protected equipment have no-entry markings posted on the entrance door. In areas containing both, protected and unprotected equipment, posts and physical barriers are used to distinguish protected equipment, along with warning markings posted on entrance door. Same as in switchyard access, those areas are either locked by key-card systems or by key locks, both of them providing entry control. Keys are issued by Work Control Centre staff member, thus controlling and denying access to the protected areas.



MECL Lokacija	B1	C2	E3	E4, E5	F6	F7	G8	H9 (zaščitena B proga)	H9 (zaščitena A proga)	I8	J7	J6 (zaščitena A proga)	J6 (zaščitena B proga)	K5, K4, K3	L2	L1	Building	Elevation	Room	SYS
CC102PMP-01A	x	x	x	x	x				x	x	x	x	x	x	x	x	CCB	100,3	CCB09	CC
10029	x	x	x	x	x				x	x	x	x	x	x	x	x	CCB	100,3	CCB09	CC
10438	x	x	x	x	x				x	x	x	x	x	x	x	x	CCB	100,3	CCB08	CC
10440	x	x	x	x	x				x	x	x	x	x	x	x	x	CCB	100,3	CCB08	CC
10034	x	x	x	x	x				x	x	x	x	x	x	x	x	CCB	100,3	CCB09	CC
10448	x	x	x	x	x				x	x	x	x	x	x	x	x	CCB	100,3	CCB08	CC
10092	x	x	x	x	x					x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
10093	x	x	x	x	x					x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
10130	x	x	x	x	x					x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
10131	x	x	x	x	x					x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
CC101HEX-001	x	x	x	x	x				x	x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
10087	x	x	x	x	x					x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
10125	x	x	x	x	x					x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
RHAHRS01	x	x	x	x	x					x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
SW101PMP-01A	x	x	x	x	x				x	x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
10753	x	x	x	x	x				x	x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
10850	x	x	x	x	x				x	x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
10852	x	x	x	x	x				x	x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
CI900STR-001	x	x	x	x	x	x	x			x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
8811A	x	x	x	x	x	x	x			x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
8810A	x	x	x	x	x					x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
8812A	x	x	x	x	x					x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
RHAPRH01	x	x	x	x	x					x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
8724A	x	x	x	x	x					x	x	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Figure 9 - List of the protected equipment by SD phase and an example how the protected equipment is marked

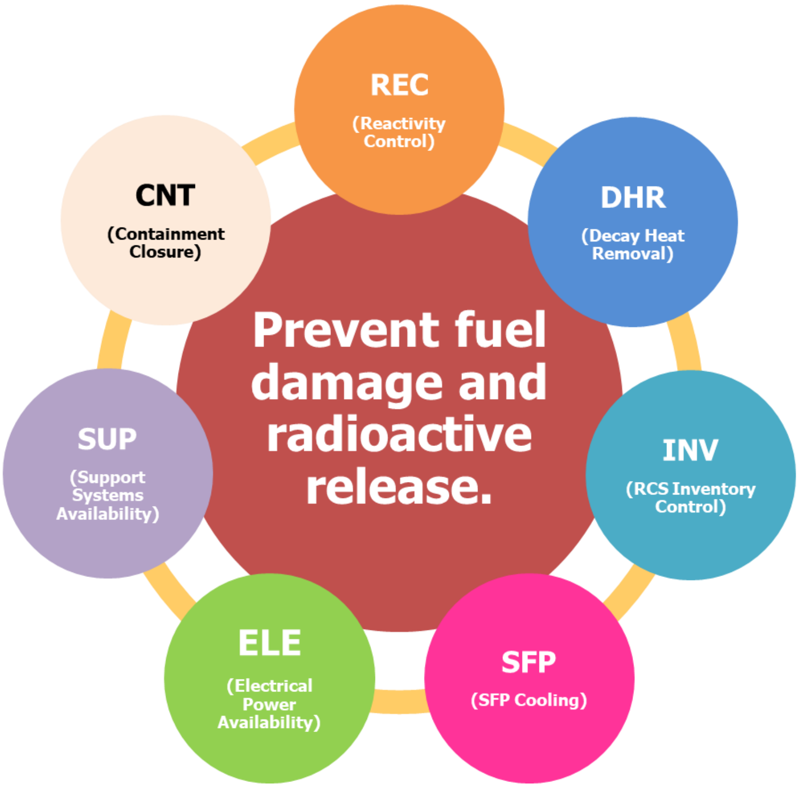
5. CONCLUSION

While performing outage activities, nuclear safety is maintained by ensuring that key shutdown safety functions are not challenged. The outage schedule is developed to maximise defence-in-depth. Risk levels are defined and actions established to ensure contingencies are in place when needed for periods of elevated risk.

The shutdown safety programme establishes system and support system requirements for each safety function and mitigation strategy. Shutdown safety training is provided to personnel commensurate with each individual's function. Shutdown safety is integrated into the outage schedule to ensure sufficient defence-in-depth. Independent reviews verify that the defence-in-depth plan is appropriate.

Defence-in-depth and outage risks are clearly communicated and understood at appropriate levels of the organisation. All personnel can identify and adhere to protected equipment requirements. Infrequently performed tests and evolutions and high-risk evolutions are identified prior to the outage start.

By adhering to Shutdown Safety principles, Krško Nuclear Power Plant assures that there is a clear oversight over all the activities conducted during outage. Outage training is comprehensive and all the critical activities have just-in-time trainings prior their execution. Outage preparation milestones are put in place and closely monitored to ensure potential risks and problems are addressed in a timely manner.



REFERENCES

[1] ADP-1.3.030 "Varnost v zaustavitvi", revision 20, 2021

[2] ADP-1.1.157 "Nadzor varnosti v zaustavitvi", revision 13, 2022

[3] NEK-ESD-TR/09/98, “NEK ORAM Risk Management Guideline Model and Shutdown External Events Evaluation”, April 1998

[4] NEK-ESD-TR/10/98, “NEK ORAM Probabilistic Shutdown Safety Assessment Final Report”, April 1998

[5] NEK-ESD-TR/20/05, “NPP KRSKO ORAM MODEL CONVERSION VERIFICATION AND VALIDATION”, May 2006

[6] NUMARC 91-06 "Guidelines for Industry Actions to Assess Shutdown Management", December 1991

[7] WANO SOER 2010-1 "Shutdown Safety", May 2010

[8] WANO GL 2008-01 "Guidelines for the Conduct of Outages at Nuclear Power Plants", December 2008

[9] WANO GL 2001-02 "Guidelines for the Conduct of Operations at Nuclear Power Plants"