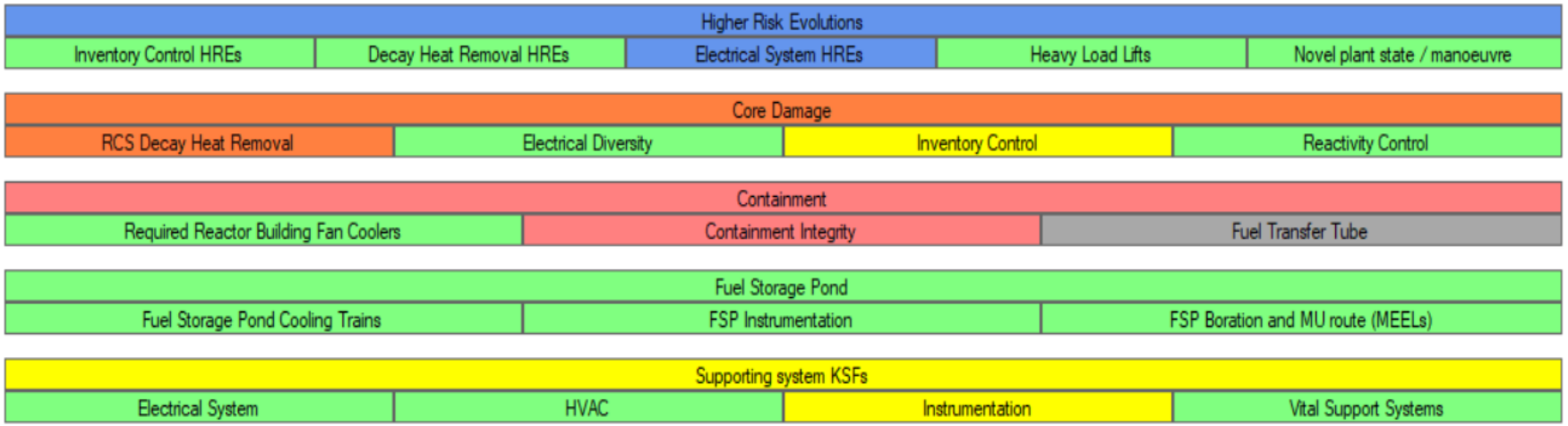
Design and Development of an Outage Planning and Risk Model



Ruth Freedman

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

Project Overview

- Sizewell B currently use ORAM for outage planning and management
  - Qualitative risk assessment model (QLRA) based on Defence in Depth (DiD) principles
  - Software no longer supported
  - Approach requires judgement, difficult to assign rules consistently

- Jacobsen developing a new model in RiskWatcher to replace the ORAM model
  - Integrate probabilistic and deterministic models in RiskWatcher
  - Based on Tech Specs and updated Minimum Essential Equipment Lists (MEELs)
  - Developed in line with international best practice based on research and guidance from the EPRI Configuration Risk Management Forum

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

Why Defence in Depth?

- During outage need to be able to perform refuelling, testing and maintenance whilst maintaining nuclear safety
  - A relatively dynamic situation, passing through multiple configurations
  - Different configurations or outage activities will impact plants ability to support key safety functions
  - Careful planning in advance to achieve optimum schedule whilst minimising time spent in reduced DID conditions
  - Quick response required to emergent conditions

- Communicating risk and required actions
  - Rapid visualisation using DID models
  - Meaningful measure of risk to managers and operators during the outage
  - Focuses management attention
  - General awareness on plant at time of increased risk
  - Can immediately understand if an action or activity will challenge a safety function
  - Understand dependencies (impact of support systems on KSFs)
  - Can link coloured endstates to recovery actions and configuration risk procedures

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

DID for Shutdown

- DID approach for shutdown first set out in NUMARC 91-06
  - Key Safety Functions
    - Decay Heat Removal Capability (including SFP)
    - Inventory Control
    - Reactivity Control
    - Containment Closure
    - Electrical Power Availability
  - Higher Risk Evolutions
    - Activities or configurations in which the plant is more susceptible to an event causing the loss of a KSF
  - Contingency planning and compensatory risk management actions linked to endstates to maintain or restore DID

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

DID for Shutdown

- NUMARC DID approach widely implemented across the industry and was used at Sizewell in the development of the ORAM model

- More recently EPRI have set up the Configuration Risk Management Forum and have developed guidance for QLRA assessments
    - Enables peer review and assessment of quality of approach
    - Consistency across the industry
    - Implementation of best practice

- Since the original guidelines were published, the understanding of the risks has evolved. Additional safety functions are now typically tracked:
    - Decay Heat Removal Capability
    - Inventory Control
    - Reactivity Control
    - Containment Closure
    - Electrical Power Availability
    - **Vital Support Systems**
    - **Spent Fuel Pool**
    - **Instrumentation**
    - **HVAC**

- Techniques for reporting the overall outage risk have also improved to ensure they are more meaningful

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

Defence In Depth Metrics

COLOR	METRIC	STATUS OF SAFETY FUNCTION
GREEN	ACCEPTABLE	Very high or maximum level of DID. Lowest risk level. Configurations with this DID do not require additional actions to manage risk (i.e. normal work controls are sufficient).
YELLOW	REDUCED	Adequate DID. Slightly elevated risk level, but still relatively low risk. Configurations with this DID may take actions to minimize the duration of exposure and/or implement compensatory actions to reduce risk.
ORANGE	MINIMAL	Reduced DID. Elevated risk, but tolerable for short durations. Configurations with this DID require detailed planning for the configuration including compensatory actions to minimize exposure time, and contingency planning to restore and/or protect alternate means of supporting the safety function. Typically represents the case where a single failure will result in loss of DID for the safety function.
RED	UNACCEPTABLE	Unacceptable DID characterized by the inability to support the safety function. Risk is unacceptably high and not tolerable for any duration. Typically represents a state that will not be planned for or entered voluntarily.

At Sizewell this is translated to entering an LCO condition (which does not necessarily mean inability to support the safety function)

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

Source: EPRI 1016231 – Development of a shutdown QRA Standard Dec 2007

Colour	DiD State	Technical Specification and MEELs Compliance
Green	Adequate	Tech Spec compliant and MEELs compliant (if MEELs contain additional requirements) OR In LCO condition that is not time limited, subject to completing the routine surveillance. Toggle must have been selected to acknowledge LCO condition
Yellow	Reduced	Tech Spec compliant (but not MEELs) OR In LCO condition with ACT >= 31 days. Toggle must have been selected to acknowledge LCO condition
Orange	Minimal	In LCO condition with ACT between 24 hours and 31 days. Toggle must have been selected to acknowledge LCO condition OR Operational Commitment not met
Red	Unacceptable	In LCO condition with ACT >= 24 hours and no toggle selected OR In LCO condition with ACT < 24 hours
Grey	N/A	Plant is in a state for which the compliance assessment is not applicable. For example, when the plant is at power, the metrics all show as grey

Proposed End State Metrics for Sizewell RiskWatcher Model

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

Sizewell model development

- End state criteria have been consistently applied to every Tech Spec and MEELs requirement and presented in tabular format to aid fault tree development.
- Have included nested indicators down to component level (red = inoperable, green = operable)
- MEELs have undergone a thorough review by station (supported by quantitative RW calculations)
- New approach for presenting overall risk based on EPRI guidance, KSFs split into frontline and secondary KSFs and grouped into plant metrics

Level	Indicator	Modes	Indicator Description	Grey	Red	Orange	Yellow	Green	Components	Fault Tree	Notes
1	1	Mode 5 Mode 6	RCS Decay Heat Removal	Mode not applicable	At least one level 2 indicator is red	At least one level 2 indicator is orange (and none are red)	At least one level 2 indicator is yellow (and none are orange or red)	All level 2 indicators are green		$_DD_DH $_DD_DH_O $_DD_DH_Y $_DD_M0-4_G	

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

Plant Metrics

- Core Damage (Analogous to Level 1 PSA risk metric)
  - Combination of Decay Heat Removal, Inventory Control and Reactivity Control.
  - One yellow KSF can be averaged to overall green if at least 2 other KSFs are green.
  - Red or orange conditions are not average to lower risk in high-level metric.
- Containment (Analogous to Level 2 PSA risk metric)
- Spent Fuel Pool
- Secondary KSFs (Supporting systems)
  - Shows the highest risk end state of all the contributing KSFs
  - Must avoid 'double counting'. If front-line system is yellow because of its support system, we don't want to count this reduction in DID twice when calculating outage risk.

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

Higher Risk Evolutions (HREs)

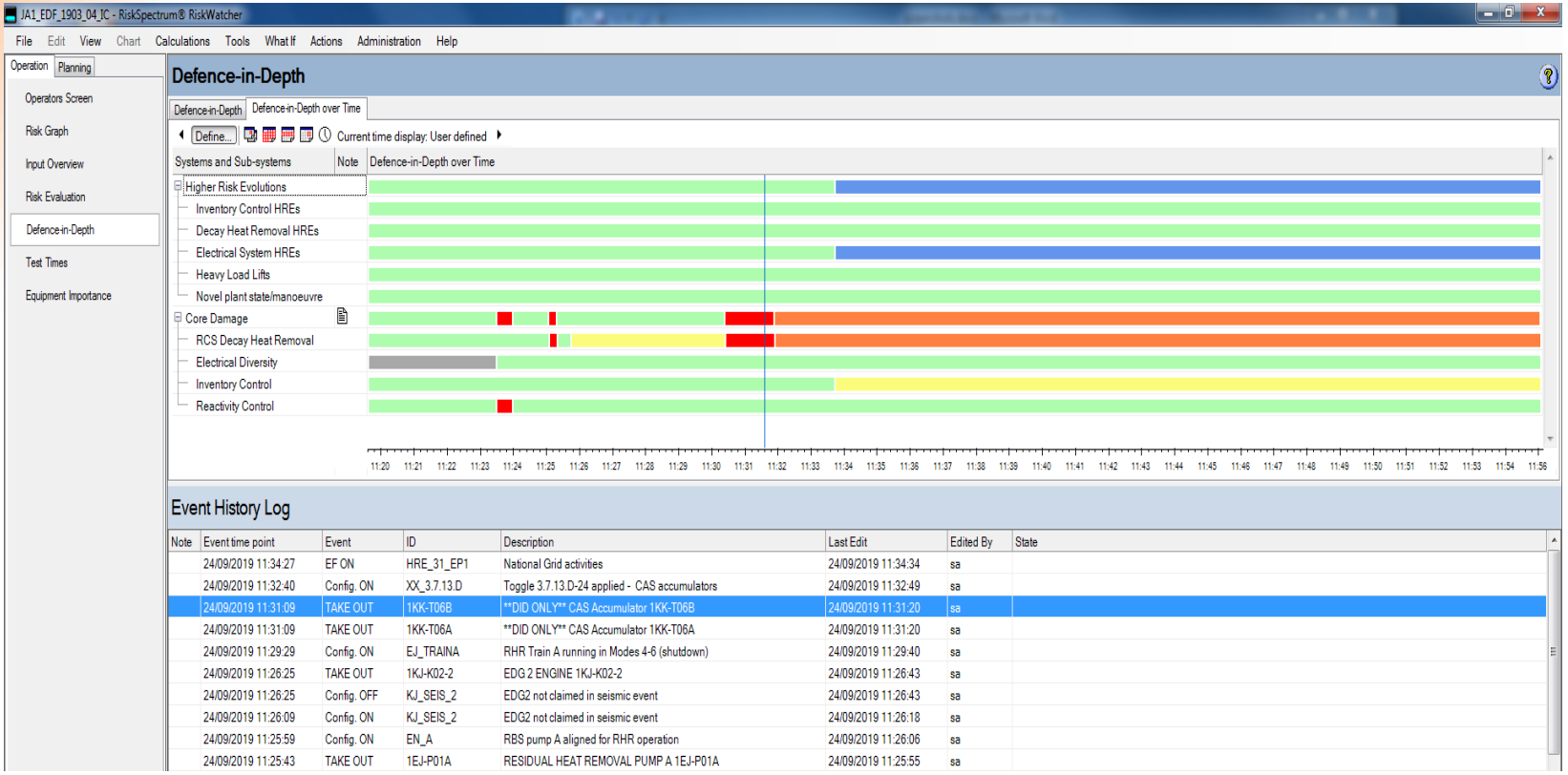
- "Higher Risk Evolutions"(HREs) are:
  - Outage activities, plant configurations or conditions during shutdown where the plant is more susceptible to an event causing the loss of key safety function.

- EPRI guidance suggests increasing risk level by 1 or 2 during HRE
  - For SZB tool, HREs will be displayed as separate indicators on the DID interface using the blue colour
  - This will be a clear indicator to the operator of an HRE but will not mask any other information shown in the KSF indicators
  - MEELs and Tech Specs more restrictive for mid-loop – so don't want to 'double count'
  - Power supplies which cannot be EDG backed will be assumed to fail when an Increased risk of LOOP or National Grid activities HRE is applied

Higher Risk Evolutions										
Inventory Control HREs			Decay Heat Removal HREs			Electrical System HREs			Heavy Load Lifts	Novel plant state/manoeuvre
Draining of the Reactor Coolant System Level below 25% in the Pressuriser	Filling up from 965mm below flange to >25% in the pressuriser or from Mid-loop to 965mm below flange	Drain-down of the Refuelling Pool below ~18m	Whilst at 965mm below flange in Mode 6 Head On, to start of filling of refuel pool, Mode 6 Head Off.	Whilst at 965mm below flange to Mode 5	All operations at Mid-loop to completion of Not Intact	National Grid activities	Increased risk of LOOP	Integrated Safeguards Actuation Testing (ISATs)		

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

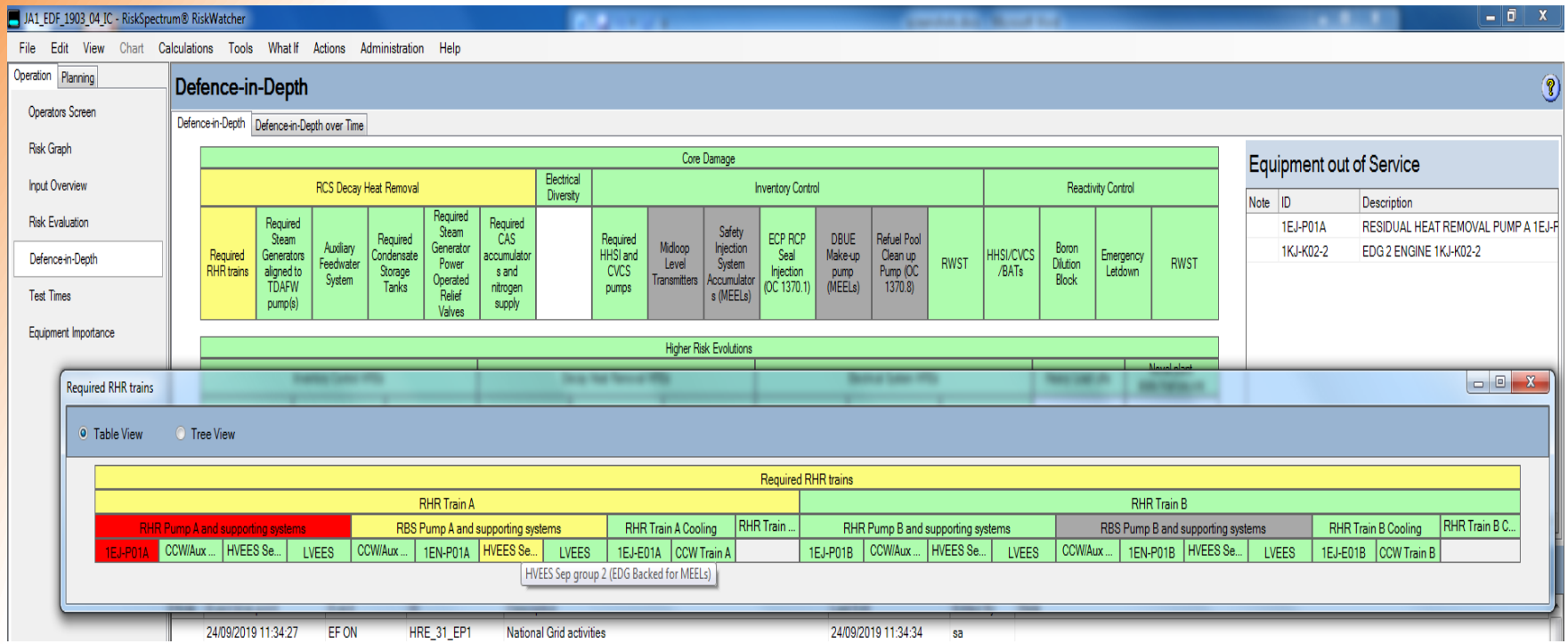
DiD Over Time



Note	Event time point	Event	ID	Description	Last Edit	Edited By	State
	24/09/2019 11:34:27	EF ON	HRE_31_EP1	National Grid activities	24/09/2019 11:34:34	sa	
	24/09/2019 11:32:40	Config. ON	XX_3.7.13.D	Toggle 3.7.13.D-24 applied - CAS accumulators	24/09/2019 11:32:49	sa	
	24/09/2019 11:31:09	TAKE OUT	1KK-T06B	**DID ONLY** CAS Accumulator 1KK-T06B	24/09/2019 11:31:20	sa	
	24/09/2019 11:31:09	TAKE OUT	1KK-T06A	**DID ONLY** CAS Accumulator 1KK-T06A	24/09/2019 11:31:20	sa	
	24/09/2019 11:29:29	Config. ON	EJ_TRAINA	RHR Train A running in Modes 4-6 (shutdown)	24/09/2019 11:29:40	sa	
	24/09/2019 11:26:25	TAKE OUT	1KJ-K02-2	EDG 2 ENGINE 1KJ-K02-2	24/09/2019 11:26:43	sa	
	24/09/2019 11:26:25	Config. OFF	KJ_SEIS_2	EDG2 not claimed in seismic event	24/09/2019 11:26:43	sa	
	24/09/2019 11:26:09	Config. ON	KJ_SEIS_2	EDG2 not claimed in seismic event	24/09/2019 11:26:18	sa	
	24/09/2019 11:25:59	Config. ON	EN_A	RBS pump A aligned for RHR operation	24/09/2019 11:26:06	sa	
	24/09/2019 11:25:43	TAKE OUT	1EJ-P01A	RESIDUAL HEAT REMOVAL PUMP A 1EJ-P01A	24/09/2019 11:25:55	sa	

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

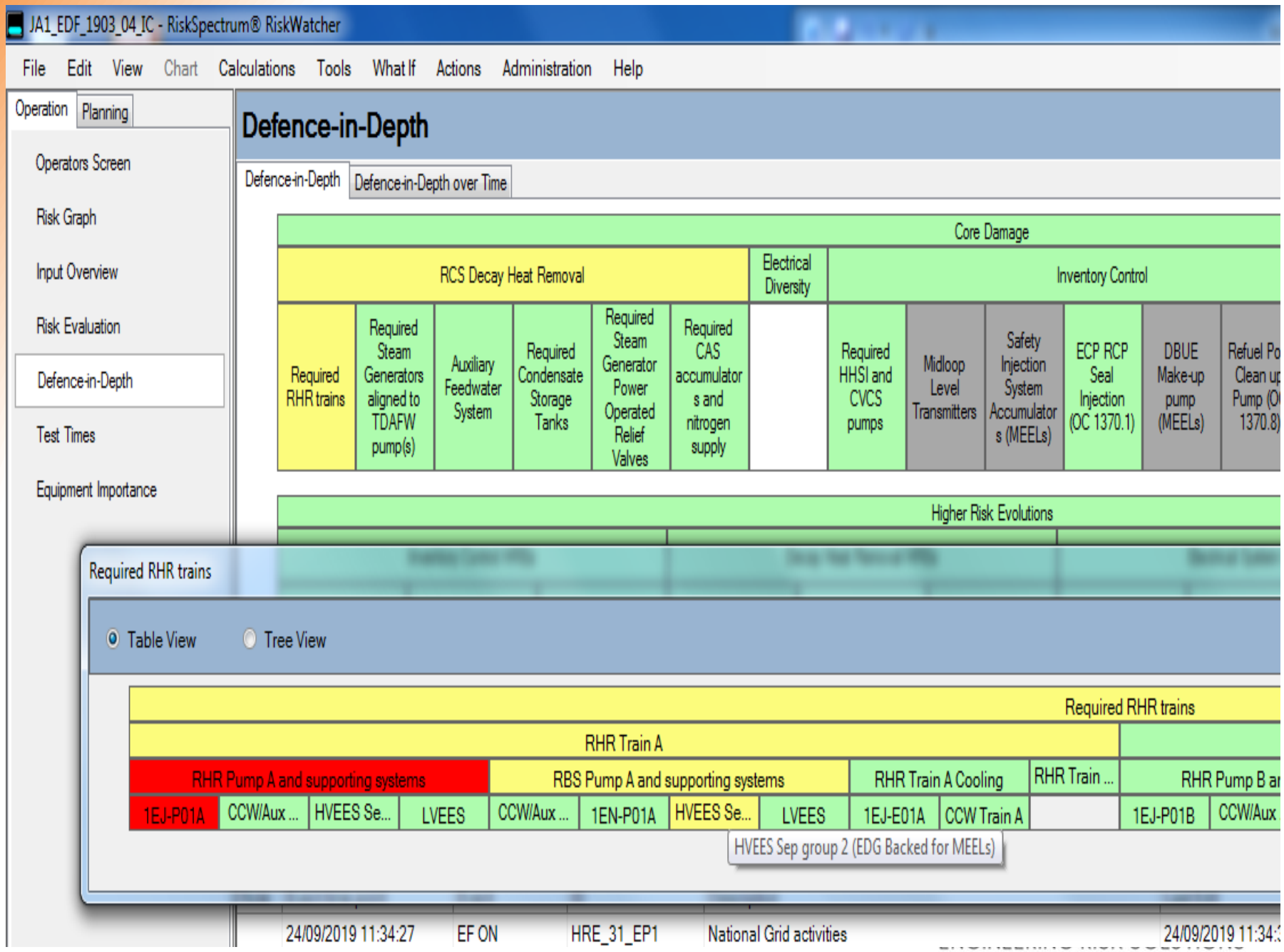
Example 1



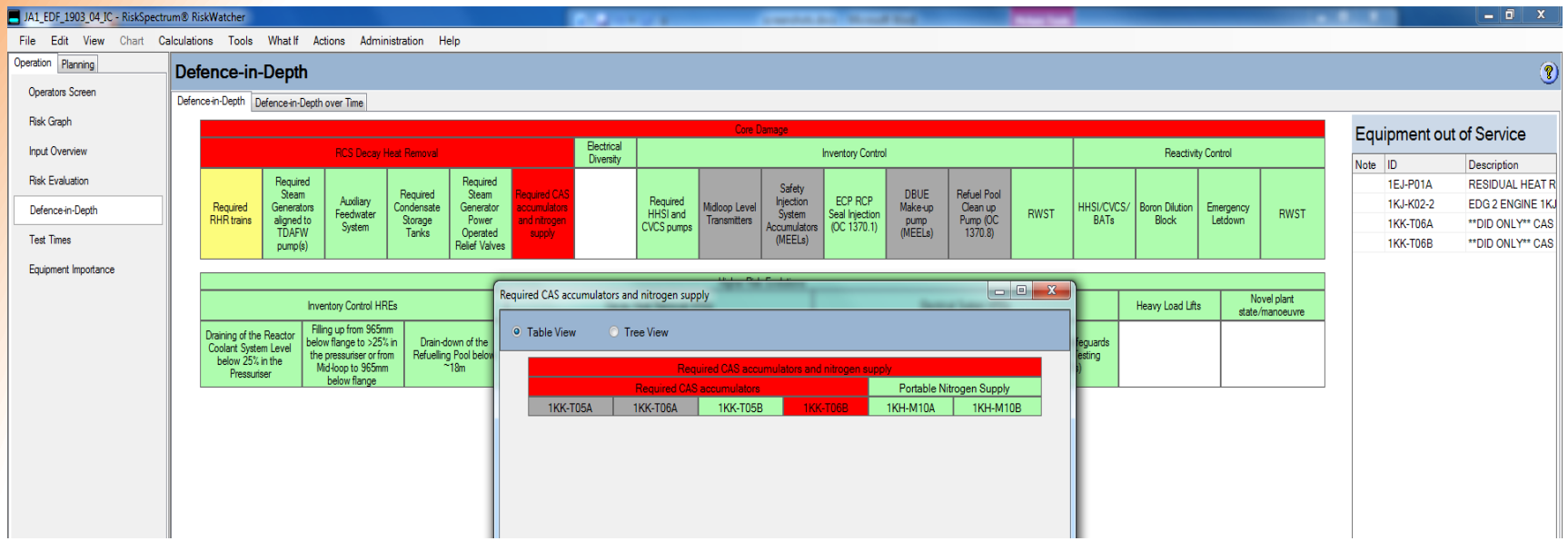
What does this screen tell the operator?

- Main screen
  - MEELs requirement for DHR not met (yellow colour)
  - Some requirements not applicable in current plant configuration (grey)
- Pop-up
  - Required pump not EDG backed (yellow colour)
  - One pump out of service but not required (red colour does not propagate up)
  - One pump not aligned for this function (grey colour)

Jacobsen analytics
ENGINEERING RISK SOLUTIONS


JA1_EDF_1903_04_IC - RiskSpectrum® RiskWatcher
File Edit View Chart Calculations Tools What If Actions Administration Help
Operation Planning
Operators Screen
Risk Graph
Input Overview
Risk Evaluation
Defence-in-Depth
Test Times
Equipment Importance
Defence-in-Depth
Defence-in-Depth Defence-in-Depth over Time
Core Damage
RCS Decay Heat Removal
Electrical Diversity
Inventory Control
Required RHR trains
Required Steam Generators aligned to TDAFW pump(s)
Auxiliary Feedwater System
Required Condensate Storage Tanks
Required Steam Generator Power Operated Relief Valves
Required CAS accumulators and nitrogen supply
Required HHSI and CVCS pumps
Midloop Level Transmitters
Safety Injection System Accumulators (MEELs)
ECP RCP Seal Injection (OC 1370.1)
DBUE Make-up pump (MEELs)
Higher Risk Evolutions
Required RHR trains
Table View
Tree View
Required RHR trains
RHR Train A
RHR Pump A and supporting systems
RBS Pump A and supporting systems
RHR Train A Cooling
RHR Train ...
RHR Pump B a
1EJ-P01A
CCW/Aux ...
HVEES Se...
LVEES
CCW/Aux ...
1EN-P01A
HVEES Se...
LVEES
1EJ-E01A
CCW Train A
1EJ-P01B
CCW/Aux
HVEES Sep group 2 (EDG Backed for MEELs)
24/09/2019 11:34:27
EF ON
HRE_31_EP1
National Grid activities
24/09/2019 11:34:3

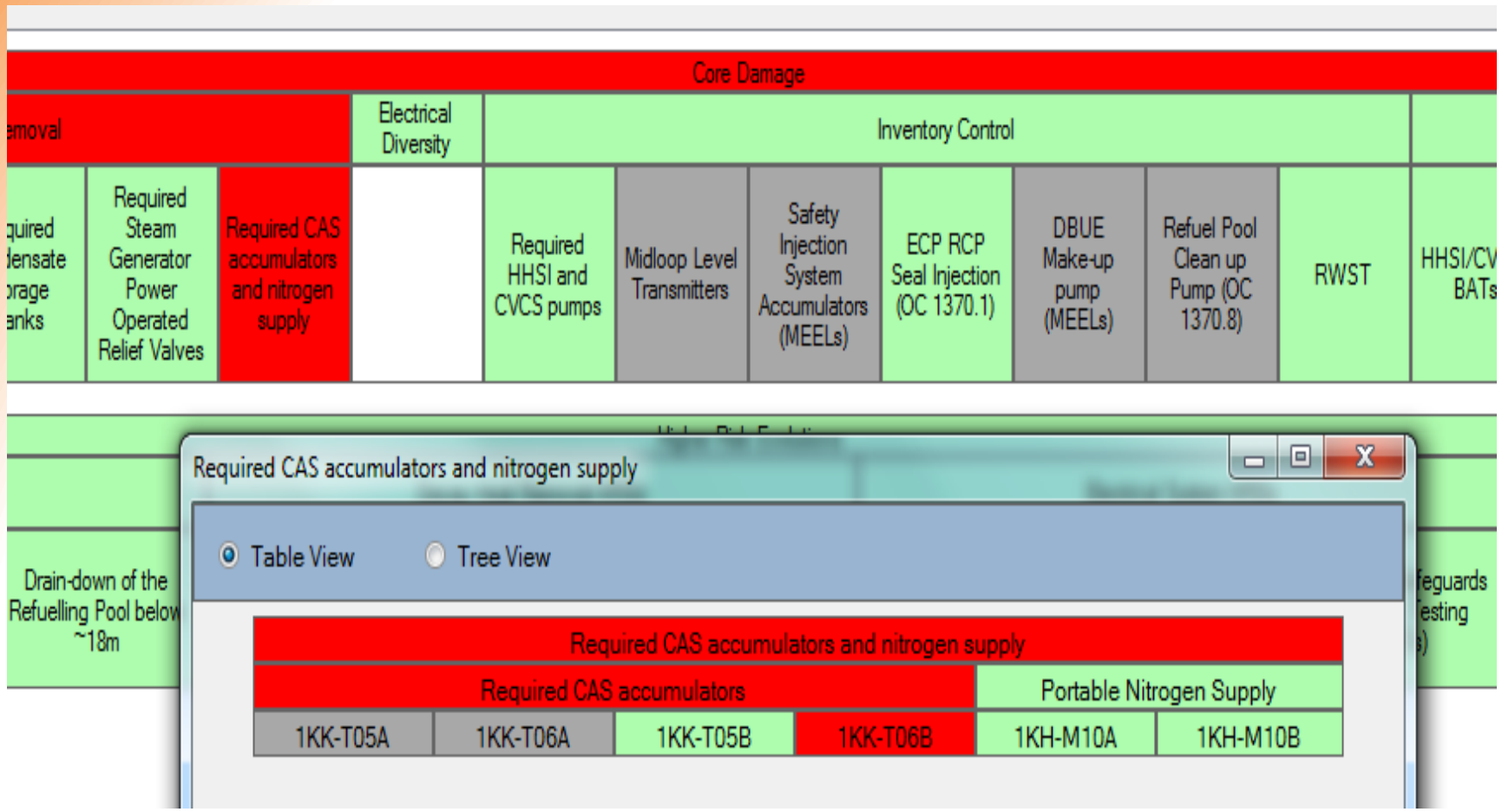
Example 2



What does this screen tell the operator?

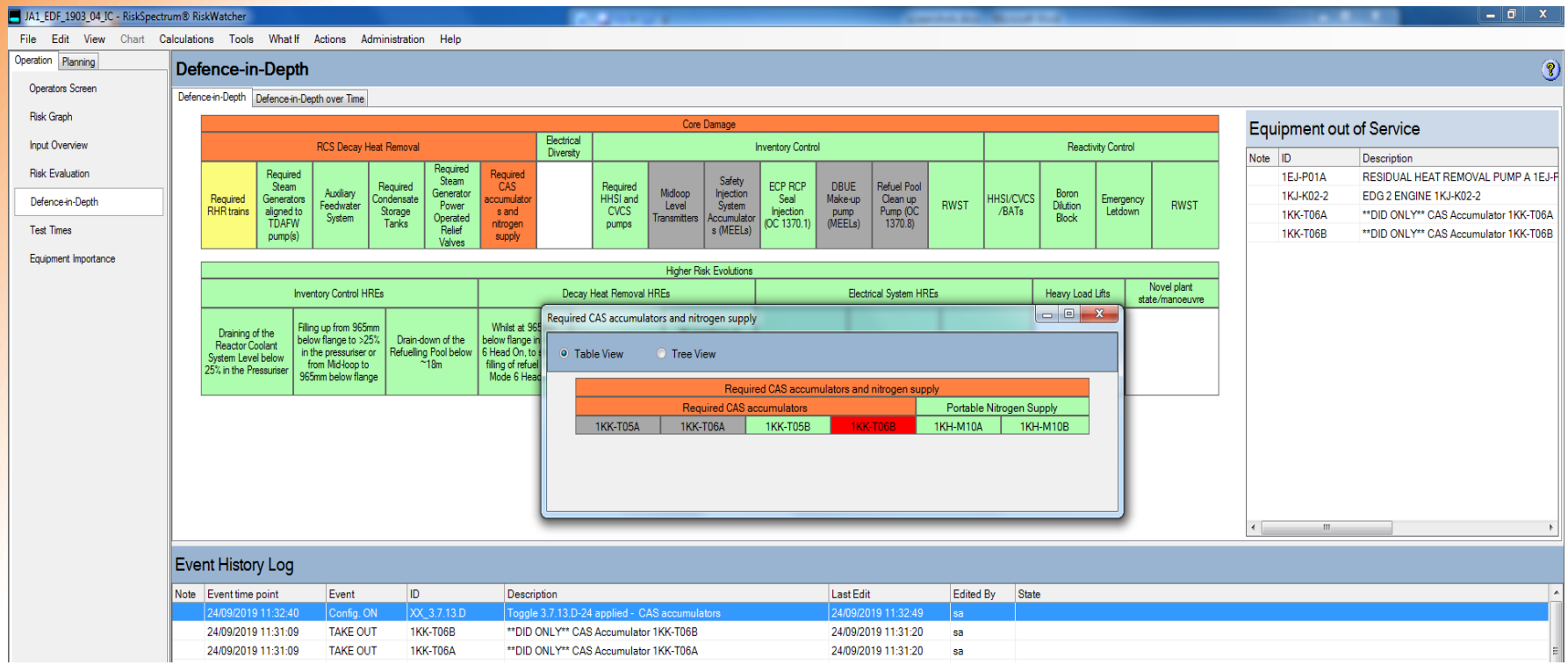
- Main screen
  - Tech Spec requirement not met (red)
  - MEELS requirement not met as per example 1 (yellow)
  - Some requirements not applicable in current plant configuration (grey)
- Pop-up
  - Required accumulator inoperable (red)
  - Two accumulators not required (grey)

Jacobsen analytics
ENGINEERING RISK SOLUTIONS



Jacobsen analytics
ENGINEERING RISK SOLUTIONS

Example 3



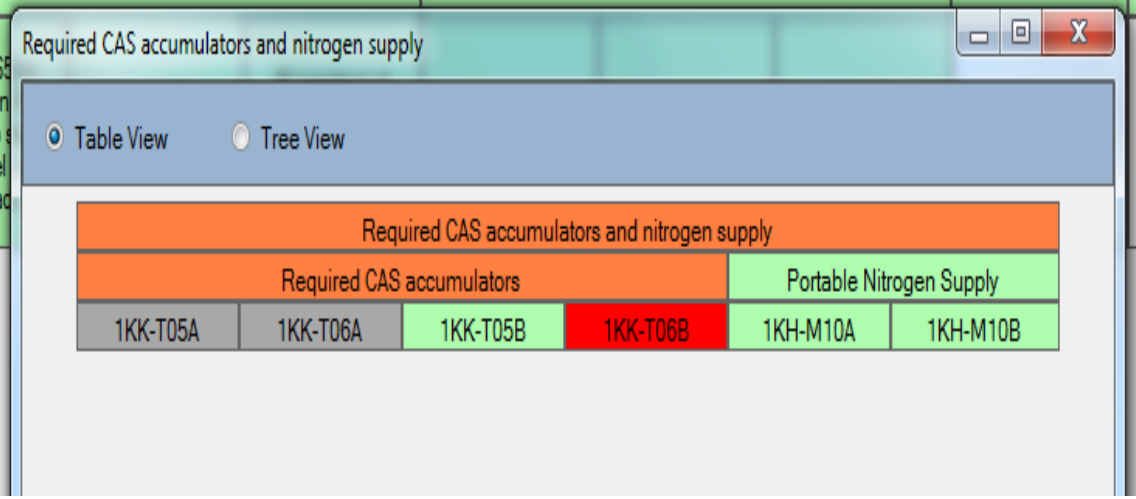
What does this screen tell the operator?

- Main screen
  - In Tech Spec condition with action completion time of less than 31 days and more than 24 hours (orange)
  - MEELS requirement not met as per example 1 (yellow)
  - Some requirements not applicable in current plant configuration (grey)
- Pop-up
  - Toggle applied (orange)
  - Required accumulator inoperable (red)
  - Two accumulators not required (grey)

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

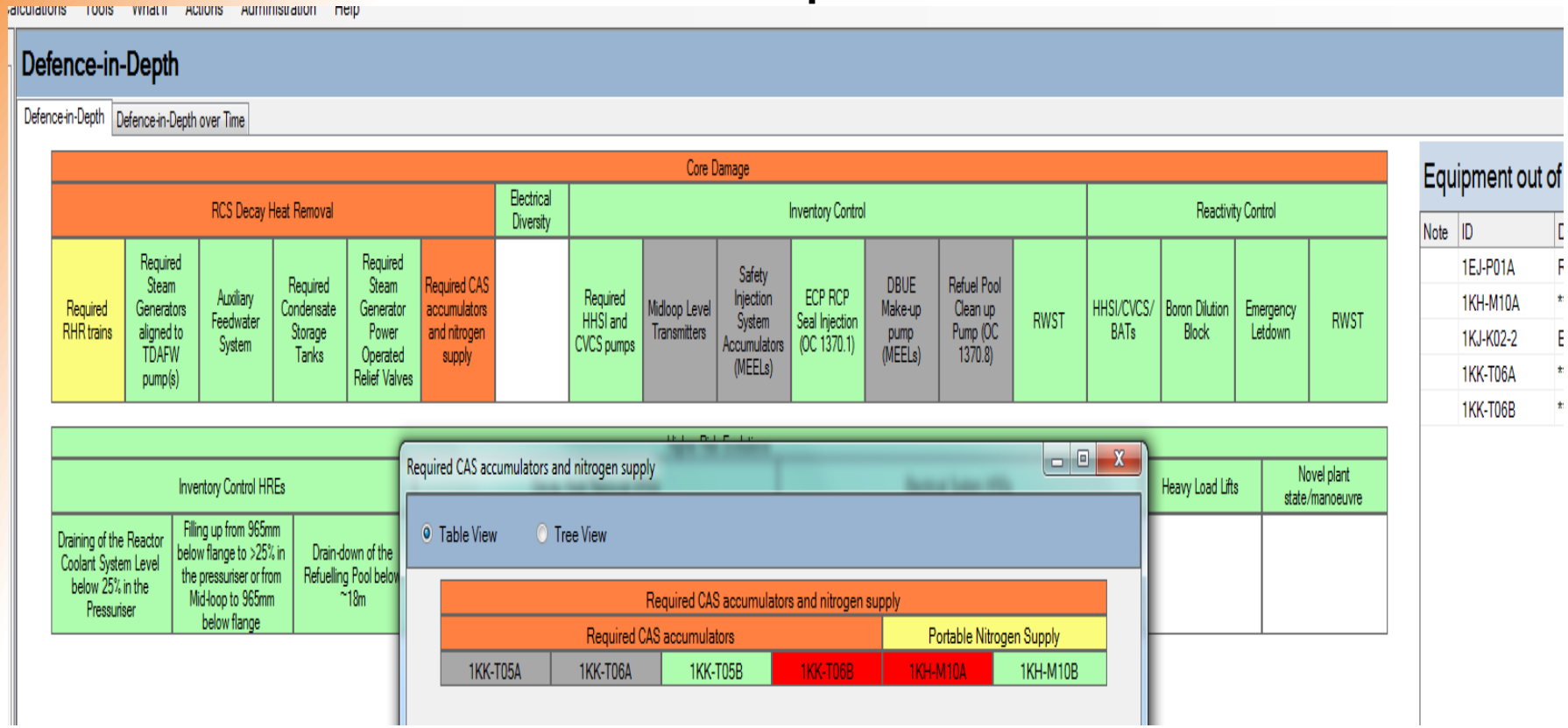
Core Damage																	
RCS Decay Heat Removal						Electrical Diversity	Inventory Control							Reactivity Control			
Required RHR trains	Required Steam Generators aligned to TDAFW pump(s)	Auxiliary Feedwater System	Required Condensate Storage Tanks	Required Steam Generator Power Operated Relief Valves	Required CAS accumulators and nitrogen supply		Required HHSI and CVCS pumps	Midloop Level Transmitters	Safety Injection System Accumulators (MEELs)	ECP RCP Seal Injection (OC 1370.1)	DBUE Make-up pump (MEELs)	Refuel Pool Clean up Pump (OC 1370.8)	RWST	HHSI/CVCS /BATs	Boron Dilution Block	Emergency Letdown	

Higher Risk Evolutions																	
Inventory Control HREs			Decay Heat Removal HREs			Electrical System HREs							Heavy Load Lifts	Novel state/ma			
Draining of the Reactor Coolant System Level below 25% in the Pressuriser	Filling up from 965mm below flange to >25% in the pressuriser or from Mid-loop to 965mm below flange	Drain-down of the Refuelling Pool below ~18m	Whilst at 965 below flange in 6 Head On, to s filling of refuel Mode 6 Head														



Jacobsen analytics
ENGINEERING RISK SOLUTIONS

Example 4



What does this screen tell the operator?

- Main screen (as example 3)
- Pop-up
  - As example 3 PLUS a required nitrogen supply inoperable (red)
  - Toggle applied – 31 days to restore nitrogen supply (yellow).

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

nce-in-Depth | Defence-in-Depth over Time

Core Damage																
RCS Decay Heat Removal						Electrical Diversity	Inventory Control									
Required RHR trains	Required Steam Generators aligned to TDAFW pump(s)	Auxiliary Feedwater System	Required Condensate Storage Tanks	Required Steam Generator Power Operated Relief Valves	Required CAS accumulators and nitrogen supply		Required HHSI and CVCS pumps	Midloop Level Transmitters	Safety Injection System Accumulators (MEELs)	ECP RCP Seal Injection (OC 1370.1)	DBUE Make-up pump (MEELs)	Refuel Pool Clean up Pump (OC 1370.8)	RWST	HHSI/CVCS/ BATs	Borc

Inventory Control HREs			Heav
Draining of the Reactor Coolant System Level below 25% in the Pressuriser	Filling up from 965mm below flange to >25% in the pressuriser or from Mid-loop to 965mm below flange	Drain-down of the Refuelling Pool below ~18m	

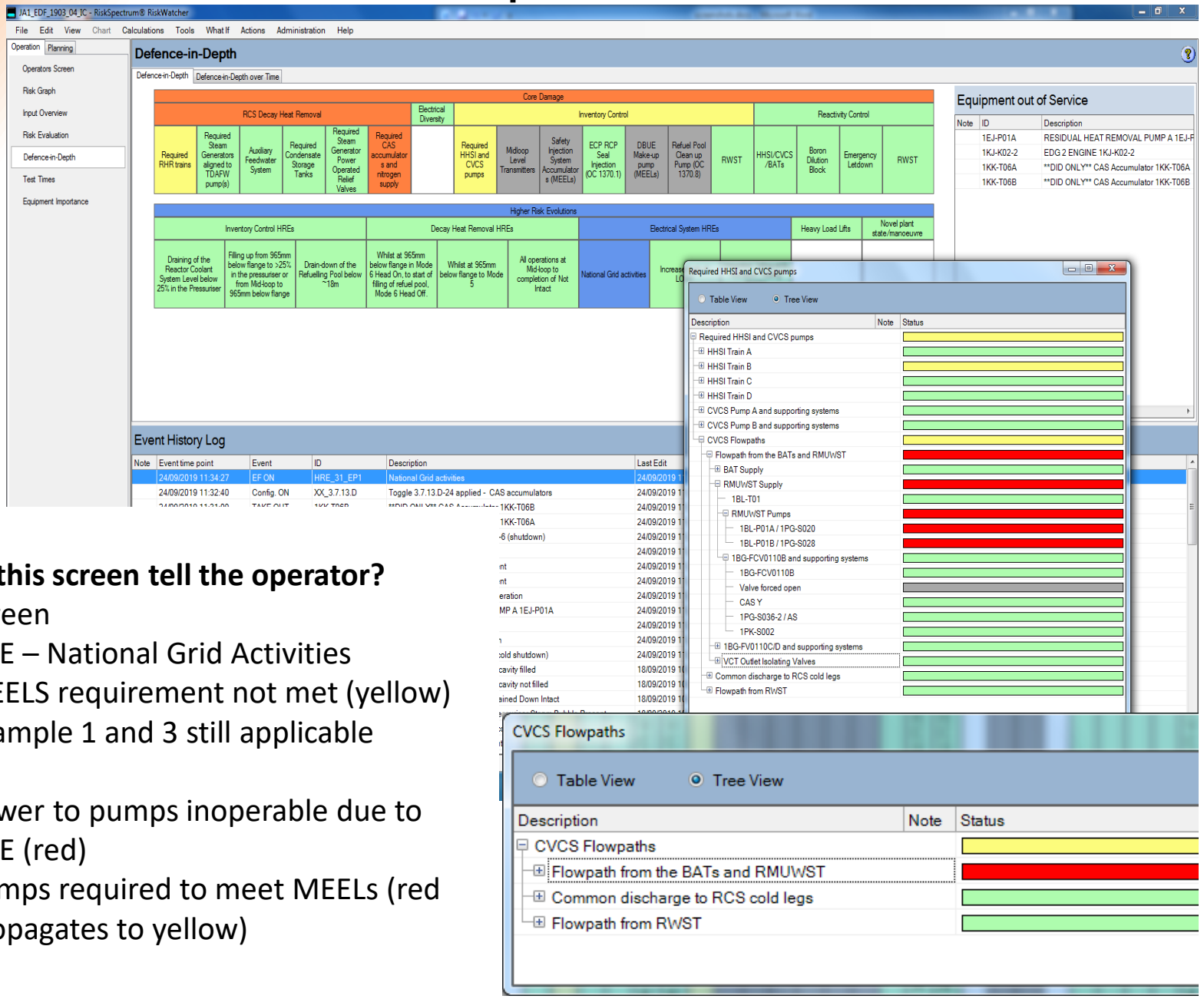
Required CAS accumulators and nitrogen supply

Table View Tree View

Required CAS accumulators and nitrogen supply					
Required CAS accumulators				Portable Nitrogen Supply	
1KK-T05A	1KK-T06A	1KK-T05B	1KK-T06B	1KH-M10A	1KH-M10B

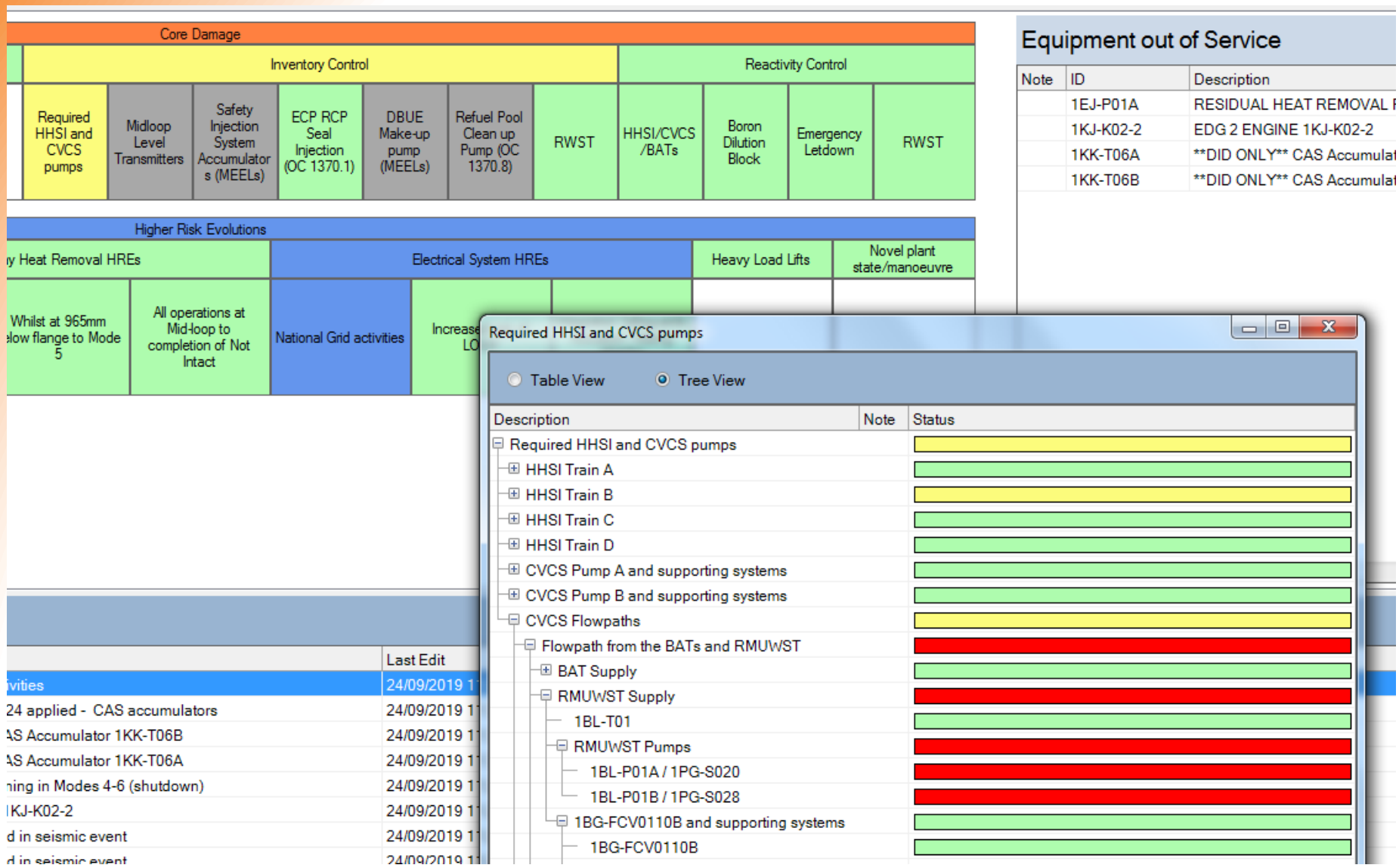
Jacobsen analytics
ENGINEERING RISK SOLUTIONS

Example 5



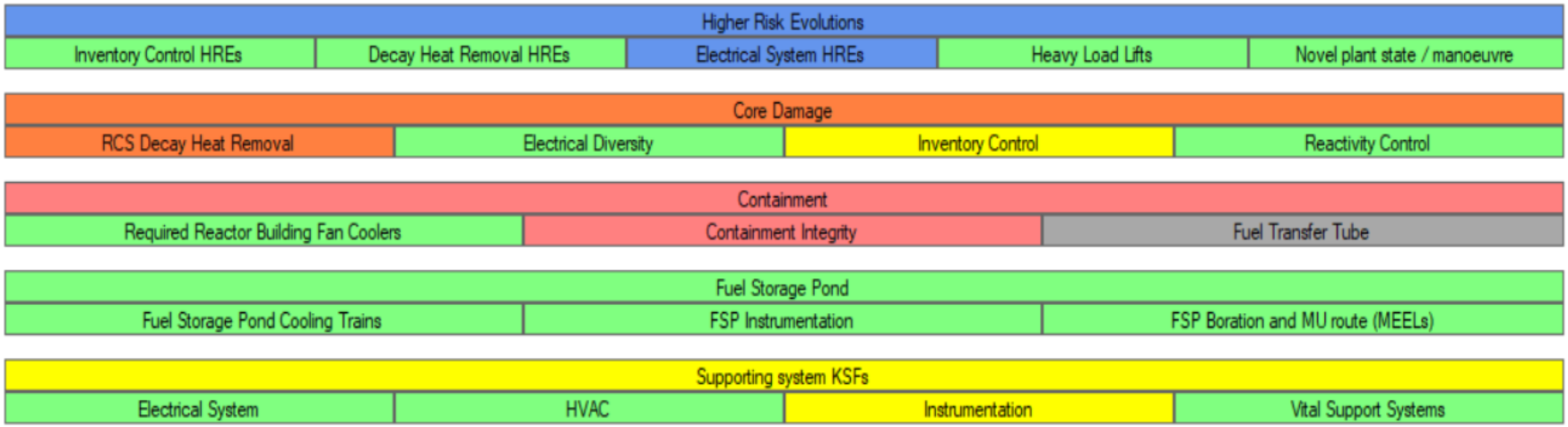
What does this screen tell the operator?

- Main screen
  - HRE – National Grid Activities
  - MEELS requirement not met (yellow)
  - Example 1 and 3 still applicable
- Pop-up
  - Power to pumps inoperable due to HRE (red)
  - Pumps required to meet MEELs (red propagates to yellow)



Jacobsen analytics
ENGINEERING RISK SOLUTIONS

Thank You!



Jacobsen analytics
ENGINEERING RISK SOLUTIONS