Other PSA's

Low power and shutdown PSA

Content

- Why shutdown PSA?
- Definitions
- Plat damage states and Plant operational states
- Specific modelling tasks of the low power and shutdown PSA
- SPSA and decision making
- Conclusions

1 WHY SHUTDOWN PSA (SPSA)?

- Earlier idea: shutdown reactor is a safe reactor!
- THIS IDEA HAS CHANGED!!!!
- Internationally, the amount of safety significant events during outages and in low power states has been high
- Even Chernobyl was a low power event (after the spurious lowering of reactor power range)!
- The number of physical and automated barriers is lower in shutdown than during the power operation
- Shutdown PSAs have shown that risk can be comparable to power operation (and the duration of outages is short)
- Some rare initiators may lead to accidents very fast (normally shutdown events are slow by their nature)

1 WHY SHUTDOWN PSA (SPSA)? (Cont.)

- See Loviisa VVER-440 Level 1 PSA example (situation 1998, main shutdown risk contributor dropping heavy loads in the containment):

INITIATORS	*CDF [1/yr]*	*% of CDF_{tot}*
Internal	$4,4 \cdot 10^{-5}$	**25,4 %**
power operation	$1,6 \cdot 10^{-5}$	9,3 %
shutdown and low power	$2,8 \cdot 10^{-5}$	*16,2 %*
External (power operation):		**74,6 %**
fire	$4,0 \cdot 10^{-5}$	23,2 %
floods	$1,0 \cdot 10^{-5}$	5,8 %
harsh weather conditions	$7,5 \cdot 10^{-5}$	43,5 %
seismic	$3,6 \cdot 10^{-6}$	2,1 %
TOTAL ~	$\mathbf{1,7 \cdot 10^{-4}}$	

- Where are risks at your plant??

2 Some definitions

- Shutdown = reactor is subcritical
- Outage = the plant has been shutdown to service equipment (planned) or to fix faults (unplanned)
- Refuelling outage = outage where fuel will be replaced partly
- Low power mode/state = reactor / turbine is producing power but less than maximal
- Operating mode = modes defined in plant technical (safety) specifications (TechSpecs)
- Plant operational state (POS) = state defined in SPSA, normally more detailed than operating modes

3 WHERE CAN I USE SPSA?

An SPSA can provide useful insights and feedback as regards:

- risk level and licensing (showing that the risk is below a certain level);
- risk monitoring and risk follow-up (see other lectures);
- outage planning (timetables);
- training, procedures and emergency planning for outages;
- shutdown technical specifications;
- outage management practices;
- hardware modifications.
- Etc, etc, ….

4 SOURCES OF RADIOACTIVITY

- Fuel in reactor vessel (core)
- Fuel in spent fuel pools - do not forget them!
- Spent fuel storage etc. fuel handling (separate study)
- Radiation accidents in other places (separate study)

5 SCOPE AND LEVEL OF DETAIL

- **Scope: an SPSA can never be a purely level 1 PSA study (see other lectures for different levels of PSA)!!**
- **This is due to the missing physical barriers in outages**

- **Outage types:**
- **1) (Yearly) refuelling outage,**
- **2) other maintenance outages,**
- **3) scram + shutdown**

- **Level of detail:**
- **Depends on the intended uses and available resources!!!**
- **Outage planning requires much more work than yearly risk average**
- **Practically may be dependent on the level of power operation PSA**

6 PLANT DAMAGE STATES

Plant damage states (PDSs) may be similar to a full power PSA.

However, an SPSA analyst may want to study more end states (with regard to the goal of the study!)

More probable end states than severe fuel damage may be studied

The following level 1(+) SPSA end states have been frequently used:

- severe fuel damage in core / pools (compare: core damage)
- core or pool boiling / heat-up above a certain point
- extensive unwanted criticality
- local unwanted criticality
- pressure vessel overpressurization in cold conditions (may lead to leaks and ruptures)
- heavy load collision (economic risk, may lead to leaks and ruptures)
- radioactive exposure to workers (occupational risk)

7 HOW TO DEFINE THE POSs

PLANT OPERATIONAL STATES:

- reactor criticality (and/or shutdown margin),
- reactor coolant system temperature and pressure,
- reactor coolant system water level,
- decay heat level
- reactor coolant system integrity (open / closed)
- containment integrity
- location of the fuel
- availability of safety and support systems
- system alignments,
- shutdown margin,
- status of the containment.

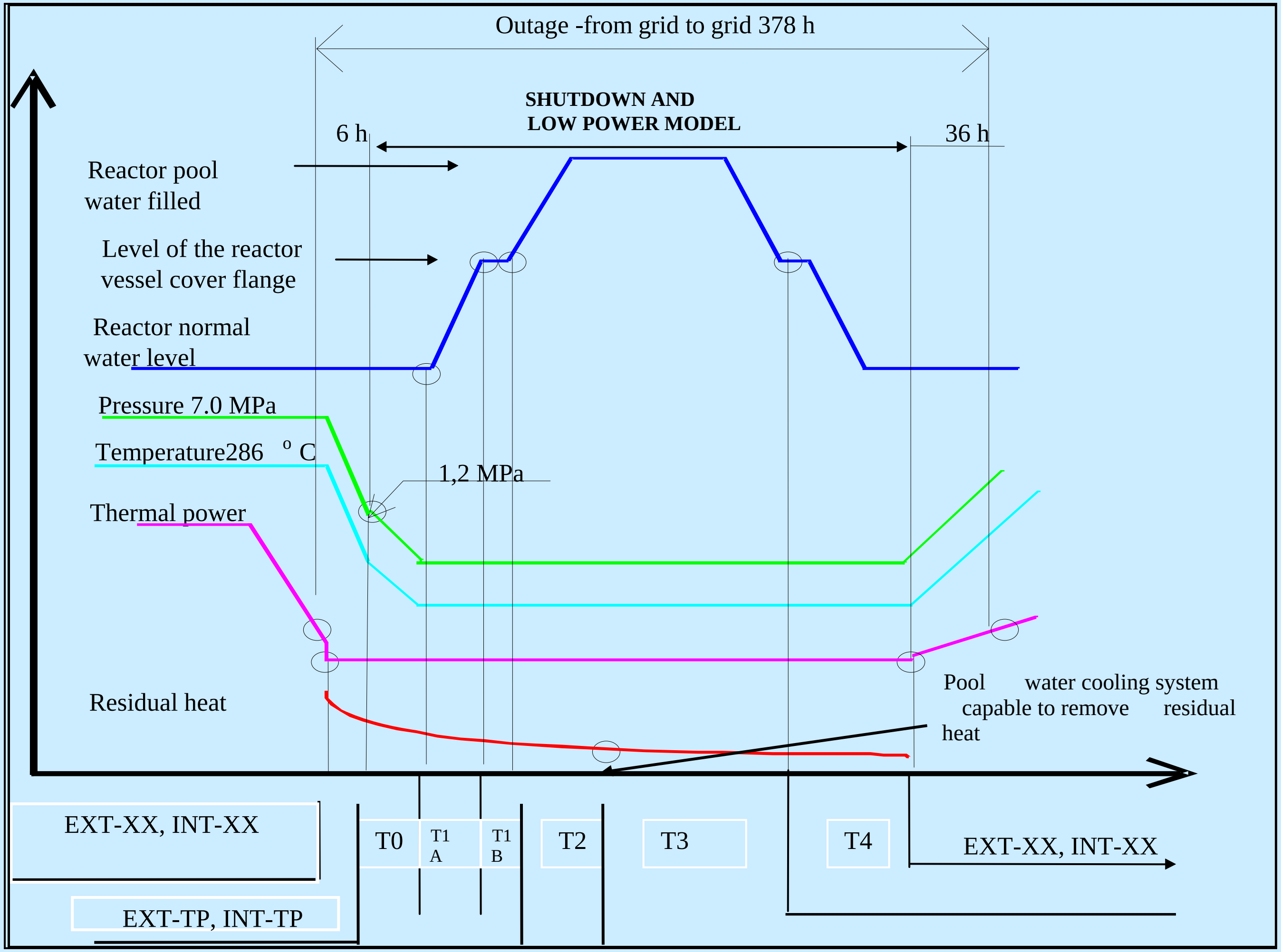
7 EXAMPLES OF POSs

Plant Operational States for Surry Unit 1 (PWR) Low Power & Shutdown Outage Activities

1. Low power operation and RX shutdown
2. Cooldown with SG (from 547°F to 345°F)
3. Cooldown with RHR (from 345°F to 200°F)
4. Cooldown with RHR (from 200°F to 140°F)
5. Drain RCS to midloop
6. Midloop operation
7. Fill for refuelling
8. Refuelling
9. Drain RCS to midloop after refuelling
10. Midloop operation after refuelling
11. Refill RCS completely
12. RCS heatup solid and draw bubble
13. RCS heatup with RCPs (from 200°F to 350°F)
14. RCS heatup with SGs (from 350°F to 547°F
15. RX startup and low power shutdown

Low power and shutdown PSA

7 EXAMPLES OF POSs (Cont.)



8 INITIATING EVENTS FOR SPSA

Events affecting critical safety functions:

(1) Loss of RHR

Can be further developed into primary, secondary side and fuel pool cooling events. Availability of heat sink has to be assessed, too.

(2) LOCAs

Primary LOCAs, interfacing system LOCAs shall be assessed with the inclusion of potential test and maintenance events that might cause them.

(3) Loss of AC power

Mostly due to loss of external grid connection leading to, e.g. loss of RHR. Man made shortcuts etc. events may prove out to be important contributors to loss of AC frequency.

(4) Events challenging the primary circuit integrity

Cold overpressure and secondary side events leading to thermal transients. Human actions may increase the PWR frequency of primary to secondary leak due to small pieces of material left to steam generators etc.

8 INITIATING EVENTS FOR SPSA (Cont.)

5) Reactivity events
Boron dilutions, return-to-criticality events and local criticality events, e.g. refuelling errors.

(6) Heavy load drop accidents
Heavy component and fuel drop events leading to material damage and potentially to large leakages. One of the worst possible initiating events that leads quickly to core damage is the drop of vessel head when lifted over the pressure vessel.

(7) Support system failures
Lead potentially to CCF initiators.

(8) On-site external events
Fires, flooding and such events leading to CCF types of initiators.

(9) Off-site external events
Storms, earthquakes, airplane crashes as for power PSA.

INITIATING EVENTS TAKE PLACE IN VARIOUS POSs

9 EXAMPLES OF IES FOR SELECTED REACTORS

Initiating events used in the French (PWR) studies:

INITIATING EVENTS	POS
LOCA	A, B, C, D, E
Steam generator tube rupture (SGTR)	A, B, C
Steam line break (SLB) - feedwater line break (FWB)	A, B
Loss of heat sink [component cooling water system (CCWS)]	A, B, C, D, E
Loss of SG feedwater	A, B
Loss of electrical supply	A, B
Loss of RHRS	
Dilutions	

10 PHYSICAL ANALYSES

The physical (reactor physical, thermal hydraulic, etc.) analyses for defining success criteria should take into account the following factors:

(1) Primary circuit status (open or closed, water level).

(2) Decay heat level (decreasing during a shutdown).

(3) Primary circuit parameters (temperature, pressure, shutdown margin), etc…

Depending on the scope of the study, the following areas may have to be addressed:

(1) Thermal hydraulic transient analysis.

(2) Reactor core analysis.

In some cases, hand calculations are enough!!

11 EVENT SEQUENCE (EVENT TREE) MODELLING

The event trees developed for full power operation can be modified for low power and specific shutdown states.

The modifications typically involve:

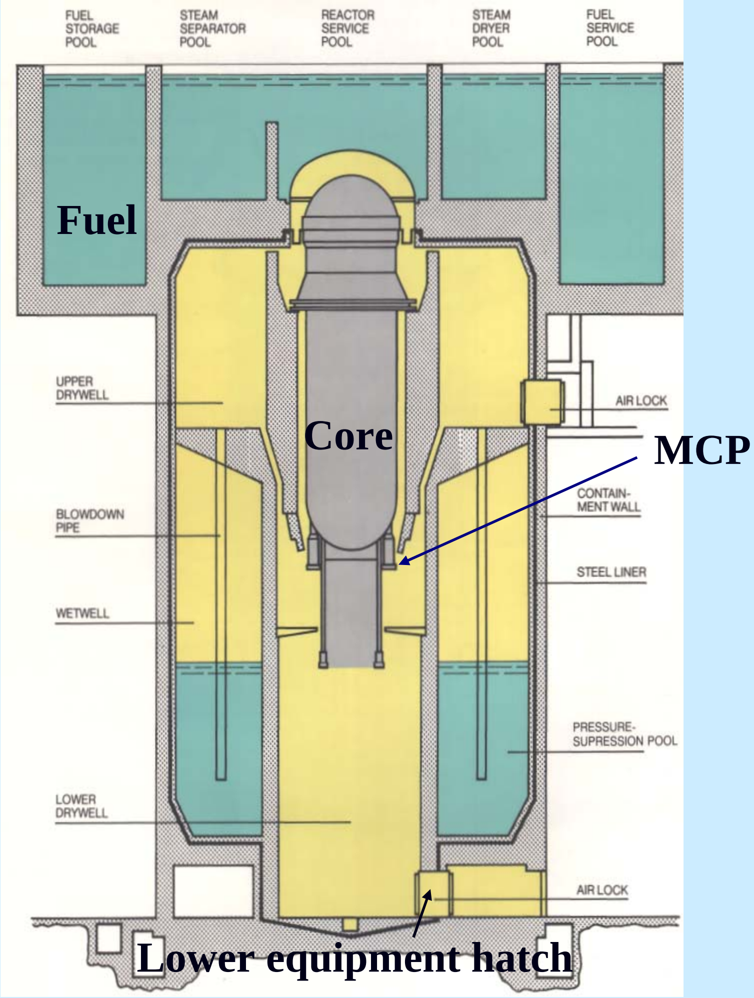
- removal of selected event headings, such as those related to reactor trip if the reactor is already shut down,
- relaxation of success criteria by modifying the functional requirements (for example, the number of pumps required)
- reviewing the accident sequences for consistency with the specific POS characteristics (which systems/trains are available, what signals are generated, what are the available indications to the operator, etc)
- event tree headings may also be added to account for operator interactions which are not relevant for the full power PSA.

12 SYSTEMS MODELLING (FAULT TREES)

Among the most important aspects:

- **Is there a model (fault tree) describing the system behaviour in different POSs - do we even need a fault tree?**
- **Is the system operating or stand-by (power operation / shutdown)?**
- **Actuation (manual/automatic)?**
- **Required mission time?**
- **Required success criteria in different POSs (k/n)?**
- **Initially available trains in different POSs (k/n)?**
- **Recovery credibility (human) in SPSA - some systems may be easily reachable and time windows long but not in all conditions?**

12 SYSTEMS MODELLING (FAULT TREES) (Cont.)



DO NOT UNDERESTIMATE OUTAGE EVENTS!

- BWR main circulation pump (MCP) LOCA (due to human failures)
- initial leak rate 750 kg/s!
- less than 2 minutes to close the lower equipment hatch before the water reaches it - wires going through the hatch
- no means to re-establish fuel cooling if it fails!
- containment open an cannot be re-closed (lid + hatch)
- less than 30 minutes to fuel (both in core and in pools) uncovery
- <u>conclusion:</u> hatch has to be closed during the critical phases of MCP overhaul

13 HUMAN RELIABILITY ANALYSIS

Human actions:

A) affect systems through planned / unplanned maintenance etc. activities before an initiating event

B) initiate an accident sequence through failures in co-ordination, understanding ("errors of commission") etc.

C) contribute in accident sequences by the means of recovery, actuation of systems (automatic mode overridden!) and taking non safety equipment into use (fire water to pools etc.).

D) Note also: accident management decisions (level 2 PSA)

Factors having impact on SPSA human reliability:

Lack of EOPs and maintenance procedures, TechSpecs(?), Simulator training limits (can it simulate shutdown states?), Lack of training, Actions outside the CCR, High number of work orders, Other duties for control room, Work overtime, External craftsmen, etc., etc.

13 HUMAN RELIABILITY AND SYSTEMS MODELLING

Tutkimus:	System recovery	Intentional (maintenance) unavailability	Other system model modifications
Zion	Not generally assumed	Unavailability was taken into account in component data	Different initial condition and actuation taken into account
Seabrook	Not generally assumed	Unavailability was taken into account in component data	Different initial condition and actuation taken into account
French studies	Recovery of RHR credited	System unavailability calculated with a) all trains b) with TechSpecs min requirements	Power PSA models were used to great extent, since system availability contribution to risk was not great
Belgian studies	Not generally assumed	Max. 1 train was assumed inoperable	Power PSA models were used where possible
NRC PWR/BWR	Recovery of RHR credited	Unavailability was taken into account in component data	Different success criteria, actuation, human errors and intentional unavailability included
Olkiluoto	Recovery of RHR credited	In each POS according to TechSpecs and working practices.	Different success criteria, actuation, human errors and intentional unavailability included

14 DEPENDENCES

There are, at least, the following dependencies:

- system dependencies
- CCFs (and some of them are born in outages by human activities)
- CCIs, common cause initiators
- etc. as in every other PSA

Specific for SPSA:

- dependencies due to POS, e.g., certain initiating events can only take place in certain POSs

15 PROBABILISTIC QUANTIFICATION

Not discussed in detail in this presentation (expert topic)

See, for example, IAEA-TECDOC-1144, Probabilistic safety assessments of nuclear power plants for low power and shutdown modes

16 SENSITIVITY, UNCERTAINTY AND IMPORTANCE

Same methods as for other PSA studies may be used

Again, note the role of human actions and their administrative control!

17 PRESENTING THE RESULTS

a) Fuel damage frequency - contribution integrated over all POSs

Dominant sequences contributing to fuel damage frequency

POS distribution over fuel damage frequency

IE distribution over fuel damage frequency

Results of fuel damage frequency uncertainty analysis - <u>what is not known!</u>

Results of fuel damage frequency importance and sensitivity analysis

(b) Presentation of results per POS

Dominant sequences contributions to fuel damage frequency

IE distribution over POS - fuel damage frequency

17 PRESENTING THE RESULTS (Cont.)

(c) Presentation of Level 2 interface

Plant damage state characteristics and frequencies

(d) Qualitative insights and conclusions

Interpretation of results and engineering insights

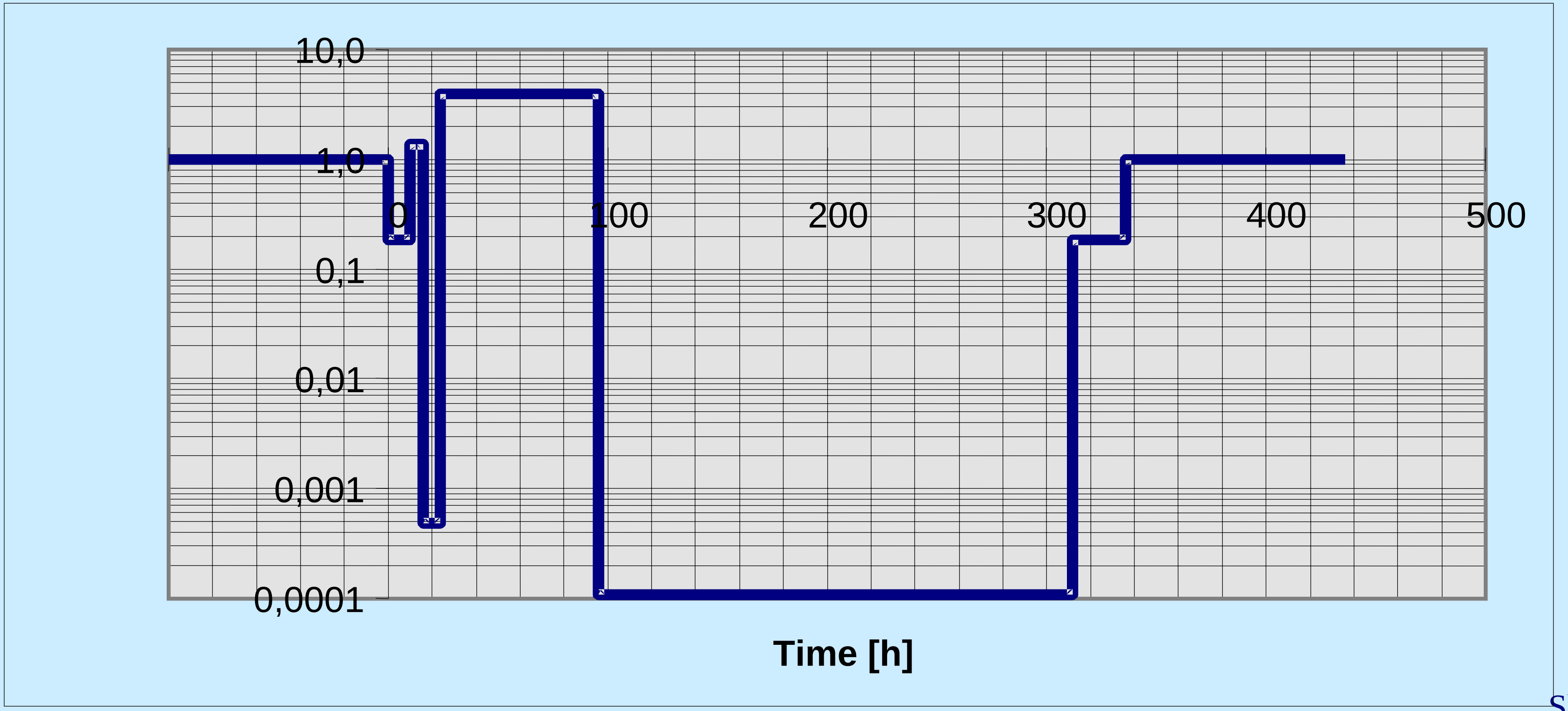
Credibility of the results

Conclusions, recommendations

17 PRESENTING THE RESULTS (Cont.)

An example on how the risk level in various phases of an outage may be shown!

Notice the dependency between some human activities and POSs (they take place after the preconditions are filled but when exactly?)



18 SPSA AND DECISION MAKING

<u>Advantages of SPSA backfittings:</u>

*May be cheap (procedural changes, preparedness etc.)

*Good analysis may (in some countries) even shorten outage time

<u>Disadvantages of SPSA backfittings:</u>

*Their bases are uncertain by definition - such as the impact

(administrative barriers - safety culture)

*There may only be interim solutions if the design is

18 SPSA AND DECISION MAKING (BWR EXAMPLE)

	Contribution to severe fuel damage frequency [%]	Annotations
Risk reduction measures taken:		**Contribution taken into account in severe f.d.f.**
MCP plugs substituted to a cotter-pin model	36	Decreases LCB initiating event frequency
Guards placed to lower equipment hatch during the MCP overhaul	28	Decreases LCB risk via improved chances to close the hatch quickly
Auxiliary feedwater piston pump use was forbidden in the waterfilling of reactor	3	Decreases cold overpressurization initiator frequency
Improved means to reduce overpressure, e.g., no more relief valve capping and new steam outlet routes	83	Decreases the overpressurization frequency and consequences via improved possibilities to reduce pressure
Total effect on the severe fuel damage frequency	**92**	
Suggested measures:		**Contribution not taken into account in severe f.d.f.**
The introduction of temporary plugs in the reactor hall and repeated training in their use	78 (max)	Decreases leakage frequency via improved chances to plug the leakage
Procedure and work practice improvements	Contribution is dependent on the renewed procedures and on the training given in their use	Improved chances to act correctly given an initiating event etc.

18 SPSA AND DECISION MAKING (Cont.)

EXAMPLES OF IMPROVEMENTS:

Design that takes into account low power requirements

Thorough analyses (FSAR, SPSA, ASAR)

TechSpecs

Procedures (based on thorough thinking)

Outage planning

Functional and other tests

Work order practices

Administrative barriers

Regulatory guidance

Information centralisation (meetings, control room)

Information flow

Safety culture (my behaviour is important, too)

CONCLUSIONS

SPSA may be more plant specific than full power PSA (outages are more plant / organisation specific than power operations)

It is not just a PSA on loss of residual heat removal!! Beware!!

Human actions are in a major role

Safety and economic improvements may be related (e.g. better planning both enhances safety and shortens outages)

Safety culture (“my behaviour is important, too!”)

Anyway, it is just hard work ...