IAEA
International Atomic Energy Agency

NARSIS Workshop
Training on Probabilistic Safety Assessment for Nuclear Facilities
International Training Course
Warsaw, Poland, September 2-5, 2019

NUCLEAR POWER PLANT ACCIDENTS

Presented by: Alexander Duchac
Division of Nuclear Installation Safety
Department of Nuclear Safety and Security

Alexander DUCHAC (IAEA)

- Education
  - MSc. in Electrical engineering
  - Post graduate in Nuclear engineering
- Professional experience
  - 1982 – 1996 Bohunice NPP (Shift Supervisor, Manager of Operation)
  - 1996 – 1999 Nuclear Safety Authority (Director of Nuclear Safety dpt)
  - 1999 – 2002 Consultant (DSA, PSA, Design reviews)
  - 2002 – 2013 European Commission JRC, Petten (Nuclear safety research, European polices on Nuclear safety, European Stress Tests)
  - Since February 2013 with the IAEA, Safety assessment section, Electrical, I&C, HFE, Ageing management, Equipment qualification, Periodic safety reviews
- Liaison with IEC SC45A and a member of IEEE NPEC SC 6

Outline

- Is an accident at nuclear installation(s) a rear event?
  - How many did we have
  - What were the contributing factors
  - What have we learnt
- Main improvements resulted from accidents
- Design requirements evolution - earlier and new concept of plant states
- Design features for preventing/mitigating accident conditions
- Conclusions

Why we have to consider accidents in the design of the plant?

- Operating experience show that accidents happen

- We are learning from these accidents in order to:
  - Better understand why these accidents happen
  - Improve (design) safety standards
  - Improve operating procedures
  - Implement accident management strategies (procedures + equipment)
  - Train the plan personnel to cope with the accident scenario in simulated (severe) environmental conditions
  - Be prepared for unexpected

How many severe accidents did we have in nuclear installations or we know about?

- Most common answer is: three (3)
  - TMI
  - Chernobyl
  - Fukushima Daiichi

- Pioneering of nuclear power for energy production resulted in more…

- How many?

19 severe accidents found$^{1)}$

Reactor/site	Reactor type	Year	INES	Country
NRX	Water and air cooled heavy water moderated research reactor	1952	4	Canada
Experimental Breeder Reactor 1	Liquid metal fast breeder research reactor	1956	3	USA
Windscale Unit 1	Air cooled, graphite moderated isotope production reactor	1957	5	UK
Heat Transfer Reactor Experiment-3	Air cooled solid hydride moderated test reactor	1958	4	USA
Sodium Reactor Experiment	Sodium cooled graphite moderated test reactor	1959	4	USA
Westinghouse Testing Reactor	Low-pressure water cooled and moderated material test reactor	1960	4	USA
SL-1	Small boiling water reactor prototype	1961	4	USA
Fermi Unit 1	Liquid metal fast breeder reactor prototype	1966	4	USA
Chapelcross Unit 2	Gas cooled, graphite moderated reactor (Magnox)	1967	3	UK
Saint Laurent Unit A1	Gas cooled, graphite moderated power reactor	1969	4	France
Lucens	Gas cooled, heavy water moderated power reactor prototype	1969	4	Switzerland
105 K-West	Water-cooled graphite moderated	1970	3	USA
KS 150	Gas cooled heavy water moderated prototype power reactor	1977	4	Slovakia
TMI-2	Pressurized water reactor	1979	5	USA
Saint Laurent Unit A2	Gas cooled graphite moderated power reactor	1982	4	France
Chernobyl Unit 4	Light water cooled, graphite moderated, dual use reactor	1986	7	Ukraine
Fukushima Daiichi Units 1,2, & 3	Boiling water reactor	2011	7	Japan

1) Johnson, G., EPRI Report on Severe Accidents Lessons Learned, No. 3002005385

19 severe accidents found[1)]

	Estimated INES Level
Chernobyl Unit 4	7
Fukushima Daiichi Units 1,2, & 3	7
Windscale Unit 1	5
TMI-2	5
Heat Transfer Reactor Experiment-3	4
National Research Experimental Pile (NRX)	4
Fermi Unit 1*	4
KS 150 (PHWR)	4
Sodium Reactor Experiment (SRE)*	4
Saint Laurent Unit A2	4
Stationary low power (SL-1)*	4
Westinghouse Testing Reactor	4
Saint Laurent Unit A1	4
Lucens*	4
Experimental Breeder Reactor 1	3
Chapelcross Unit 2	3
105 K-West	3

*Prototype and demonstration plant

Types of Plants

4 LWR

7 Gas cooled, graphite or ^{2}H moderated reactors

2 Isotope production reactors

6 Test or research reactors

- I&C contributed to most events because the operators were not presented with the information that they needed
- Human factors contributed to most events because procedures and training did not prepare them for what occurred

---

1) Johnson, G., EPRI Report on Severe Accidents Lessons Learned, No. 3002005385

Severe accidents are “black swans”

Things
that were unknown or thought not credible

led to

Unexpected events

which

Neither plant systems nor operators* could bring under control

before

Significant fuel melt occurred

***Because they didn’t have adequate instrumentation, procedures, training, or systems**

Consider TMI-2 (March 1979)

Pressurizer safety valves failed to close, although they indicated ‘closed position’ at MCR

led to

Unexpected event sequence

which

Prevented operators for having accurate and timely situation awareness*

before

Significant fuel melt and hydrogen release into the containment occurred

***Because they didn’t have adequate instrumentation, procedures, training, or systems**

Consider Chernobyl-4 (April 1986)

Inadequate safety analysis, inadequate review of the test procedure, delaying the test by grid dispatcher

led to

Operators to maintain the core criticality at very low power level where the reactor is instable

which

Resulted in conducting the test in the worst possible plant conditions

before

Operators recognized* it was too late to initiate trip to prevent an accident

***Because they didn’t have adequate instrumentation, procedures, training, or systems**

Consider Fukushima Daiichi (March 2011)

IAEA

The maximum tsunami at the site was unknown.

Tsunamis > 6 m were considered not credible

led to

Failure of plant AC and DC power and

failure to plan for extended loss of AC & DC

which

Deprived operators* the information, systems, procedures and training needed to bring the plant under control

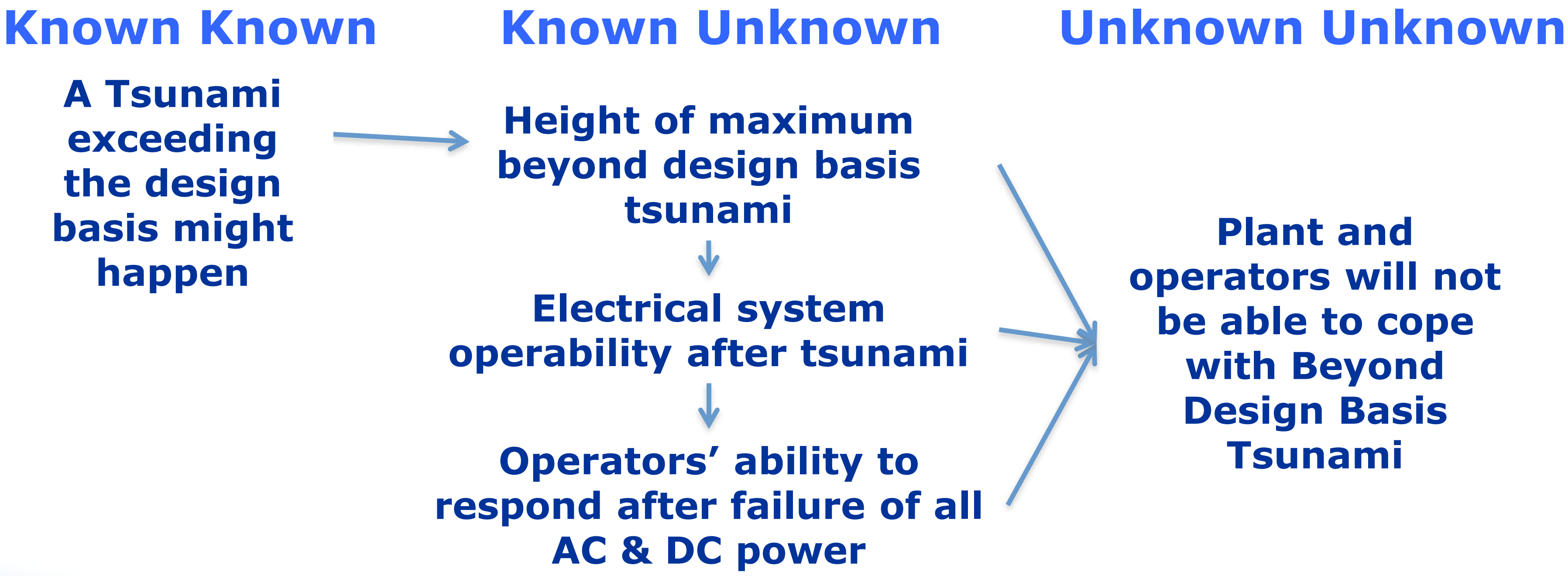
before

Significant fuel melt and radiation release occurred

***Because they didn't have adequate instrumentation, procedures, training, or systems**

An alternative model

- They were caused by unknown-unknowns
  - For example at Fukushima-Daiichi



Known Known

A Tsunami exceeding the design basis might happen

Known Unknown

Height of maximum beyond design basis tsunami

Electrical system operability after tsunami

Operators' ability to respond after failure of all AC & DC power

Unknown Unknown

Plant and operators will not be able to cope with Beyond Design Basis Tsunami

  - See real situation at Fukushima Daiichi in March 2011 in the following slides

Tsunami height observed at 14-15 meter

(Courtesy of TEPCO)

0 sec

6 sec

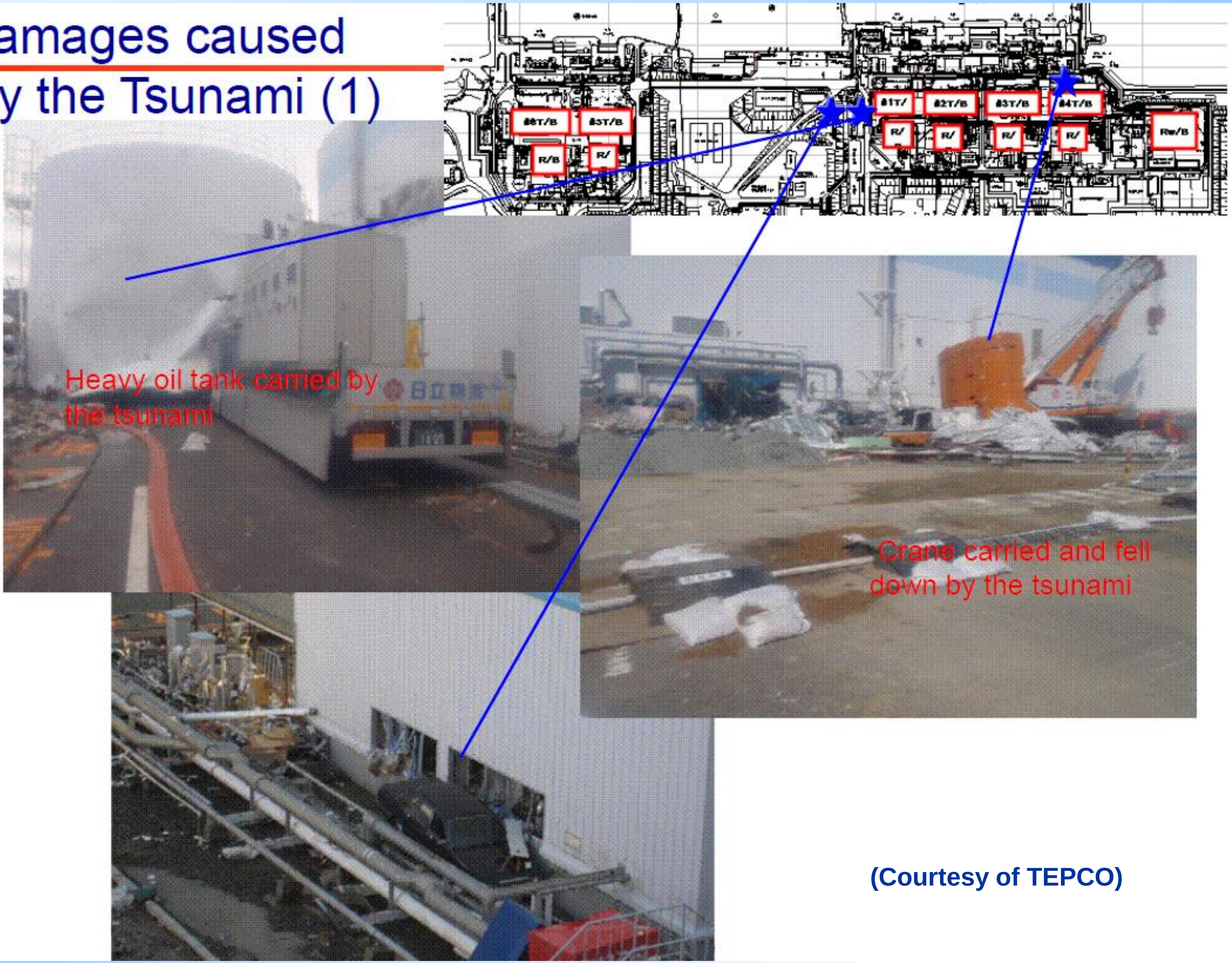
46 sec

56 sec

74 sec

98 sec

Damages caused by the Tsunami (1)

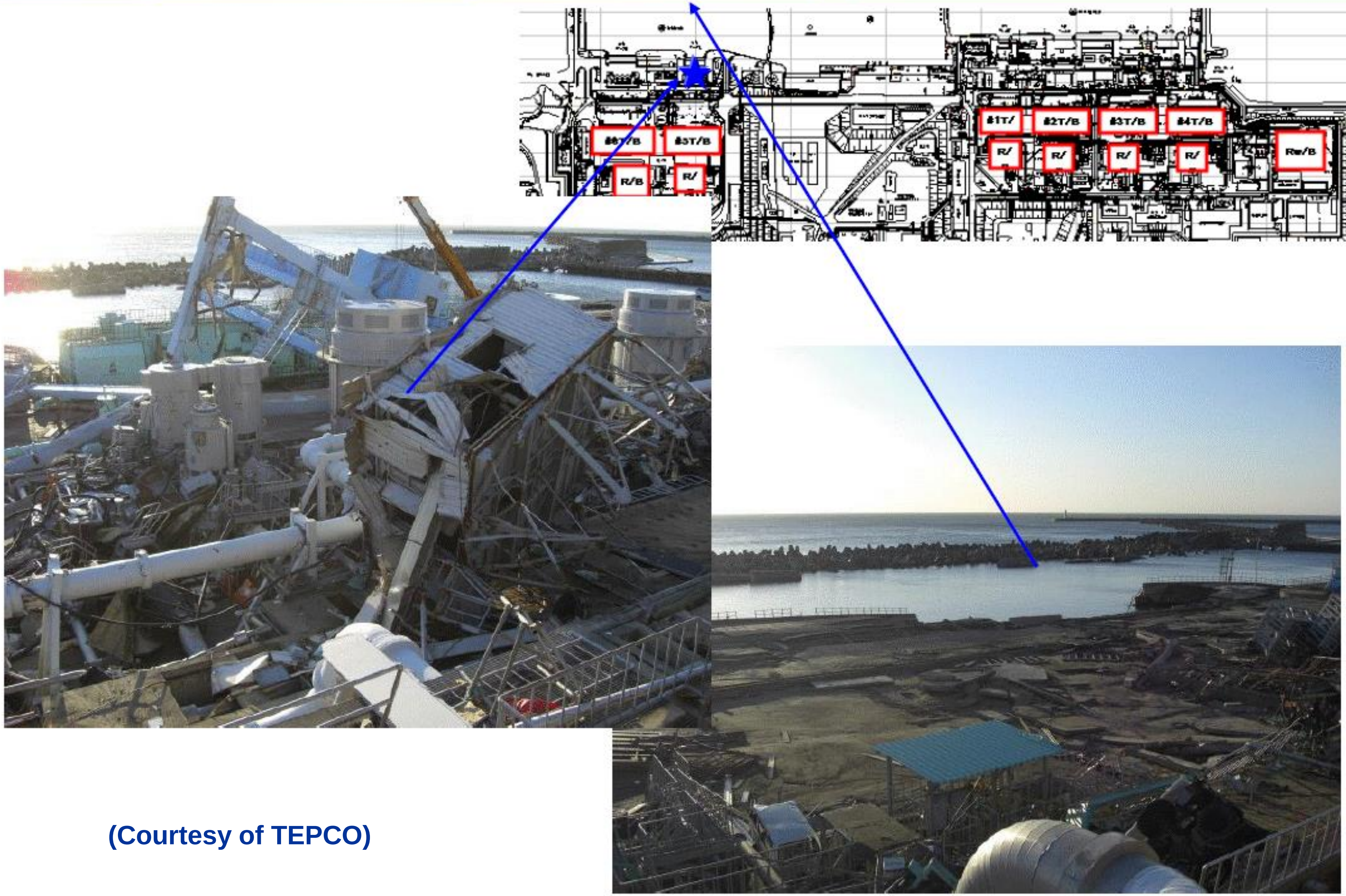


Heavy oil tank carried by the tsunami

Crane carried and fell down by the tsunami

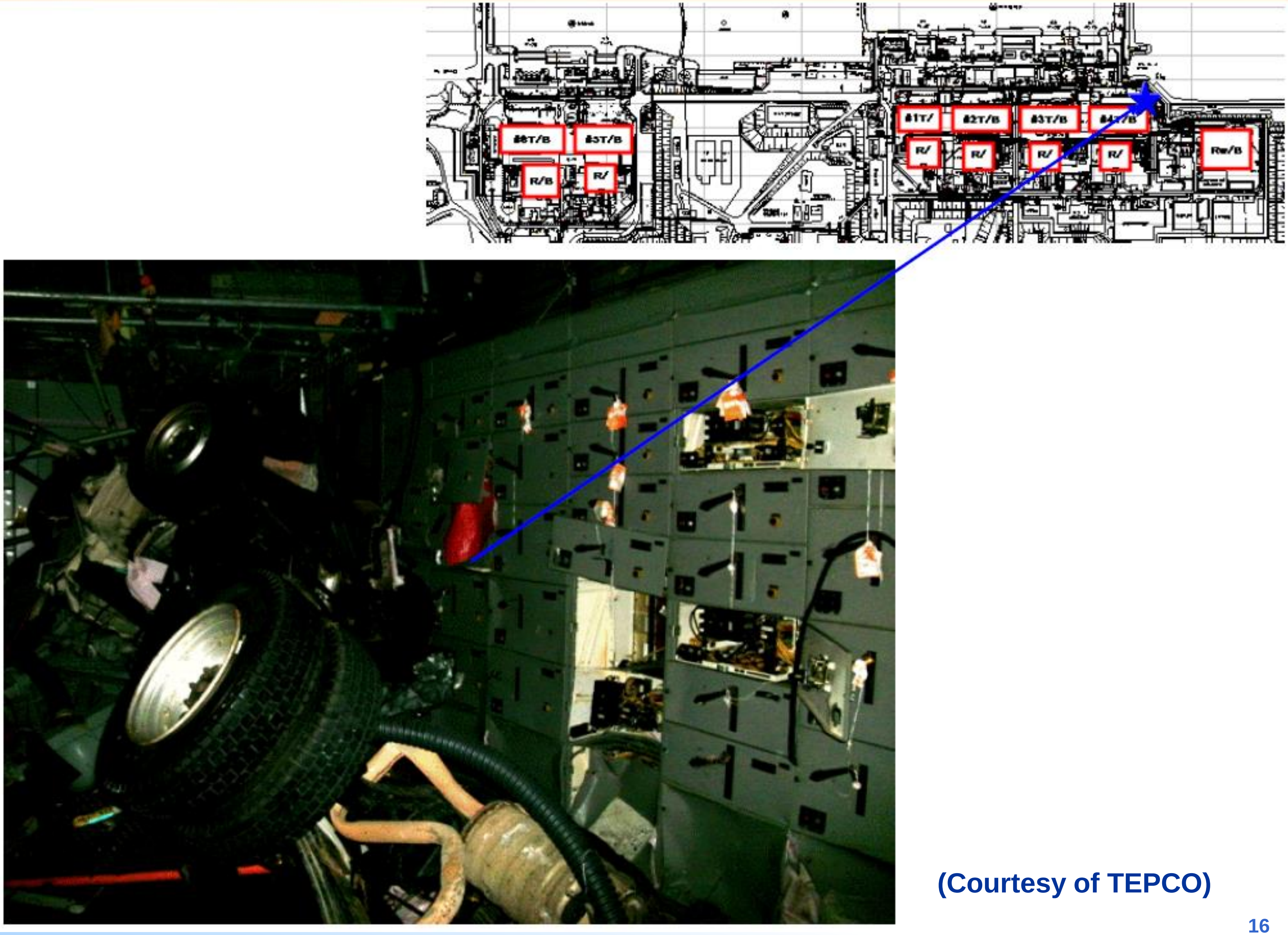
(Courtesy of TEPCO)

Damages caused by the Tsunami (2)



(Courtesy of TEPCO)

Damages caused by the Tsunami (3)



(Courtesy of TEPCO)

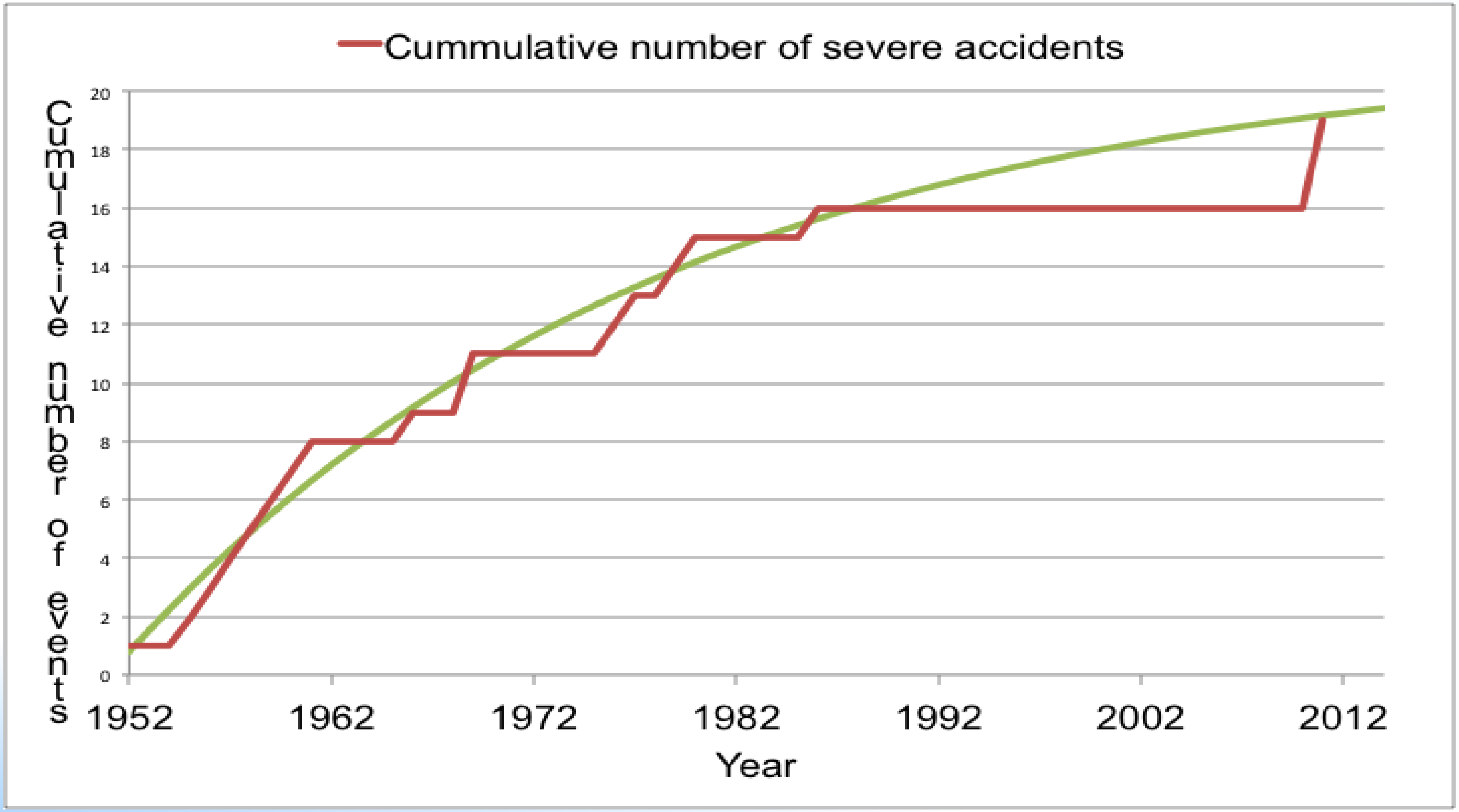
Yet another model

- There are always tradeoffs between safety and economics
- No one, and no organization can ever fully understand the risks and benefits of these tradeoff
- A history of successful operation tends to support a reduction of safety margins
- Eventually something bad happens

We must expect severe accidents

$$\frac{\text{2 events*}}{\text{16000 reactor years}} \approx 10^4\text{/Reactor Year}$$

*In Gen 2 reactors, counting Fukushima-Daiichi as a single event



All of the accidents involved bypass of DiD

<table>
<tr><th rowspan="2">Events ordered by date</th><th colspan="5">INSAG-10 Defense in Depth Levels</th><th></th></tr>
<tr><th>Level 1</th><th>Level 2</th><th>Level 3</th><th>Level 4</th><th>Level 5</th><th></th></tr>
<tr><td>Fukushima Daiichi U3</td><td colspan="3">Inadequate design basis for external hazards</td><td>Accident management can't deal with effects of extreme external hazards</td><td>Operators provide cooling of corium</td><td></td></tr>
<tr><td>Fukushima Daiichi U2</td><td colspan="3">Inadequate design basis for external hazards</td><td>Accident management can't deal with effects of extreme external hazards</td><td>Operators provide cooling of corium</td><td></td></tr>
<tr><td>Fukushima Daiichi U1</td><td colspan="3">Inadequate design basis for external hazards</td><td>Accident management can't deal with effects of extreme external hazards</td><td>Operators provide cooling of corium</td><td></td></tr>
<tr><td>Chernobyl U4</td><td colspan="5">Operators unaware of design's hazards. Inadequate, procedures, and operational discipline. Poor accident response</td><td>Core disassembly</td></tr>
<tr><td>Saint Laurent A2</td><td colspan="3">In vessel components came loose unexpectedly, No loose parts monitoring. Reactor trip setpoint on fission product release too high to prevent damage</td><td>Automatic trip: High Fission Product Activity</td><td></td><td></td></tr>
<tr><td>TMI-2</td><td colspan="2">Poor training, procedures, operational discipline, MCR design, & I&C design</td><td colspan="2">Operators shut down ECCS and don't recognize symptoms of loss of coolant/flow</td><td>Operators restore core cooling</td><td></td></tr>
<tr><td>KS 150</td><td colspan="2">Inadequate QA for fuel assemblies. Operation with unreliable fuel temperature channels</td><td>Shutdown delayed to check fuel temperature readings</td><td>Manual trip: High Fuel Temperature</td><td></td><td></td></tr>
<tr><td>Lucens</td><td colspan="3">Fuel assembly prone to flow blockage. Effects of water leakage into coolant not considered. Fuel assembly instrumentation not sensitive enough</td><td>Automatic trip: High Fission Product Activity</td><td></td><td></td></tr>
<tr><td>Chapelcross U2</td><td colspan="3">Provisions for detecting fuel damage inadequate
Fuel failure not detected before melt due to instrument time delays</td><td>Manual trip: High Fission Product Activity</td><td></td><td></td></tr>
<tr><td>Saint Laurent A1</td><td>Training, SW-V&V, HMI, RTS setpoint inadequate</td><td colspan="2">Operator overides interlock</td><td>Automatic trip: High Fission Product Activity</td><td></td><td></td></tr>
<tr><td>Fermi 1</td><td colspan="3">No safety analysis for metal sheets in reactor vessel coolant inlet Hydrodynamic loads caused sheets to come loose and block two fuel assemblies.</td><td>Manual trip: High containment radiation</td><td></td><td></td></tr>
<tr><td>WTR</td><td colspan="3">Inadequate operating procedures, training & fuel QA. No reactor trip on fuel failure. No confinement isolation</td><td>Fuel relocation and manual shutdown</td><td></td><td></td></tr>
<tr><td>SL-1</td><td>Single rod withdrawal could cause criticality</td><td colspan="3">Operator withdraws central control rod too far & too fast</td><td>Core disassembly & moderator ejection</td><td></td></tr>
<tr><td>SRE</td><td colspan="2">Pump shaft coolant properties unknown resulting in flow blockage within core</td><td>Operators didn't investigate causes of reactor trips</td><td colspan="2">Manual shutdown to investigate fuel condition</td><td></td></tr>
<tr><td>HTRE-3</td><td colspan="3">Inadequate CM. Failure to validate automatic control system design and configuration settings before use. Control/protection interaction.</td><td>Beneficial common cause failure of high fuel temperature trip</td><td></td><td></td></tr>
<tr><td>Windscale U1</td><td colspan="4">Inadequate knowledge about Wigner release. Inadequate core temperature measurement. Inadequate procedures. Confinement only partially effective.</td><td>Burning fuel removed from core</td><td></td></tr>
<tr><td>EBR-I</td><td colspan="3">Inadequate test procedure. Lack of common operating terminology between test director and operator. RTS set point for high power trip too high for test conditions.</td><td>Manual trip: Short period</td><td></td><td></td></tr>
<tr><td>105 KW</td><td colspan="3">Inadequate control of temporary changes and instrument calibration. 1oo1 reactor trip on low flow in channel</td><td>Automatic trip: high flow in channel (rupture)</td><td></td><td></td></tr>
<tr><td>NRX</td><td>Inadequate safety analysis, procedures & I&C.</td><td>Operator error</td><td colspan="2">Safety rods fail to fully insert after scram.</td><td>Manual trip: diverse shutdown system</td><td></td></tr>
</table>

🟨 **Causes**

🟩 **Termination**

We’ve done a good job of limiting the public’s radiation exposure

- Few events involved offsite emergency response
- No deterministic effects of radiation exposure to the public
- Only Chernobyl had identifiable stochastic effects
- 14 events had low or no offsite release
- Two events killed operators

At two sites radiation exposure was not the most important consequence

- Chernobyl and Fukushima Daiichi
  - Widespread contamination which disrupted lives, created anxiety and heavily impacted the economy

- At Fukushima Daiichi, for example
  - 210,000 people were evacuated
  - About 60 hospital patients died because of difficulties with evacuation
  - About 300 km^2 of land removed from use for a long time
  - Serious economic consequences

- We must prevent this in the future

I&C or HSI issues contributed to every event

Inadequate functionality	6 events
I&C availability	7 events
Design issues	14 events
HMI issues	8 events
I&C lifecycle issues	5 events
Lack of data for investigation	5 events

- Most events involved more than one issue

Additional contributing factors

Inadequate knowledge of the plant	13 events
Procedure issues	12 events
Operational discipline issues	6 events
Training issues	9 events

Design requirements evolution - earlier and new concept of plant states

What have we learnt from accidents to improve plant designs

Accident ‘driven’ improvements

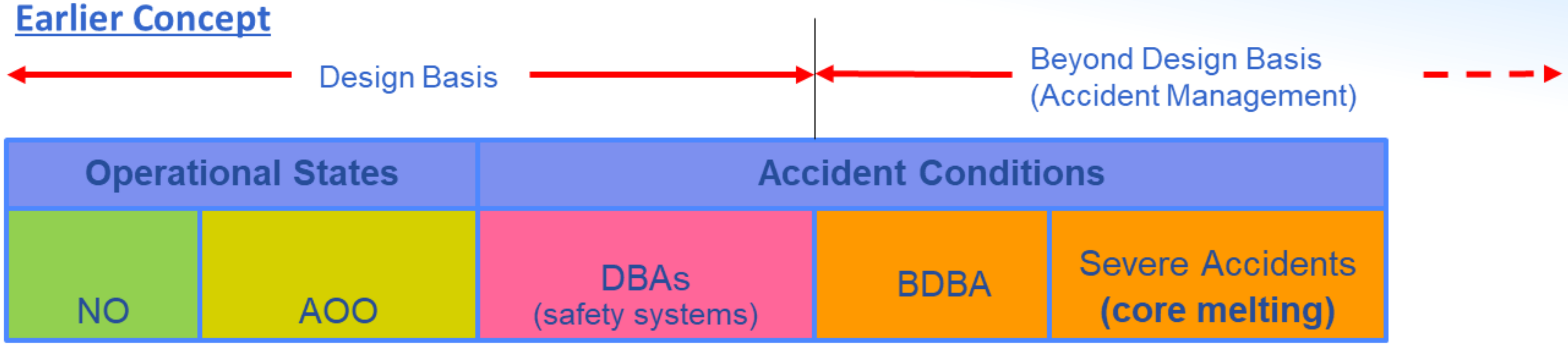
- After TMI
  - Operating procedures, EOPs
  - HMI design
  - Operator training in understanding transients (FSS, glass model)
  - Emergency plans
- After Chernobyl
  - Safety culture
  - Design of core (reduce positive void coef.)
  - Concept of non-routine tests
  - Training programmes (incorporate FSS training)

Accident ‘driven’ improvements

- After Fukushima
  - Assessment of external events (seismic, tsunami)
  - Procedures and means for coping with extended SBO
  - Preserving containment integrity (H_2 management, venting)
  - SAMG and accident mitigation equipment (multiunit approach)
  - Operator training and drills
  - Robust instrumentation, availability of information at TSC
  - Equipment qualification (external events, severe accident conditions)
  - Conducting Stress Tests

Concept of plant states and design envelope

Earlier Concept



Design Basis

Beyond Design Basis
(Accident Management)

Operational States

Accident Conditions

NO

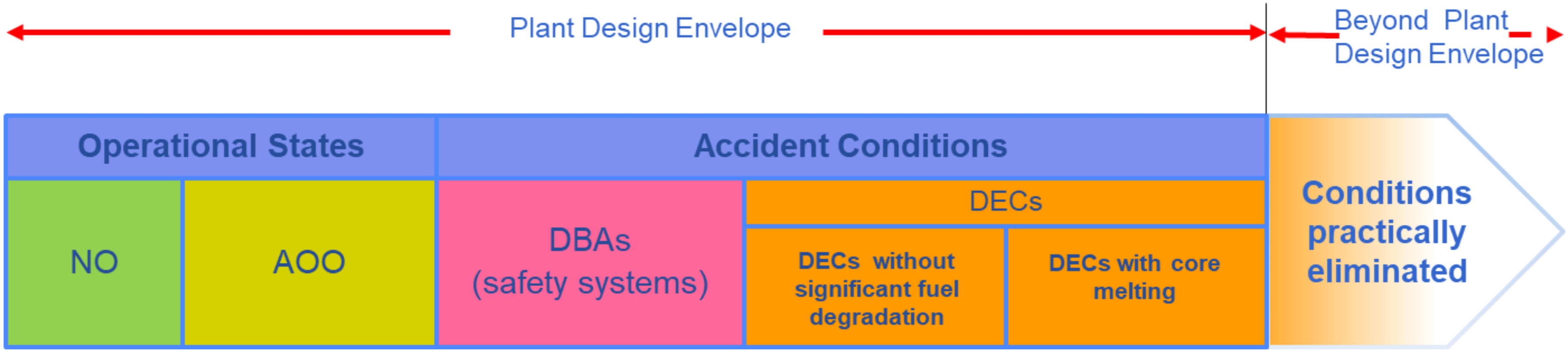
AOO

DBAs
(safety systems)

BDBA

Severe Accidents
(core melting)

SSR-2/1, 2012



Plant Design Envelope

Beyond Plant
Design Envelope

Operational States

Accident Conditions

NO

AOO

DBAs
(safety systems)

DECs

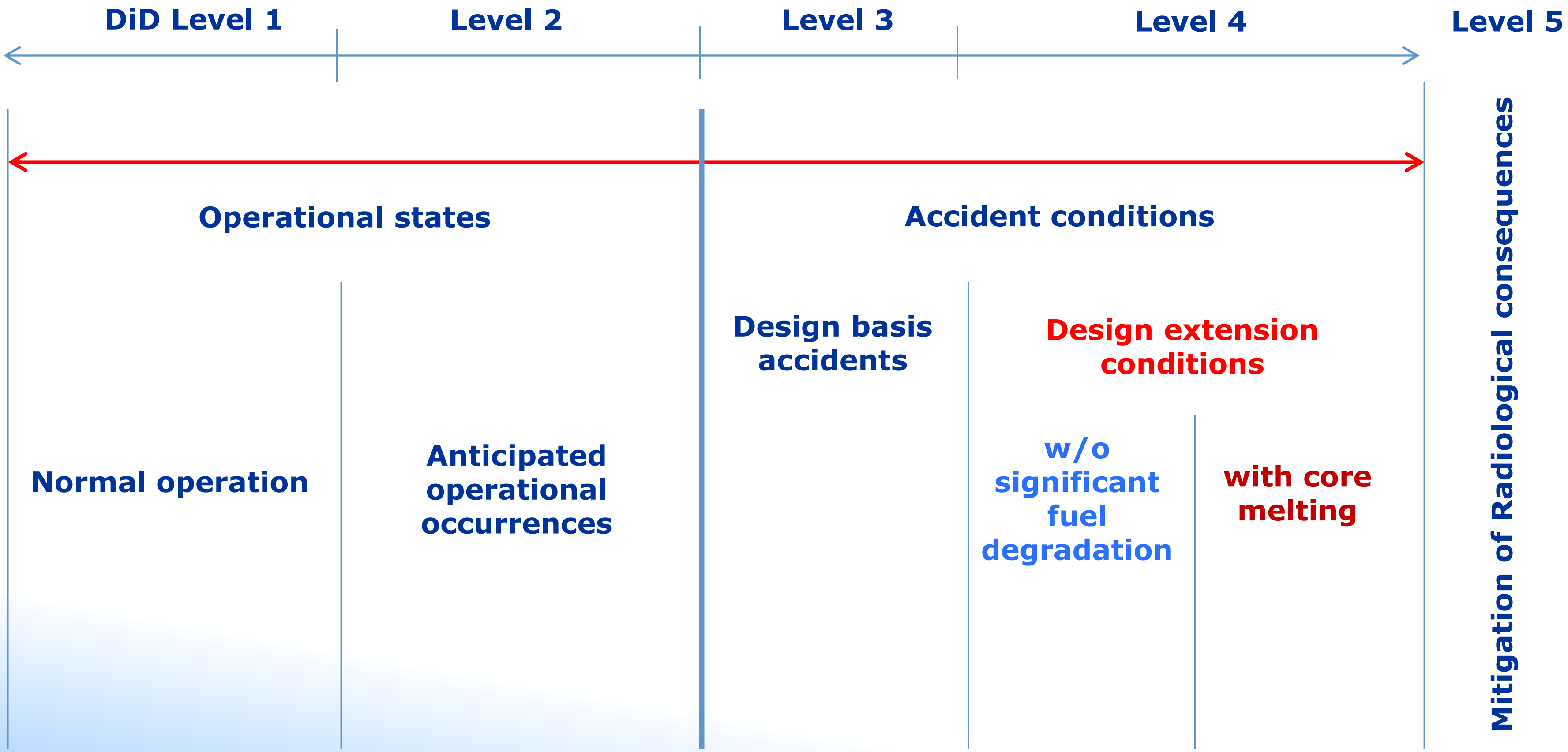
DECs without significant fuel degradation

DECs with core melting

Conditions practically eliminated

Plant states considered in the design (SSR 2/1, rev.1)

- Within the ‘design basis’
- In Design Extension Conditions (DEC)



DiD Level 1

Level 2

Level 3

Level 4

Level 5

Operational states

Accident conditions

Normal operation

Anticipated operational occurrences

Design basis accidents

Design extension conditions

w/o significant fuel degradation

with core melting

Mitigation of Radiological consequences

Design requirements for accident conditions (SSR 2/1, rev.1)

- Design basis accident (DBA)
  - A postulated accident for which a facility is designed
  - Established design criteria
  - Conservative safety assessment methodology
  - “Postulated’ internal and external events (natural and human induced)
  - Radiological criteria kept within established limits
- Design extension conditions (including SA)
  - Postulated accident conditions ‘beyond’ DBA
  - Considered in the design process of the facility
  - External events with low probability considered
  - Best estimate methodology used
  - Radiological criteria for off-site releases kept within acceptable limits

IAEA Safety Standards

for protecting people and the environment

Safety of
Nuclear Power Plants:
Design

Specific Safety Requirements

No. SSR-2/1 (Rev. 1)

IAEA

International Atomic Energy Agency

How we identify a set of DEC?

- Operating experience, particularly for LWR technology
- Deterministic evaluations (DSA)
- Probabilistic insights (PSA)
- Engineering judgement

Examples of DEC w/o significant fuel degradation identified deterministically

- Anticipated transient without scram (ATWS)
- Station blackout (SBO)
- Loss of core cooling in the residual heat removal mode
- Extended loss of cooling of fuel pool and inventory
- Loss of normal access to the ultimate heat sink

Examples of DEC w/o significant fuel degradation derived from PSA

- Total loss of feed water
- LOCA + loss of one emergency core cooling system (high pressure or the low pressure emergency cooling system)
- Loss of the component cooling water system or the essential service water system
- Uncontrolled boron dilution
- Multiple steam generator tube ruptures (for PWRs)
- Steam generator tube ruptures induced by main steam line break (for PWRs)
- Uncontrolled level drop during mid-loop operation (for PWRs) or during refueling

DEC with core melting (severe accident)

- A representative group of severe accident conditions to be used for defining the design basis of the mitigatory (safety) features

- Important
  - Sufficient knowledge on different severe accident phenomena

- Main objectives
  - Preventing the loss of containment integrity
  - Cooling and stabilization of the molten core
  - Preventing ex-vessel scenario
  - Keeping radiological criteria for off-site releases within acceptable limits

Design features for DEC (SSR 2/1, rev.1)

- Shall be identified and designed for preventing or mitigating events considered in DEC

- Shall have the following characteristics
  - Be independent, to the extent practicable, of those used in more frequent accidents (e.g. DBA)
  - Be capable of performing in the environmental conditions pertaining to these design extension conditions, including severe accidents
  - Have reliability commensurate with the function that they are required to fulfil

Conclusions

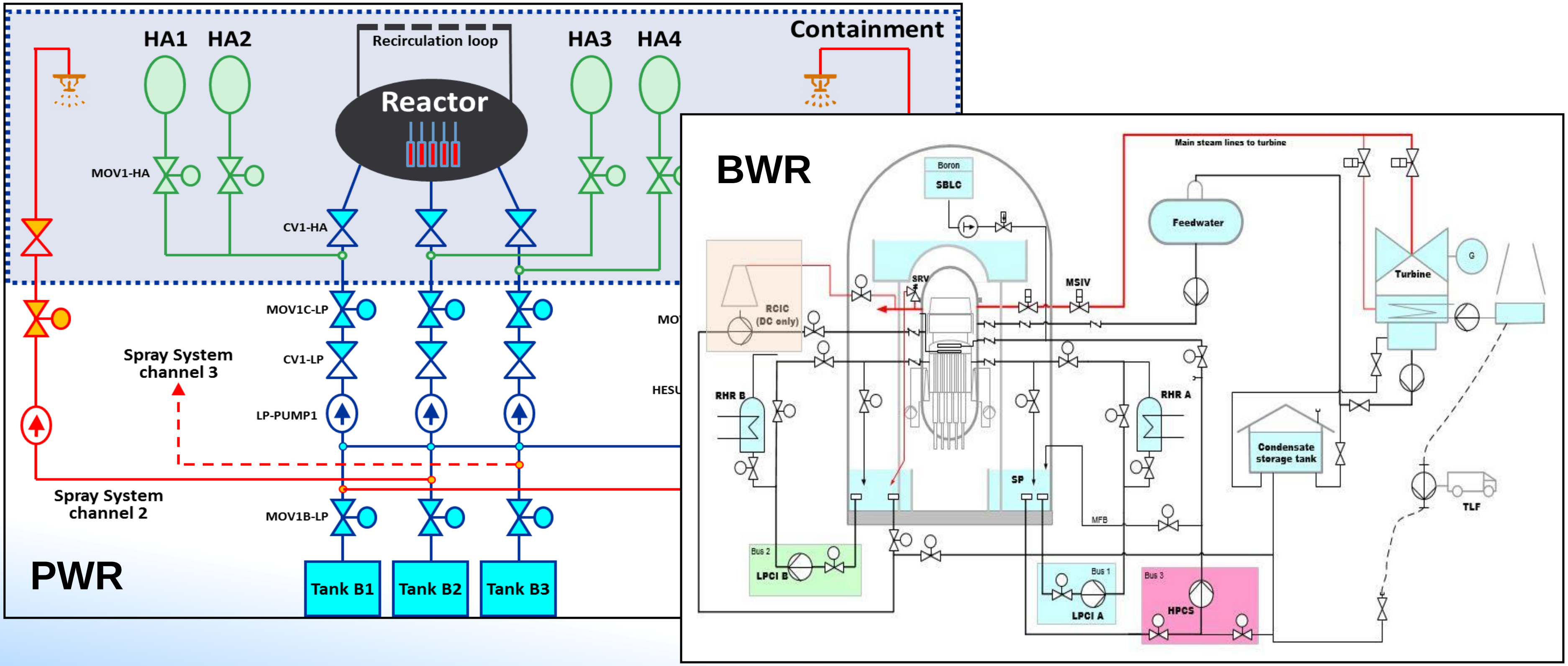
- We will never completely eliminate the possibility of a severe accident
- But we can make better provisions for protecting people and environment
  - More robust provisions to ensure core cooling (e.g. passive cooling, containment heat removal)
  - More robust methods for dealing with molten core (e.g. provisions for corium retention)
  - Severe accident management procedures, training, and equipment that can deal with the unexpected
    - Minimize reliance on active components in plant systems
    - Have default paths that can deal with missing information including no information
  - Alternative means for powering minimum set of devices needed to establish core cooling

PSA training

- Full scope PSA trainings (tailored for audience)
- Theory + Practical exercises
- Topical workshops on specific PSA areas:
  - PSA approaches and applications (newcomers)
  - L2 PSA, Shutdown PSA, Fire PSA, Seismic PSA, etc.
  - International, regional and national platforms

Education & Trainings

- Trainees act as PSA team: aim is to construct PSA model for simplified NPP (see below)
- Simplified NPP: different designs, major systems



*** Examples available for PWR and BWR, could be adjusted to the needs of MS**

IAEA
International Atomic Energy Agency

Thank you!