Nuclear Safety – Defence In Depth

Jerzy Grynblat
Nuclear Business Director

Lloyd's Register Consulting

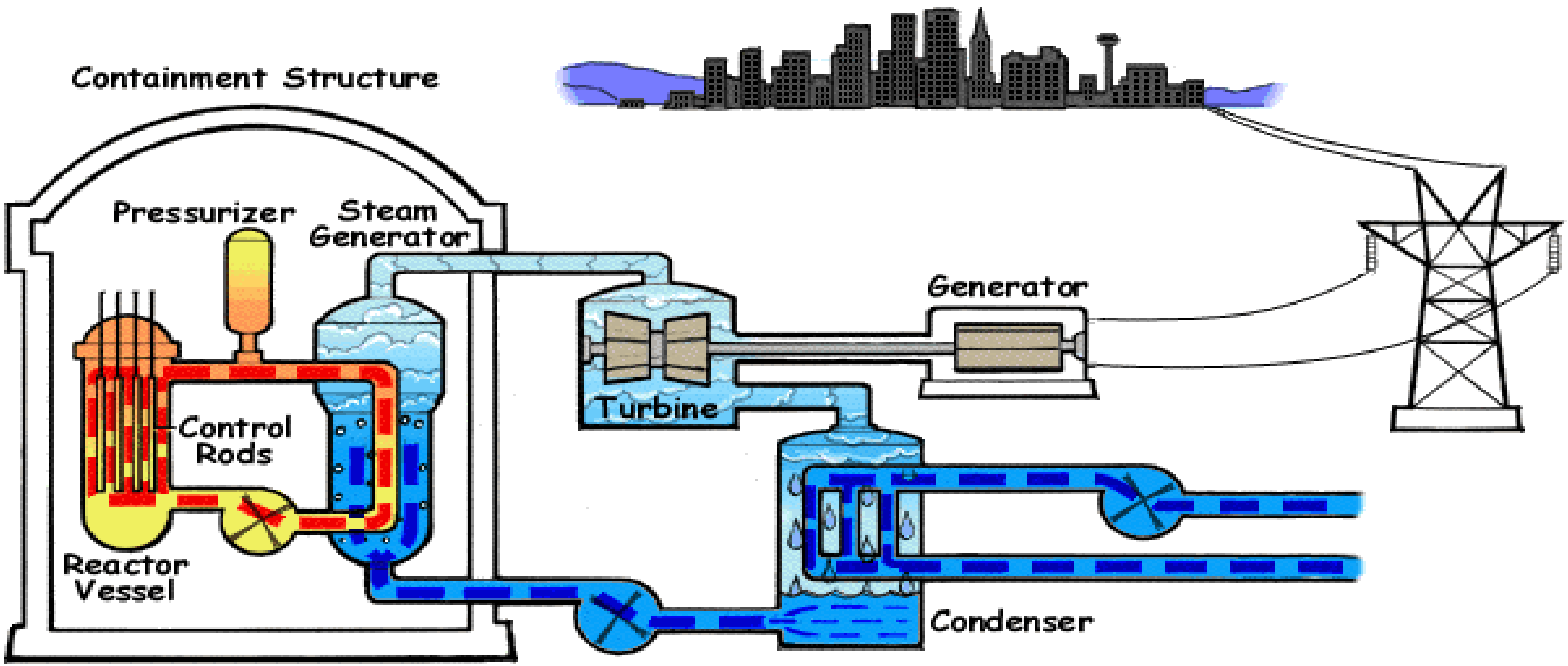
Working together
for a safer world

Content

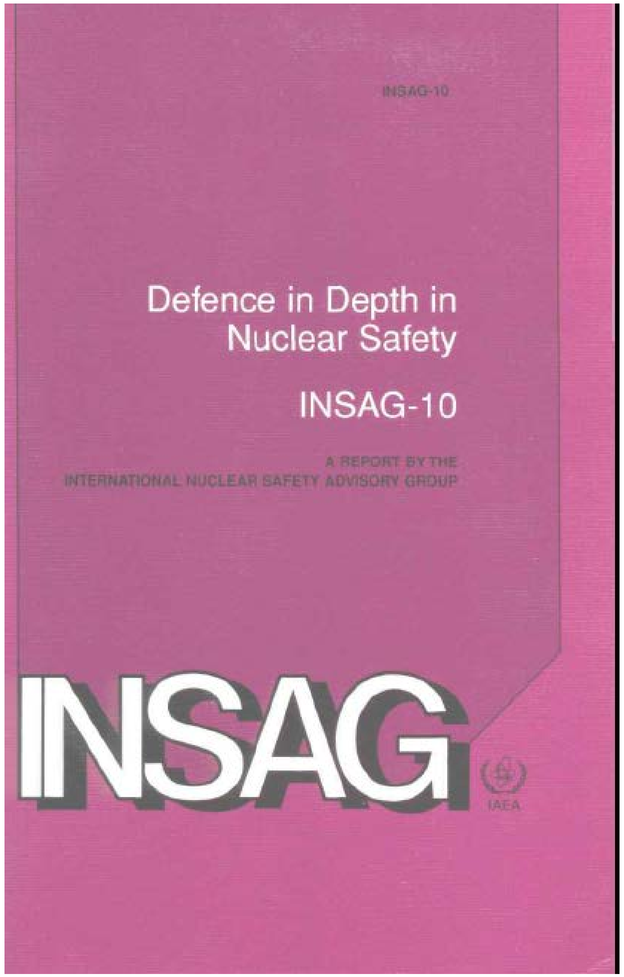
- Nuclear Power Plant technology
- Nuclear safety objectives and principles
- Defence In Depth
- Challenges that may influence the safety barriers – countermeasures
- Risk Informed Applications

Pressurized Water Reactor (PWR)

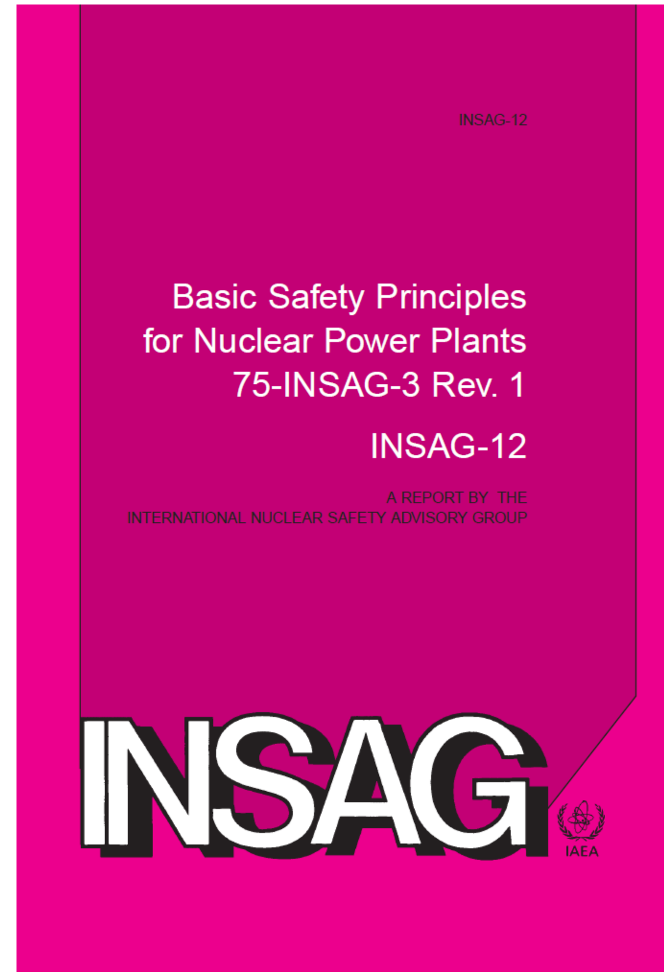
- Most common NPP type in the world
- Primary loop (radioactivity) and secondary loop (no radioactivity)



IAEA Safety Guides



http://www-pub.iaea.org/MTCD/publications/PDF/Pub1013e_web.pdf



http://www-pub.iaea.org/MTCD/publications/PDF/P082_scr.pdf

Nuclear safety objectives and principles

Objectives	General nuclear safety objective	Radiation protection objective	Technical safety objective					
Fundamental safety management principles	Safety culture	Responsibility of operating organization	Regulatory control and verification					
Fundamental defence in depth principles	Defence in depth	Accident prevention	Accident mitigation					
General technical principles	Proven engineering practices (3.3.1)	Quality assurance (3.3.2) Self-assessment (3.3.3) Peer reviews (3.3.4)	Human factors (3.3.5)	Safety assessment and verification (3.3.6)	Radiation protection (3.3.7)	Operating experience and safety research (3.3.8)	Operational excellence (3.3.9)	
Specific principles	Siting	Design	Manufacturing and construction	Commissioning	Operation	Accident management	Decommis-sioning	Emergency preparedness

FIG. 1. INSAG safety objectives and principles for nuclear plants. The numbers refer to the relevant subsections in Section 3.3.

IAEA INSAG 12

Defence In Depth (DiD) - Overview

Strategy	Accident prevention			Accident mitigation	
Operational state of the plant	Normal operation	Anticipated operational occurrences	Design basis and complex operating states	Severe accidents beyond the design basis	Post-severe accident situation
Level of defence in depth	Level 1	Level 2	Level 3	Level 4	Level 5
Objective	Prevention of abnormal operation and failure	Control of abnormal operation and detection of failures	Control of accidents below the severity level postulated in the design basis	Control of severe plant conditions, including prevention of accident progression, and mitigation of the consequences of severe accidents, including confinement protection	Mitigation of radiological consequences of significant releases of radioactive materials
Essential features	Conservative design and quality in construction and operation	Control, limiting and protection systems and other surveillance features	Engineered safety features and accident procedures	Complementary measures and accident management, including confinement prodection	Off-site emergency response
Control	Normal operating activities		Control of accidents in design basis	Accident management	
Procedures	Normal operating procedures		Emergency operating procedures	Ultimate part of emergency operating procedures	
Response	Normal operating systems		Engineered safety features	Special design features	Off-site emergency preparations
Condition of barriers	Area of specified acceptable fuel design limit		Fuel failure; Severe fuel damage	Fuel melt; Uncontrolled fuel melt	Loss of confinement
Colour code	NORMAL		POSTULATED ACCIDENTS		EMERGENCY

IAEA INSAG 12

Defenece In Depth – Physical Barries

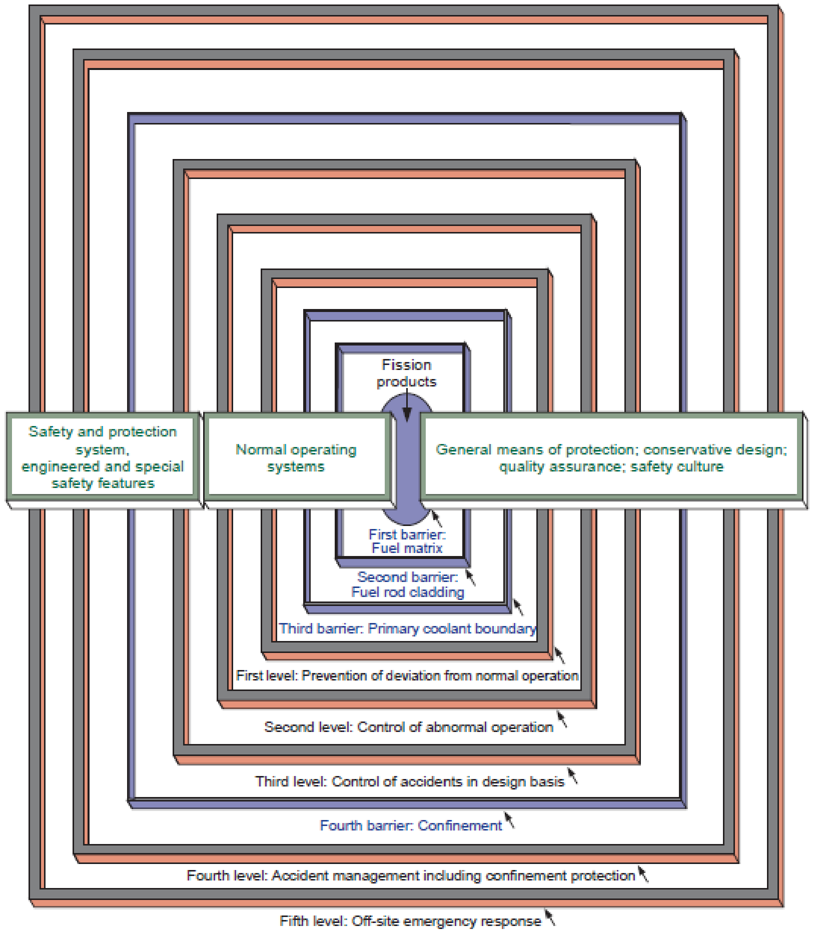
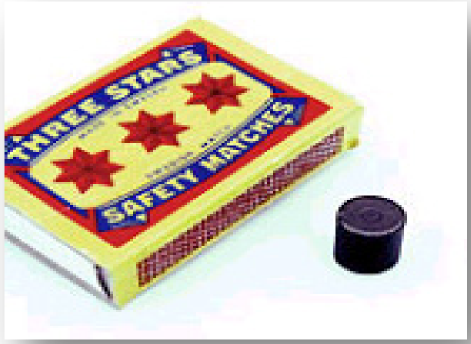


FIG. 4. The relation between physical barriers and levels of protection in defence in depth.

IAEA INSAG 12

Nuclear fuel

- One fuel pellet - 800 liters of diesel fuel
- One reactor core ~ 15 million fuel pellets piled in long pipes assembled to fuel elements
- Burnout
  - Energy content decreases during operation
  - Fuel elements are in operation for about 5 years
    - PWR – change of 25% every year
    - BWR – change of ~17% every year
  - Fuel elements are rearranged during refuelling to optimise the core layout (safety and fuel efficiency)



Defence in Depth

- Applied to all safety activities, whether organizational, behavioural or design related, ensures that they are subject to overlapping provisions, so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures.

DiD 5 levels

- The aim of the **first level** of defence is to prevent deviations from normal operation, and to prevent system failures. This leads to the requirement that the plant be soundly and conservatively designed, constructed, maintained and operated in accordance with appropriate quality levels and engineering practices, such as the application of redundancy, independence and diversity.

- The aim of the **second level** of defence is to detect and intercept deviations from normal operational states in order to prevent anticipated operational occurrences from escalating to accident conditions. This is in recognition of the fact that some PIEs are likely to occur over the service lifetime of a nuclear power plant, despite the care taken to prevent them.

DiD 5 levels

- For the **third level** of defence, it is assumed that, although very unlikely, escalation of certain anticipated operational occurrences or PIEs may not be controlled by a preceding level of defence, and a more serious event may develop. These unlikely events are anticipated in the design basis for the plant, and inherent safety features, fail-safe designs, and additional equipment and procedures are provided to control their consequences and to achieve stable and acceptable conditions following such events.

DiD 5 levels

- The aim of the **fourth level** of defence is to address severe accidents in which the design basis may be exceeded and to ensure that radioactive releases are kept as low as practicable. The most important objective of this level is the protection of the confinement function.

- The **fifth and final level** of defence is aimed at mitigation of the radiological consequences of potential releases of radioactive materials that may result from accident conditions. This requires the provision of an adequately equipped emergency control centre, and plans for the on-site and off-site emergency response.

Safety Principles

Diversity: Systems that employ different principles of operation.

Redundancy: Multiple components and systems to guard against individual failure.

Independence: System and components are not interdependent and are physically separated.

Failsafe: Failure results in the component adopting a safe mode.

Testable: Can be tested without disrupting operations or with redundancy so that one system can be withdrawn for testing.

Challenges that may influence the safety barriers - Countermeasures

Decline in Safety culture

- It is not what we write and/or say, it is the matter of what and how we do things
- Independent Safety Review
- ALARA / ALARP-principles
  - ALARA = As Low As Reasonably Achievable
  - ALARP = As Low As Reasonably Practicable

Inproper status monitoring of the safety systems and components

- Maintenance
- Status control and verification
- Risk Monitoring

Limited resources, optimisation/prioritization

- Risk Inform (RI) Decision Making, RI Applications

Initiating events influencing several barriers simultaneously

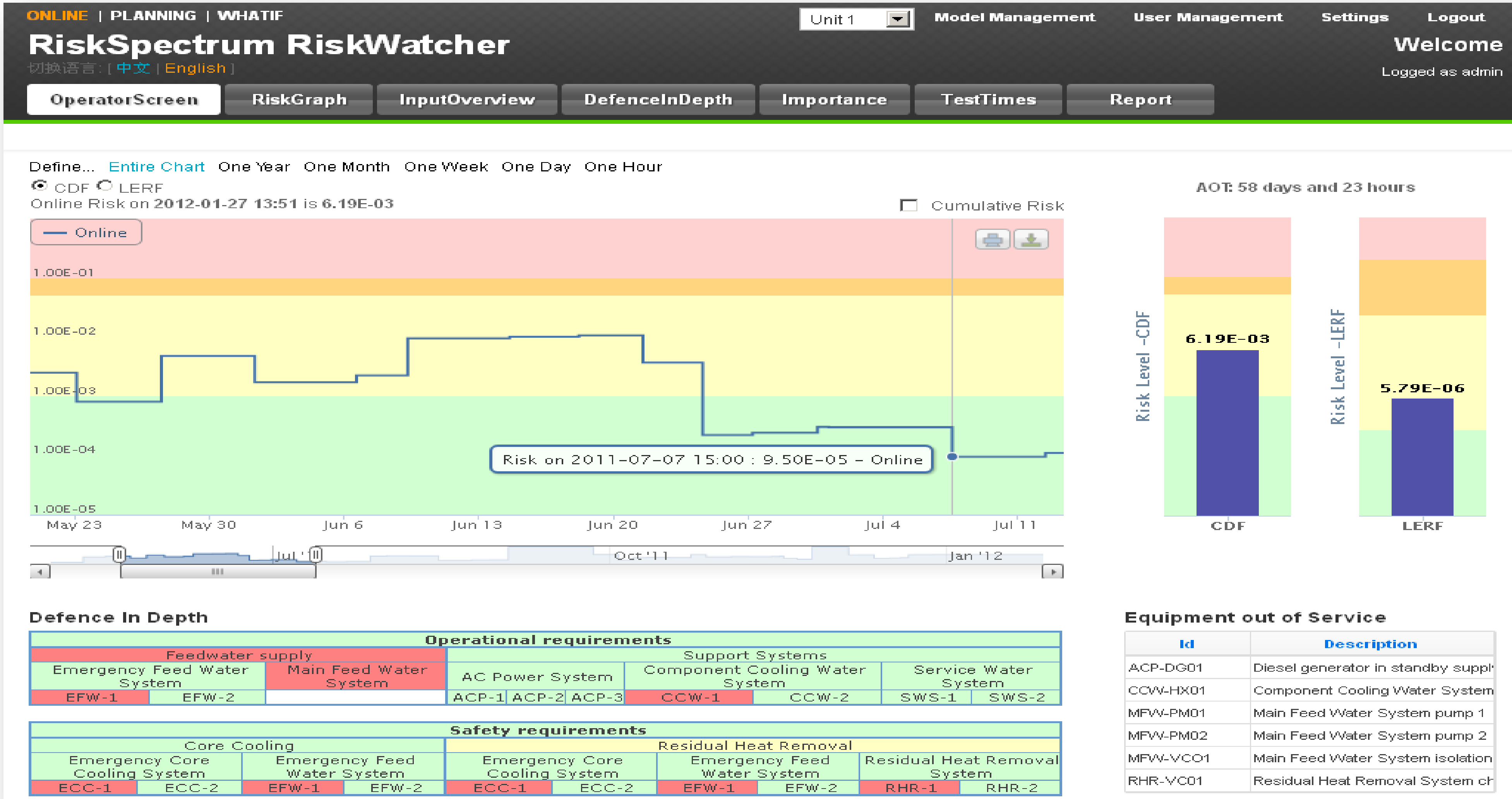
- Safety analysis, deteministic and probabilistic
- Physical independence, diversity
- Comprehensive safety analysis

Challenges that may influence the safety barriers - Countermeasures

Risk Informed applications

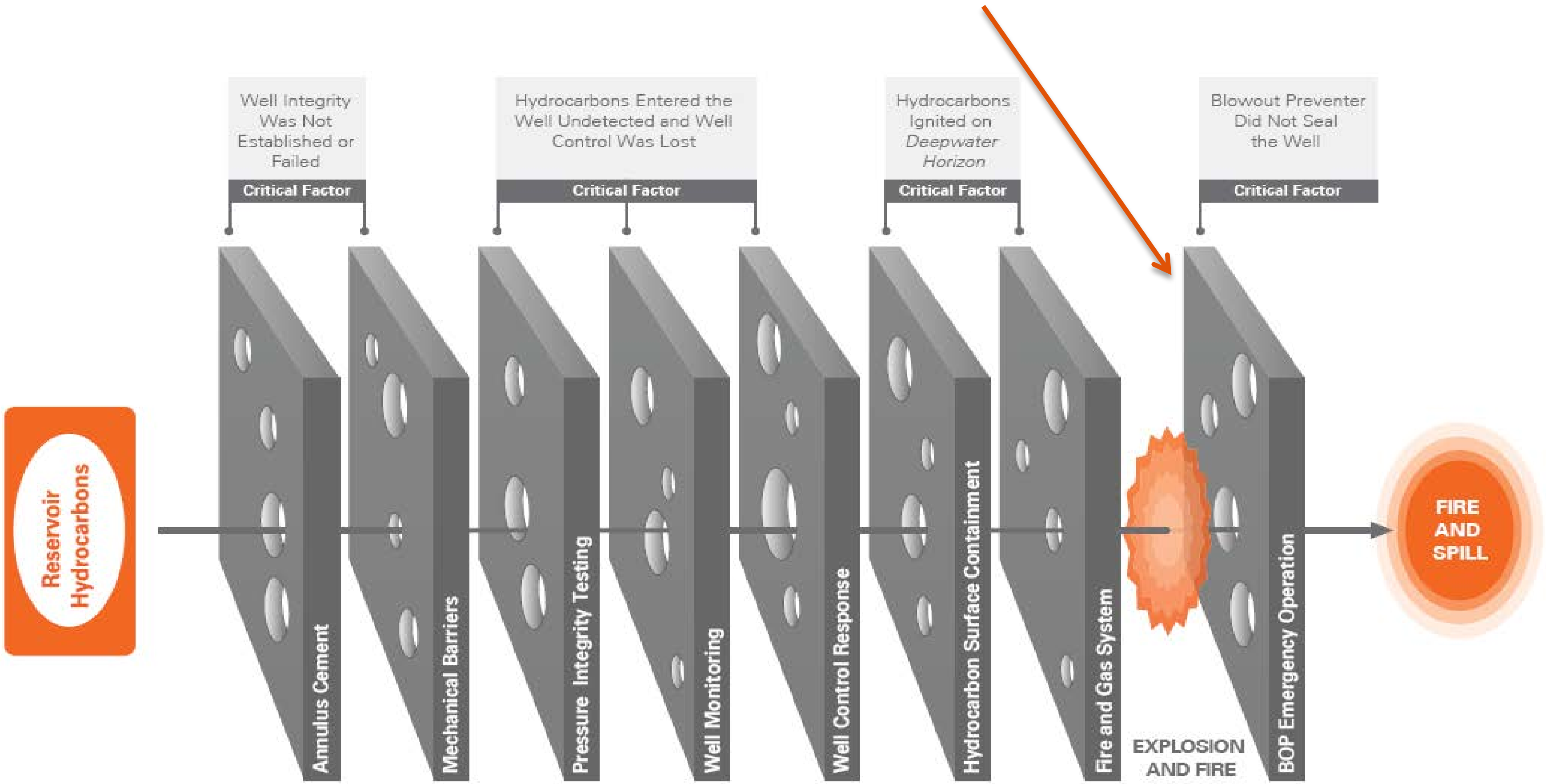
- Risk Monitor for on-line risk monitoring
- Risk Monitor for maintenance risk evaluation
- Mitigation Systems Performance Indicators (MSPI) for safety supervision
- MSPI for plant internal use (to improve safety and reliability)

RiskSpectrum RiskWatcher

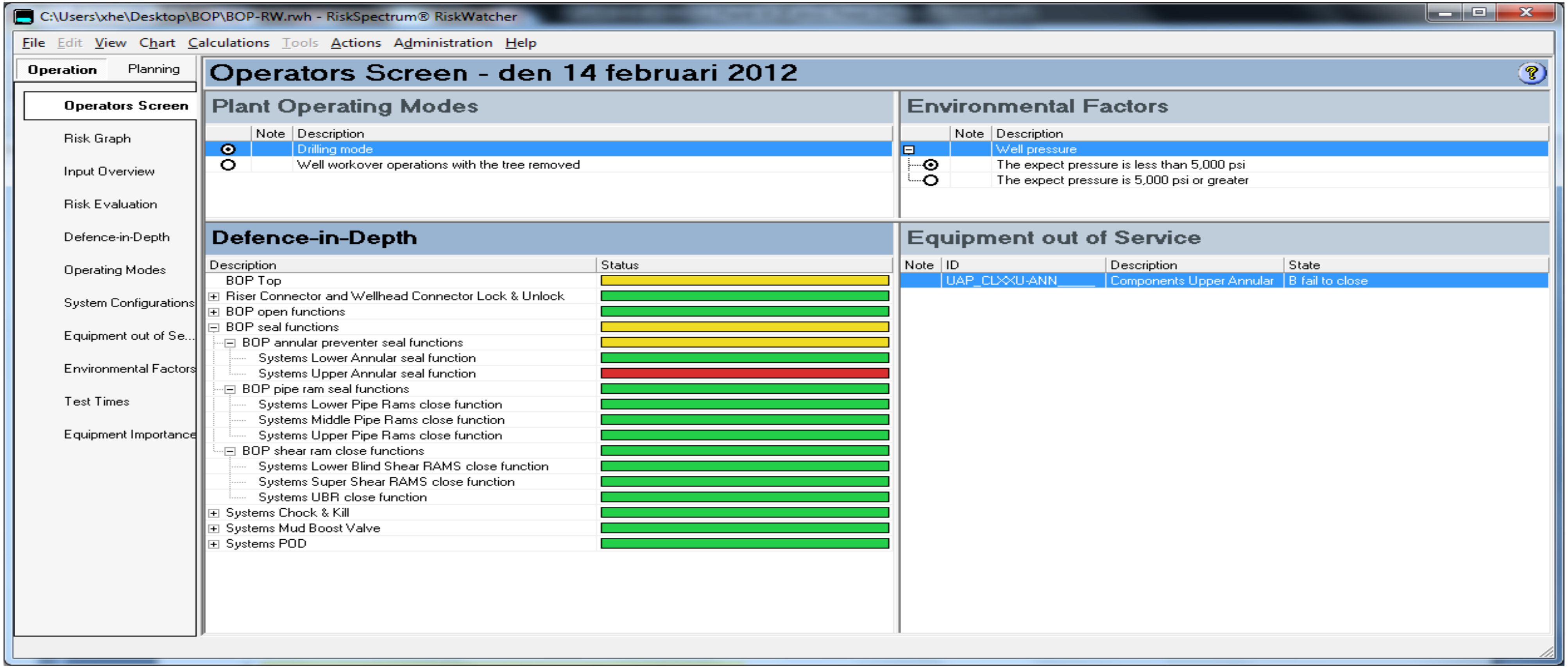


RM application in O & G

The blowout preventer (BOP) is often the final line of defence to isolate the wellbore prior to and after the explosions and the fire.



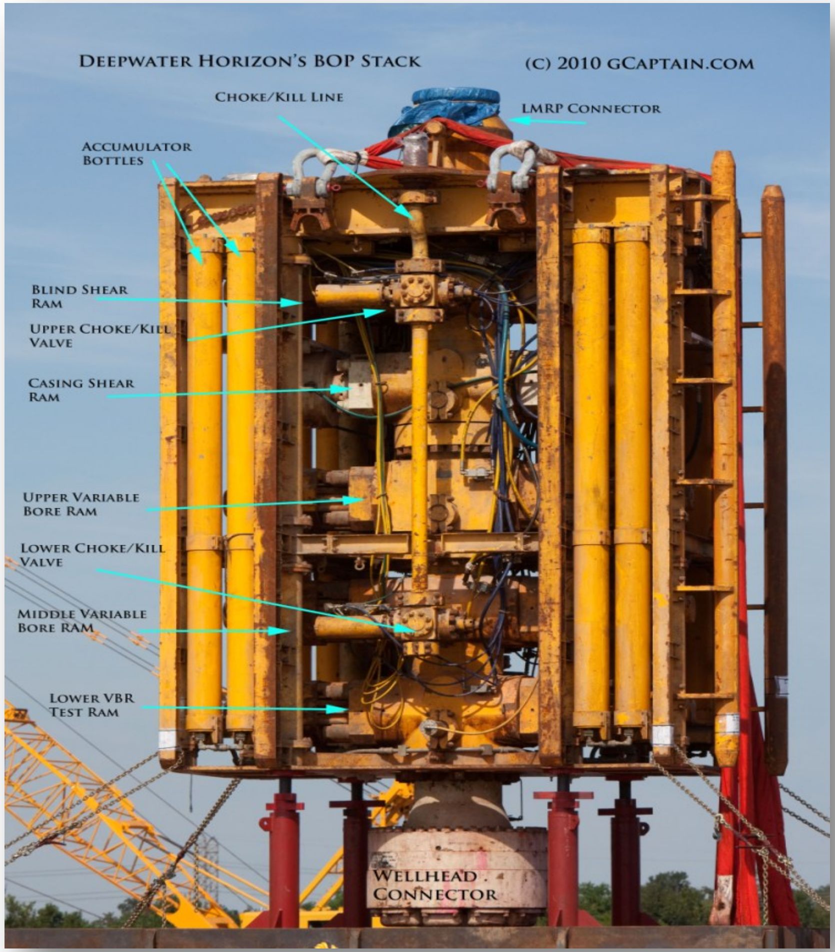
RiskWatcher for BOP, example interface



Here the upper annular preventer is totally out of service (red), the lower annular preventer is working (green), and we see that the defence in depth level has changed for the BOP annular preventer function (yellow).

BOP Risk Model software (RiskWatcher)

http://www.youtube.com/watch?v=UkLa1x6amHQ



BOP Risk Model - Solutions

- Gives a clear understand of the seriousness of the issue within minutes;
- Each model is:
  - Custom built to the specific BOP;
  - Custom built to specific country waters;
  - Custom built to company rules, regulations and operational procedures;
  - Utilises proven software for risk analysis.
- Risk assessment is fast, logical and based on sound engineering principles;
- It gives consistent, objective decisions 100% of the time;
- Historical data is collected;
- Winner of EIC Award for Supply Chain Excellence, 2013;
- Engineering Innovations – Meritorious Award, 2014.

Jerzy Grynblat
Nuclear Business Director
Lloyd's Register Consulting
T +46 70 773 06 33 E jerzy.grynblat@lr.org

Lloyd's Register Consulting
www.lr.org/consulting

Lloyd's Register
Consulting

Working together
for a safer world