The Abdus Salam
International Centre for Theoretical Physics

United Nations
Educational, Scientific and
Cultural Organization

IAEA
International Atomic Energy Agency

2291-21

Joint ICTP-IAEA Course on Science and Technology of Supercritical Water Cooled Reactors

27 June - 1 July, 2011

INTRODUCTION TO SAFETY AND SCWR

David NOVOG

McMaster University Faculty of Engineering
Department of Engineering Physics, 1280 Main Street West
John Hodgins Engineering Building
Hamilton L8S4L7 Ontario
CANADA

Introduction to Safety and SCWR (SC20)

Prepared by Prof. David Novog (Ph.D., P.Eng.)

Director – McMaster Institute for Energy Studies

McMaster University (Canada)

Module Objective

- ***SCWR designs are either in the conceptual or pre-conceptual design stages.***
  - During the design stages we have the greatest (and most cost effective) opportunity to improve the safety of the design.
  - On the other hand we may have reduced levels of specific information on equipment, materials and components.
- The objectives of this module are to:
  - Provide a working level interpretation of nuclear safety by reviewing basic concepts (e.g., IAEA-SF, INSAG, etc..).
  - Define the components which lead to safe design, operation, and decommissioning.
  - Outline the methodologies used to assess “safety” in SCWR
  - Discuss the general approach to assessing nuclear safety for SCWR designs

GEN-IV

- From the outset, GEN-IV concepts were assessed based on enhanced safety, economics, proliferation resistance and fuel cycle capabilities.
- Each technology must demonstrate a significant improvement in safety performance relative to existing designs.
  - What does this mean?
  - How do we evaluate it for SCWR?
  - What is the requirement?

Energy Utilization and Conversion

- Energy, by its very nature, is dangerous as it represents the ability to “do work”.
  - Work can be positive?
  - Uncontrolled it can cause an accident.
- In the history of energy utilization there have been a large number of accidents.
- Many more military (weapons) and naval (subs and ship) accidents.

Energy Related Accidents Since 1986

Piper Alpha, North Sea	1988	167	explosion of offshore oil platform
Asha-ufa, Siberia	1989	600	LPG pipeline leak and fire
Dobrnja, Yugoslavia	1990	178	coal mine
Hongton, Shanxi, China	1991	147	coal mine
Belci, Romania	1991	116	hydro-electric dam failure
Kozlu, Turkey	1992	272	coal mine methane explosion
Cuenca, Equador	1993	200	coal mine
Durunkha, Egypt	1994	580	fuel depot hit by lightning
Seoul, S.Korea	1994	500	oil fire
Minanao, Philippines	1994	90	coal mine
Dhanbad, India	1995	70	coal mine
Taegu, S.Korea	1995	100	oil & gas explosion
Spitsbergen, Russia	1996	141	coal mine
Henan, China	1996	84	coal mine methane explosion
Datong, China	1996	114	coal mine methane explosion
Henan, China	1997	89	coal mine methane explosion
Fushun, China	1997	68	coal mine methane explosion
Kuzbass, Russia/Siberia	1997	67	coal mine methane explosion
Huainan, China	1997	89	coal mine methane explosion
Huainan, China	1997	45	coal mine methane explosion
Guizhou, China	1997	43	coal mine methane explosion
Donbass, Ukraine	1998	63	coal mine methane explosion
Liaoning, China	1998	71	coal mine methane explosion
Warri, Nigeria	1998	500+	oil pipeline leak and fire
Donbass, Ukraine	1999	50+	coal mine methane explosion
Donbass, Ukraine	2000	80	coal mine methane explosion
Shanxi, China	2000	40	coal mine methane explosion
Muchonggou, Guizhou, China	2000	162	coal mine methane explosion
Zasyadko, Donetsk, E.Ukraine	2001	55	coal mine methane explosion
Jixi, China	2002	115	coal mine methane explosion
Gaoqiao, SW China	2003	234	gas well blowout with H2S
Kuzbass, Russia	2004	47	coal mine methane explosion
Donbass, Ukraine	2004	36	coal mine methane explosion
Henan, China	2004	148	coal mine methane explosion
Chenjiashan, Shaanxi, China	2004	166	coal mine methane explosion
Sunjiawan, Liaoning, China	2005	215	coal mine methane explosion
Shenlong/ Fukang, Xinjiang, China	2005	83	coal mine methane explosion
Xingning, Guangdong, China	2005	123	coal mine flooding
Dongfeng, Heilongjiang, China	2005	171	coal mine methane explosion

Source: WNA, June 2008.

Nuclear Energy

- "*The energy contained within a nuclear reactor core is equivalent to 10000 747's flying at maximum altitude and speed.*"

  WANO (World Association of Nuclear Operators)

  – WANO was establish post Chernobyl to ensure sharing of operating experience (OPEX) and in realization that an accident at one station affects all operators.

Nuclear Accidents

- A majority of accidents have occurred:
  - In military installations
  - Experimental and research reactors performing non-standard operations.
- 3 major accidents involving nuclear power facilities where the cores were significantly damaged.
  - TMI 2
  - Chernobyl
  - Fukushima Daiichi
- Several “’near-misses”:
  - Browns Ferry
  - Davis-Besse
  - France A2

Nuclear Related Accidents

Reactor	Date	Immediate Deaths	Environmental effect	Follow-up action
NRX, Canada (experimental, 40 MWt)	1952	Nil	Nil	Repaired (new core) closed 1992
Windscale-1, UK (military plutonium-producing pile)	1957	Nil	Widespread contamination. Farms affected (c 1.5 x 10^{15} Bq released)	Entombed (filled with concrete) Being demolished.
SL-1, USA (experimental, military, 3 MWt)	1961	Three operators	Very minor radioactive release	Decommissioned
Fermi-1 USA (experimental breeder, 66 MWe)	1966	Nil	Nil	Repaired and restarted, then closed in 1972
Lucens, Switzerland (experimental, 7.5 MWe)	1969	Nil	Very minor radioactive release	Decommissioned
Browns Ferry, USA (commercial, 2 x 1080 MWe)	1975	Nil	Nil	Repaired
Three-Mile Island-2, USA (commercial, 880 MWe)	1979	Nil	Minor short-term radiation dose (within ICRP limits) to public, delayed release of 2 x 10^{14} Bq of Kr-85	Clean-up program complete, in monitored storage stage of decommissioning
Saint Laurent-A2, France (commercial, 450 MWe)	1980	Nil	Minor radiation release (8 x 10^{10} Bq)	Repaired, (Decomm. 1992)
Chernobyl-4, Ukraine (commercial, 950 MWe)	1986	47 staff and firefighters (32 immediate)	Major radiation release across E. Europe and Scandinavia (11 x 10^{18} Bq)	Entombed
Fukushima Diichi	2011			Ongoing

(The well publicised accident at Tokai-mura, Japan, in 1999 was at a fuel preparation plant for experimental reactors, and killed two people from radiation exposure. Many other such criticality accidents have occurred, some fatal, and practically all in military facilities prior to 1980.) Source: WNA, June 2008

Module Approach

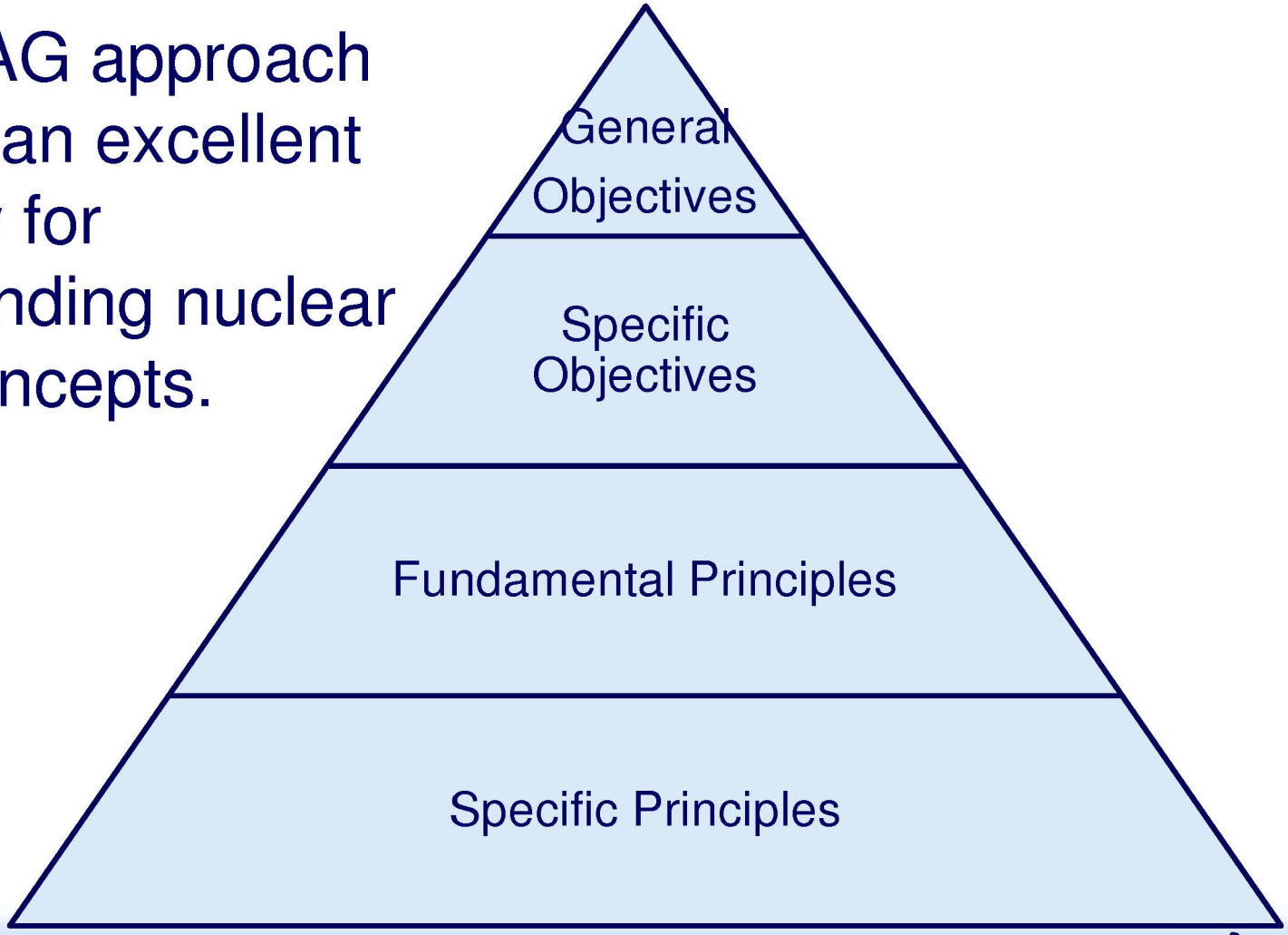
- Most nations have specific regulatory requirements for nuclear power reactor safety and licensing.
- The IAEA document IAEA-SF-1:
  - The IAEA's Statute authorizes the Agency to establish standards of safety to protect health and minimize danger to life and property
  - their application in achieving in the Member States a high level of protection for people and the environment worldwide.
  - Used here to establish the overall general requirements for the SCWR concept
- INSAG documents
  - Guidance and recommendations on approach and principles
  - Used as a structure in this module to organize the concepts.

IAEA SF-1

- **The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation.**
  - To control the radiation exposure of people and the release of radioactive material to the environment;
    - ALARA and “reasonable” economics come into play
  - To restrict the likelihood of events that might lead to a loss of control;
  - To mitigate the consequences of such events if they were to occur.

International Nuclear Safety Group INSAG - Recomendations

- The INSAG approach provides an excellent hierarchy for understanding nuclear safety concepts.

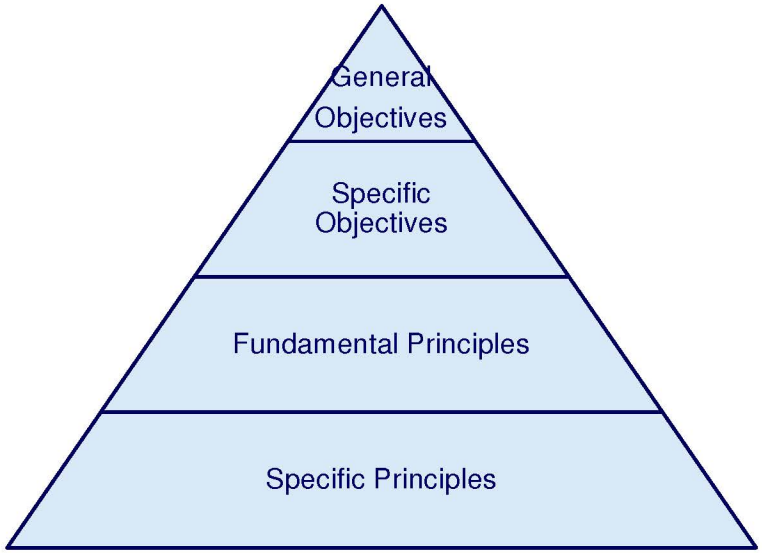


What is “Nuclear Safety”?

- *Nuclear power plant safety requires a continuing quest for excellence. All individuals concerned need constantly to be alert to opportunities to reduce risks to the lowest practicable level…. INSAG-12*
- ***GENERAL NUCLEAR SAFETY OBJECTIVE → To protect individuals, society and the environment by establishing and maintaining an effective defence against radiological hazard.***
    - *radiological hazard means adverse health effects of radiation on both plant workers and the public, and radioactive contamination of land, air, water or food products.*
    - *Consistent in principle with IAEA-SF-1*

Specific Objectives

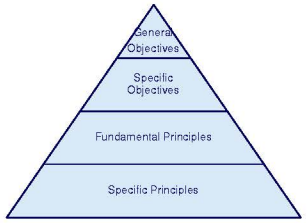
- Specific Objectives
  - Radiation Protection
    - ICRP
    - Acceptance Criteria
  - Technical Safety
    - Control, Cool and Contain
    - Prevent, Manage and Mitigate
    - Safety Goals



How do we achieve nuclear safety?

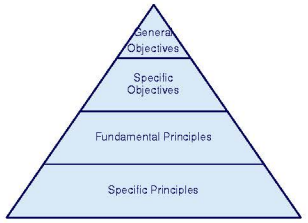
- The 3-C's of nuclear safety
  - **CONTROL** the reactions
  - **COOL** the fuel
    - Implies a reliable heat sink is in place at all times
  - **CONFINE** the radioactivity
    - Typical physical barriers to fission products
      - Fuel matrix
      - Fuel Sheath
      - HTS boundary
      - Containment
      - Exclusion zone

Specific Nuclear Safety Objectives 1



- **RADIATION PROTECTION OBJECTIVE**
  - *in normal operation radiation exposure within the plant and due to any release of radioactive material from the plant is as low as reasonably achievable and below prescribed limits,*
  - *to ensure mitigation of the extent of radiation exposure due to accidents.*
- *Prescribed limits usually based on recommendations from International Commission on Radiological Protection (ICRP).*
  - doses sufficiently low that deterministic effects are precluded and the probability of stochastic effects is limited to levels deemed tolerable

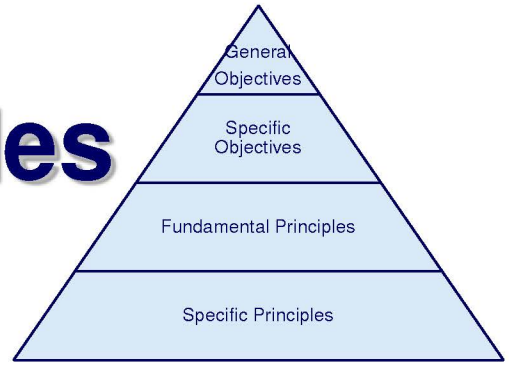
Specific Nuclear Safety Objectives 2



- **TECHNICAL SAFETY OBJECTIVE**
  - To prevent with high confidence accidents in nuclear plants
  - Radiological consequences would be minor for accidents
  - To ensure that the likelihood of severe accidents with serious radiological consequences is extremely small.
  - *The technical safety objective for accidents is to apply accident* ***prevention, management and mitigation***
    - *that overall risk is very low and*
    - *no accident sequence, whether it is of low probability or high probability, contributes to risk in a way that is excessive in comparison with other sequences.*

THIS IS THE MAIN OBJECTIVE OF THIS MODULE.

Fundamental Principles



- **Management Responsibilities**
  - Safety culture
  - Responsible operator
  - Regulation and Verification
- **Defence in Depth**
  - DinD in design and operation
  - Accident Prevention
  - Accident Mitigation
- **General Technical**
  - Proven engineering and OPEX
  - QA and EQ
  - Peer review and human factors
  - *Safety assessments and radiation protection*

Defense in Depth

To compensate for potential human and mechanical failures, a defence in depth concept is implemented, centred on several levels of protection including successive barriers preventing the release of radioactive material to the environment.

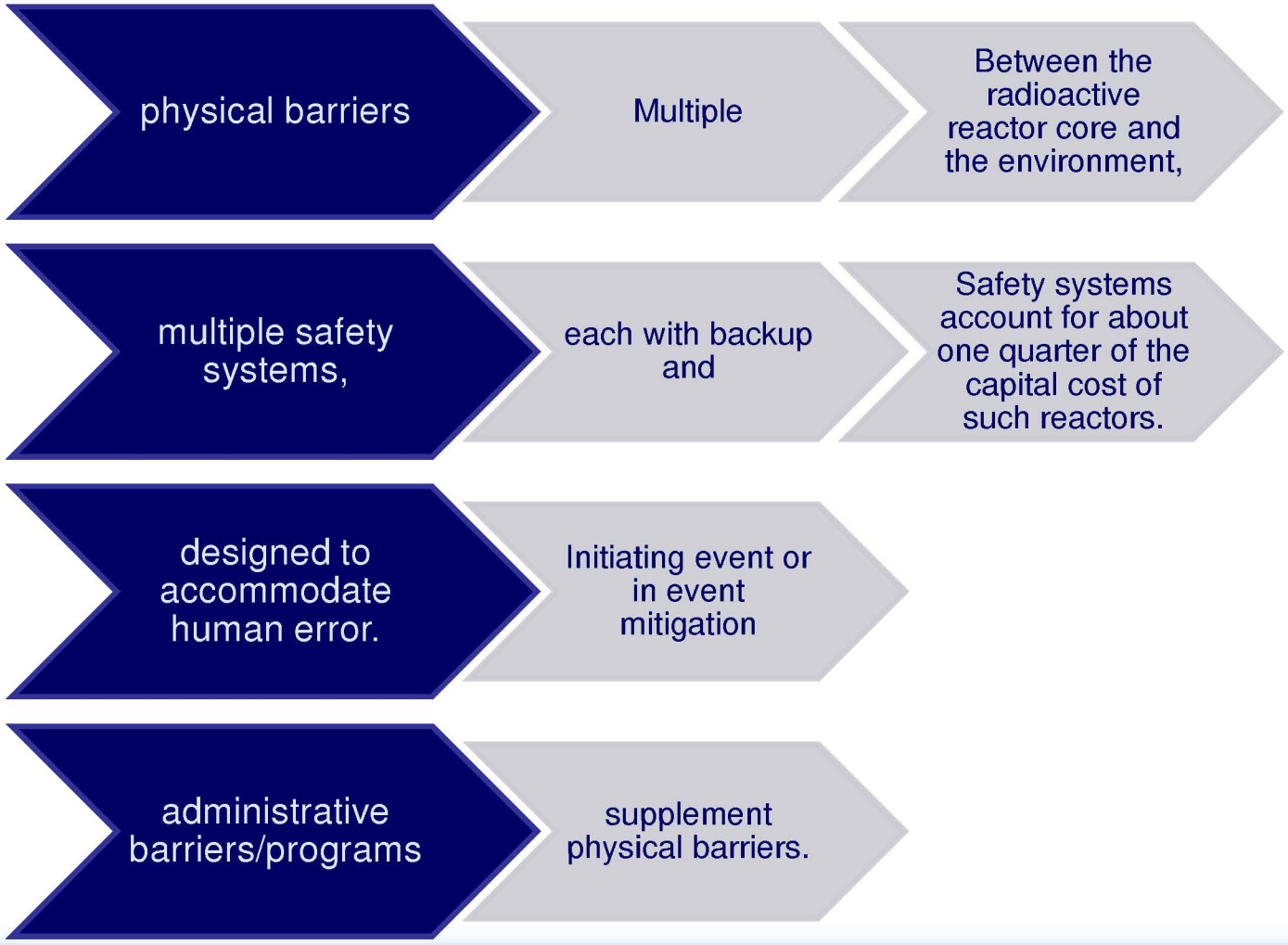
- *The concept includes protection of the barriers by averting damage to the plant and to the barriers themselves.*
- *It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective.*

- Defence in depth helps to ensure that the three basic safety functions (controlling the power, cooling the fuel and confining the radioactive material)

Defence-in-Depth

- "**defence-in-depth**" → multiple "barriers" (physical and administrative) with safety systems supplementing the natural features of the reactor core.
  - Assume that no single feature, equipment or person need act to prevent an accident (implies the single-failure criterion)
  - Natural features include things like feedback effects

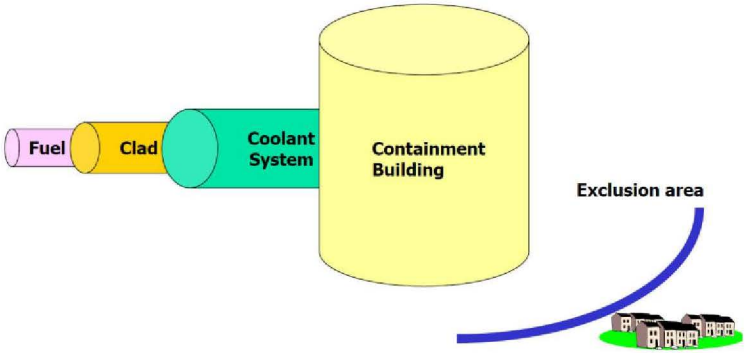
Defence-in-Depth



Physical Barriers

- Eg. NUREG 6402

Barrier or Layer	Function
1. Ceramic fuel pellets	Only a fraction of the gaseous and volatile fission products is released from the pellets.
2. Metal cladding	The cladding tubes contain the fission products released from the pellets. During the life of the fuel, less than 0.5 percent of the tubes may develop pinhole sized leaks through which some fission products escape.
3. Reactor vessel and piping	The 8- to 10-inch (20- to 25-cm) thick steel vessel and 3- to 4-inch (7.6- to 10.2-cm) thick steel piping contain the reactor cooling water. A portion of the circulating water is continuously passed through filters to keep the radioactivity low.
4. Containment	The nuclear steam supply system is enclosed in a containment building strong enough to withstand the rupture of any pipe in the reactor coolant system.
5. Exclusion area	A designated area around each plant separates the plant from the public. Entrance is restricted.
6. Low population zone, evacuation plan	Residents in the low population zone are protected by emergency evacuation plans.
7. Population center distance	Plants are located at a distance from population centers.



Defence in Depth Levels

Levels	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

- Taken from INSAG-10

DinD - Prevention and Mitigation

physical protection	provides protection against intentional acts
maintaining stable operation	provides measures to reduce the likelihood of challenges to safety systems;
protective systems	provides highly reliable equipment to respond to challenges to safety;
maintaining barrier integrity	provides isolation features to prevent the release of radioactive material into the environment
protective actions and procedural barriers	provides planned activities to mitigate any impacts due to failure of the other strategies.

INSAG-12 Hierarchy

IAEA-NS-R-1

- Determine Postulated Initiating Events (PIE)
- Systematically identify Structures, Systems, and Components (SSCs) important to safety.

  (1) the safety function(s) to be performed by the item;

  (2) the consequences of failure to perform its function;

  (3) the probability that the item will be called upon to perform a safety function;

  (4) the time following a PIE at which, or the period throughout which, it will be called upon to operate.
- The design basis shall specify the necessary capabilities of the plant to cope with a specified range of operational states and design basis accidents within the defined radiological protection requirements.
  - Deterministic Analysis
  - PRA

The Safety Case

Normal Operation	• Environmental impact • Worker dose • Chronic releases
Abnormal Operating Occurrences	• Control system corrections • Prevention → high reliable process and control systems (DCS)
Design Basis Accidents	• Prevention → process and systems important to safety • Mitigation → SDS & RHR • Prevent fuel and plant damage
Beyond Design basis Accidents	• (IAEA-SF-1) The performance of the plant in specified accidents beyond the design basis, including selected severe accidents, shall also be addressed in the design (post Fukushima this will be a focus area).

Initiating Events

- Probable Initiating Events (PIE) – IAEA-NS-R-1
  - Internal Events
    - Equipment failure
    - Human error
    - Other (internal fires, floods or explosions, projectiles, pipe-whip).
  - External Events
    - Earthquake, floods, winds, tsunami, tornado ….
  - Logical Combinations of Events
    - “Certain events may be the consequences of other events, such as a flood following an earthquake. Such consequential effects shall be considered to be part of the original PIE.”

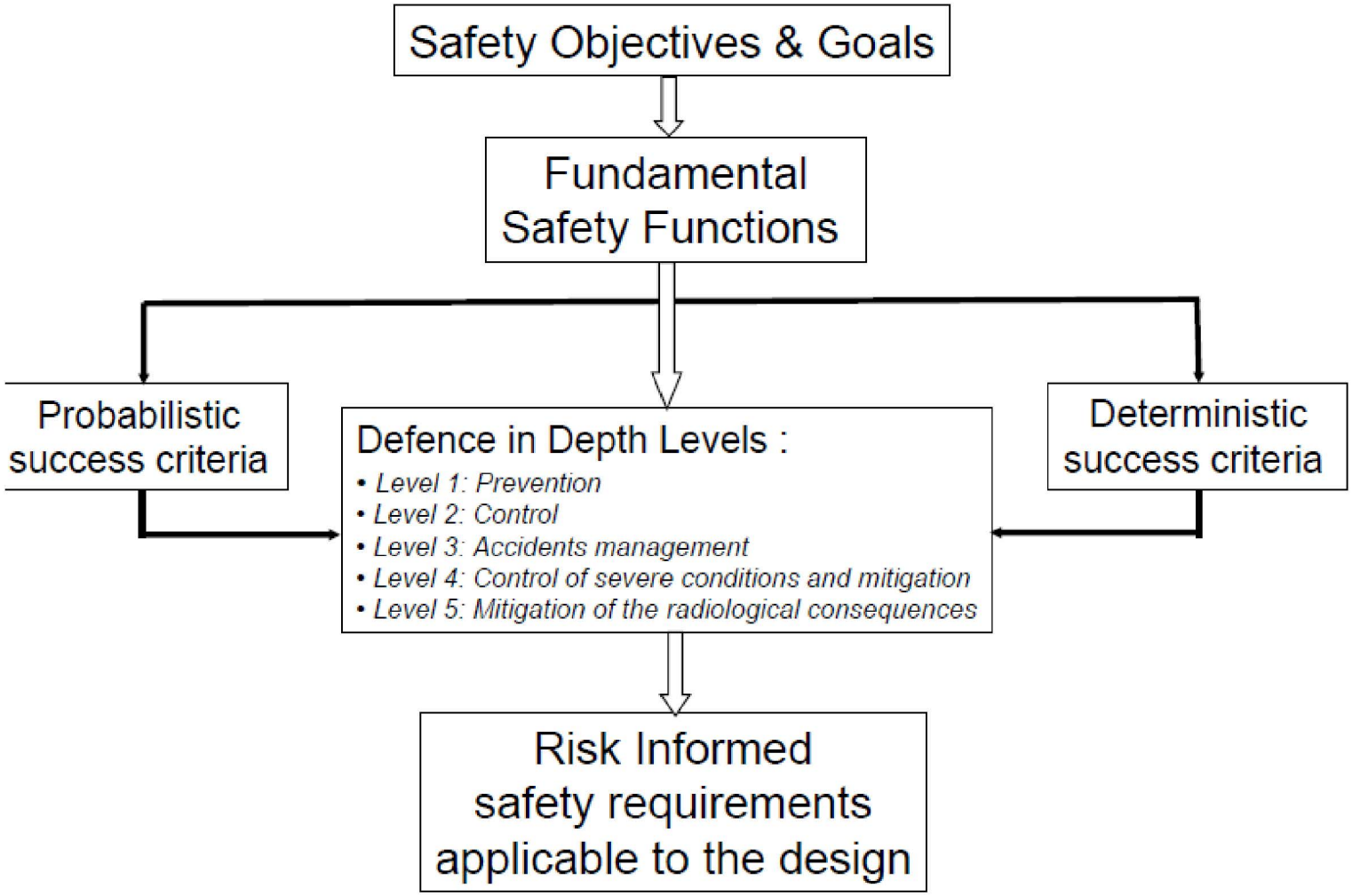
Nuclear Safety

- Quantitative demonstration of achieving the “safety goals”:
  - Deterministic Safety Analysis
  - Probabilistic Safety Analysis
  - Monitoring and Continuous Updating/Improvement

(IAEA-NS-1) Ensure that the overall safety concept of defence in depth is maintained, the design shall be such as to prevent as far as practicable:

(1) challenges to the integrity of physical barriers;
(2) failure of a barrier when challenged;
(3) failure of a barrier as a consequence of failure of another barrier

Demonstration of Safety



GIF/RSWG/2007/002, 2008

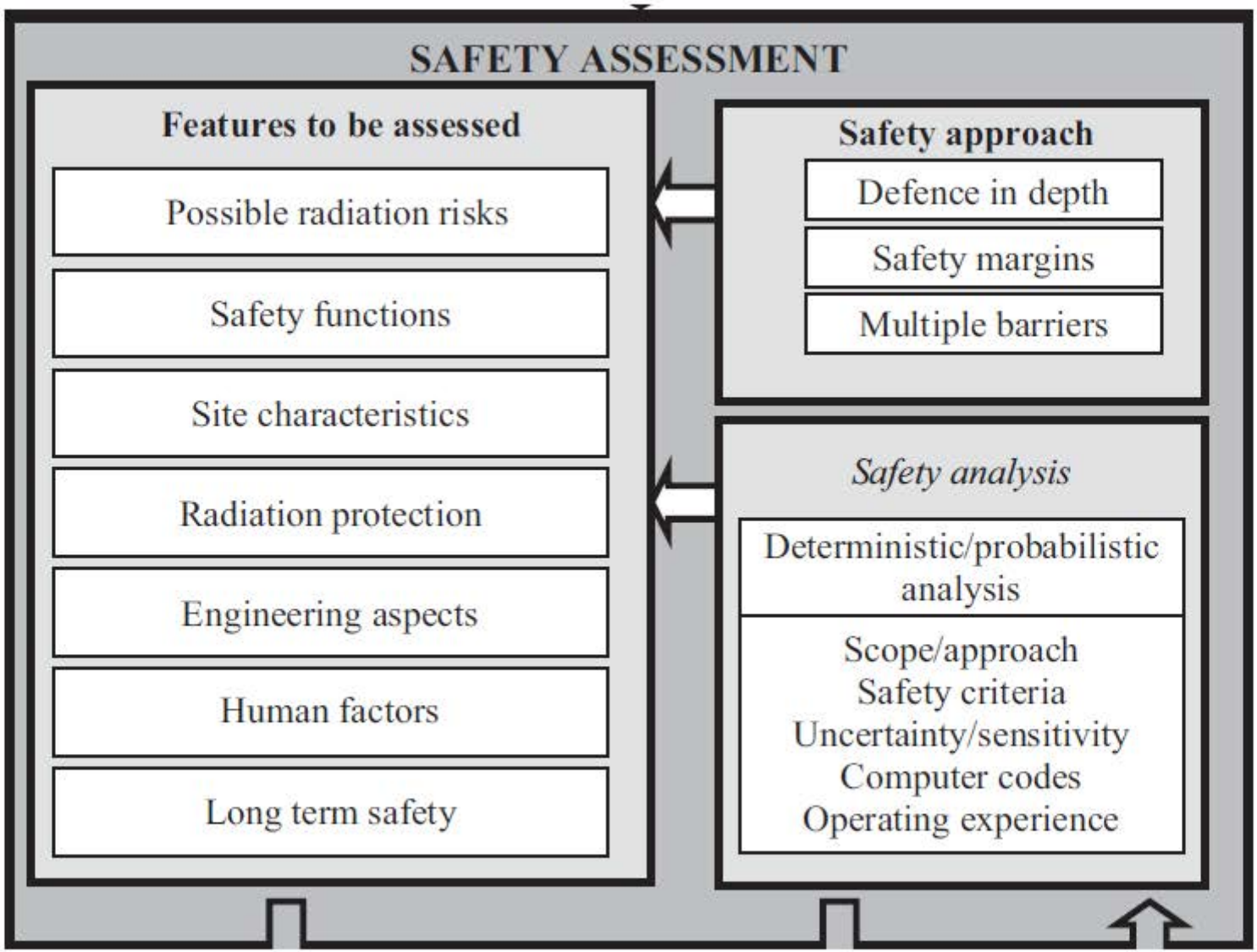
Key Analyses of Safety

Deterministic

- Provide a "point wise" measure of margin to safety
  - specific event and initial condition
  - specific methodology (computer programs, assumptions etc…).
  - OUTCOMES → event timing, fuel sheath temperature, fuel centerline temperature, fission product release, dose…
  - Subjected to uncertainty due to initial plant conditions, models, methods and users.
  - Historically conservative assumptions applied to cover uncertainties.
  - Best Estimate and Plus Uncertainty (BEPU) type of approaches emerging.

Probabilistic

- Provide a measure of the probability that an undesirable outcome will occur.
  - Fuel damage frequency, core damage frequency (CDF), early release frequency…
  - Subjected to the uncertainty in the initiating event and in equipment/systems reliability.
  - Event Tree or Fault Tree Approaches



From IAEA Safety Standards GSR-4

Deterministic Analysis Goals IAEA-NS-R-1

Operational limits	Determine limits and confirmation that conditions are in compliance with the assumptions and intent of the design for normal operation of the plant;
Characterization	Characterization of the PIEs that are appropriate for the design and site of the plant;
Analysis	Analysis and evaluation of event sequences that result from PIEs;
Acceptability	Comparison of the results of the analysis with radiological acceptance criteria and design limits;
Design Basis	Establishment and confirmation of the design basis; and
Mitigation	Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by automatic response of safety systems in combination with prescribed actions of the operator.

Single Failure Criterion

- **IAEA-NS-R-1** *The single failure criterion shall be applied to each safety group incorporated in the plant design.*
- **Fluid and electric systems are considered to be designed against an assumed single failure if neither of the bellow results in a loss of the capability of the system to perform its safety functions**
  - **a single failure of any active component (assuming passive components function properly) nor**
  - **a single failure of a passive component (assuming active components function properly),**
- **The intent was to achieve high reliability on a systems level.**
  - *Even the exercise of determining the limiting component is useful in the design stage*
  - Insight into design vulnerabilities reliability issues

GEN IV Safety

- Need to examine the General, Radiological and Technical safety objectives.

Emphasis on DESIGN related to accidents

1. ***prevention,***
2. ***management and***
3. ***mitigation***

- How might this be achieved?

reduced common mode failures

reduced complexity

increased inspectability

optimized human–machine interface

Improved safety margins

construction/modularization

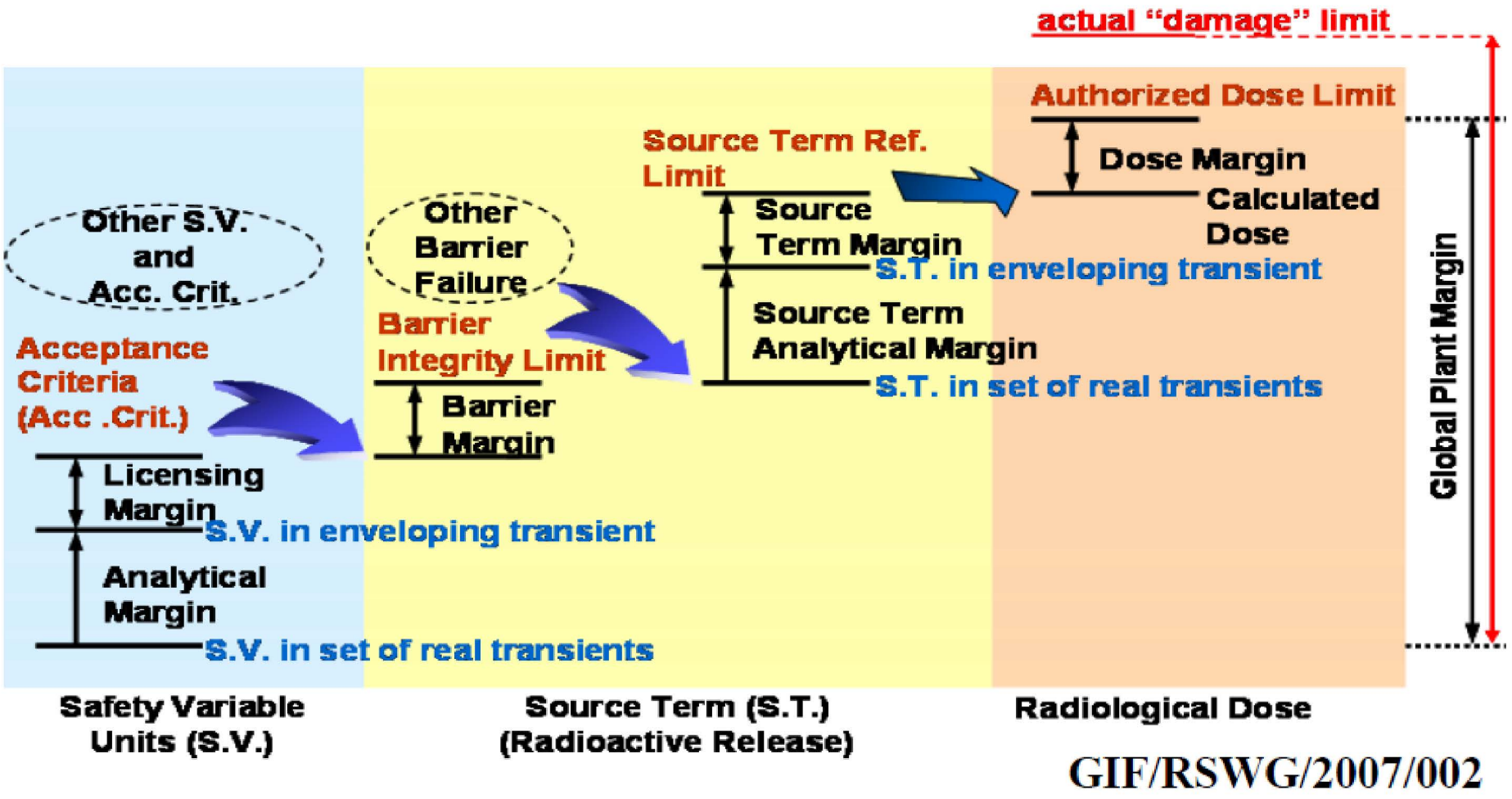
extended use of passive features,

increased maintainability

extended use of information technology

improved reliability

GIF Safety Margin Concept



GIF/RSWG/2007/002

Passive Safety Systems

- Safety system operation (from IAEA-TECHDOC-626)
  - there must be "intelligence" such as a signal or parametric change to initiate action;
  - there must be power and potential difference or motive force to change states; and
  - there must be the means to continue to operate in the second state.
- PASSIVE → all three of these considerations are satisfied in a self-contained manner.
- ACATIVE → if external inputs are needed.
- Passive has a connotation of superior performance that cannot be accepted without evaluation and justification.
  - reliability and availability in the short term, the long term and under adverse conditions;
  - longevity; the equivalent of shelf life, against corrosion or deformation by creep etc;
  - the requirements for testing or demonstration; and
  - simplification and man-machine interaction.

Characteristic	Category A	Category B	Category C	Category D
Signal Inputs of Intelligence	No	No	No	Yes
External power sources or forces	No	No	No	No
Moving mechanical parts	No	No	Yes	Either
Moving working fluid	No	Yes	Yes	Either
Example	**Barriers such as fuel clad, containment; core cooling relying only on radiation or conduction to outer structural parts**	**Heat removal by natural circulation to heat exchangers in water pools, from the core or containment**	**Rupture disk or spring-loaded valve for overpressure protection; accumulator isolated by check valve**	**Shutdown System #1 and #2 in CANDU**

From Snell, 2009, UNENE Courseware Package

Probabilistic Safety Assessment

IAEA-NS-R-1 PSA goals

(1) confidence that the general safety objectives are met;

(2) balanced design (no particular feature or PIE makes a disproportionately large or significantly uncertain contribution to the overall risk)

the first two levels of defence in depth bear the primary burden of ensuring nuclear safety;

(3) assess small deviations in plant parameters do not cause significant problems ('cliff edge effects');

(4) probability of severe core damage states and assessments of the risks of major off-site releases necessitating a short term off-site response,

particularly for releases associated with early containment failure (LERF)

(5) probability of occurrence and the consequences of external hazards (i.e., plant site specific);

(6) to identify systems that reduce severe core damage probability or consequences;

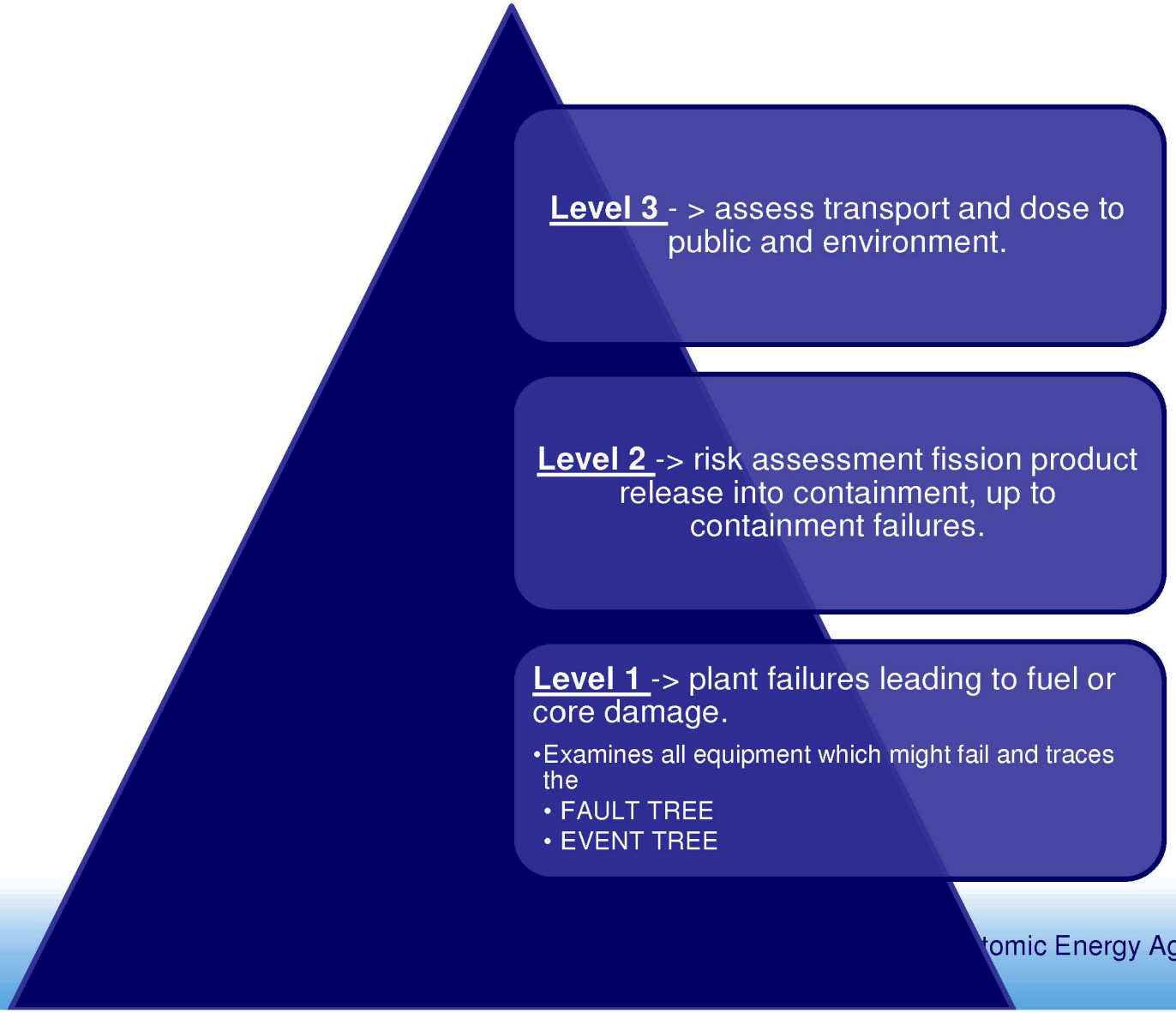
(7) to assess the adequacy of plant emergency procedures;

Probabilistic Risk Analysis

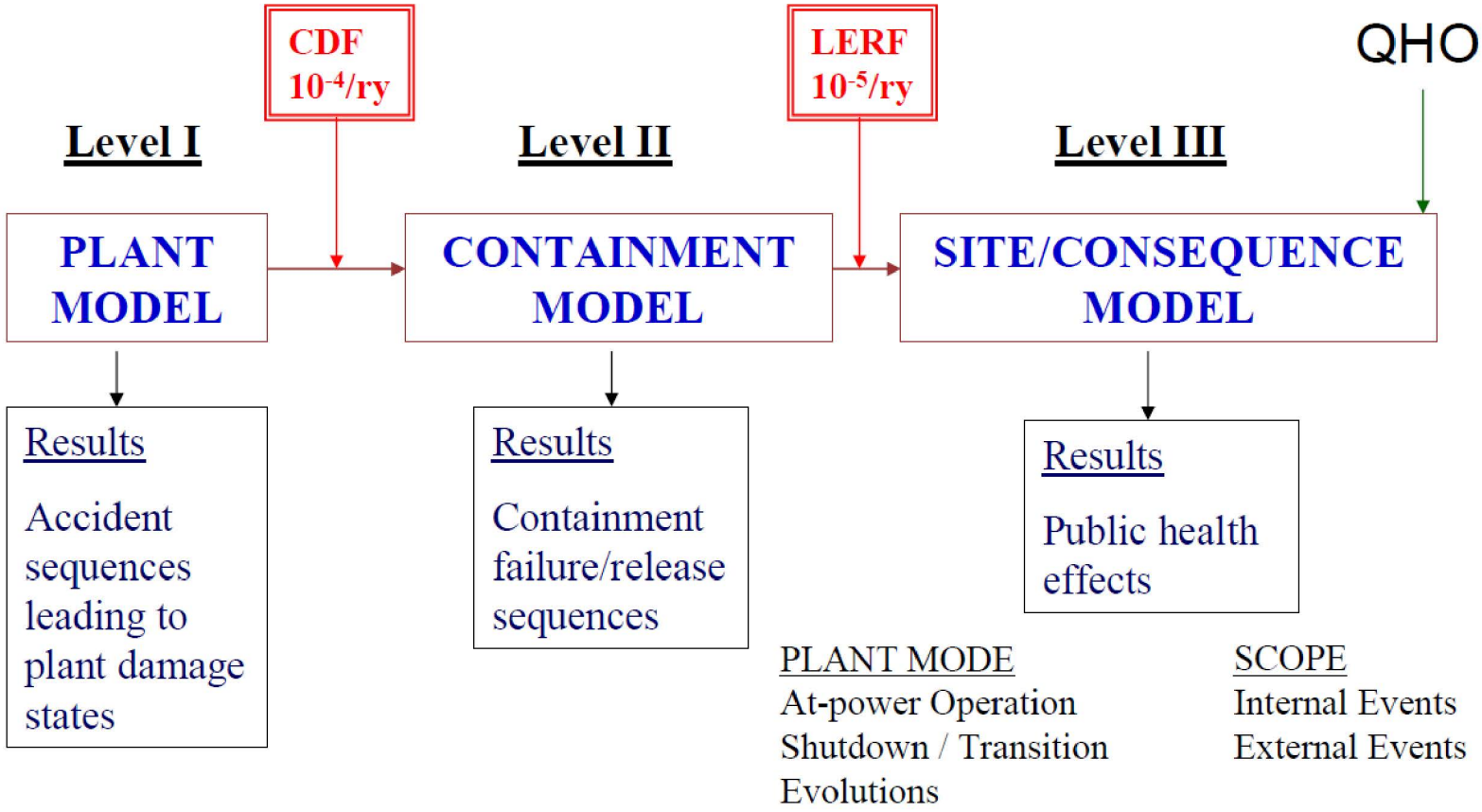
- Requirements for PRA/PSA were developed after TMI accident.
  - Driven by WASH-1400 report →TMI
- PSA is one of the tools used to quantify RISK.
- RISK = P x C

  P = Probability and C = consequence.
- The most utilized consequence metrics
  - Core damage frequency
  - Fuel damage frequency
  - Large release frequency (LRF) and Large Early Release Frequency

PRA Levels


Level 3 - > assess transport and dose to public and environment.
Level 2 -> risk assessment fission product release into containment, up to containment failures.
Level 1 -> plant failures leading to fuel or core damage.
•Examines all equipment which might fail and traces the
• FAULT TREE
• EVENT TREE

PRA Levels

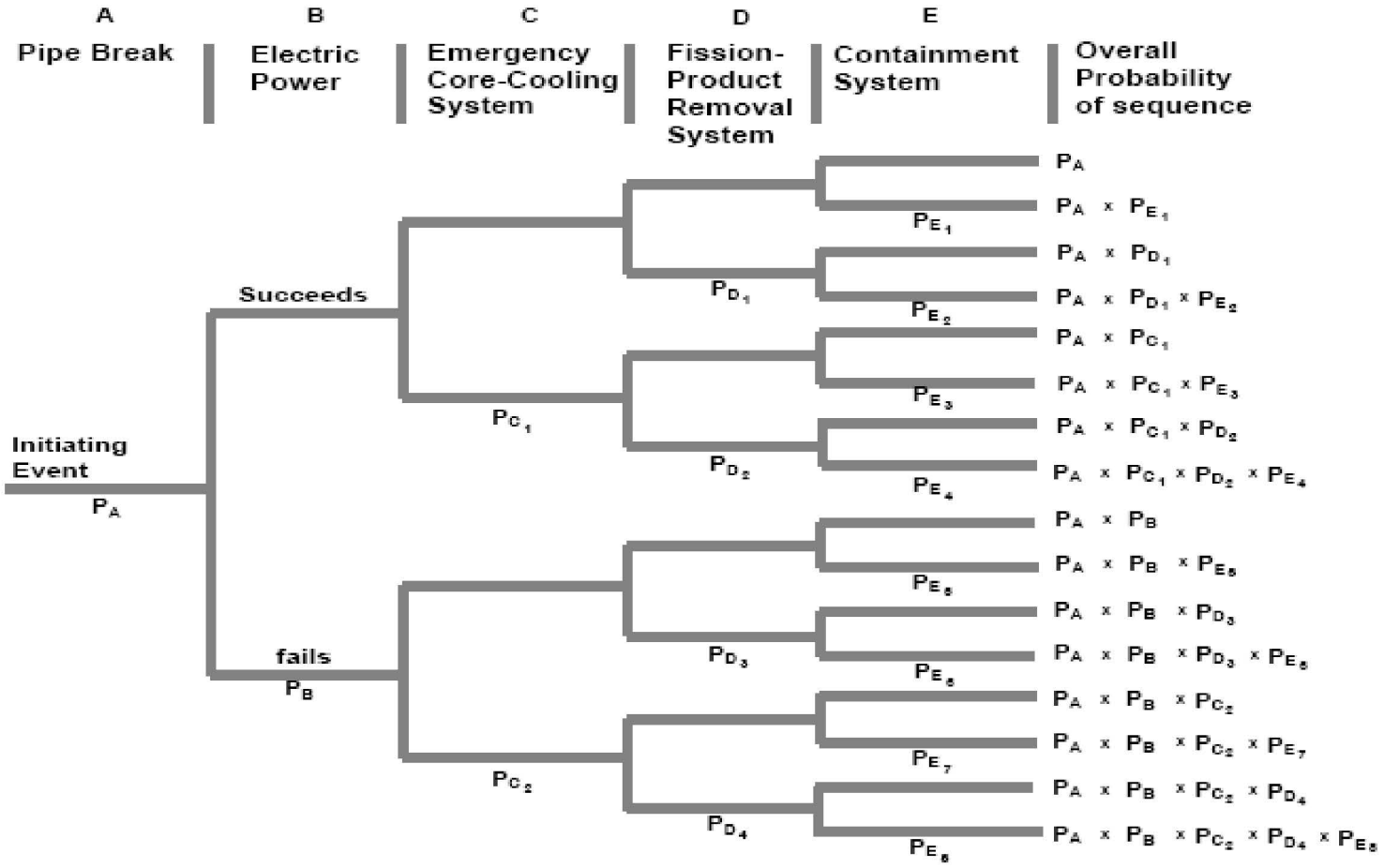


- Kadak 2008, MIT Custom Courseware

Event Tree

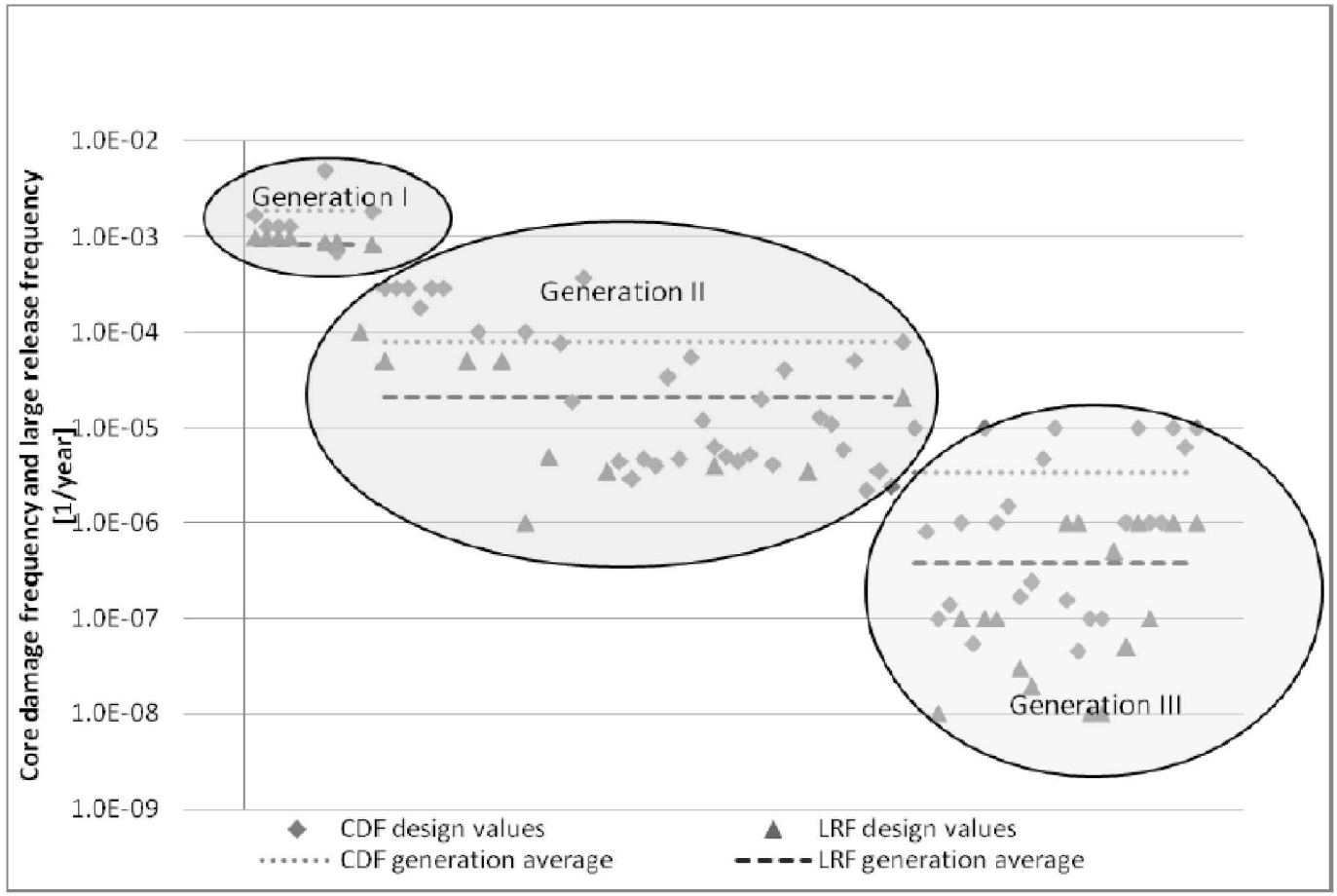
- "An analytical technique for systematically identifying potential outcomes of a known initiating event."
  - Select candidate initiating event
  - Using inductive reasoning, construct sequences of subsequent events or scenarios that end in a 'damage state'
  - Estimate probability of each event on the pathway leading to the accident

Event Sequence/Tree



Source: Reactor Safety Study WASH-1400 analysis of the 1975 Brown's Ferry accident After Lewis, 1980.

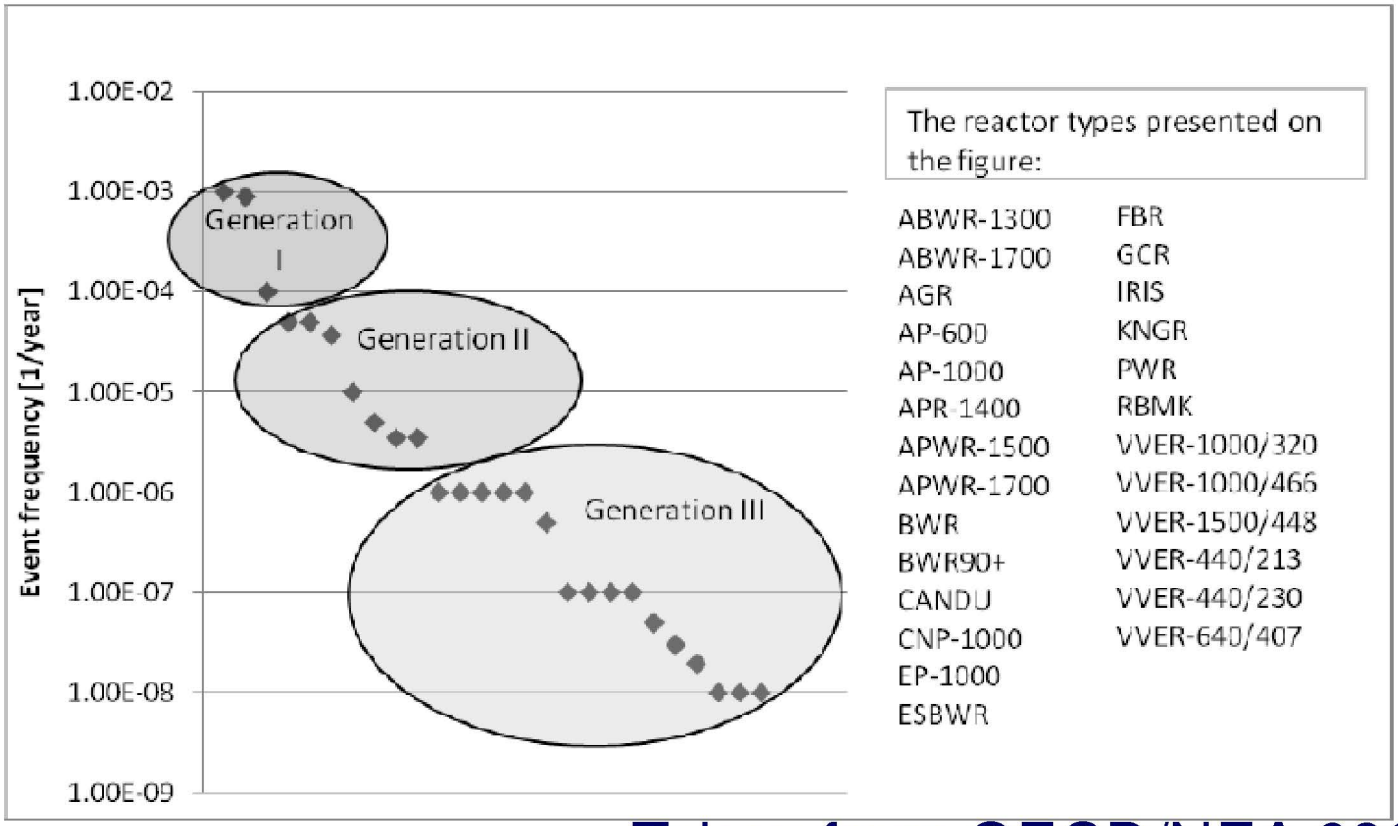
Generational Improvement in CDF



Taken from OECD/NEA 6861, 2011

Evolution of Large Early Release Frequency

Figure 6: Reduction in design estimates of the large release frequency between reactor generations over the past five decades



Taken from OECD/NEA 6861, 2010

Probabilistic Influence on SCWR Design

- **Overall Objective:**
  - **Prevent and mitigate accidents (also assess PIE list).**
  - **Eliminate/Reduce Severe Accident Vulnerabilities**
    - **Quantify CDF and LERF**
  - **Identify Design Sensitivities**
  - **Determine KEY mitigation strategies**
- **PRA Provides a Systematic Method for Achieving these goals.**
  - **Effectiveness may be limited by information availability early in design phase**
  - **Easier to make corrections earlier in design phase**
  - **Imperfect tool is better than none at all**

Design & Information Evolution (Apostolakis 2005)

Conceptual Design	Design Base (DCD)	Detailed Design	Construction Design	Plant in Operation
Is Design Feasible?	Can Design be Licensed?	Will Design be Licensed?	Confirmation of Assumptions	Confirmation of Assumptions
Low Design Detail	Major Components Specified	All Components Specified	All Components Described	All Components Described
Qualitative Risk Assessment	Qualitative & Quantitative PRA	Quantitative PRA with Gaps	Quantitative PRA with Fewer Gaps	As-Built As-Operated PRA
Defense-in-Depth Concepts	Defense-in-Depth Analyzed	Defense-in-Depth Mostly Resolved	No Defense-in-Depth Issues	No Defense-in-Depth Issues
Past Vulnerabilities Addressed	Sequence Level Vulnerabilities Eliminated	System Level Vulnerabilities Eliminated	Component Level Vulnerabilities Eliminated	All Vulnerabilities Eliminated

SCWR Safety Systems

- Most international designs (Japan, EU, Canada)
  - ABWR safety systems as a practical starting point.
- Shutdown System(s)
- SRV – pressure relief
- ECC
  - HPCI / LPCI
  - ADS
  - Power availability
- Containment
  - Venting
  - Scrubbing
- RHR
  - Passive - Active
- Severe Accident
  - Use of Passive systems
  - Core Catcher
  - Containment Cooling
  - Hydrogen mitigation

SCW Proposed Safety System

- Example Japanese design:

Safety system designs of ABWR and SCFR. %: percent ratio to the rated core flowrate

Contents	ABWR	SCFR
◦RCIC	— Turbine driven (TD): 1 unit •50 kg/s/unit: 2.4% at 72 bar	— TD-RCIC: 1 unit •160 kg/s/unit: 8.0% at 250 bar
◦HPCF/HPCI	— Motor driven (MD): 2 units •50 kg/s/unit at 72 bar	— 1TD-HPCI: 160 kg/s at 250 bar - 1MD-HPCI: 16 kg/s at 250 bar
◦ADS	— 8 units: 105 kg/s/unit at 81 bar	— 8 units: 420 kg/s/unit at 250 bar
◦ACT	—MD-HPCF LPFL/RHR	— 3 units, Operat. pressure < 15 bar TD-HPCI LPCI/RHR Total volume: 25 m^3/unit
◦LPFL/LPCI	— MD-LPFL: 3 units •264 kg(13%)/s/unit at 12 bar	— MD-LPCI: 3 units •400 kg(20%)/s/unit at 10 bar
◦Safety system configuration	TD-RCIC LPFL/RHR MD-HPCF LPFL/RHR	TD-RCIC LPCI/RHR MD-HPCI LPCI/RHR
◦Emerg. D/G required cap.	— 3 units: 306 kW/unit (for only HPCF & LPFL)	— 3 units: 340 kW/unit (for only HPCI & LPCI)

Lee et al, Reliability Engineering, 1999.

Shutdown System and Trip Parameters

Scram conditions of the SWFR.

Main coolant flow rate low (90%)	Main stop valve closure
Reactor power high (120%)	MSIV closure (90%)
Reactor period short (10%)	Reactor coolant pump trip
Pressure high (26 MPa)	Condensate pump failure
Pressure low (24 MPa)	ECCS start-up
Loss of offsite power	Drywell pressure high
Turbine control valve quickly closed	Earthquake acceleration large

Satoshi Ikejiri; Yuki Ishiwatari; Yoshiaki Oka 2010

SCWR Basic Safety System Concept (non-External Events)

- Example from Japanese Design

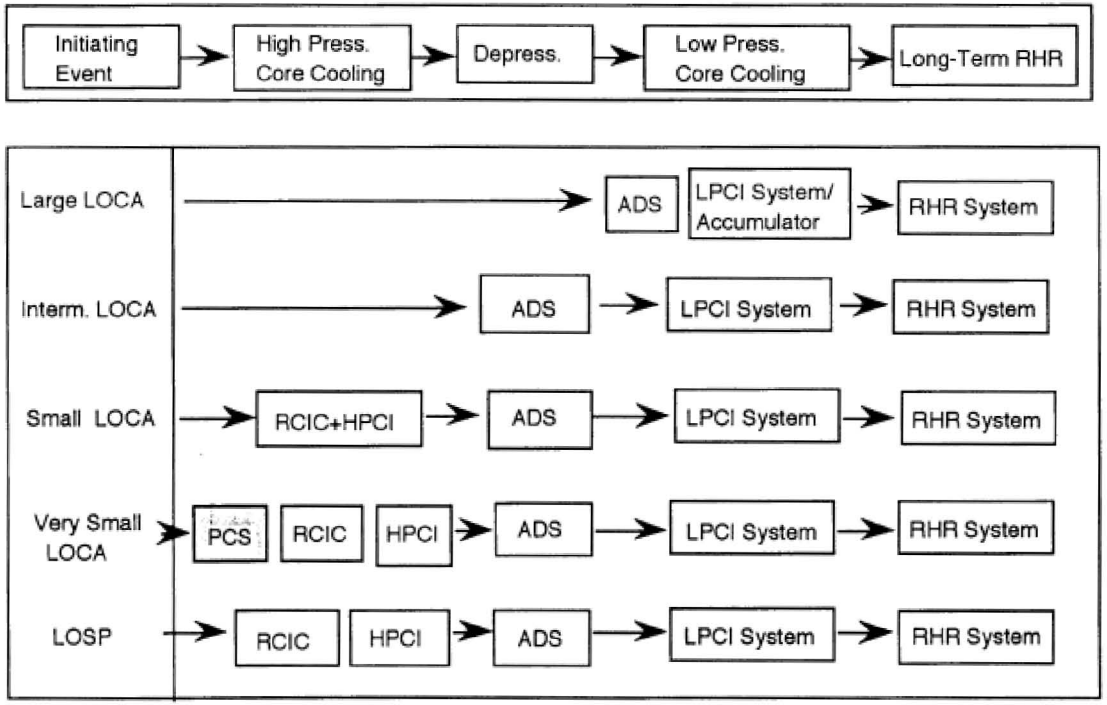


Fig. 4. Mitigation sequences of core cooling for initiating events.

Calculated core damage frequency

Initiating event	Core damage frequency
◦LOCA	3.11×10^{-7} (54.3%)
— large-break LOCA (A)	1.2×10^{-7} (20.9%)
— intermediate-break LOCA (Im)	1.6×10^{-7} (27.9%)
— small-break LOCA (S1)	3.1×10^{-8} (5.0%)
— very-small-break LOCA (S2)	1.2×10^{-10} (0.0%)
◦Loss of offsite power (LOSP)	1.56×10^{-7} (27.2%)
◦ATWS	1.06×10^{-7} (18.5%)
◦Total	5.73×10^{-7} (100.0%)

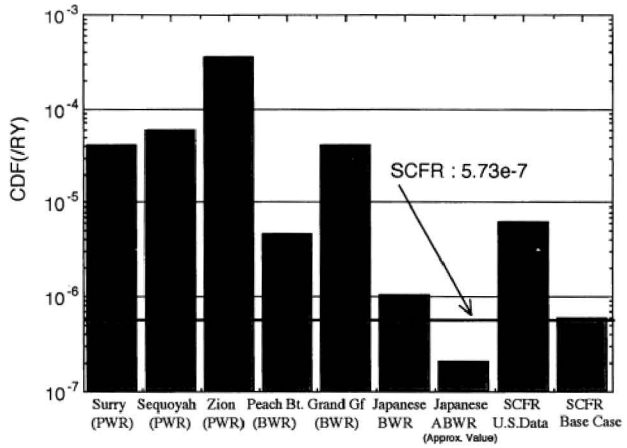


Fig. 10. Comparison of the total CDF with the current plants.

Lee et al, Reliability Engineering, 1999.

CDF Contributors

- No single accident dominates risk.

Initiating event	Core damage frequency
◦LOCA	3.11×10^{-7} (54.3%)
— large-break LOCA (A)	1.2×10^{-7} (20.9%)
— intermediate-break LOCA (Im)	1.6×10^{-7} (27.9%)
— small-break LOCA (S1)	3.1×10^{-8} (5.0%)
— very-small-break LOCA (S2)	1.2×10^{-10} (0.0%)
◦Loss of offsite power (LOSP)	1.56×10^{-7} (27.2%)
◦ATWS	1.06×10^{-7} (18.5%)
◦Total	5.73×10^{-7} (100.0%)

Recent Generic Issues in Nuclear Safety – Learning From Mistakes

- Reactor Vessel Integrity → low leakage cores
  - Depending on weld and metal materials some vessels vulnerable to embrittlement
  - Of particualr concern to SCWR cores and vessel materials.
- ECC Sump Performance
  - Debris clogging ECC sump screens → similar issues in SCWR.
- Weld issues
  - SCC and fatigue
  - Corrosion concerns is SCWR → weld overlays and coatings
- Fire protection integral to design
  - Prevent and manage fires (common cause).
- Security and Terrorism
- Low Power Issues
- Total Loss of Heat Sink
  - Fukushima Daiichi
  - New focus on sever accidents
- Source Kadak 2008 and D.R. Novog 2011.

Low Power Issues

- Many accidents and near misses have happened either apost-shutdown or in a low power state:
- Attention in the scwr design should address.
- Xe transient and low power instabilities
  - Xenon is a neutron poison which is naturally produced and destroyed from the fission product decay chain.
  - For a period of time after shutdown, Xe is still produced from I decay
  - No longer burnt by neutrons.
  - Build-up of Xe
  - 3D neutronic-thermalhydraulic instabilities (similar to BWR)
- Instrumentation issues
  - Instrumentation is optimized for high power
  - Approach to critical a difficult procedure which does not occur often.
- Mistaken belief of large margin
  - Also large margin to safety system action.
  - Reactor stability issues.
- Residual Heat Removal

Additional References

- IAEA-NS-R-1, INSAG-10, INSAG-12, IAEA-SF-1
- IAEA-TECHDOC-1200 (PSA), WASH-1400
- OECD/NEA 6861 (Comparing Nuclear Accident Risk to Those of Other Energy Sources).
- NUREG 1860 – generic framework for new reactors
- Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems *Revision 1* November 24, 2008 Prepared by: The Risk and Safety Working Group Of the Generation IV international Forum
- George E. Apostolakis, Risk-Informed Design Guidance for Gen IV Reactors, 2006