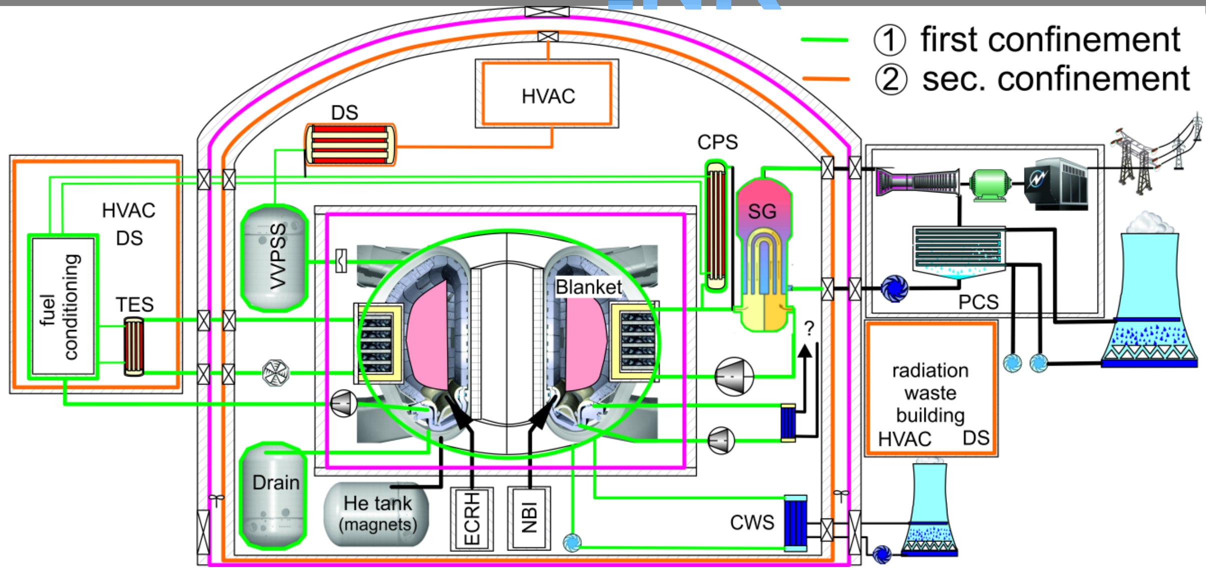
Karlsruher Institut für Technologie

Fusion Reactor Safety

- Terminology (reliability , safety, security, ……..)
- Risk analyses (FTA-FaultTree Analysis, FMEA-Failure Mode Effect Analysis)
- Nuclear safety analysis (objectives, operationalisation, MLD- Master Logic Diagram, demonstration)
- Dose concept (ALARA-Principle)
- Fusion Safety Concept   (comparison with NPP- where are we today?)

INSTITUT für NEUTRONENPHYSIK und REAKTORTECHNIK (INR)



Terminology-Reliability

- **reliability = probability that system meets the required specified function**
  - within a certain time interval **and**
  - under normal operation conditions

Measures of reliability technology

- elimination of errors /failures/ malfunctions
- early detection
- initiation of countermeasures (messaging, design measures: redundancy, diversity)

robust design + operational monitoring

regular inspection intervals

Proof of realibility

- reliability calculation (result: e.g. guarantee time)

➡ reliability = part of the quality assurance

Terminology-Reliability

Reliability analysis

- **Goals**:
  - prognosis of expected reliability (hazard)
  - detection and elimination of vulnerabilities
  - conduction of comparative studies

- **Options :**
  - **quantitative:** calculation of reliability, failure rate analysis, probabilistic reliability prediction (Markov or Boole model, lifetime distributions, **Fault tree analysis-FTA**)
  - **qualitative**: systematic investigation of fault effects and failures, failure modes analysis (ABC analysis, check lists, **failure mode effects analysis-FMEA**, **Fault tree analysis-FTA**)

Terminology-Reliability

Types of reliability analysis

- **inductive** : forward tracking of events leading leading to accidents –**FMEA**
- **deductive**: backward derivation of possible failures, leading to accidents – **FTA**

- **Failure Mode and Effects Analysis (FMEA)**
  - qualitative, inductive reliability analysis
  - detection of error sources in order to avoid or reduce consequences
  - error prevention (preventive measure)
  - identify the vulnerabilities to revise this then constructively

- **Fault Tree Analysis (FTA)**
  - qualitative or quantitative, deductive reliability Analysis
  - representation of a top event (system failure, **risk**) in relation to the causes that lead to this top event
  - identify causes that lead alone or in combination with other causes to an error

Terminology - safety

Karlsruher Institut für Technologie

- **safety** = system state, from which within **given limits** and for a **prescribed time interval** no danger emanates.
- ➡ **safety = absence of danger (system does not pose danger to outside)**
- **safe state= state in which despite failure(s) (**by operator, malfunctions,… **no danger emanates**

- **Examples:**

thermal plant: exceeding max. pressure

loop systems: unintended leakage

driving car:

Terminology - safety

Safety measures

- **actions directed against dangerous effects of errors and failures**
- **prevention of danger in case of error/failure**

- control of reaction
- stop media service
- relief valve

- design measures
- intrumentation
- personnel protection

- material choices (code&standards)

- fabrication quality

- operat. monitoring
- personnel equipment (protective clothing)

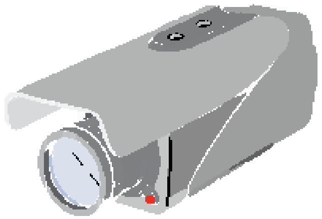
driving cars are intrinsically unsafe !!!

- **rationale for safety measures** ➡ **approval by a safety authority**
- **detection method** ➡ **safety case**

Terminology- plant safety

NOTE (difficult in many languages)

- **SAFETY = prevention of hazards originating from the plant itself**
- **SECURITY= prevention of human or environmental threads on the system leading to states, in which system(plant) can get dangerous.**
- **Most known to you in terms of security:**



video survaillance

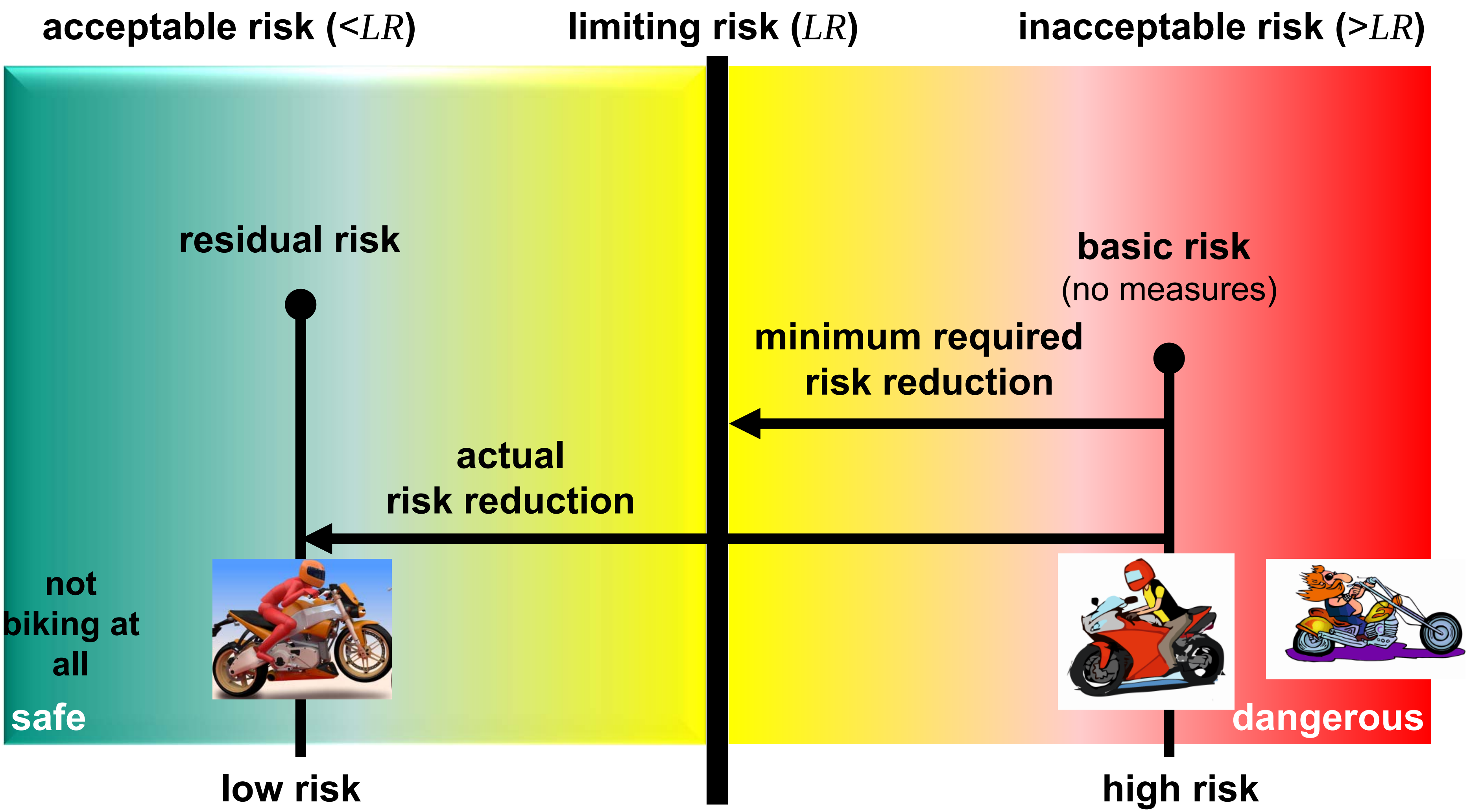
airport security

<u>For nuclear systems:</u>

- Protection against external hazards (terrorist attack, flooding, earth quake, …..)
- ➡ Design measures according to (nat. and/or internat.) prescriptions
- **SYSTEM (PLANT) SAFETY= SAFETY + SECURITY**

Terminology – how to correlate safety and risk ?

- **What is the difference ?   risk – danger – safety**

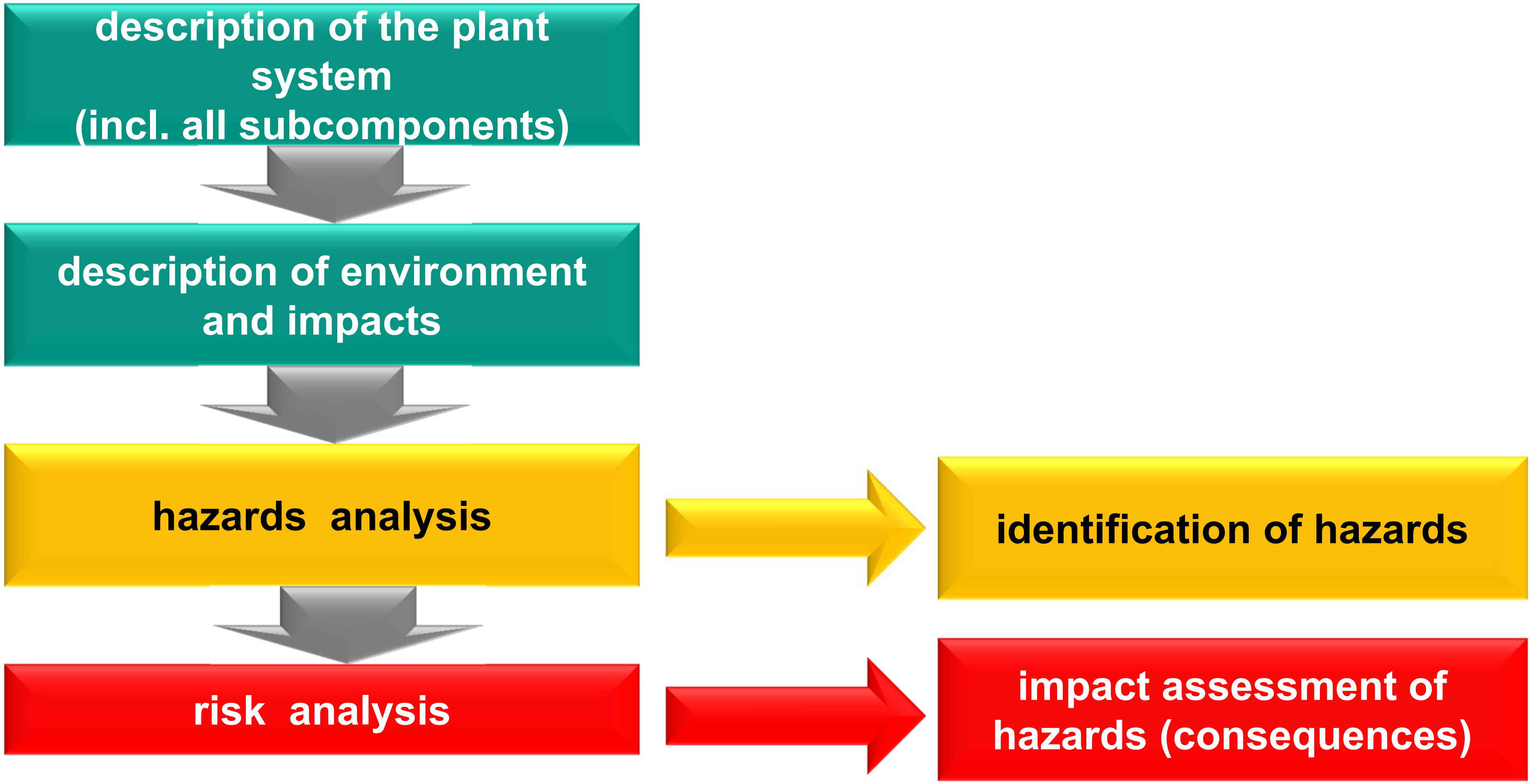


Terminology – safety analysis

- **safety analysis = requirement for operational (nuclear) license**

Safety Assessment

- consecutive process



Terminology- phrases around

What means ?

- **availability = time fraction of system usability**
  (probability of a repairable system to be functional at a given point in time)
- **reliability = safety + availability + robustness**
  (system property allowing to trust in the provided functionality)

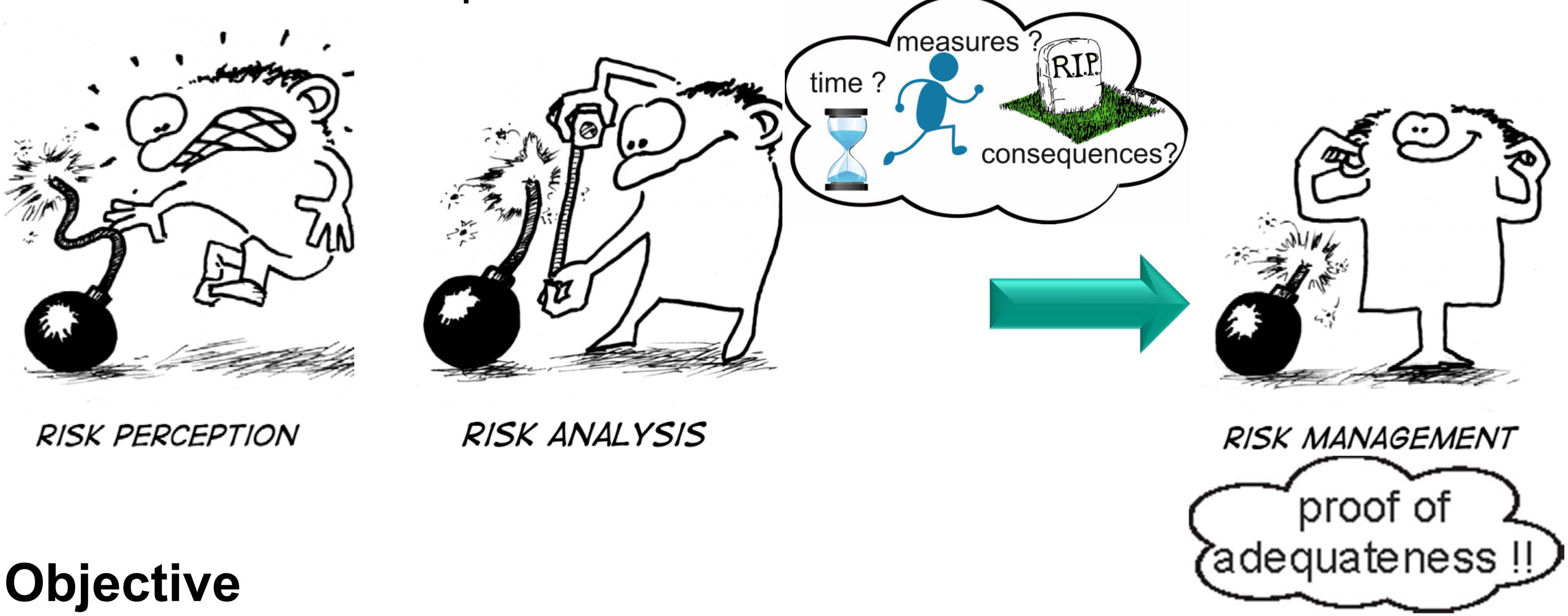
➡ **availability ≠ reliability**

Other often used words:

- **hazard =** physical situation with potential for human injury, damage to property, damage to the environment or any combination. **ability to create harm.**
- **risk =** likelihood of undesirable events (hazards) to occur within specified time and/or specified circumstances
  (system property allowing to trust in provided functionality)

Introduction- Risk analyses

What to do ? ➡quantification of risk by numbers



Objective

- identify hazards
- analyze and evaluate the risk associated with each hazard
- elaborate appropriate measures/means/methods to eliminate or reduce hazards
- if you can not eliminate or reduce hazards, **identify appropriate ways to** eliminate or **reduce the risks** associated

➡ **holds for any engineering system (from mobile ➡reactor)**

Risk analyses- Fault Tree Analysis (FTA)

Context

- FTA =deductive method. It establishes a graphical relation between a top event (system failure, threat, ...) and causes leading to this top event.
- starting from the undesired top event, the possible causes are searched.
- causes can occur alone or in combination with other causes, leading to a defined error

Aims

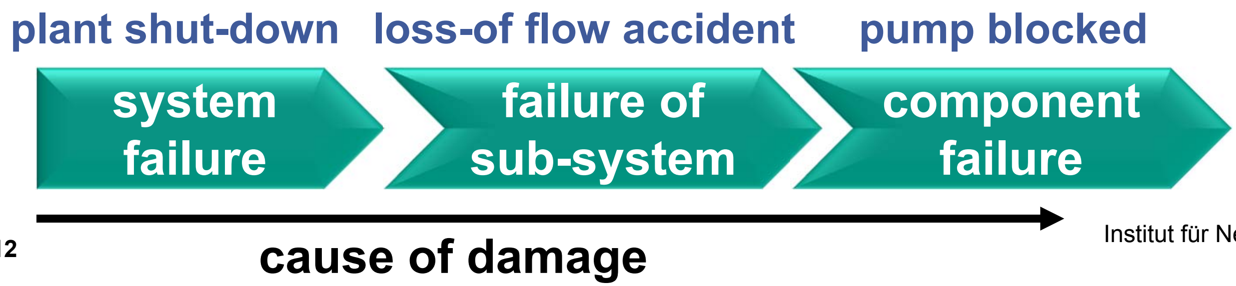
- realistic modeling of the system on component basis in order to analyze
  - failure mode and failure causes
  - establishiment of functional relations of failures
  - description of impact of failures on the system

Use of FTA

- preventive quality assurance
- system analysis
- troubleshooting for newly emerging errors

FTA –structure

- Graphical representation across several system levels, which are connected via logical connections



Risk analyses- Fault Tree Analysis (FTA)

Qualitative FTA -execution

- Sequence

1. system analysis
2. postulation of events of failure criteria
3. evaluation of component failure mode
4. elaboration of fault tree
5. qualitative assessment (consequences)

- **identification** of all failures, critical events and event combinations
- creation of **objective assessment** criteria
- **documentation**

1 system analysis

- determination of required system functions and their allocation to individual elements
- identification of relationships between system functions (cooperation of elements to attain required function, response to environmental impact, system response to internal failures of elements, system response to external failures linked to the system)

2 definition of adverse events and failure criteria

- Define preventive and corrective measures
  - Prevention: definition of adverse events by noncompliance with functions/requirements
  - Corrective measures: definition of an occurred failure/malfunction as adverse event

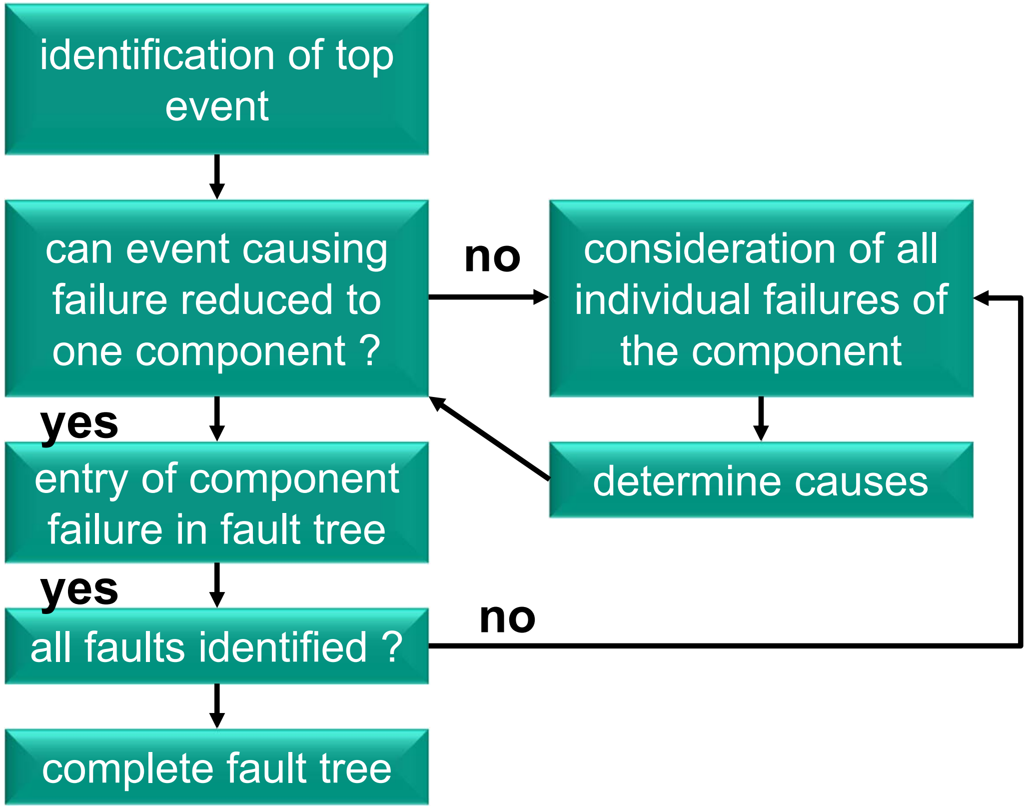
➡ in view of damage severity (radiological impact)

Risk analyses- Fault Tree Analysis (FTA)

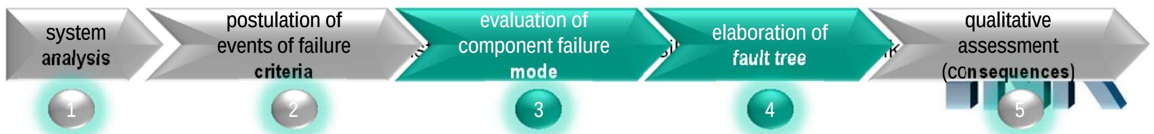
3 Determination of component/system failure modes

- Primary failure: component failure due to weakness or errors a priory present in the system – **failure in permissable operating conditions**
- Secondary failure: component failure caused by environmental or operational conditions – **loss in design extension conditions**
- Forced failure: component failure of functioning system by incorrect operation or false/invalid signals/links – **operational of maintenance error but also deliberate mistakes**

4 Creation of fault tree



➡ **often quite complex, good preparation mandatory, adequate splittings sensible**



Risk analyses- Fault Tree Analysis (FTA)

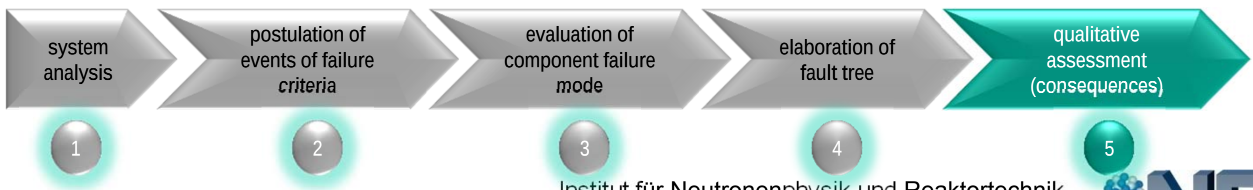
5 Qualitative assessment

- Reliability assessed qualitative via graphical structure, assessment of system weakness
  - Critical path: fault tree branches, in which component failures are not protected by system inherent prevention /check mechanisms
  - Critical quantity: subtree of the fault tree, which contains the minimum combination of individual elements whose failure leads to the adverse event.

➡ Critical path/quantity allows statement on strongest/weakest branch of fault tree

How good is a FTA ?

- Benefits
  - precise adjustment to the object of investigation possible
  - deeper system content information by evaluation of the fault tree
  - allows identification of (still) unknown causes of failure
- Disadvantages
  - Precise adjustment to the object of investigation possible
  - intensive time/money consuming analysis
  - expert know-how indispensable



Risk analyses- Fault Tree Analysis (FTA)

Quantitative FTA (similar approach as qualitative FTA)

- computation of discrete reliability parameters evidence for reliability requirements
- **collection of reliability parameters from data bases** *1 (code & standards, ministery, supplier, estimates)
- summary of total reliability R_{total} along indivdual paths
- ➡ exact comparable, objective results **but**
- ➡ limited flexiblity and not all failure sources assessable (e.g. reliability factor „**human behavior**“)

*1 Data basis: Ministry e.g Germany: BfS: Data for probabilistic safety assessment of nuclear power plants, 2005

Risk analyses-Failure Mode Effect Analysis (FMEA)

Karlsruher Institut für Technologie

FMEA- what is it about ?

- FMEA=qualitative method of reliability
- inductive procedure to identify all system failure modes
- depiction of all possible causes and effects of faults
- determination of consequences for the system

FMEA = preventive measure to

- prevent errors/failures
- to detect errors

FEMA Sequence

1. creation of structure of functions/mal-functions of all system components
2. evaluation of a causes leading to a malfunction
3. execution of risk analysis of malfunctions
4. risk assessment in FMEA sheet
5. system measures to avoid or detect potential errors

FEMA tools

- Fishbone – cause –effect diagram
- Fault Tree Analysis (FTA)
- Event Tree Analysis
- Matrix Diagrams (➡product management, economics)

Risk analyses-Failure Mode Effect Analysis (FMEA)

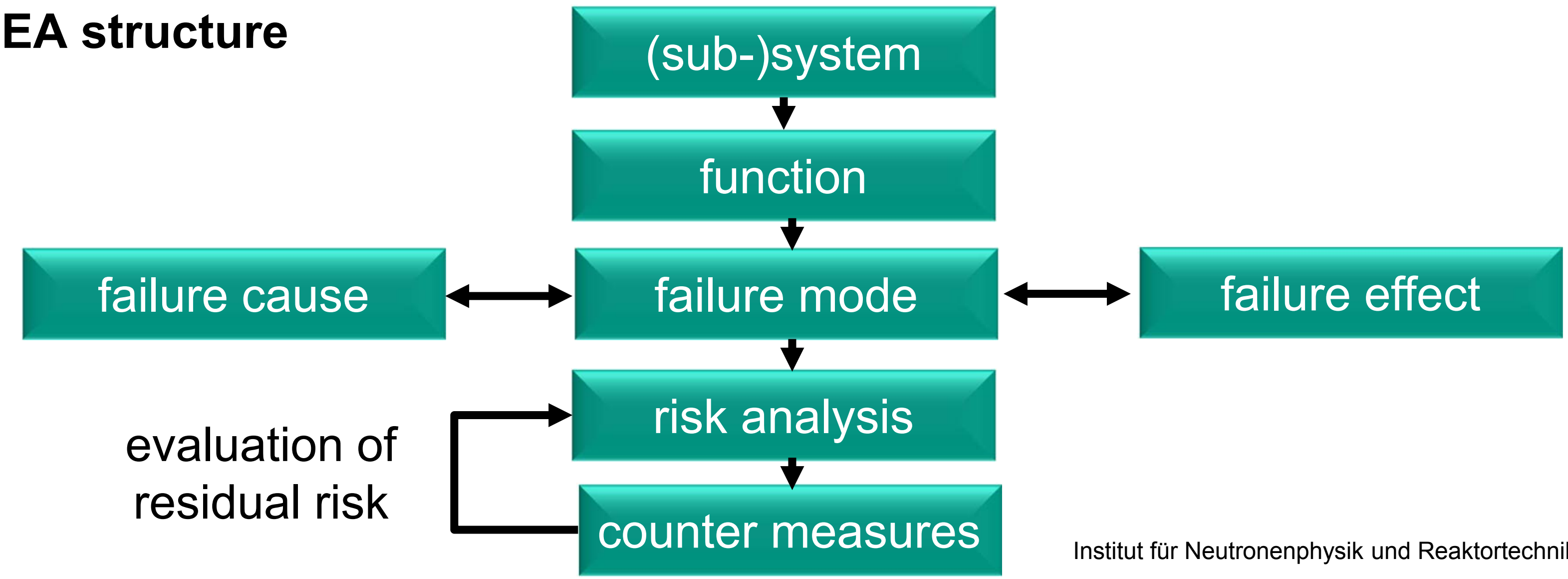
Event Tree Analysis (ETA)

- ETA=inductive procedure to evaluate potential consequences of an error (DIN 25419)
- events/logic links are depicted in event trees (with branches, AND/OR links)
- ETA similar to FTA but
  - **FTA**: evaluation of all **causes leading to a hazard**.
  - **ETA**: evaluation of all **hazards emanating by a certain error/incident**.
- ➡ assigment of probabilites for quantitvative evaluation possible

Aspects for execution of a FMEA

- FMEA analysis focuses on a single component/(sub-)system – („bottom up- approach“)
- based on this all imaginable occuring failures are determined
- additionally als failure effects and further consequences are considered
- ➡ FMEA execution has a certain degree of freedom
- ➡ result is team/expert know-how dependent ➡ **subjectivity**

FMEA structure



Risk analyses-Failure Mode Effect Analysis (FMEA)

nuclear engineering

FMEA sheet components – example

com-ponent	operational state	failure mode	freq.-cat.	causes	preventive action	conse-quence	preven. action on conseq.	postulated initiating event (PIE)	comment /specific occurence frequency/codes and standards used
piping	no	ext. leak	III	weld fault, pipe wall flaw, constr. fault	des. materials selection , pre-service inspect., low flow-induc. vibration in design, NDT	leaks small to moderate amount of coolant to equatorial port	small loss of coolant accident. shut down by the end of seq., drain to drain tank to limit radiologic release, increase cooling of neighboring system to limit superheat of other systems	small LOCA	xy m piping length oper. 3360h/y ;liquid nonreactive in air /H_2O, should not pose chemical reactivity concern. spill must be kept from bellows seal. **$9 \cdot 10^{-9}$ /h/m** e.g. EGG-SSRE-8875
		ext. rupture	III	….					
		plugging	III	……					

➡ **RESULT: (hopefully) full list of elementary failures (and quantification !!)**

Risk analyses-Failure Mode Effect Analysis (FMEA)

FEMA – system analysis- provides individual results for an antipicated plant internal failure/malfunction incident and/or an assumed external hazard (eg.flooding, earthquake …..)

ANSWERS provided are related to

- **Safety**
- **Robustness**
- **Availability**

➡ **Reliability**

➡ **Quantity : events per hour/min/years ➡ FREQUENCY !!!!**

➡ **Meaning: a probability of an event to occur** (stochastic –could also occur just now)

What are the next steps ?

- elaboration of technical power plant set-up (specification)
- definition of the safety objectives (translating into primary &secondary safety functions to be met by techn. equipment & plant)
- classification of the plant in certain classes

Risk analyses-Failure Mode Effect Analysis (FMEA)

Karlsruher Institut für Technologie

FEMA – system safety analysis

- Classification of plant states in event classes

Event category	I	II	III	IV
category description	operational events/ plant conditions planned/required for normal operation	likely event sequences not planned but likely to occur once or more during the life time but not included in category I.	unlikely sequences that are postulated but not likely to occur during lifetime	extremely unlikely event sequences that are postulated but are not likely to occur during lifetime with a very large margin.
frequency range [per year]		$f < 10^{-2}$	$10^{-2} < f < 10^{-4}$	$10^{-4} < f < 10^{-6}$
system condition	normal	incident	**accident**	**accident**

Risk analyses-Failure Mode Effect Analysis (FMEA)

- **What FMEA results mean in terms of SAFETY?**
  - **CLASS 1: Normal operation**
    - No failure of the nuclear first barrier (walls)
    - Performance of the purification system consistent with a few leaking rods

  - **CLASS 2: Low frequencies events**
    - No failure of the first barrier

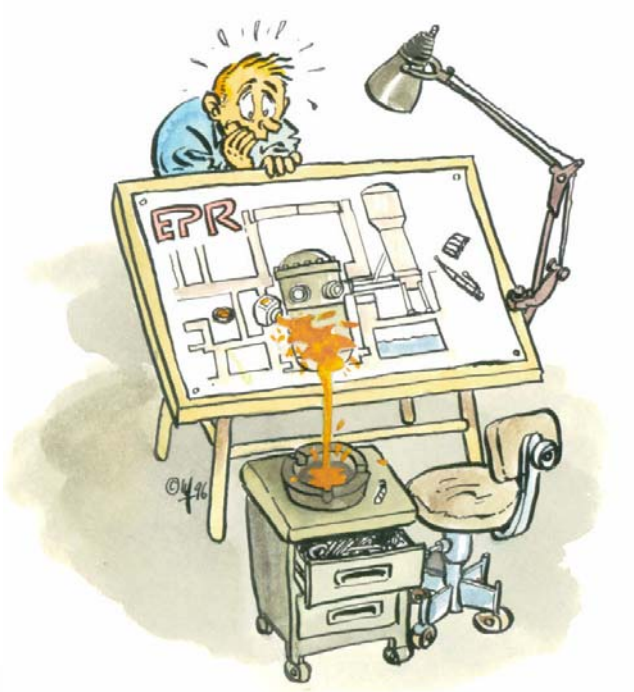
  - **CLASS 3: Low probabilities accidents**
    - Nuclear materials barriers might be damaged
    - Bring back the reactor to a safe state (use of diverse/redundant systems)

  - **CLASS 4 : Hypothetical accidents**
    - Termination of nuclear reaction,
    - Reactor geometry remains coolable
    - Geometry of reactor remains intact

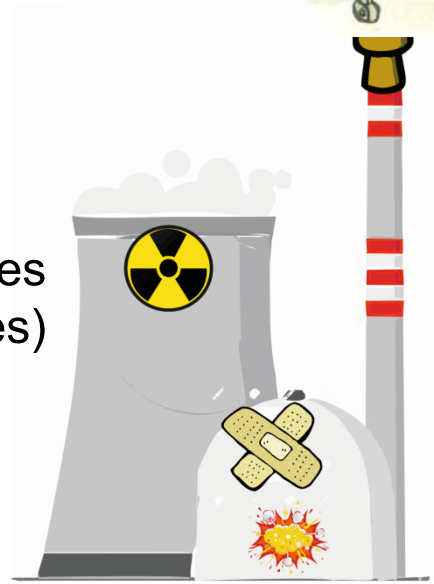
Risk analyses-Failure Mode Effect Analysis (FMEA)

Beyond design basis accidents

- **> CLASS 4 accidental conditions**
  - Objective to preserve plant withdrawn
  - Preservation of ability to ensure
    - **coolability and**
    - **confinement of radioactive products**
- **Causes: Multiples Accidents**
  - Steam Pipe Break (LOCA, LOFA) + Steam Generator Tube Failure
  - First wall leak + explosion + failure of fusion power system shut down system



- **CLASS 5**
  - Design mitigating radiological consequences outside plant (off-site emergency responses)



Karlsruher Institut für Technologie

FEMA – system analysis

- grouping of elementary error list in classes exhibiting similar consequences
- assign the PIE lists to operational phases (system conditions)
- summation of events for each phase together with the expected occurences leads total (cumulative) rate for each PIE (Postulated Initiating Event)

PIE family	FEMA faults/annular frequency	cumulative rate/event category
…		
small LOCA to port cell	valve leak $3.3 \cdot 10^{-2}$, pump leak 10^{-2}, piping leaks $6 \cdot 10^{-3}$ ……..	$5.6 \cdot 10^{-2}$/year , category II
….		

Risk analyses - Failure Mode Effect Analysis (FMEA)

Failure rates

Why important to collect/analyze data related to component failures ?

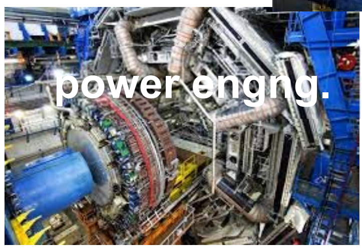
aging of components → **component failure**

preventive maintenance | **corrective maintenance**

unavailability / operational safety (worker doses)

unreliability / potential radioactive releases

Where to find information?



Nuclear safety objectives

- **Protection** of public and environment **against radiological hazards**
- **Protection** of site workers against radiation exposure according to ***ALARA***-principle (As Low As Reasonably Achievable)
- Employment of **measures to prevent accidents** and **mitigate** their **consequences**
- **Elimination** of need for public **evacuation** in any accident
- **Minimization** of activated **waste**

➡ **Assignment of safety functions**
(buildings, components, design measures,…….)

Nuclear safety analyses- Objectives & Operationalization

Safety functions of a nuclear power plant (FPP)

- **Primary safety functions**
  - ***Confinement*** *of radioactive materials*
  - ***Control*** *of operational releases*
  - ***Limitation*** *of accidental releases*
  - ***No control of reactivity control in FUSION required***
    (absence of nuclear chain reactions like in NPP !!!)

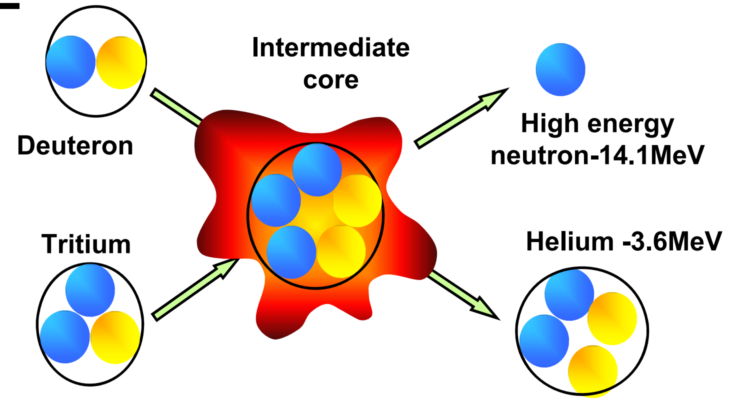
- **Secondary safety functions**
  - *Ensure emergency power shutdown*
  - *Provisions for decay heat removal (potentially passive)*
  - *Control of thermal energy (coolant(-s) enthalpy)*
  - *Control chemical energies*
  - *Control of other potentially likely energy discharges or interactions*
  - *Limitation of airborne & liquid operating releases to environment*

Nuclear safety analyses- Objectives & Operationalization

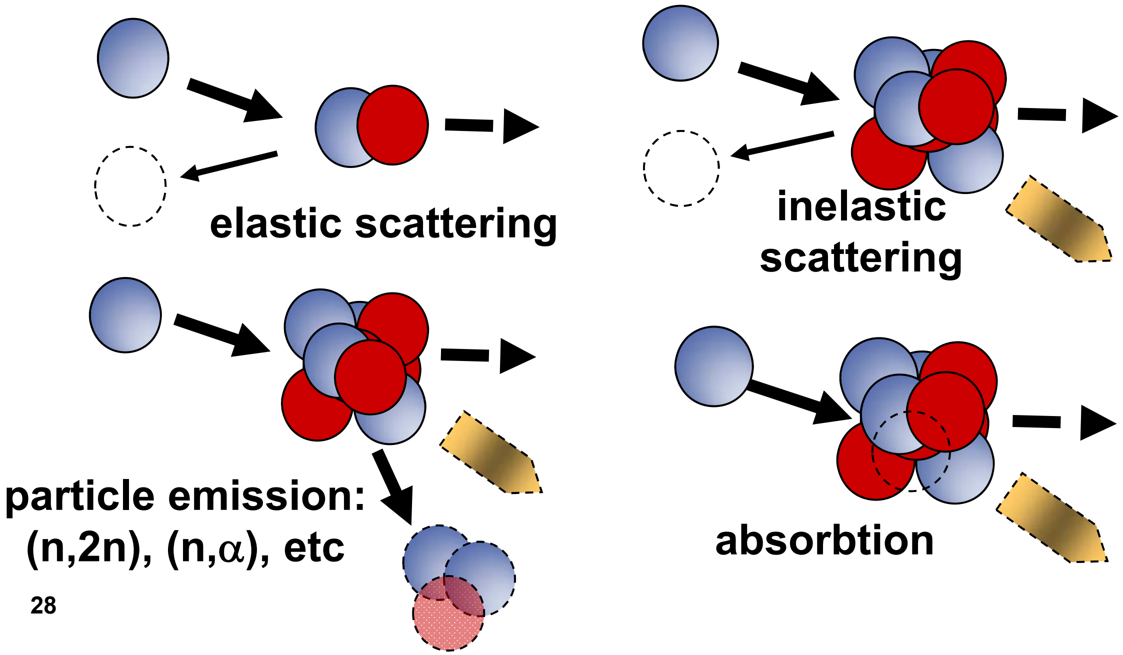
Karlsruher Institut für Technologie

From where does the radio-nuclides arise?

- 14MeV neutrons from D-T reaction



- **Neutron interaction with matter** ➡ excited material states, radiation (α,β,γ)
  ➡ material transmutation (new nuclides)



Crucial parameter:

- **nuclear cross-section σ** (measured in barn=10^{-24}cm^2)
- σ dependent on incident neutron energy (E) and angle (φ)
- Computation by MCNP (Monte Carlo Neutron Particle Transport)

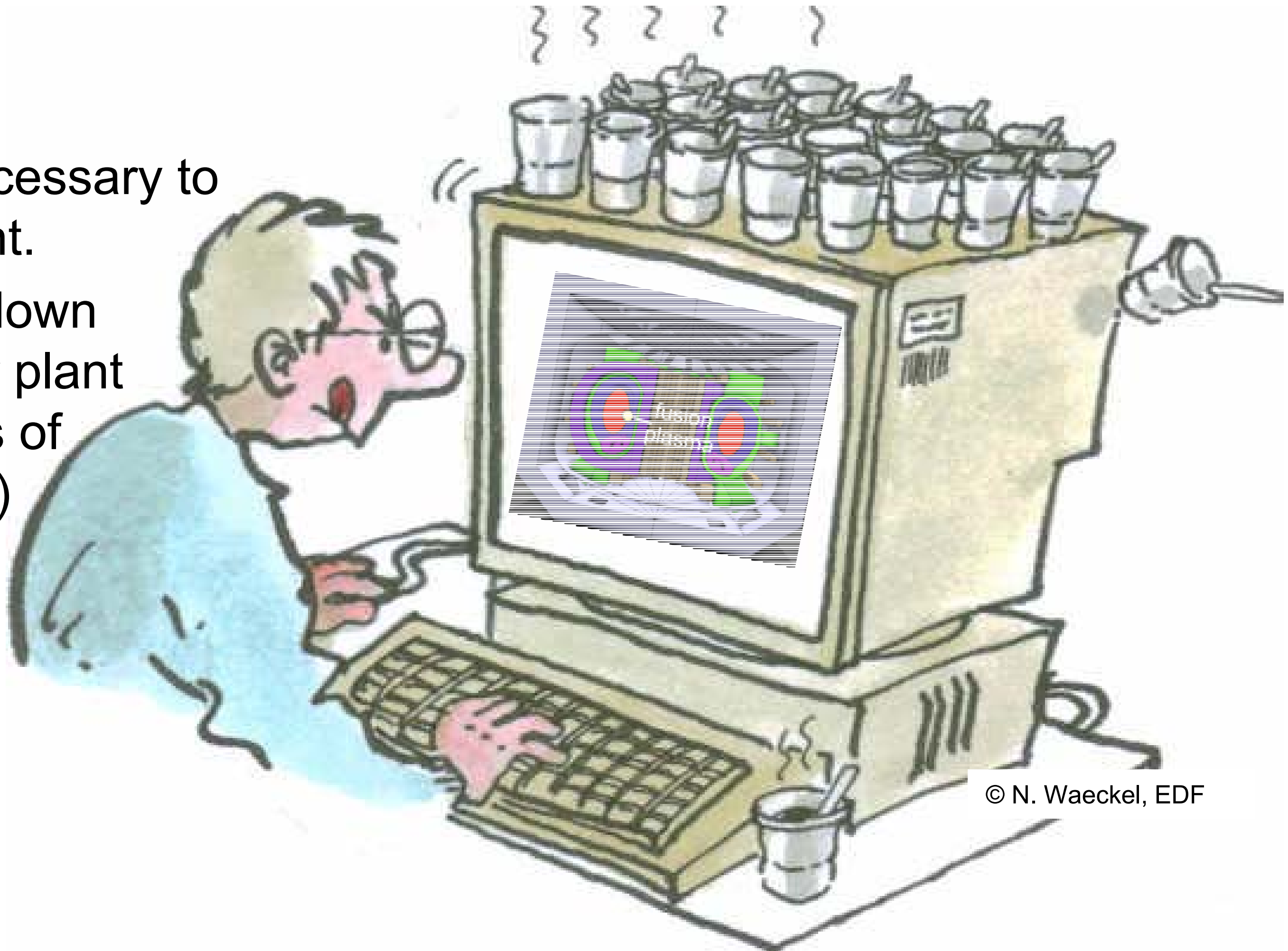
Nuclear safety analyses- Objectives & Operationalization

Where to start for the safety analyses ?

- **built a generic fusion reactor**

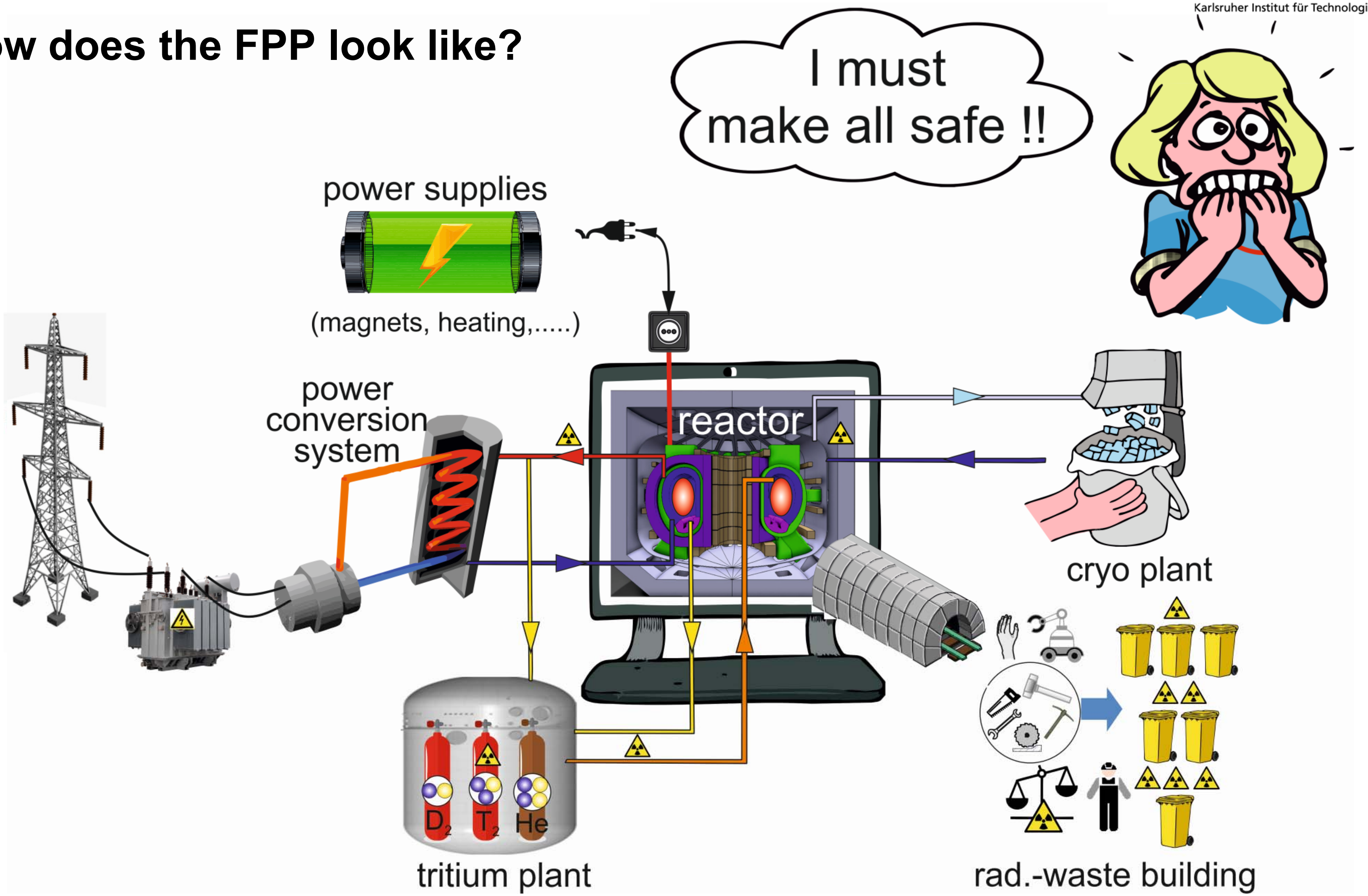
Ingredients

- all components necessary to operate fusion plant.
- ➡ provision of a top down view of the nuclear plant structure (interlinks of major components)



Nuclear safety analyses- Objectives & Operationalization

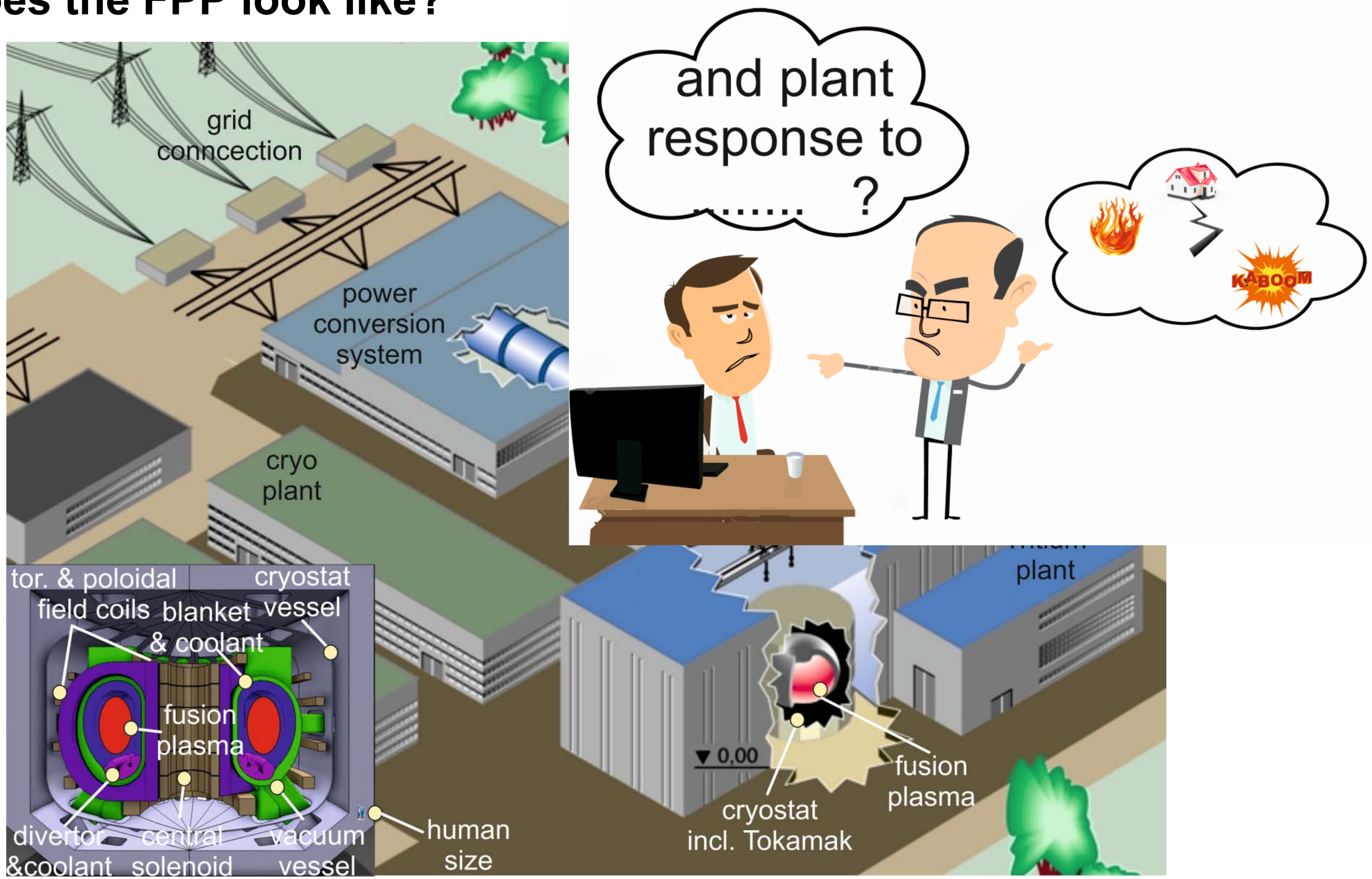
How does the FPP look like?



➡ housing of components by buildings (static barriers)

Nuclear safety analyses- Objectives & Operationalization

How does the FPP look like?



What to do next ?

- **Identify all sources of energy and plant internal radiological potential**

What does this scope ?

- coolant (stored enthalpy)
- radionuclide inventory (tritium, volatile fission products, activated corrosion product(-s))
- chemical reaction(-s)
- nuclear decay heat (operation time, materials used)
- ➡ **as for nuclear power plants (NPP)**
- fusion plasma (stored energy)
- magnetic energy (coils)
- cryo-inventory
- heating systems
- ➡ **specific fusion power plant (FPP)**

Sufficient ? NO !!!

- release time, fractions,
- detection time, capability

DONE ? NO !!!

Nuclear safety analysis-Master Logic diagram (MLD)

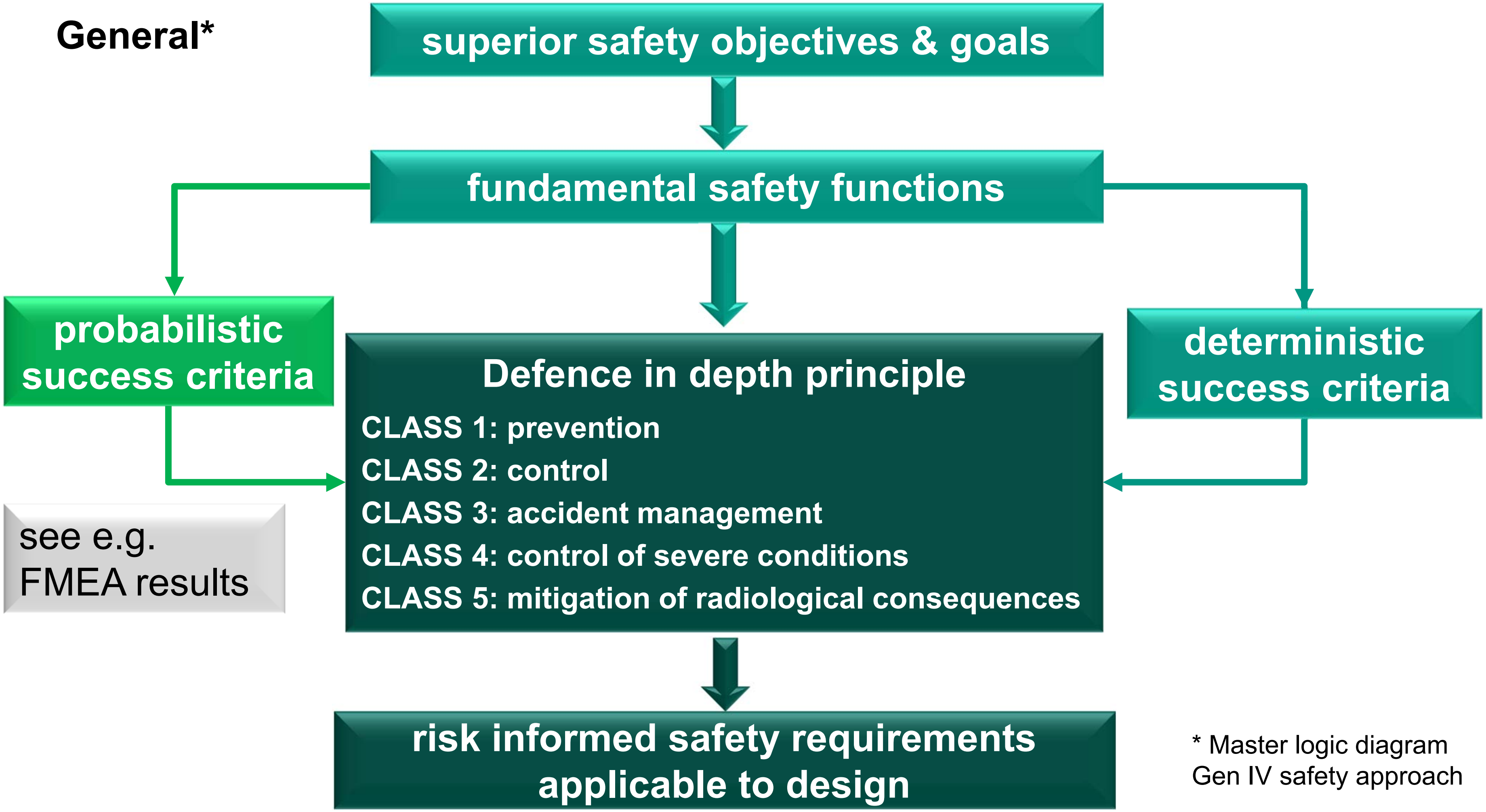
Karlsruher Institut für Technologie

MLD-sequence

- ‘top-down’ view of nuclear installation as whole system ➡ global perspective of possible failures through a global fault tree
- global fault tree contains elaboration of failure combinations via logic gates (and/or functions)
- start with **top-level event** “excessive off-site releases” (i.e. radiological doses in excess of regulatory limits) and further break-down to the contributing elements:
  (1) release origin,
  (2) release paths and species (tritium, activation products, dust, ….),
  (3) barriers that would have to fail to open release path,
  (4) safety functions that protect these barriers,
  (5) failure events that could degrade/disable these safety functions.
- at (3), (4) AND gates appear ➡ presence of barriers protected by multiple safety functions (more than one failure required to cause radiologic release) .
- MLD approach = plant-level functional nature (less detailed than FMEA !!!!).
- MLD list of failure event types = alternative approach to FMEA,
  used to obtain completeness in identification of all PIEs.

Nuclear safety analysis- Master Logic diagram (MLD)

General*

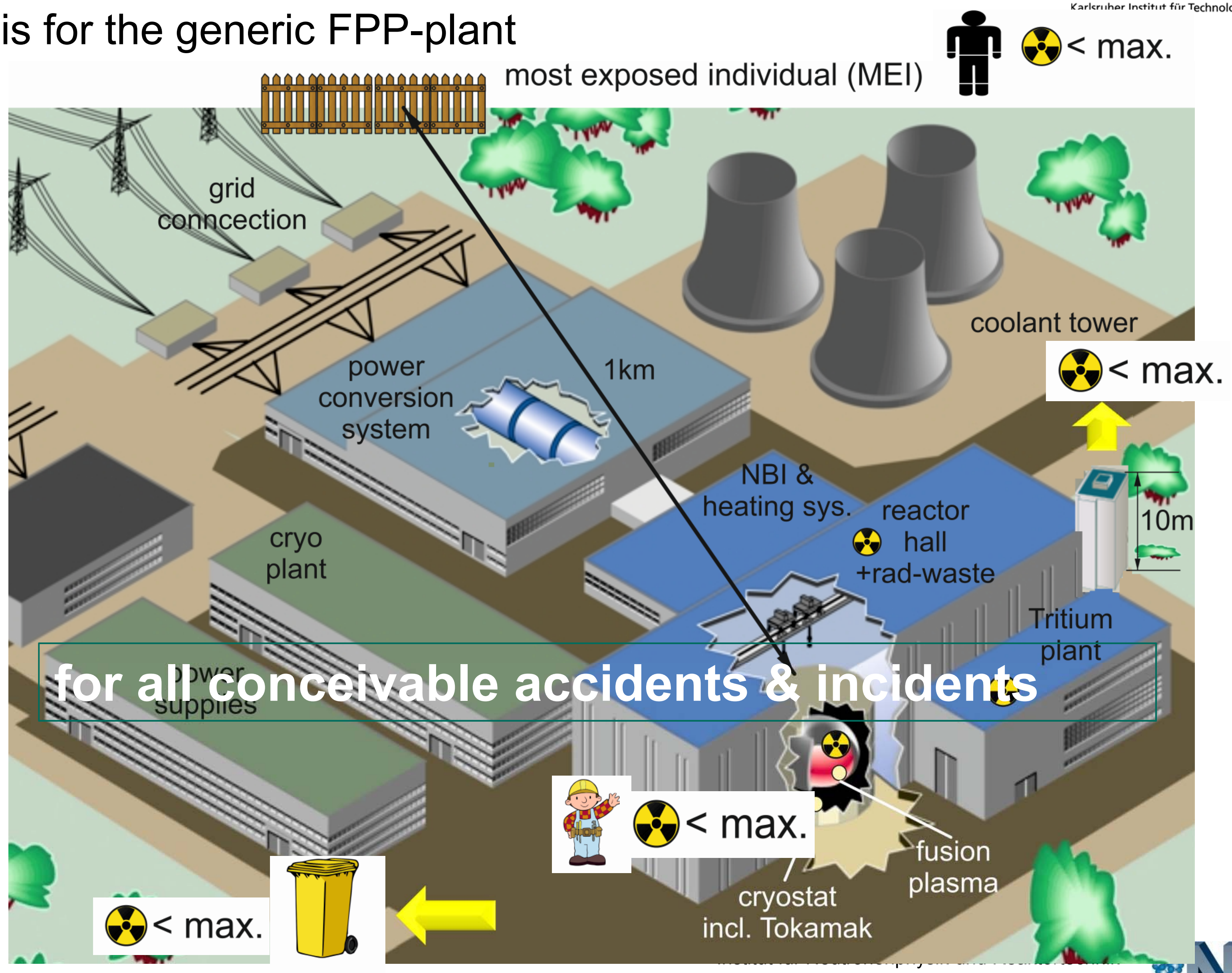


* Master logic diagram
Gen IV safety approach

➡ applied in hierarchical from plant to subsystem level

Nuclear safety analysis- Master Logic diagram (MLD)

- Analysis for the generic FPP-plant



Elements of the safety analysis

- event tree (sequence) analysis,
- fault tree analysis,
- dependent failures,
- personnel actions,
- internal impacts,
- external hazards (earth quake, flooding , terrorist attack,….)
- documentation and presentation of results.

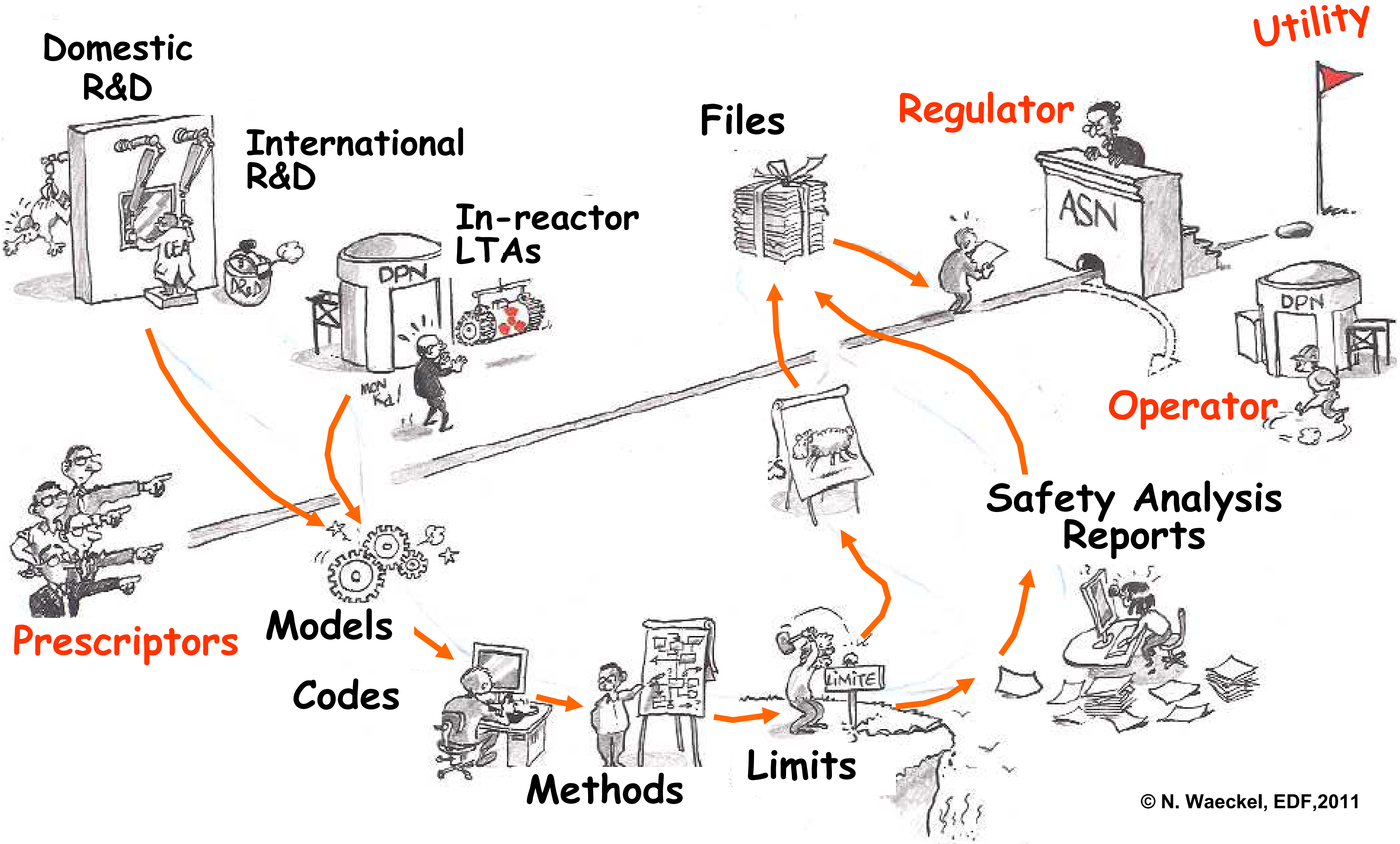
Nuclear safety analysis- Safety demonstration

Granting of a nuclear operation license scopes *

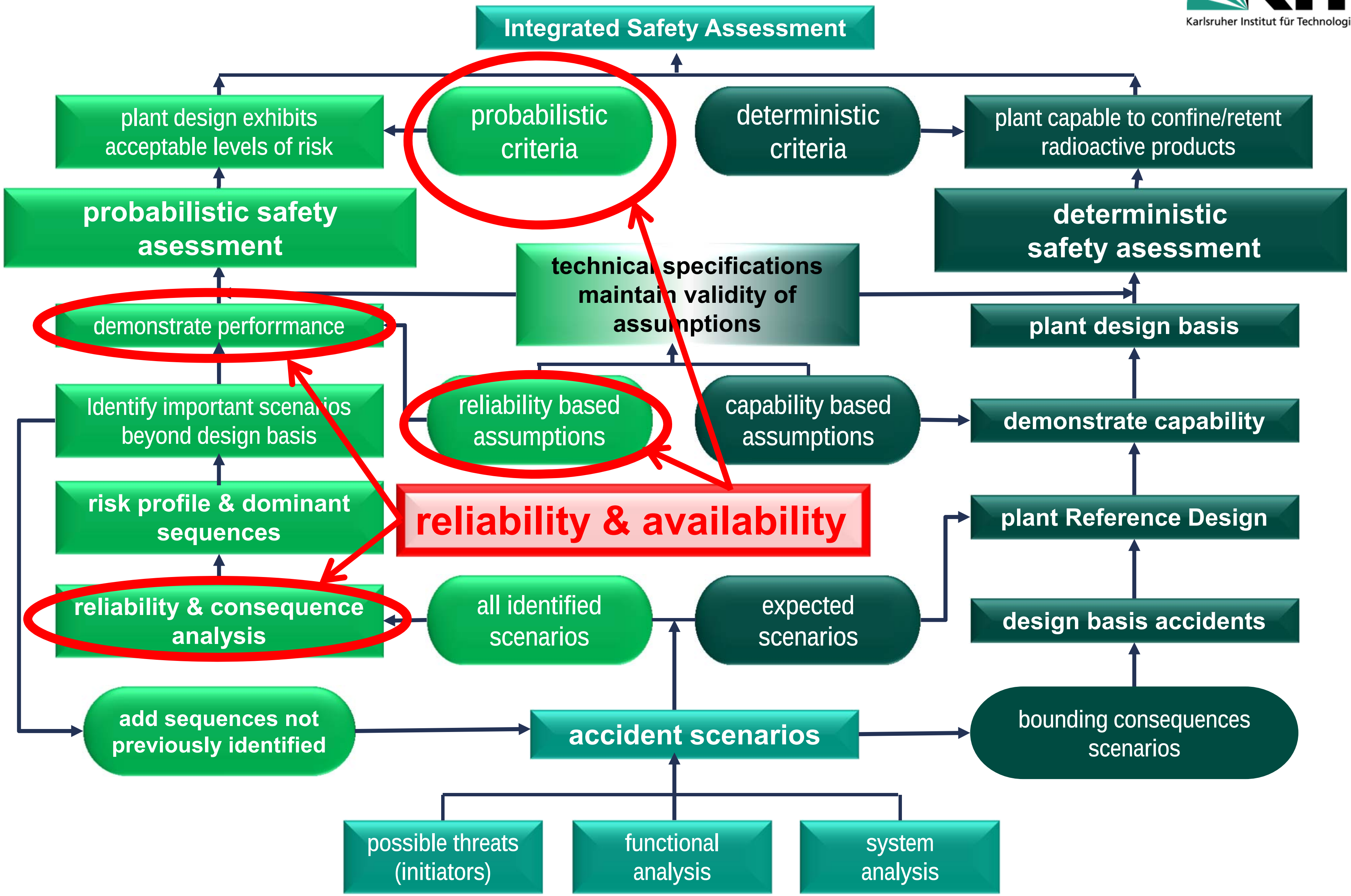
- safety report (essential design plant characteristics) and safety status report,
- system descriptions (specifications), circuit diagrams for safety-related systems,
- component descriptions & specifications, component basic position lists of safety-related components,
- building plans, installation plans, piping isometrics,
- instrumentation & control documents (reactor protection report, function block diagrams, control diagrams, measuring device characteristics, signal processing with limit alarm settings,
- emergency electricity budgets,
- system dynamic investigation of transients, reports of loss of coolant accidents,
- used effectiveness conditions and constraints,
- operating manual, testing manual,
- documentation of maintenance concept and implementation
- **documentation of the safety status analysis,**
- management system and operational reports,
- emergency manual, documentation of emergency exercises,
- information on sources for determination of reliability indices,
- information on disorders (legacy body) and reportable events.

* Bundesamt für Strahlenschutz, 2005, Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke

Nuclear safety analysis- Safety demonstration



Safety analysis: Integrated Safety Assessment



Nuclear safety analysis- Safety demonstration

Safety functions related to fusion power plants (FPP)

- **Primary safety functions**
  - ***Confinement*** *of radioactive materials*
  - ***Control*** *of operational releases*
  - ***Limitation*** *of accidental releases*

  ➡ ***No control of reactivity required (no nuclear chain reactions as in NPP !!!)***

- **Secondary safety functions**
  - *Ensure emergency power shutdown*
  - *Provisions for decay heat removal (potentially passive)*
  - *Control of thermal energy (coolant(-s) enthalpy)*
  - *Control chemical energies*
  - *Control of other potentially likely energy discharges or interactions*
  - *Limitation of airborne & liquid operating releases to environment*

Dose concept – 1(5)

- all exposures shall be kept **As Low As Reasonably Achievable,** economic and social factors being taken into account*
- **§ 5 Dose Limits*:**
  20 mSv per year for occupationally exposed persons,
  1 mSv per year for members of the public.

persons under the age of 18

1 mSv per year

<u>members of the general public</u>

1 mSv per year

<u>occupationally exposed persons</u>

20 mSv per year

occupational life dose

400 mSv per year

* ICRP Recommendations 60, 103,
Directive 96/29/EURATOM

dose

Dose- concept - 3(5)

HURLY-BURLY?

Ambient Dose

H'(0,07)

Dose Equivalent

Gy

Kerma

mSv

Ion Dose

Tissue Dose

Absorbed Dose

H*(10)

Organ Dose

Body Dose

$H_p(10)$

Effective Dose

W_T

Committed Dose

$H_P(0,07)$

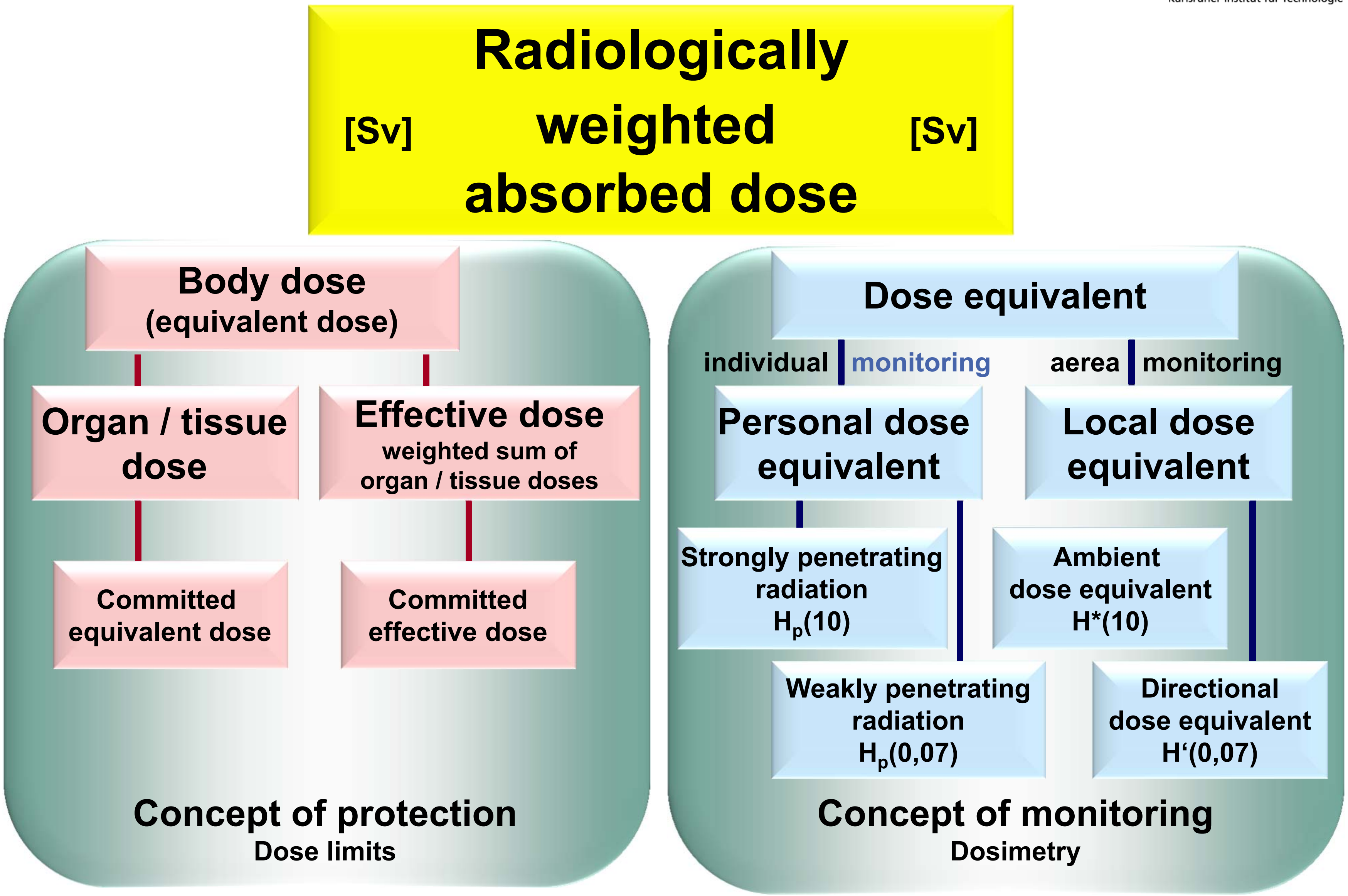
Equivalent Dose

Directional Dose

D

Local Dose

Dose Concept - 4(5)



Dose concept - 5(5)

Radiation Protection

- DOSE usually applied in radiation protection is a measure for the risk of (stochastic) effects caused by radiation.
- measuring unit: Sievert (Sv)

Representative values for effective dose

fatal dose	7000 mSv
threshold dose for deterministic health effects	500 mSv
X-ray tomography torso	up to 20 mSv
annual average of radiation exposure in Germany	4 mSv
annual dose limit for members of the general public	1 mSv
head radiography	0.1 mSv
threshold dose for stochastical health effects	0 mSv

Risk caused by ionising radiation

- dose determines the risk of stochastic health effects.
- risk of fatal cancer: 5 % per Sv (0,005 % per mSv)
- risk of heritable effects: 1 % per Sv (0,001 % per mSv)
- (e.g. exposure of 1Million persons with 1mSv **each** causes 50 cases of fatal cancer.)

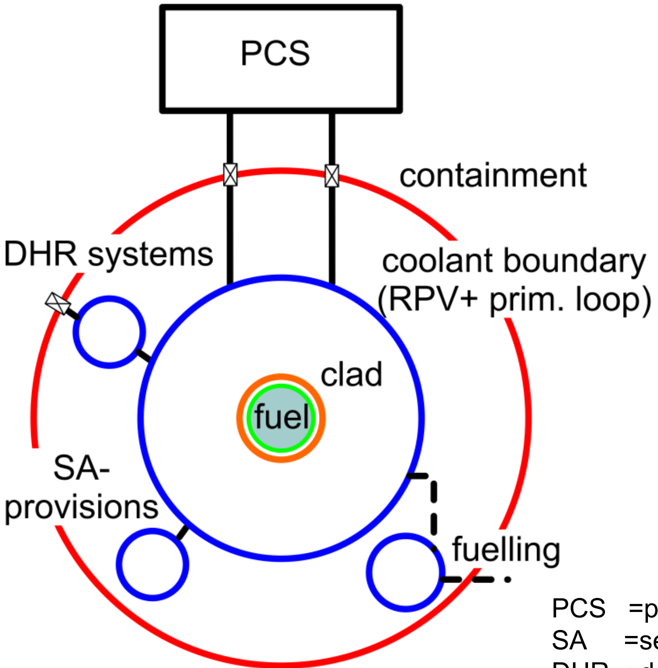
Fusion Safety Concept – NPP vs. FPP 1(3)

Nuclear Power Plant (NPP)

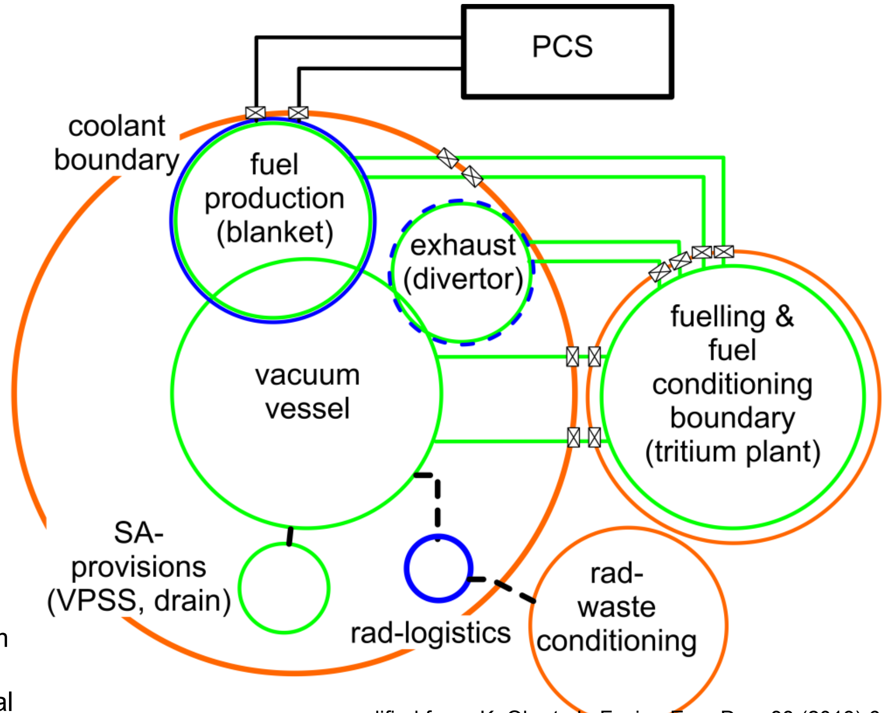
- nested physically static barriers
- high volumetric power density
- off-site fuel conditioning
- criticality prevention measures
- 1% of P_{th} decay power
- very high radioactive inventory

Fusion Power Plant (FPP)

- 2 static but also dynamic barriers
- low volumetric power density
- on-site fuel management
- criticality arguments absent
- 0.6% of P_{th} decay power
- high radioactive inventory (many mobile, different nuclide vectors)



PCS =pow. conv. System
SA =severe accident
DHR =decay heat removal
VPSS=vacuum vessel pressure suppression system



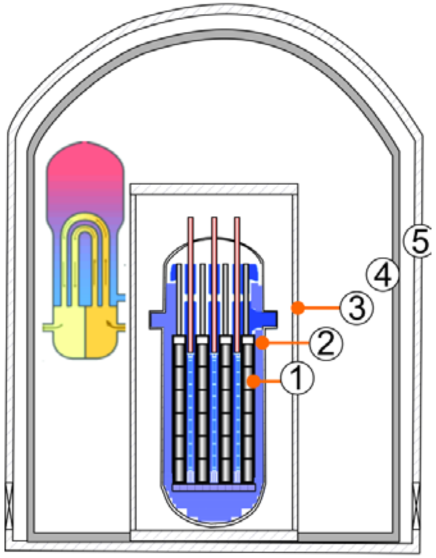
modified from K. Oh et al., Fusion Eng. Des. 88 (2013) 648

Fusion Safety Concept – NPP vs. FPP 2(3)

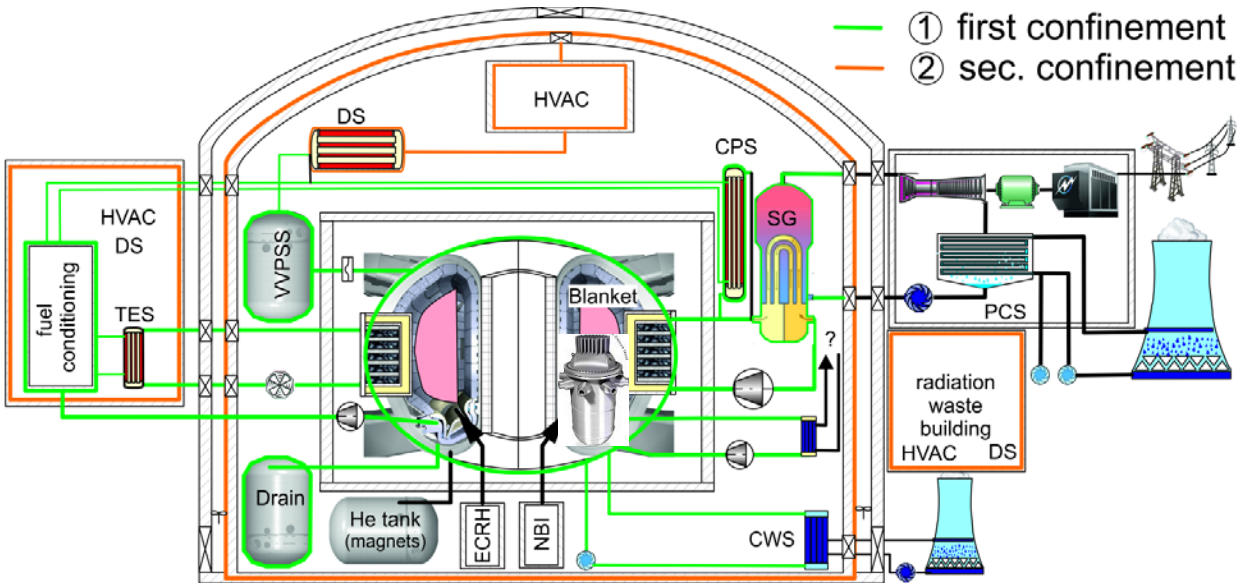
- **Safety functions**

Primary safety functions
- Confinement
- Control of releases
- Limitation of releases

NPP- PWR



FPP



- 4/5 static subsequent enveloped barriers
- Static barriers for release control (mainly related to barriers + PAR+ PRS)
- „practical elimination“ of level 5 by design + core catcher + mitigation chains
- ➡ Compact system, small control volume, high power density, rare release paths

- Two static barriers extended over large scale
- Mixture of static and dynamic barriers (DTS, TES, HVACS)
- Large sets of active + passive systems (but lower inventory and energy content ☺)
- ➡ Large volume, low power density, several release paths, dedicated rad. contaminants

PAR=Passive Autocatalytic Recombiners
PRS=Pressure Relief System

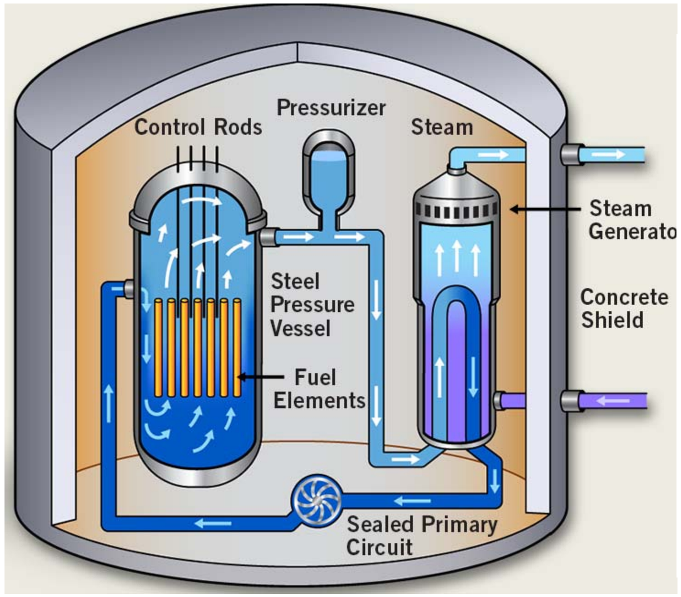
DTS=Detritiation Systems
TES= Tritium Extraction System
HVACS=Heating Vewntilation Air Cooling System

Fusion Safety Concept – NPP vs. FPP 3(3)

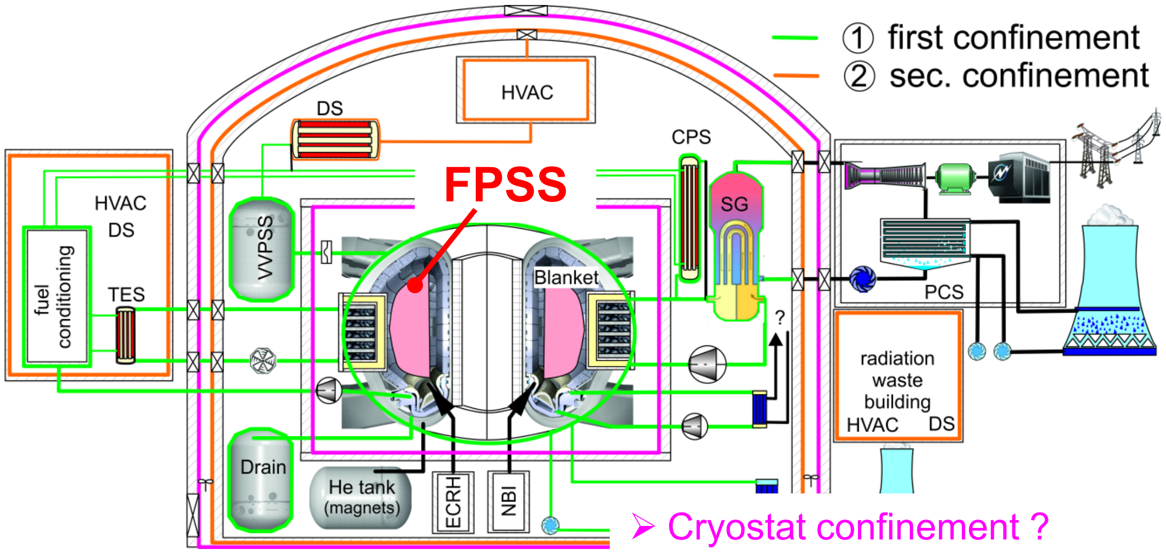
Secondary safety functions

- **terminate nuclear reactions**
- **ensure decay heat removal**
- **controlled chemical, magnetic, and thermal discharge**
- **limit release to environment**

PWR



FPP



- ➢ Cryostat confinement ?
- ➢ Double-walled containment ?

- Design measures (CR, n-poison)
- DHR systems
- not required (limited on-site storage of SA)
- Multi-stage systems for severe accidents

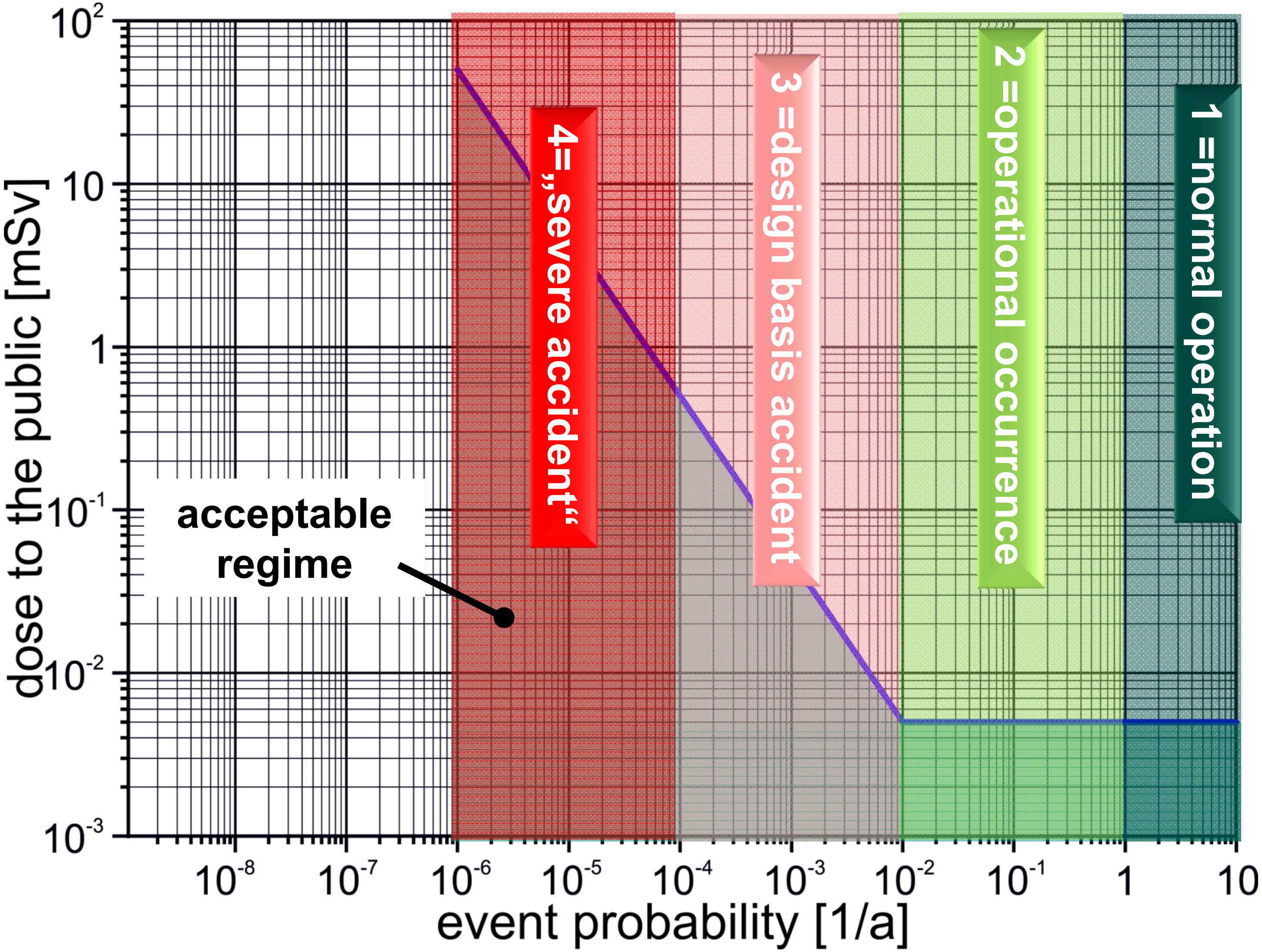
- FPSS (intrinsic feature-but early detection)
- Passive design provisions
- Physically different sub-systems required
- Mobile species to identify

CR=control rod
n=neutron

FPSS= Fusion Power Shut Down System

Fusion Safety Concept – plant state description 2(5)

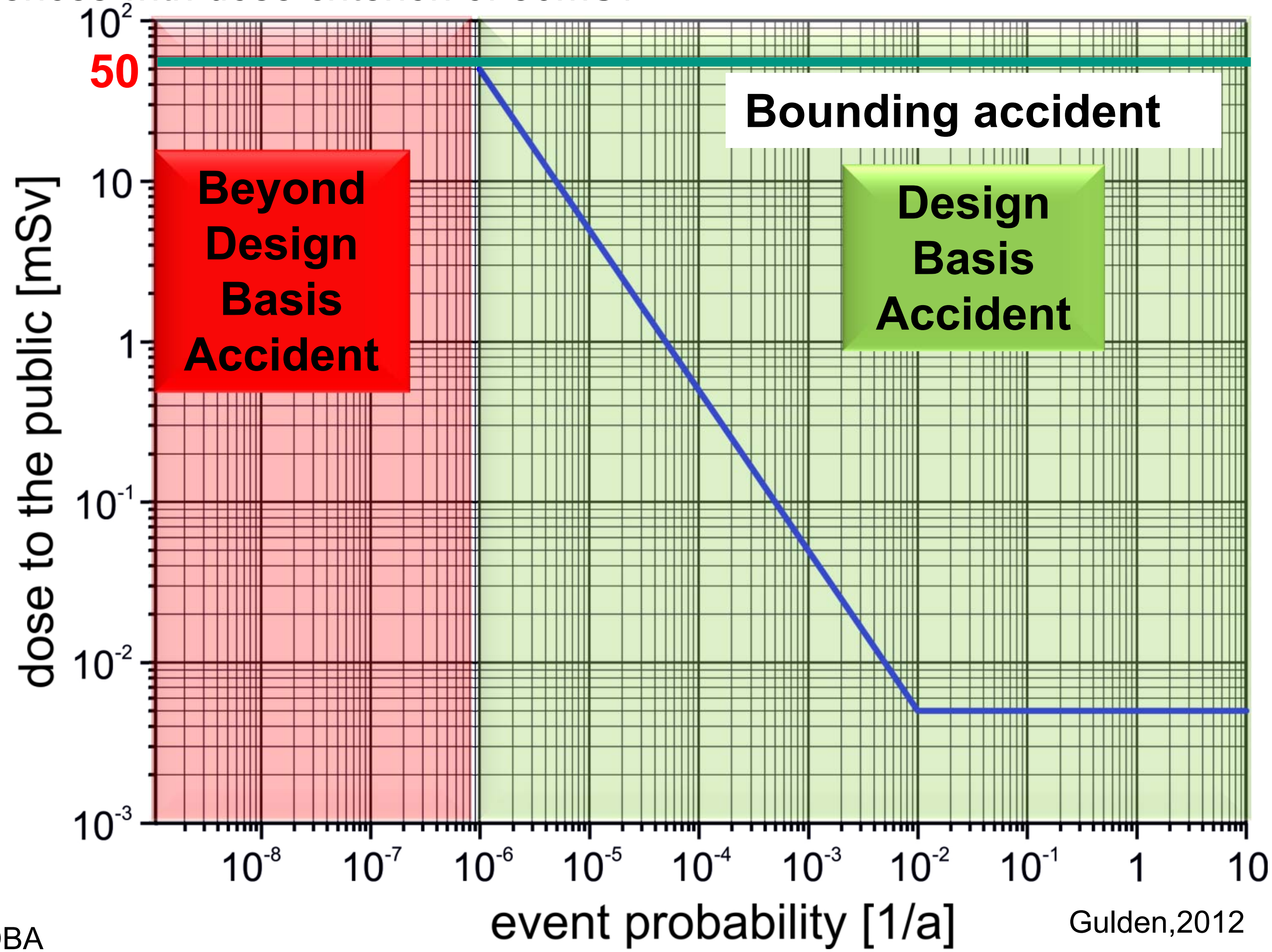
- **Definition of plant state levels in DiD**



*INSAG 2010, WENRA2012

Fusion Safety Concept – plant state description 3(5)

- **Safety risk approach**
  - Discrimination
    Design Basis Accidents (DBA) ⟺ Beyond Design Basis Accidents (BDBA)*
  - Bounding accident sequences with dose criterion of 50mSv



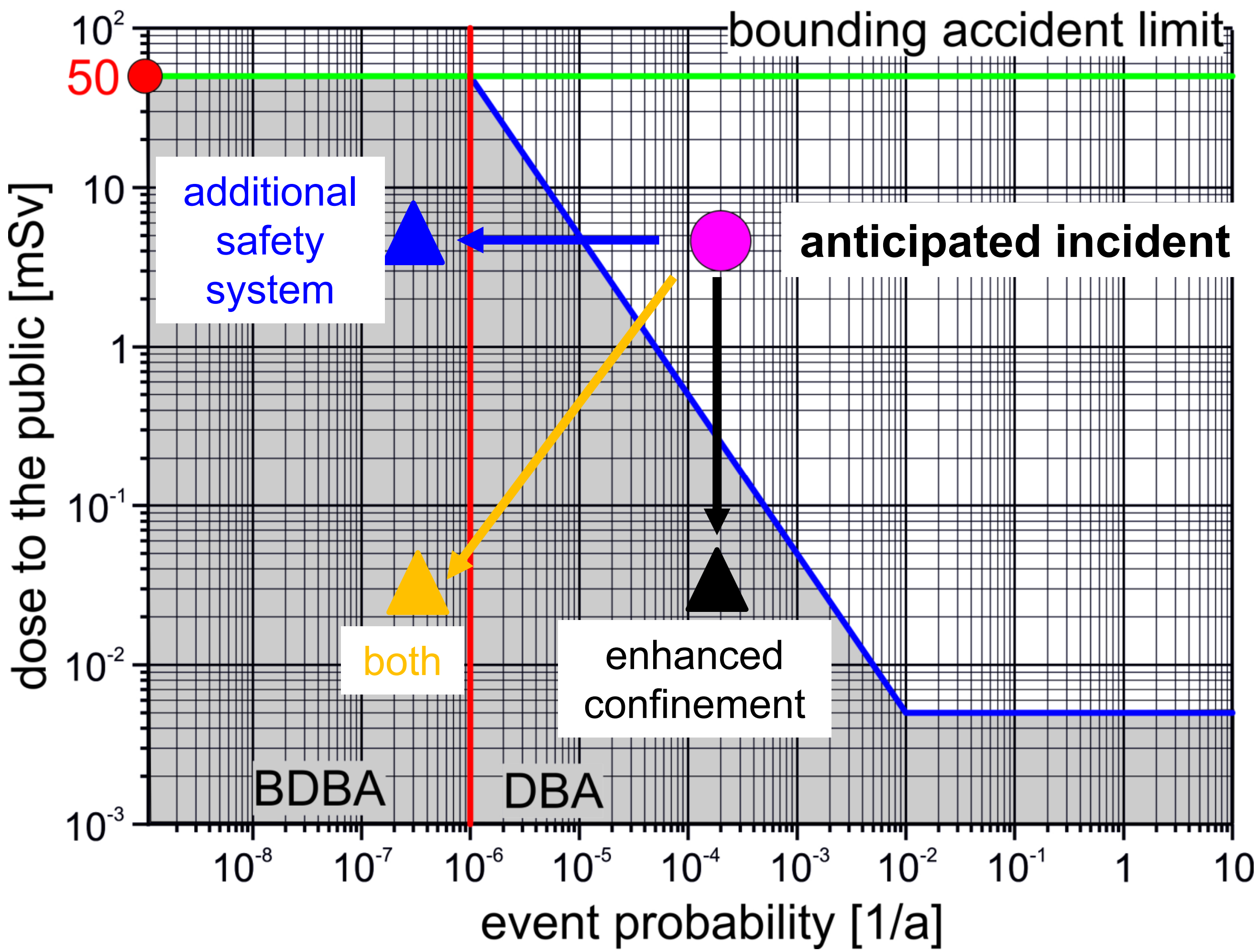
Dose limits Germany

public	worker	Evac. dose
1mSv/a	20mSv/a	100mSv/a
20µSv/w		2mSv/w
3µSv/d	0,3mSv/h	0,3mSv/d
mean nat. dose 1mSv/a		

* Design Basis Extension in ITER ~ BDBA

Fusion Safety Concept – plant state description 4(5)

- **Safety risk approach**
  - Mitigation into the acceptable risk zone by countermeasures
  - Diminution of dose rate by enhanced confinement



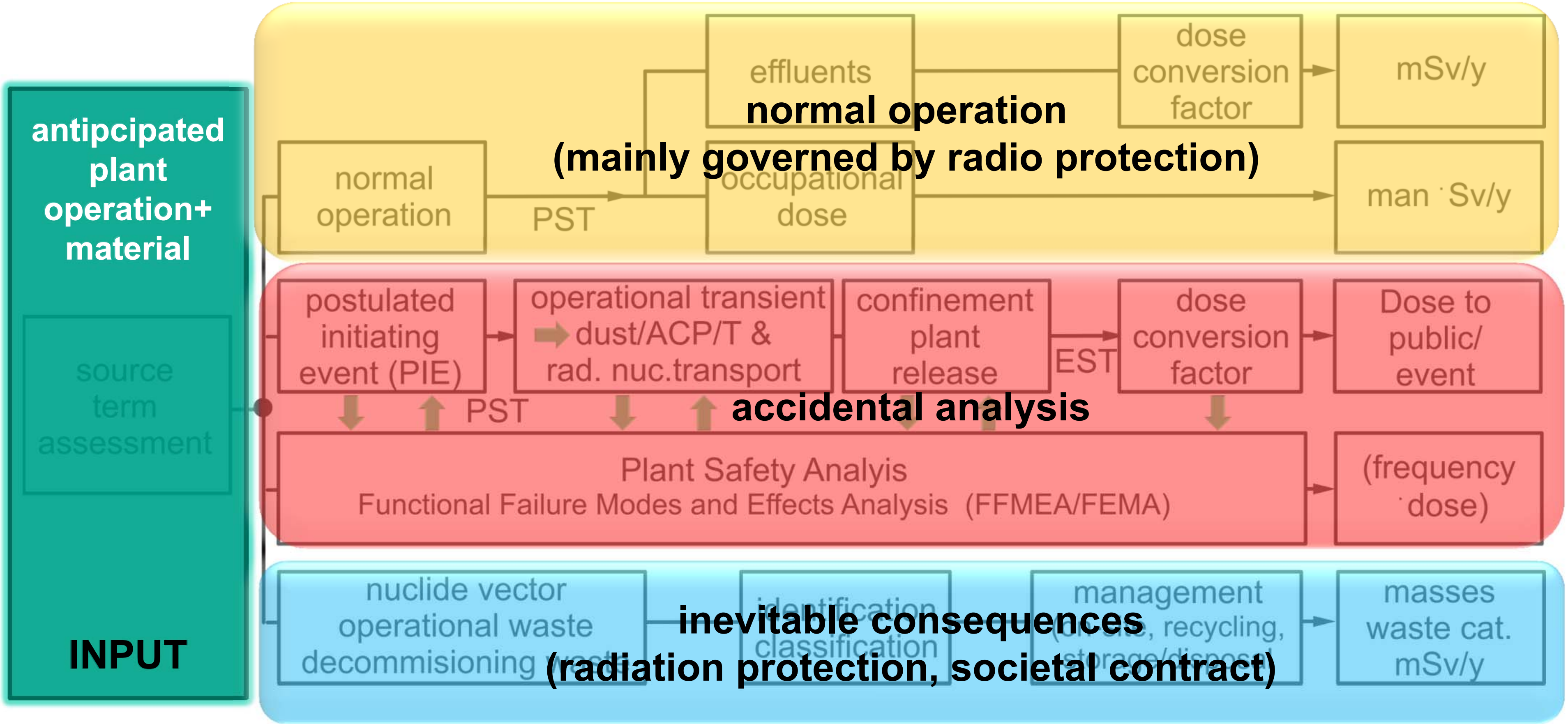
Gulden,2012

Fusion Safety Concept – plant state description 5(5)

Systematic Safety Analysis (SSA) - Success criteria

■ normal operation	dose to worker on site	< limit
■ accidental analysis :	worst dose to public (MEI)	< limit
■ consequences:	mobility in long term storage	< limit (what ?)

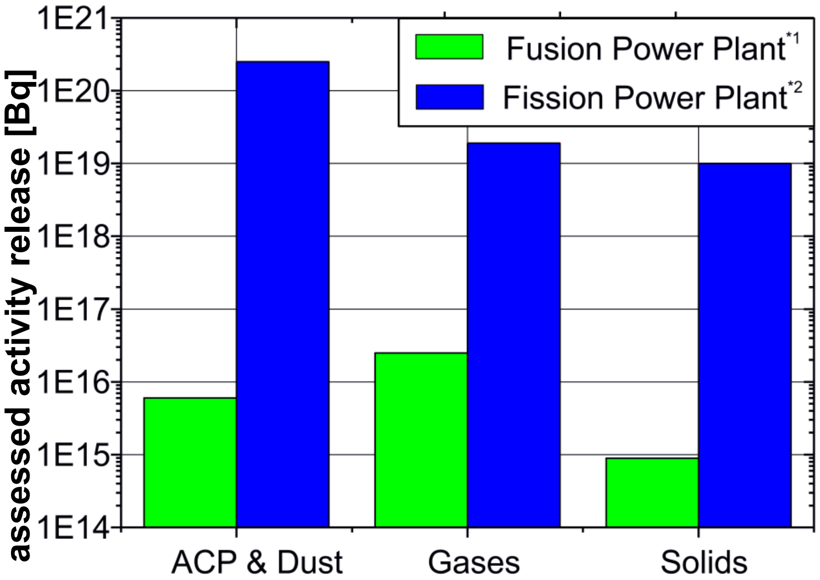
➡ **all to be met**

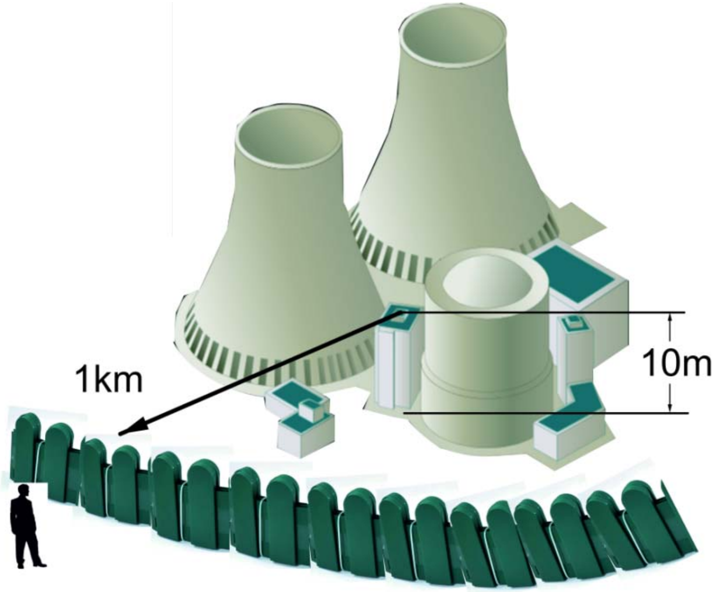


PST=process source term
EST=environmental source term

Fusion Safety Concept – NPP vs. FPP

- **Worst dose rates estimates (for the same power)**
  - Different source terms
    - *Fusion: tritium, dust, activation products, Activated Corrosion products (ACPs), neutron sputtering products. Tritium inventory in the Vacuum Vessel (VV) ~1kg.*
    - *Fission nuclides of PWR: Iodine, Cs-137, noble gases, aerosols, ...*
  - NPP: effective dose of DBA ≤ 50mSv. BDBA e.g. 100mSv ➡ **evacuation**
  - Fusion: bounding accident ≤ 50mSv ➡ **no evacuation**



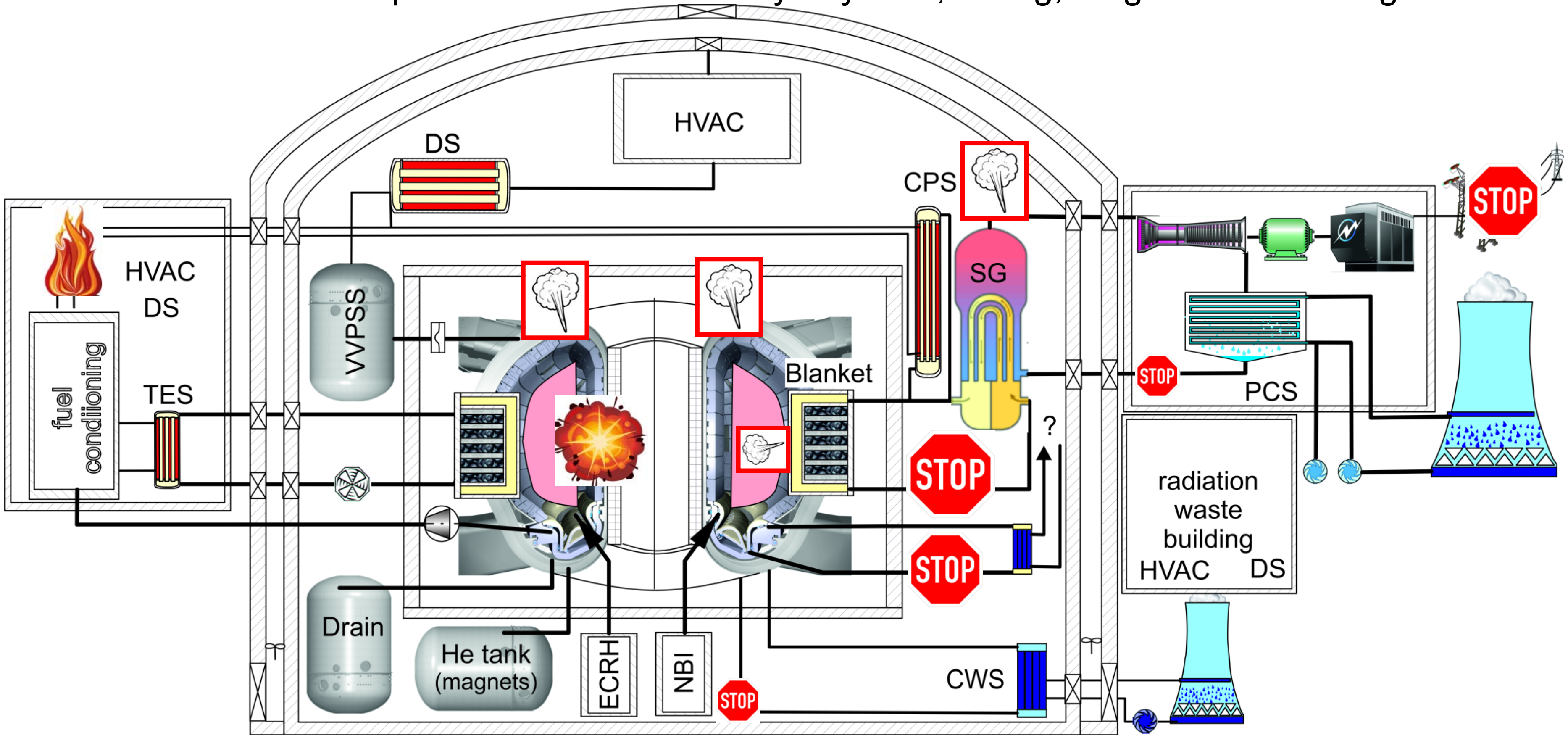


accidental releases FPP by in-plant energies several orders of magnitude lower than in NPPs.

*1 Karditsas,PPCS,2004
*2 Broeders, KANEXT,2011

Fusion Safety Concept – challenges safety analyses

- **Postulated initiating events (internal events)**
  - similar as in nuclear power plants such as
    - Loss of flow accident (LOFA),Loss of offsite-power (SBO), Leaks (VV, Primary System, …), Fire & explosion
  - additional fusion specific events: loss of cryo-system, arcing, magnets ➡ affecting barriers

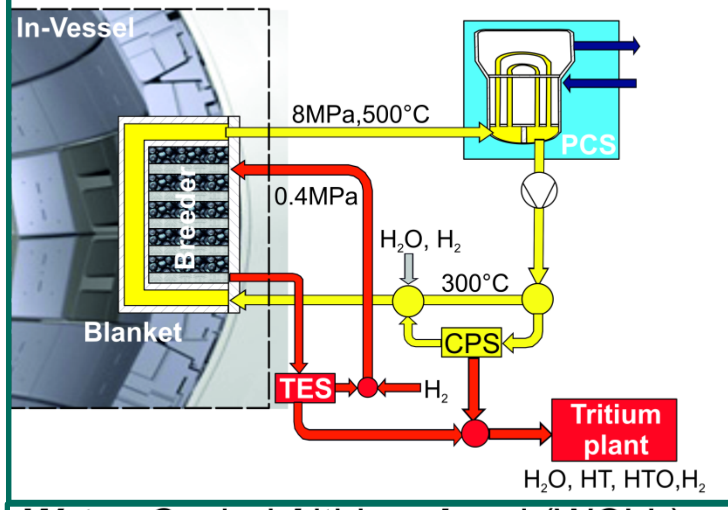


  - analyses shows: strongest radiological impact arises from thermo-nuclear core
- ➡ **Blanket**

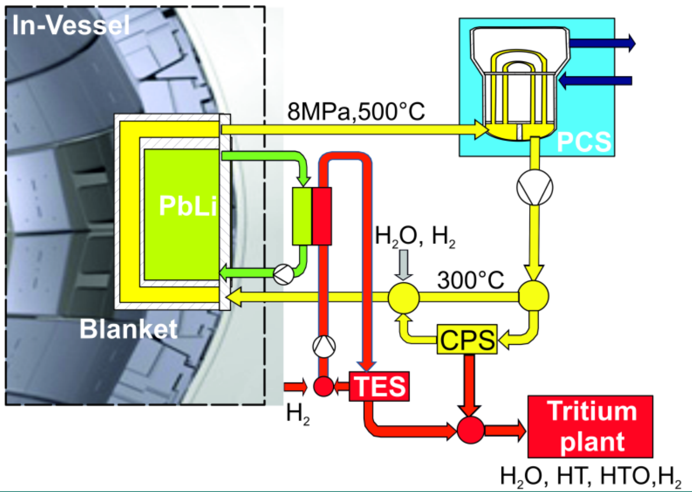
Fusion Safety Concept – challenges safety analyses

- focus on performance of thermonuclear core - Blanket (~83%)

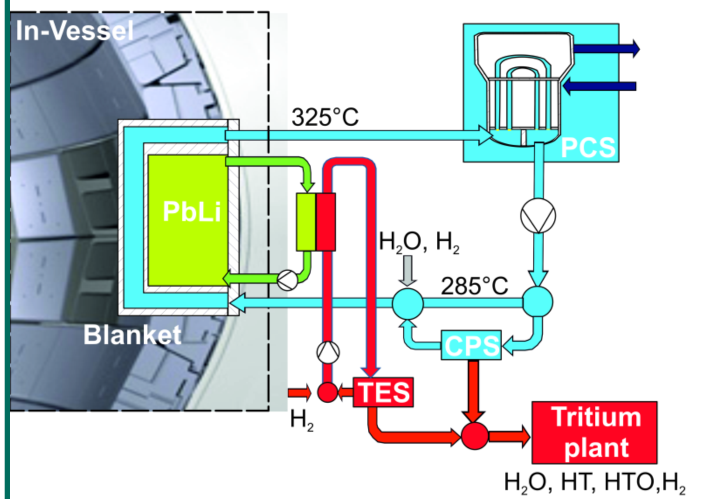
Helium-Cooled Pebble Bed (HCPB)



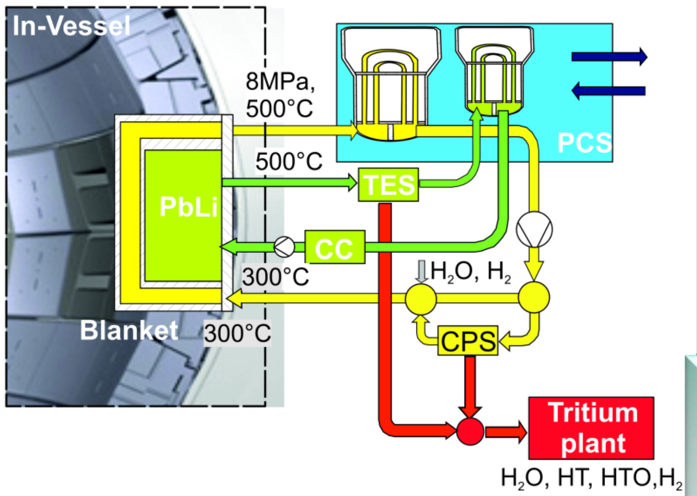
Helium-Cooled Lead Lithium (HCLL)



Water-Cooled Lithium Lead (WCLL)



Dual-Coolant Lithium Lead (DCLL)



Concept features
- ❑EUROFER –struct.
- ❑PFC –Material –W

Differences
- ❑Coolant(s)
- ❑Neutron multiplier
- ❑Temperatures
- ❑Neutron wall load
- ❑…..

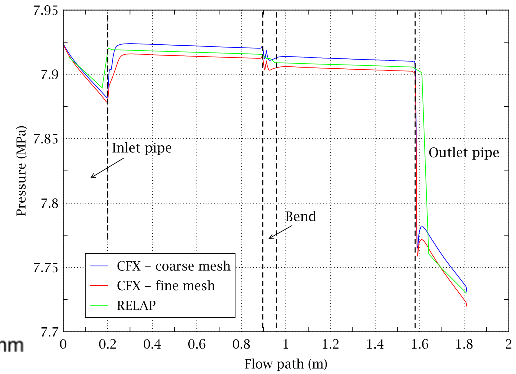
Consequences
- ❑diff. enthalpy
- ❑diff. chem. potential
- ❑varying components

PCS=Power conversion system
TES=Tritium extraction system
CC =Chemical control
CPS=Coolant purification system

Fusion Safety Concept – challenges safety analyses

Deterministic safety assessment :

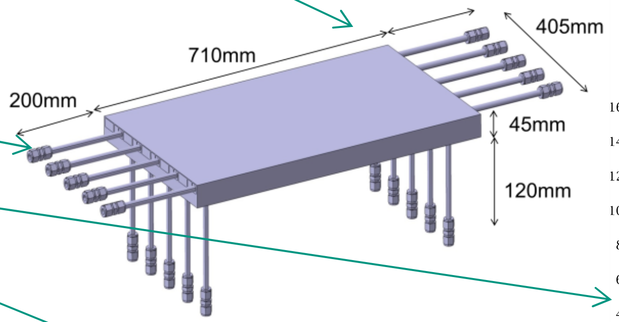
PIE : Loss of flow accident (LOFA) in the first wall (FW)



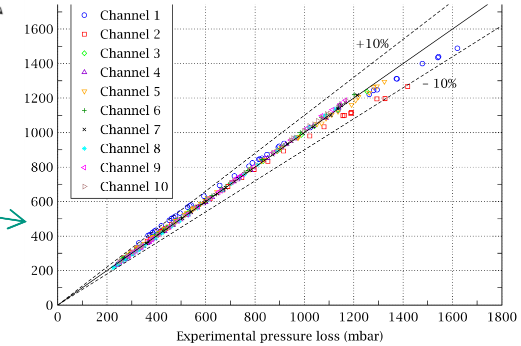
Sequence

- CFD model set-up for one / two channels
- Reduction to simplified model – system code

➡ ***Verification***

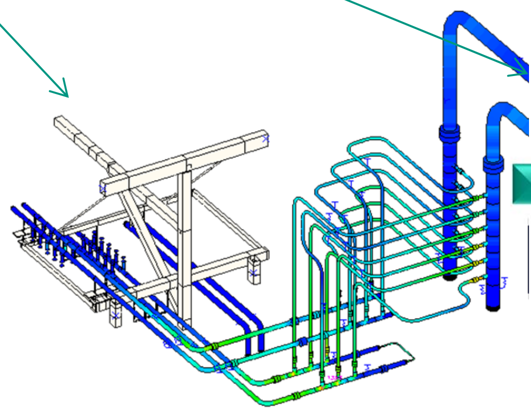


- Experimental development
  - Design of the test mock-up
  - Isothermal validation



- Integration in the helium loop
- Full scope single experiment
- System analysis
- Full 3D safety analysis

➡ ***Validation***



Challenges FPP Safety Analysis

- extension of existing nucl. safety codes to fusion specifities
- generation of a validation data

if single component analysis verified

➡ transfer to entire reactor (0 to 1D formulation)

next slide

Fusion Safety Concept – challenges safety analyses

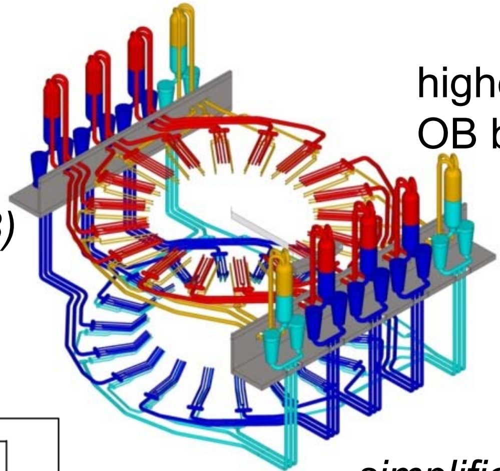
Karlsruher Institut für Technologie

PIE :Loss of coolant flow (LOCA) in the cooling plate of the breeder unit / FW

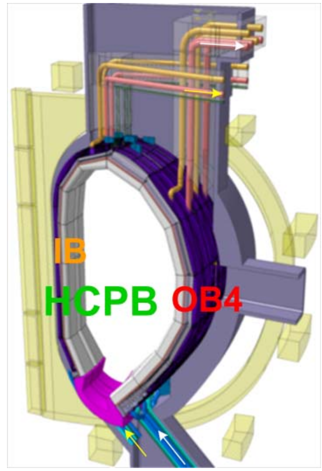
- **Partial system analyses**

HCPB in 18 sectors – primary heat transfer system (PHTS) design:

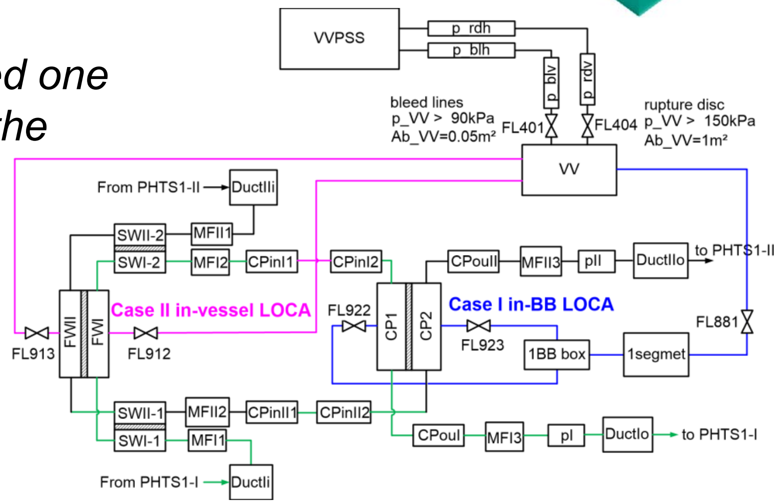
- *6 loops outboard (OB), 3 loops inboard (IB)*
- *1 OB-loop 3 sectors / 1 IB-loop 6 sectors*
- *1 sector: 3 OB segments & 2 IB segments*



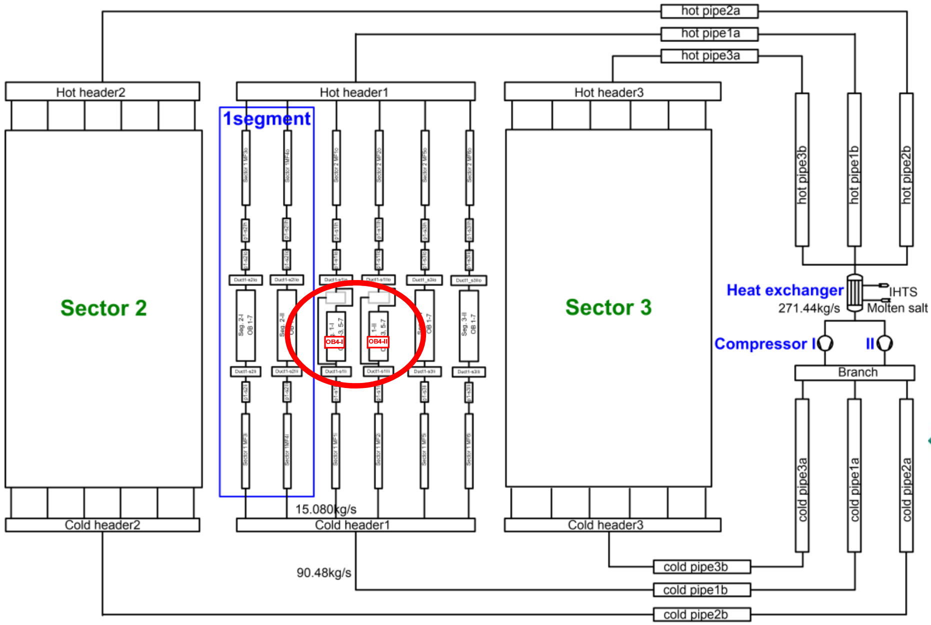
highest loaded OB blanket



simplified blanket model depiction (OB4)



simplified one loop of the PHTS



© Jin, Di Marcello, Stieglitz, ISFNT-2017

Fusion Safety Concept – NPP vs. FPP

- Most severe event = LOCA at end of life (where activation is highest and decay heat as well)

Goal

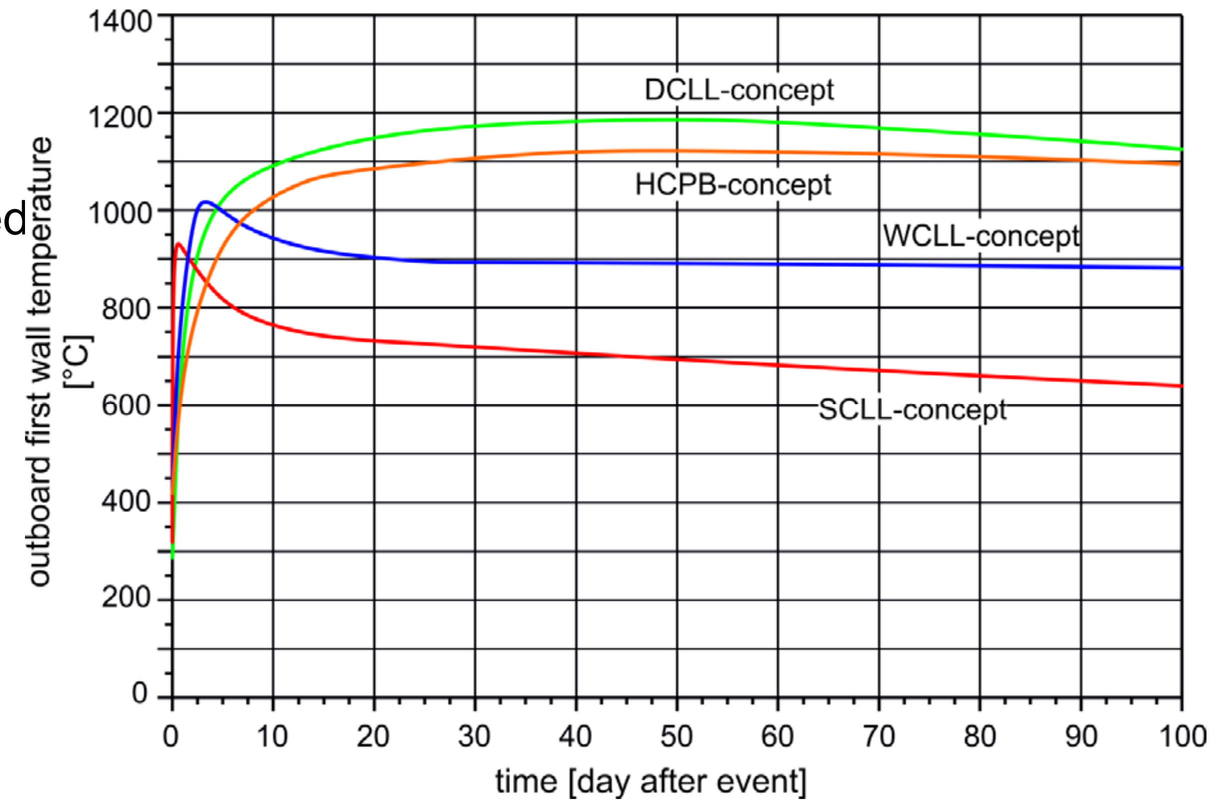
- Safe heat removal without loss of functional integrity or confinement

Example:

- PIE: LOCA in PCS and simulateneous station black out (with anticipated failure of emergency power supply

Result:

- temperatures remain on long term on levels in range of preventing failure and rad. release
  (although thermal deformations will appear not allowing to restart plant)



Note:

- Any safety demonstration design and system (including sec. site) dependent !

Summary

- general **definition** of **risk analyses** terms and **methodologies** for safety assessments.
- **objectives**,**elements** of a **safety demonstration** of **nuclear facilities**.
- **transfer in fusion power plant (FPP) safety concepts**

Fusion Power Plant (FPP) –Current safety concept &status

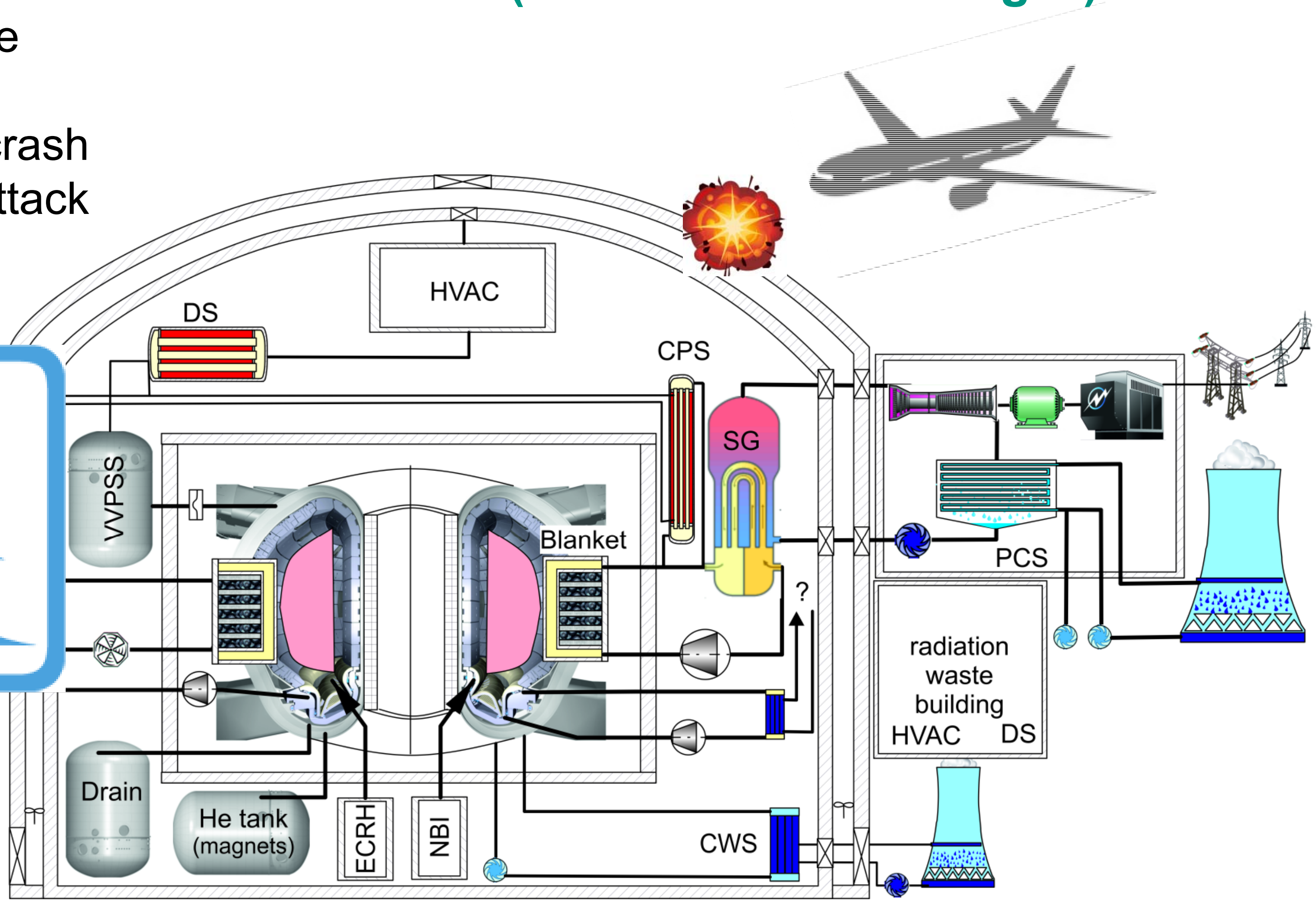
- FPP safety concept relies on **state-of-the-art safety concepts** for nuclear installations.
- Similarities and differences between safety concepts of fusion and fission.
- **Plant-internal events do not** lead to **off-site evacuation**
- **Systematic assignment** of measures & installations to the different levels of defence, But, an **adequately detailed design level** for **FPP** is not reached.Safety function “cooling” demands detailed design of in-vessel components (blanket & others) and necessitates demonstration of safe decay heat removal ➡ **development of validated tools mandatory.**

Open Aspects

- **External hazards** must be **included** in the future safety analysis (site dep.)
- **Waste management** not enveloped treated (but first steps made :material encyclopedia is established defining upper limits of elements to be used, detritiation techniques,….)

Fusionreactor DEMO - severe accidents?

- **Safety against external hazards- (“Fukushima challenge”)**
  - Earthquake
  - Flooding
  - Air plane crash
  - Terrorist attack



➡ more stringent rules for robustness demonstration against external hazards for NPP (➡FPP) are expected

Institut für Neutronenphysik und Reaktortechnik