Safety II and Nuclear Power

2019 International Nuclear Atlantic Conference
INAC-2019

Motivation

What is safety?

Why accidents happen?

Motivation

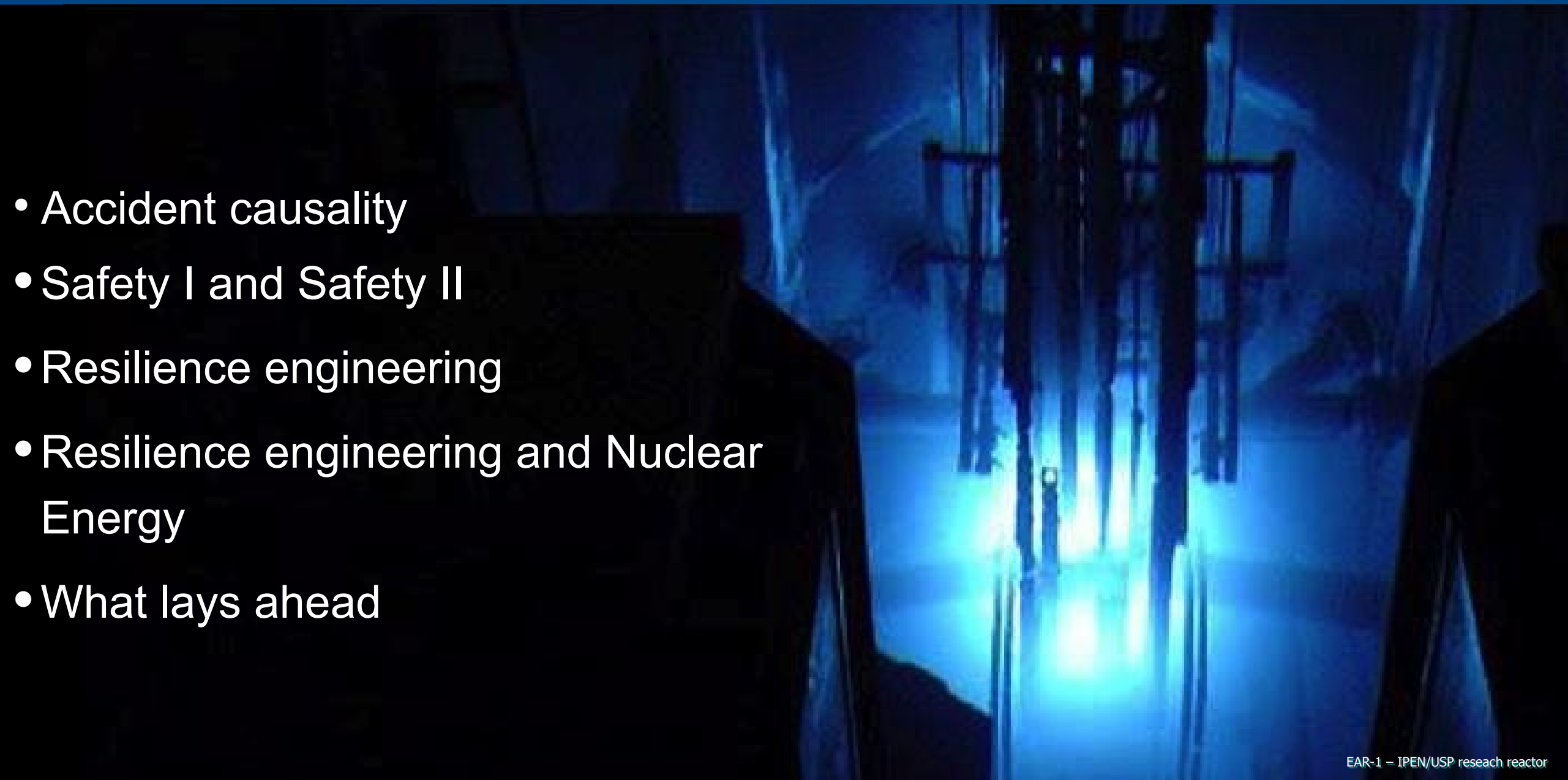
Safety II:

- **Untoward events**: **combination of a number of conditions**, not the consequence of the failure of a single function or component.
- **Failures and successes are equivalent**, so addressing failure mechanisms is futile.
- Failures and successes originate form **performance variability** on the different levels within the system.
- **Only the outcomes separate** one from the other.

(Hollnagel, Woods and Leveson, 2006)

Summary

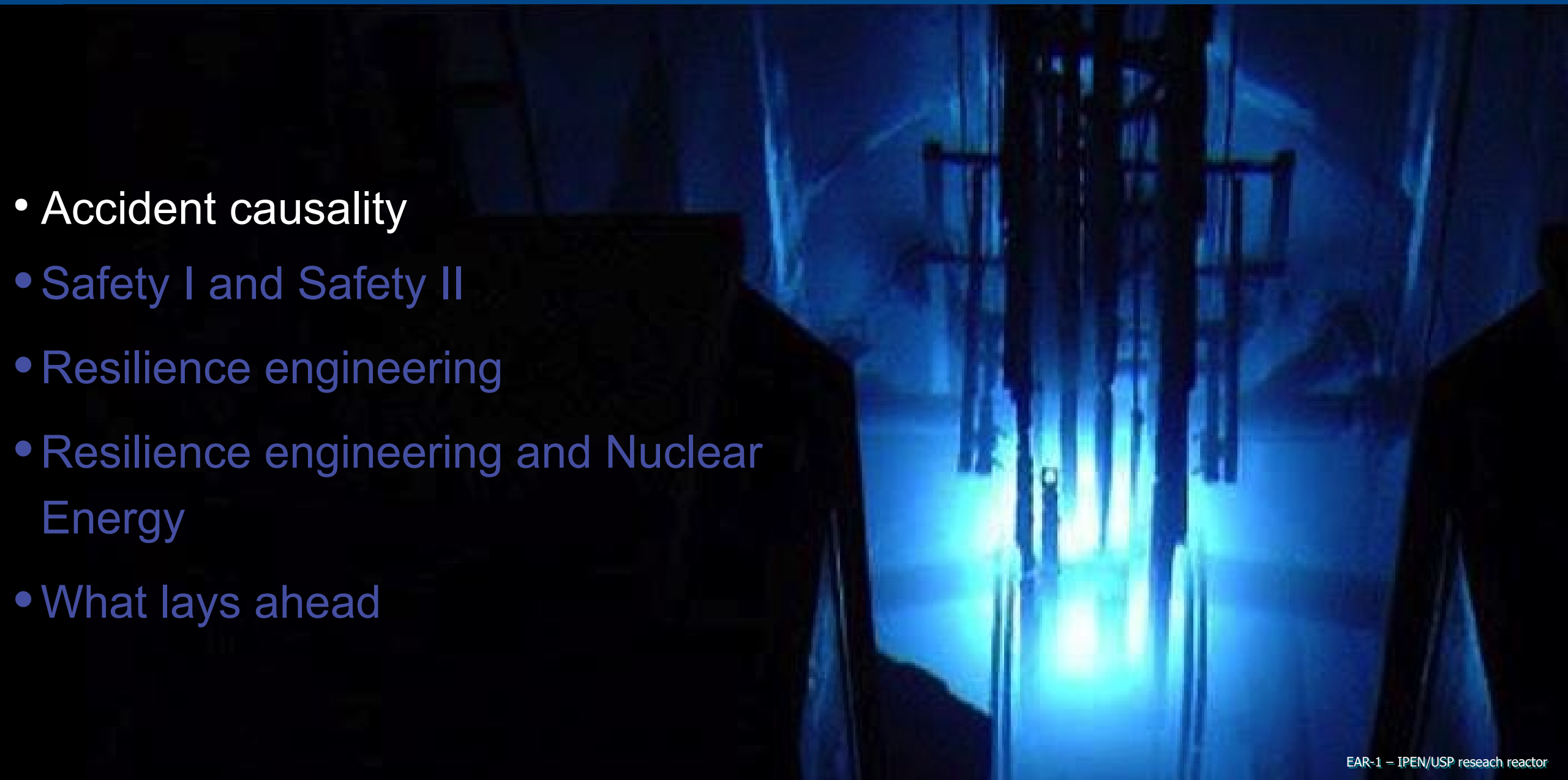
- Accident causality
- Safety I and Safety II
- Resilience engineering
- Resilience engineering and Nuclear Energy
- What lays ahead



EAR-1 – IPEN/USP reseach reactor

Summary

- Accident causality
- Safety I and Safety II
- Resilience engineering
- Resilience engineering and Nuclear Energy
- What lays ahead



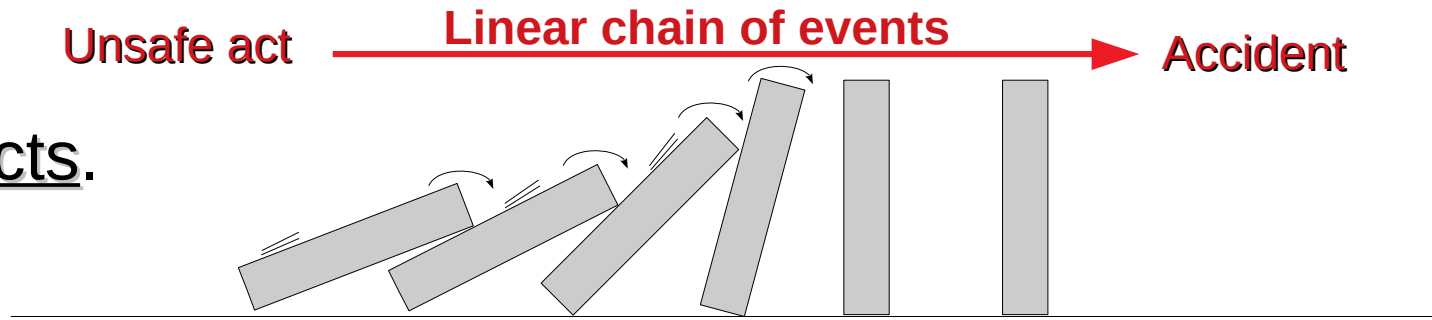
EAR-1 – IPEN/USP reseach reactor

Accident causality

Accident prone individual:

- Accidents are caused by unsafe acts.

Human!

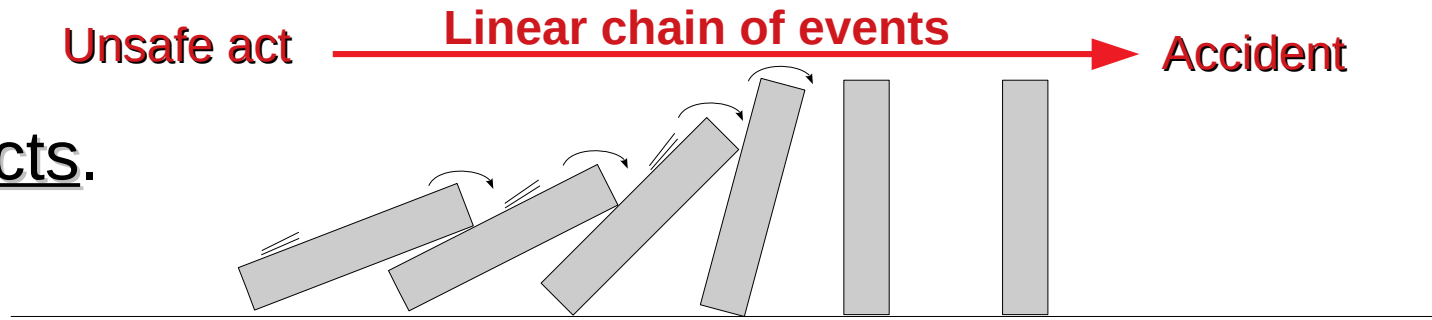


Accident causality

Accident prone individual:

- Accidents are caused by unsafe acts.

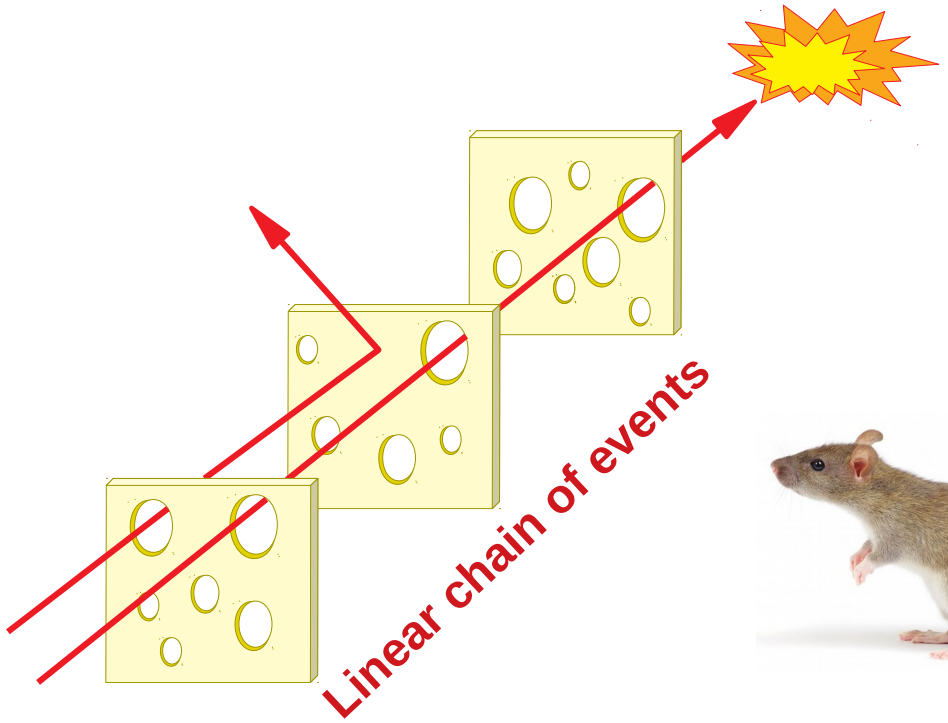
Human!



Organizational accidents:

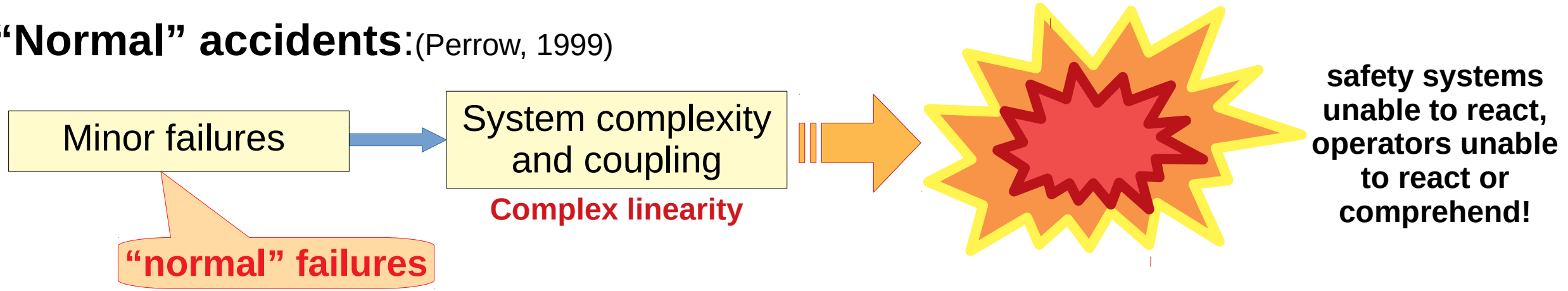
Human!

Accidents stem from active failures and latent organizational flaws (Reason,1997).



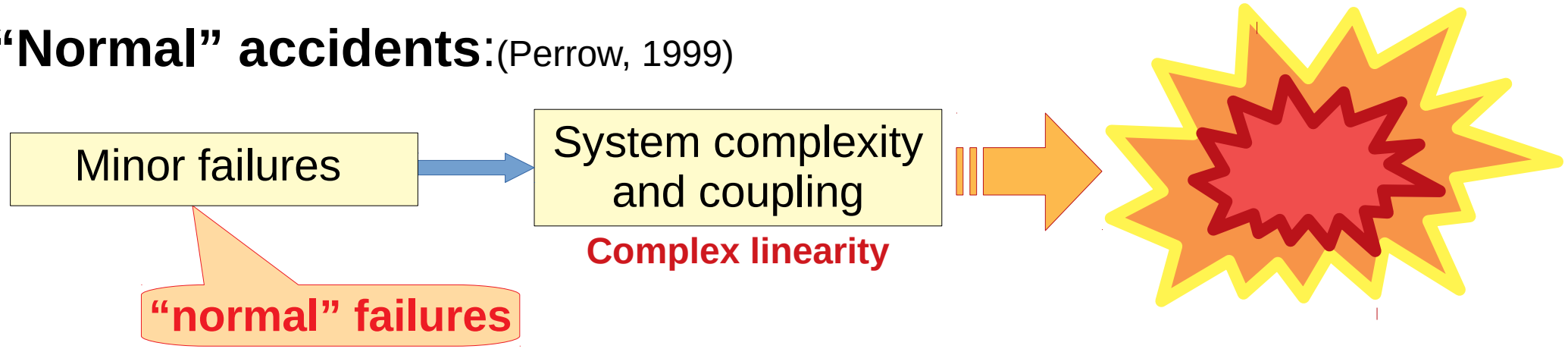
Accident causality

“Normal” accidents:(Perrow, 1999)



Accident causality

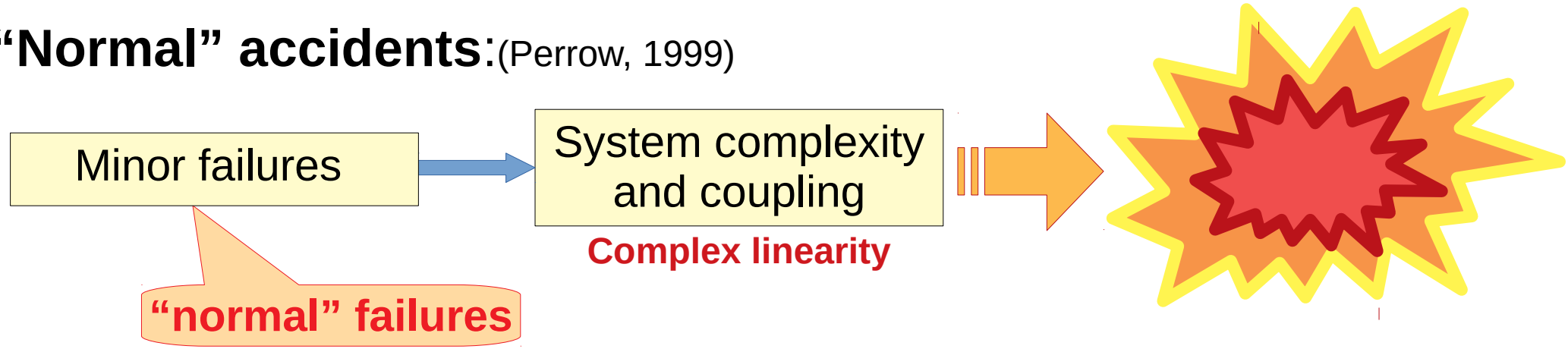
“Normal” accidents:(Perrow, 1999)



Abandon, downscale or radically redesign tight-coupling, high-complexity and high risk activities.

Accident causality

“Normal” accidents:(Perrow, 1999)



Abandon, downscale or radically redesign tight-coupling, high-complexity and high risk activities.

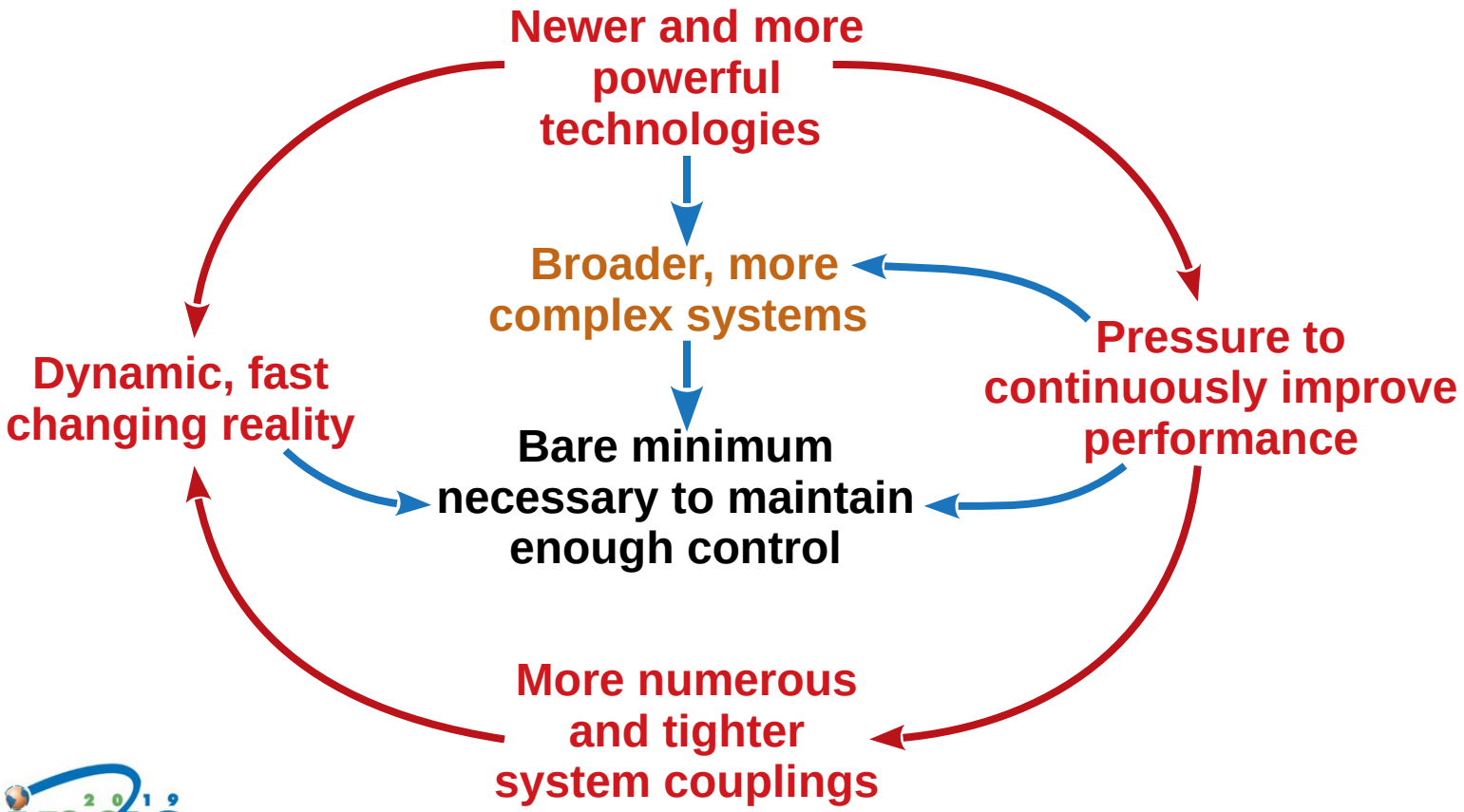
High Reliabilty Organizations:(Weick & Sutcliffe, 2015)

- Mindfull organizing: stable structures, cognitive alignment, formal procedures, hierarchy, expertise networks….

Accident causality

Performance variability:

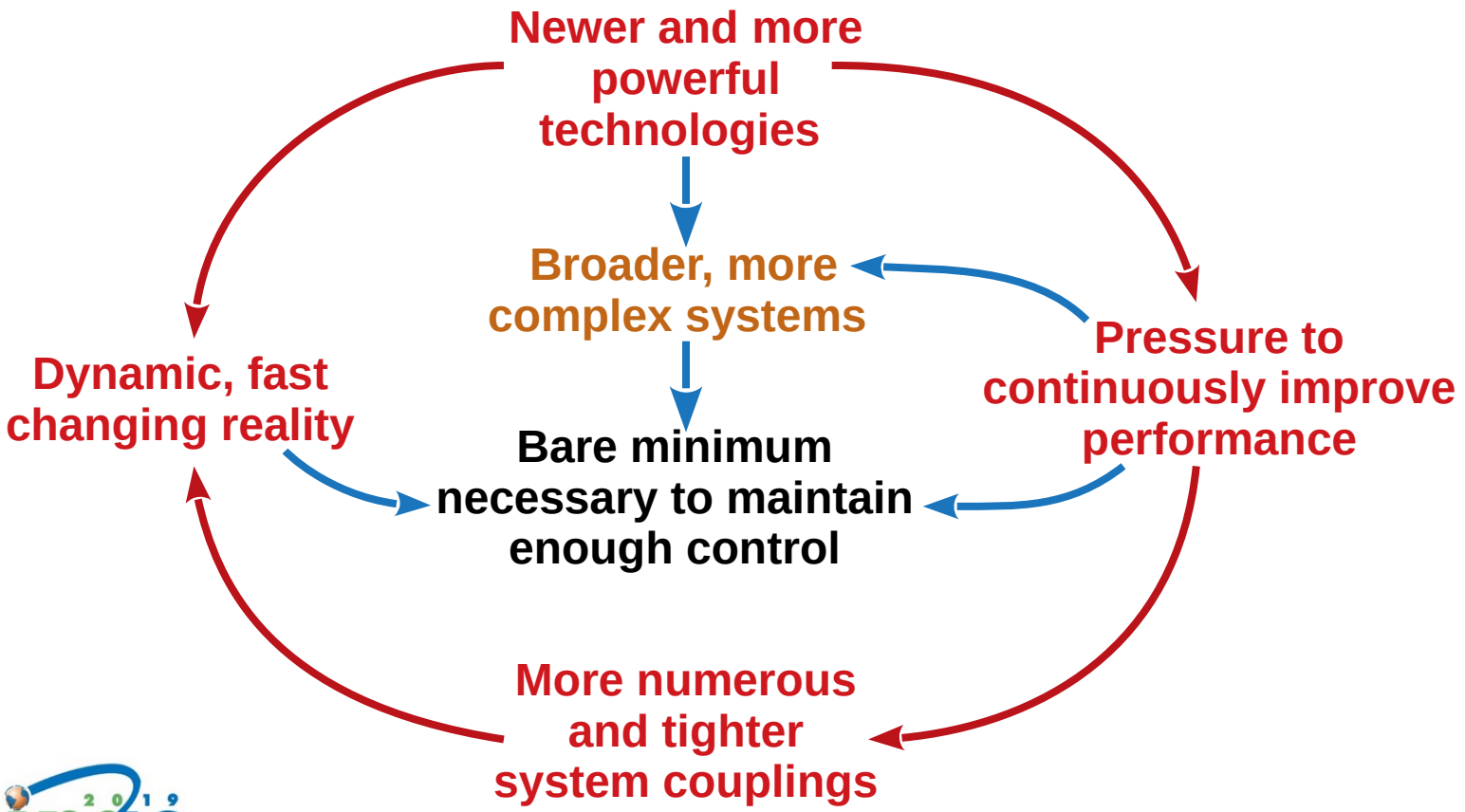
Efficiency-Thoroughness Trade-Off: **The ETTO principle**. (Hollnagel, 2009)

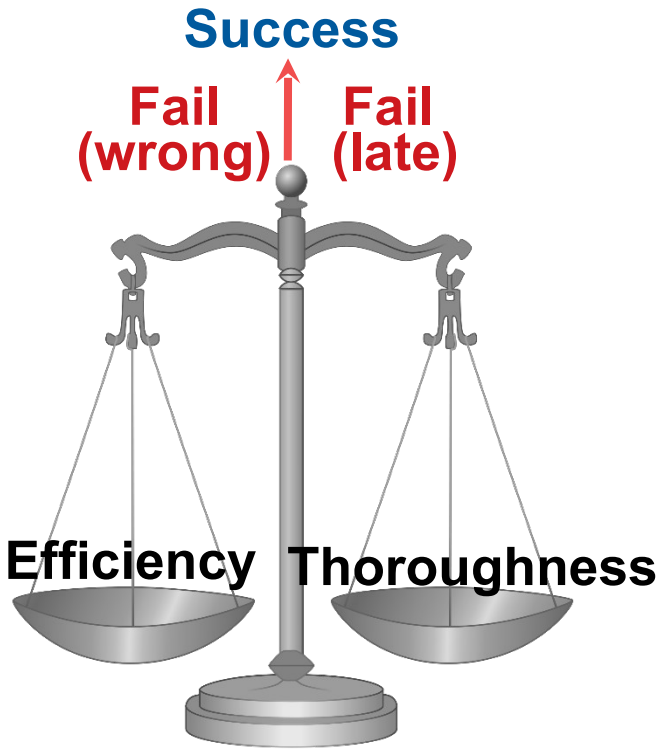


Accident causality

Performance variability:

Efficiency-Thoroughness Trade-Off: **The ETTO principle**. (Hollnagel, 2009)





Accident causality

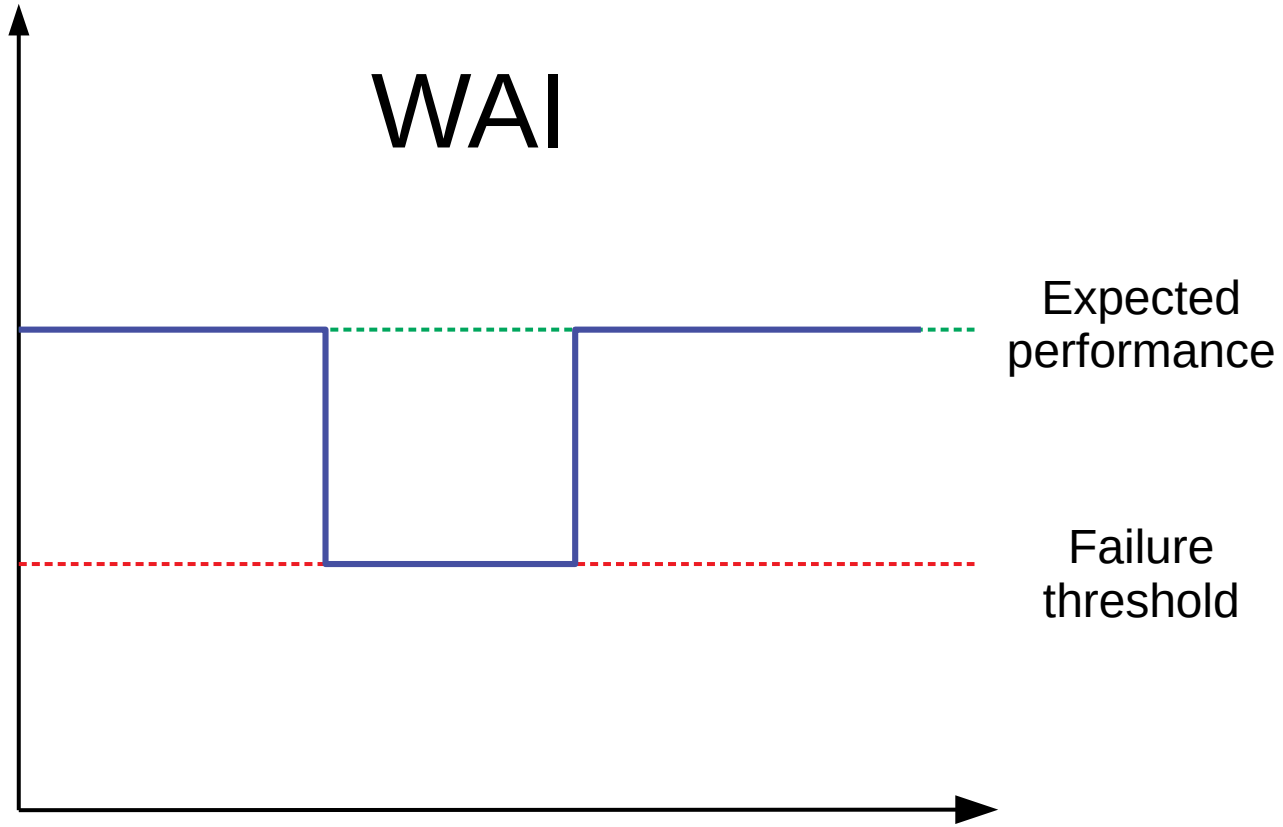
Performance variability:(Hollnagel, 2009)

Efficiency-Thoroughness Trade-Off: **The ETTO principle**.

WORK AS IMAGINED (WAI)	≠	WORK AS DONE (WAD)
• Deterministic; • Model based; • Formal; • Limited to current knowledge; • Static; • Reflects past experiences...		• Stochastic; • Reality based; • Social; • Limited to current proficiency; • Dynamic; • Actual circunstances...

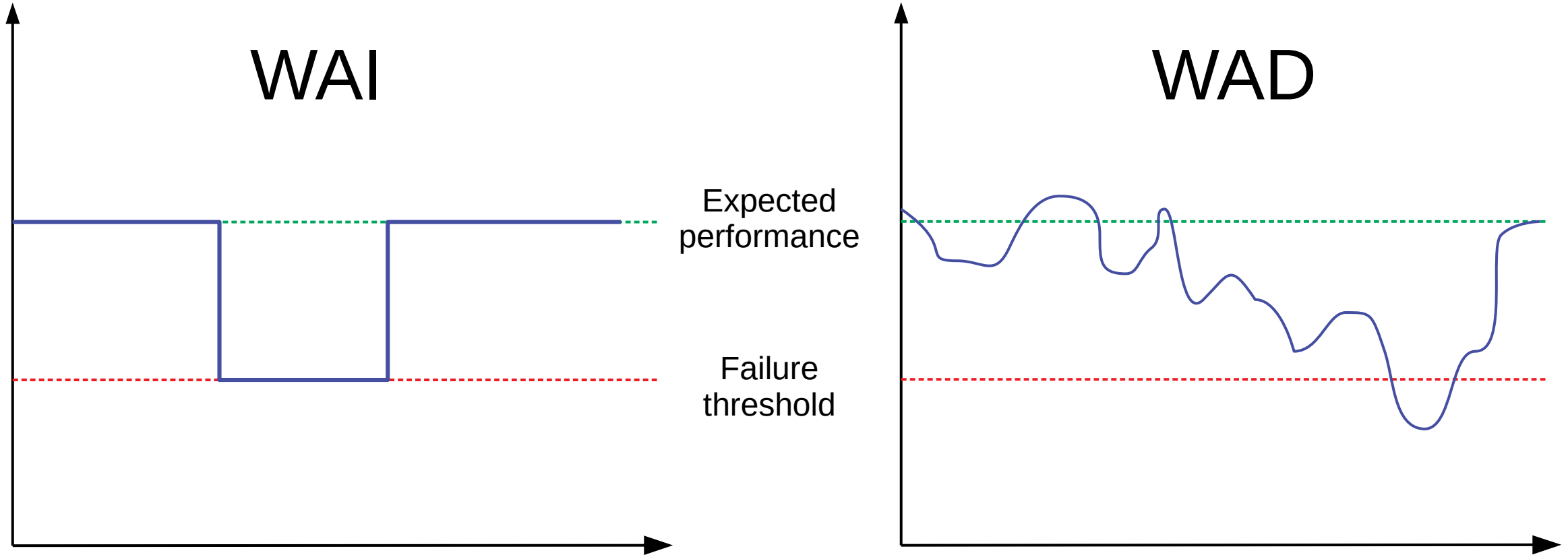
Accident causality

Performance variability:(Hollnagel, 2009)

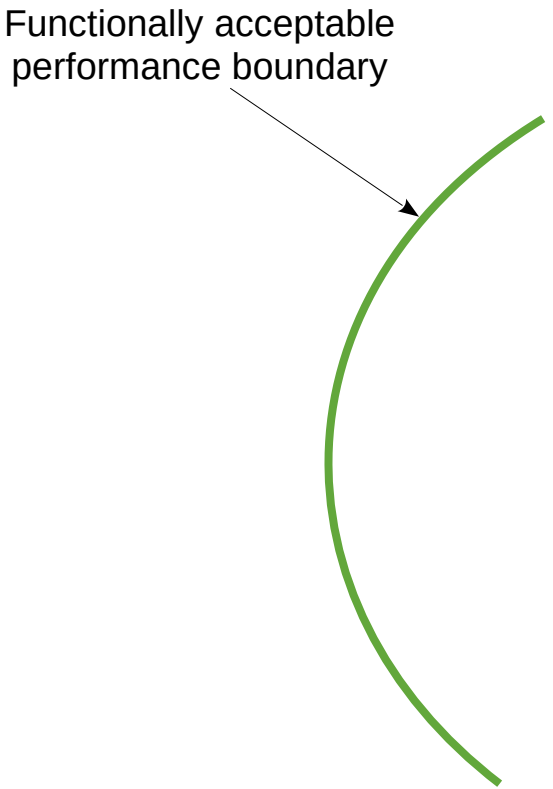


Accident causality

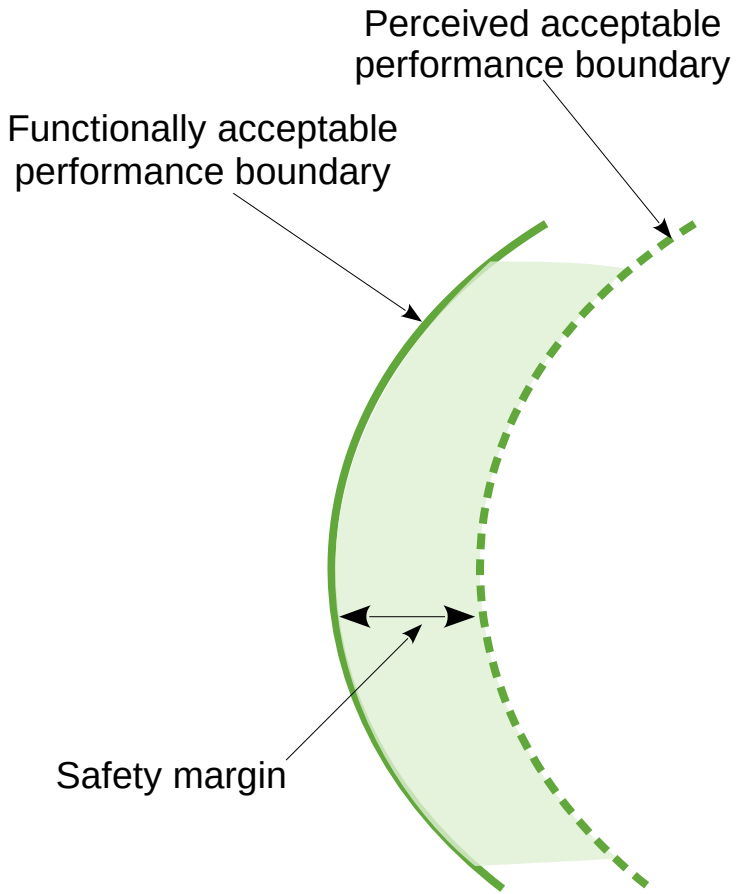
Performance variability:(Hollnagel, 2009)



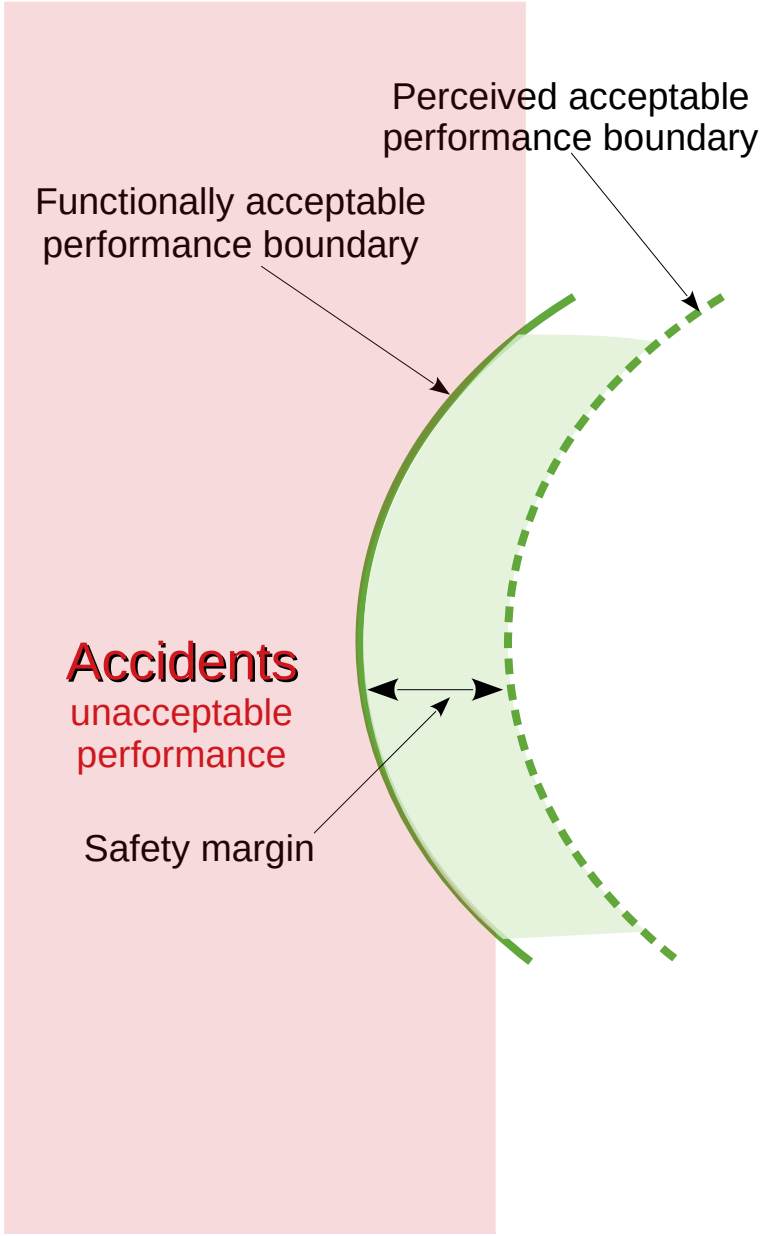
Accident causality



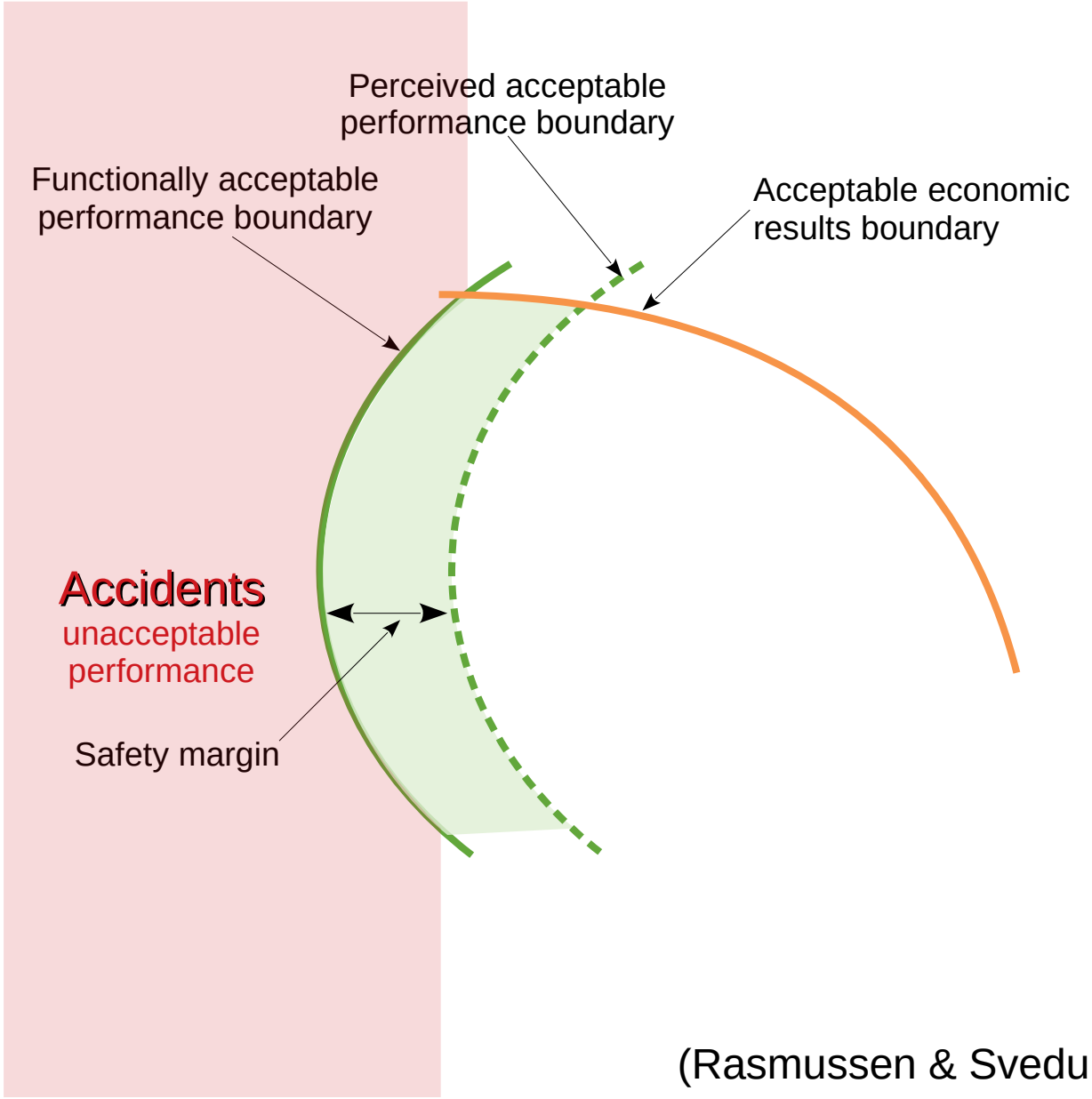
Accident causality



Accident causality

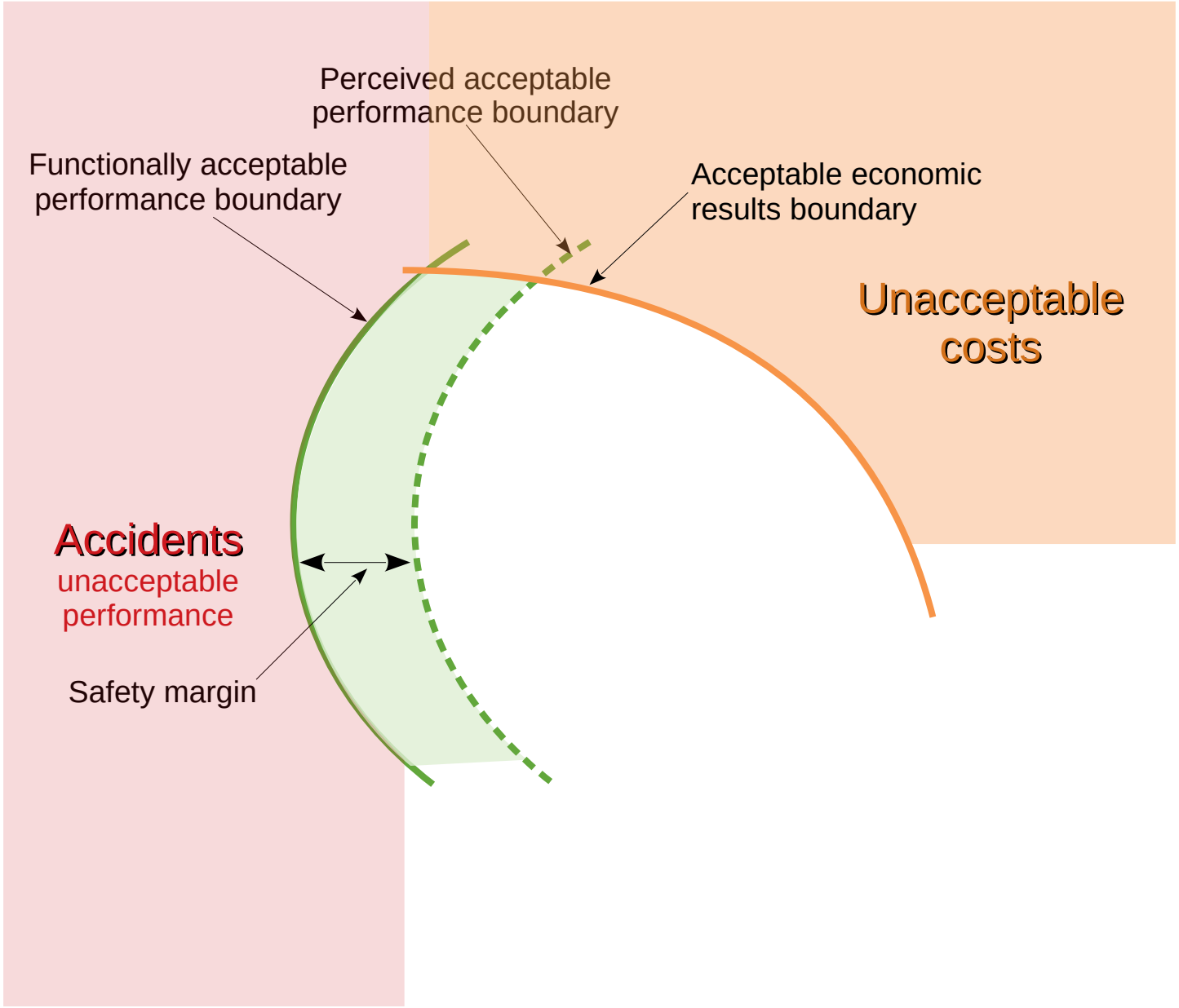


Accident causality

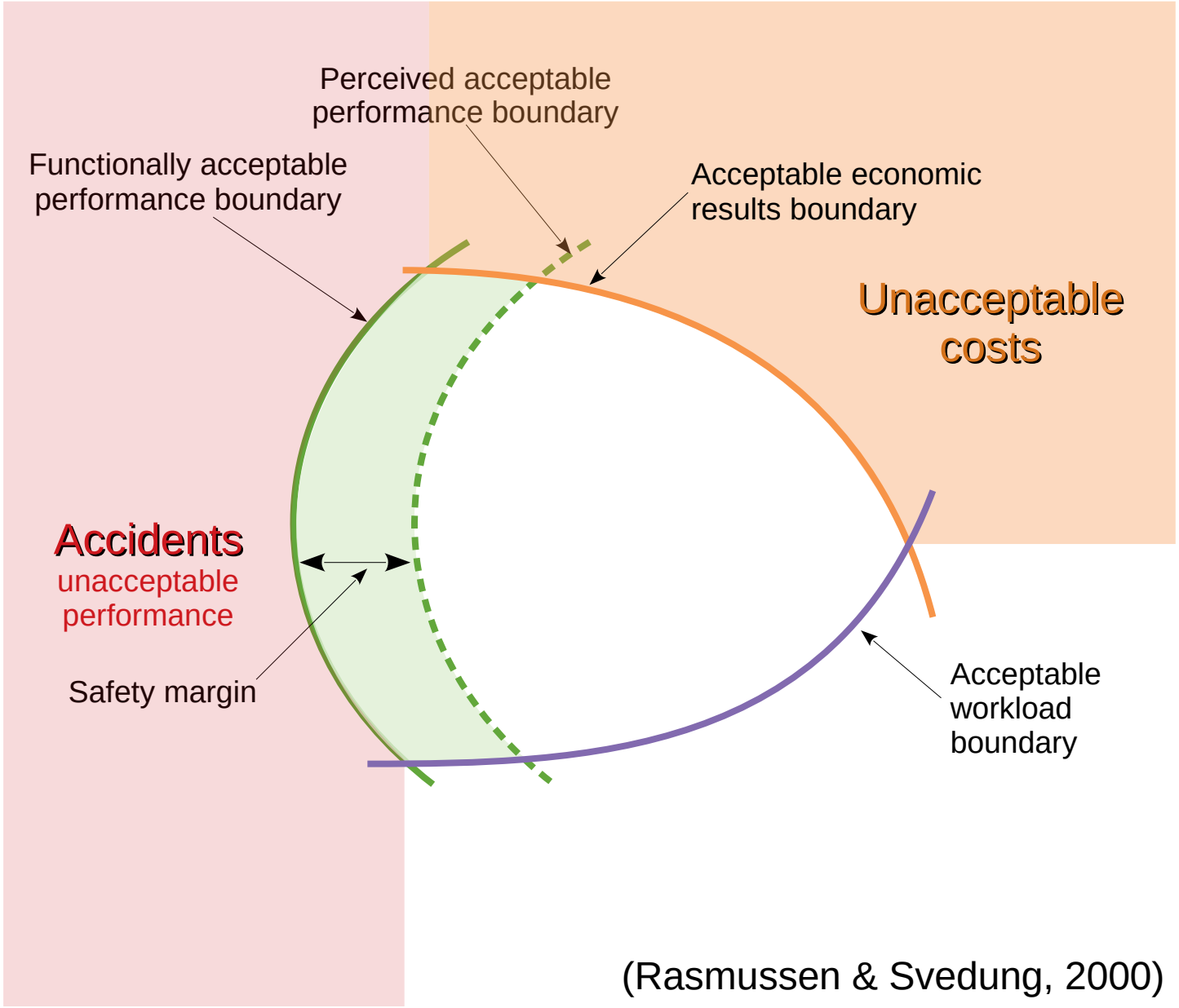


(Rasmussen & Svedung, 2000)

Accident causality

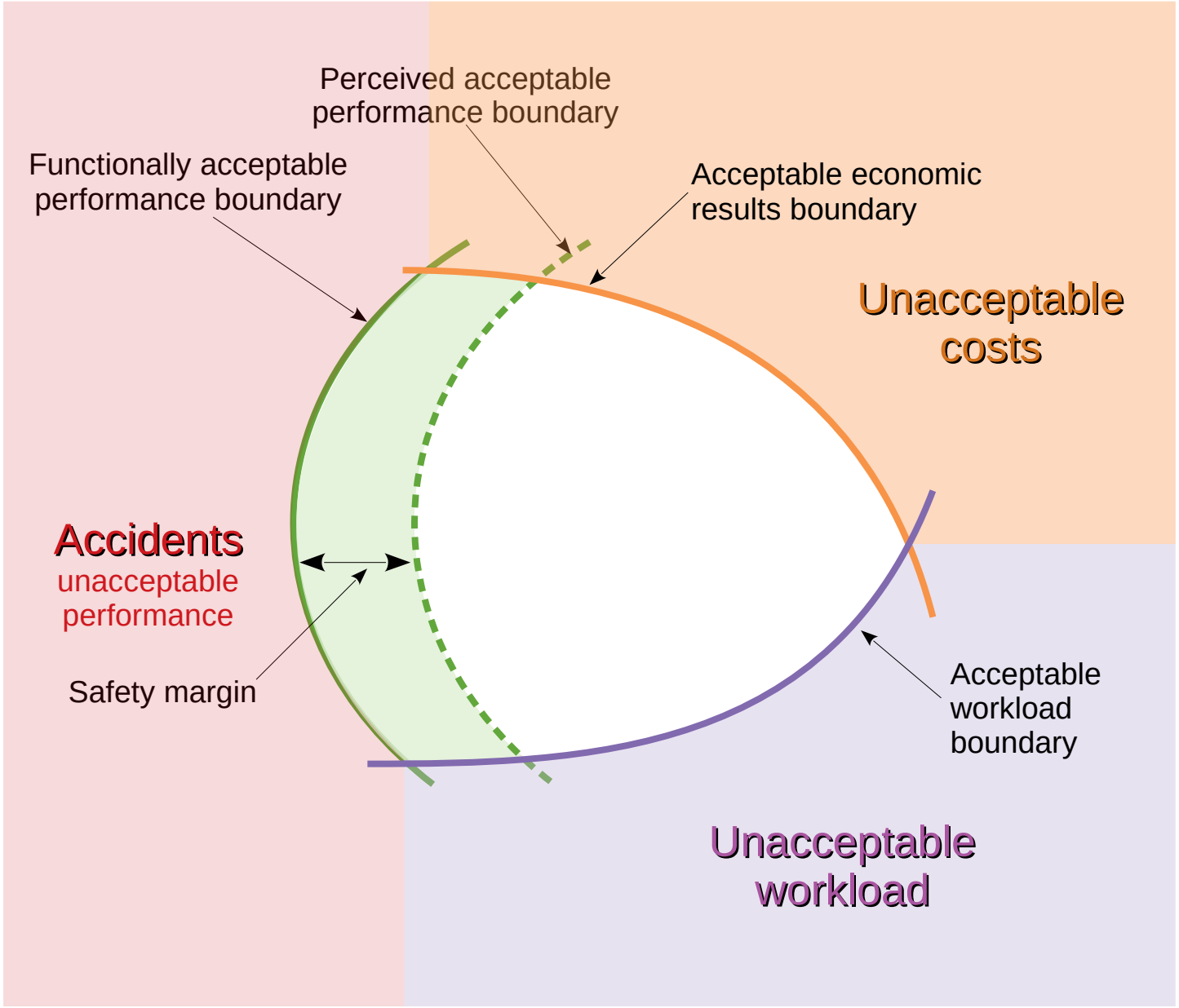


Accident causality

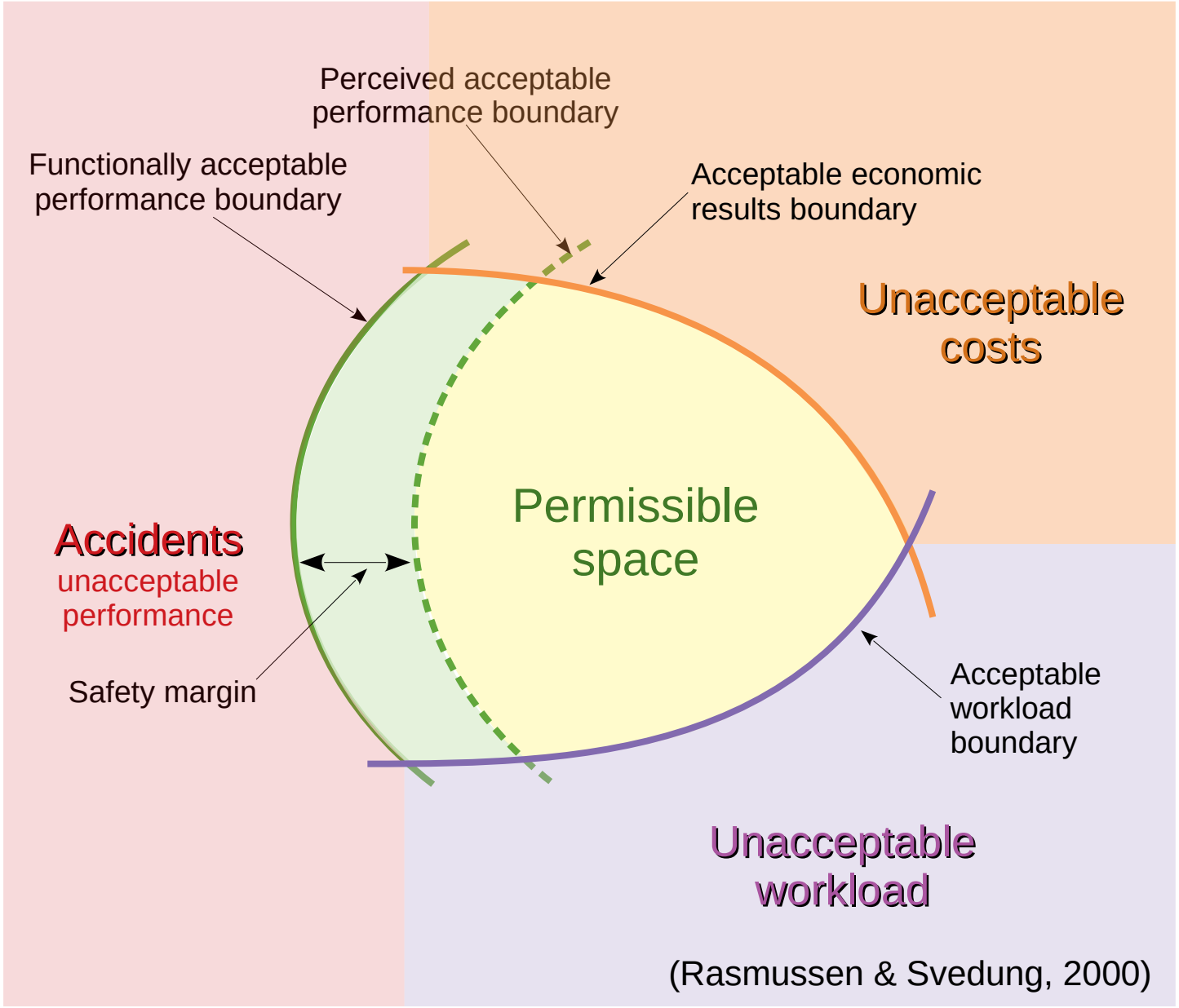


(Rasmussen & Svedung, 2000)

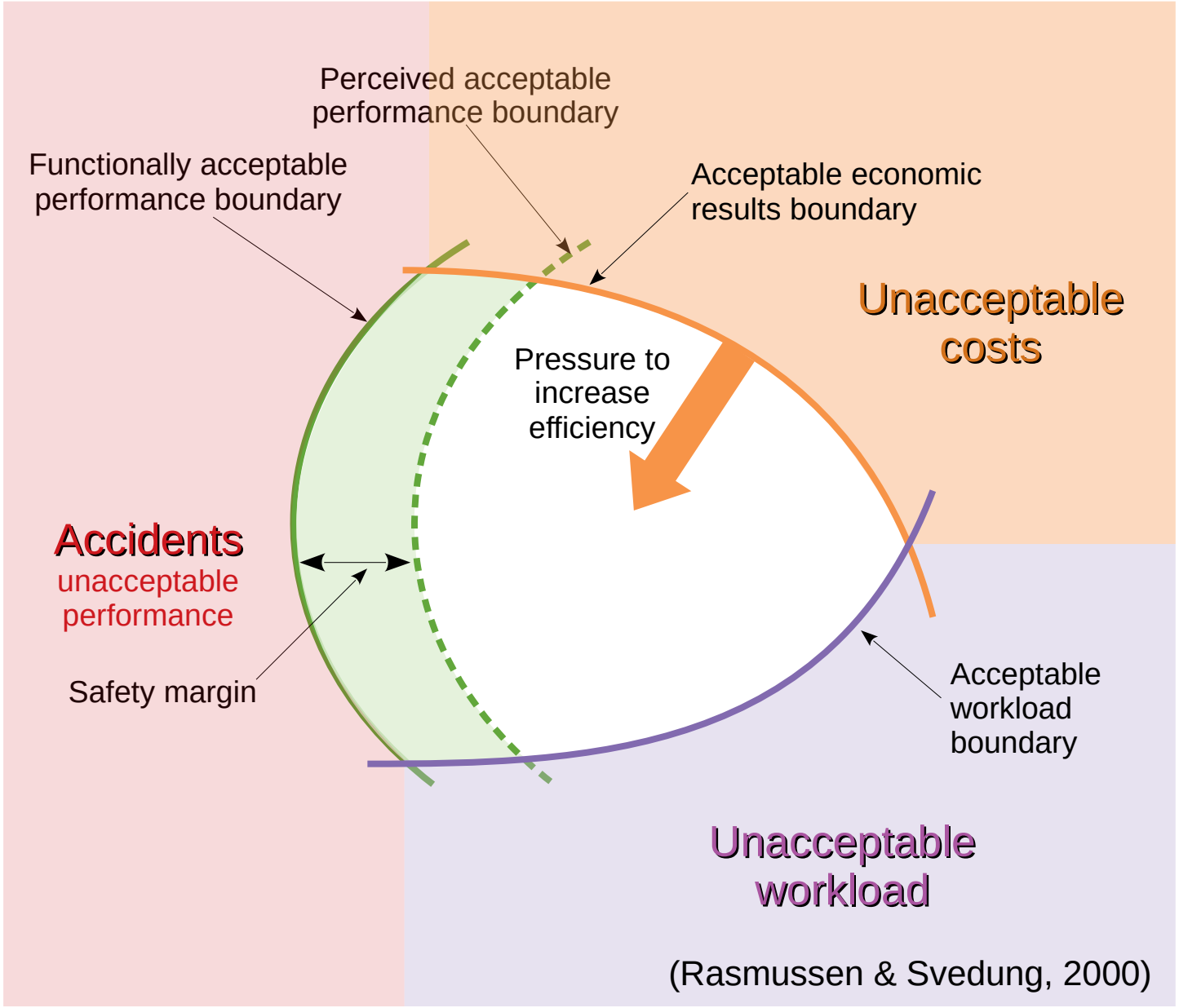
Accident causality



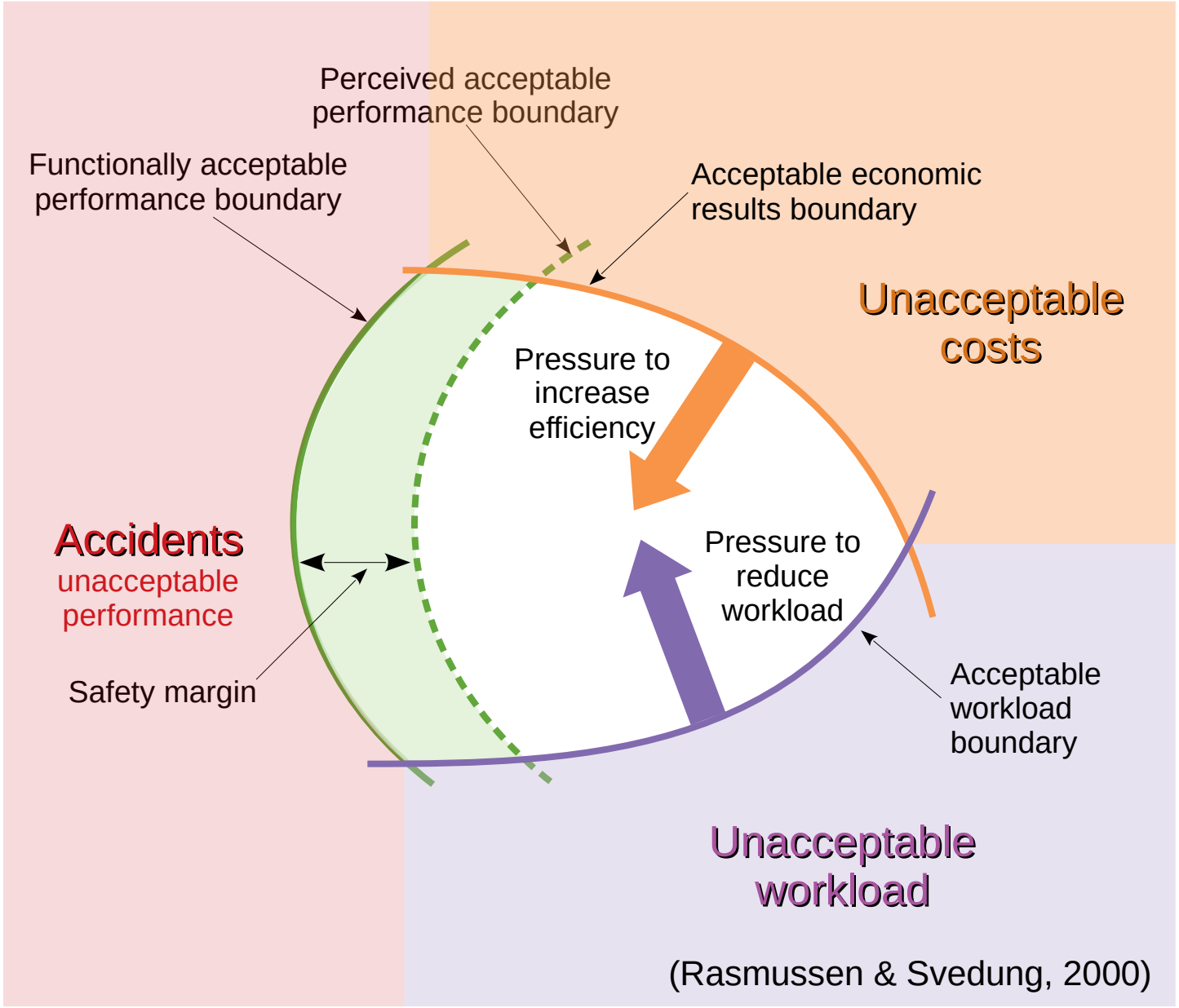
Accident causality



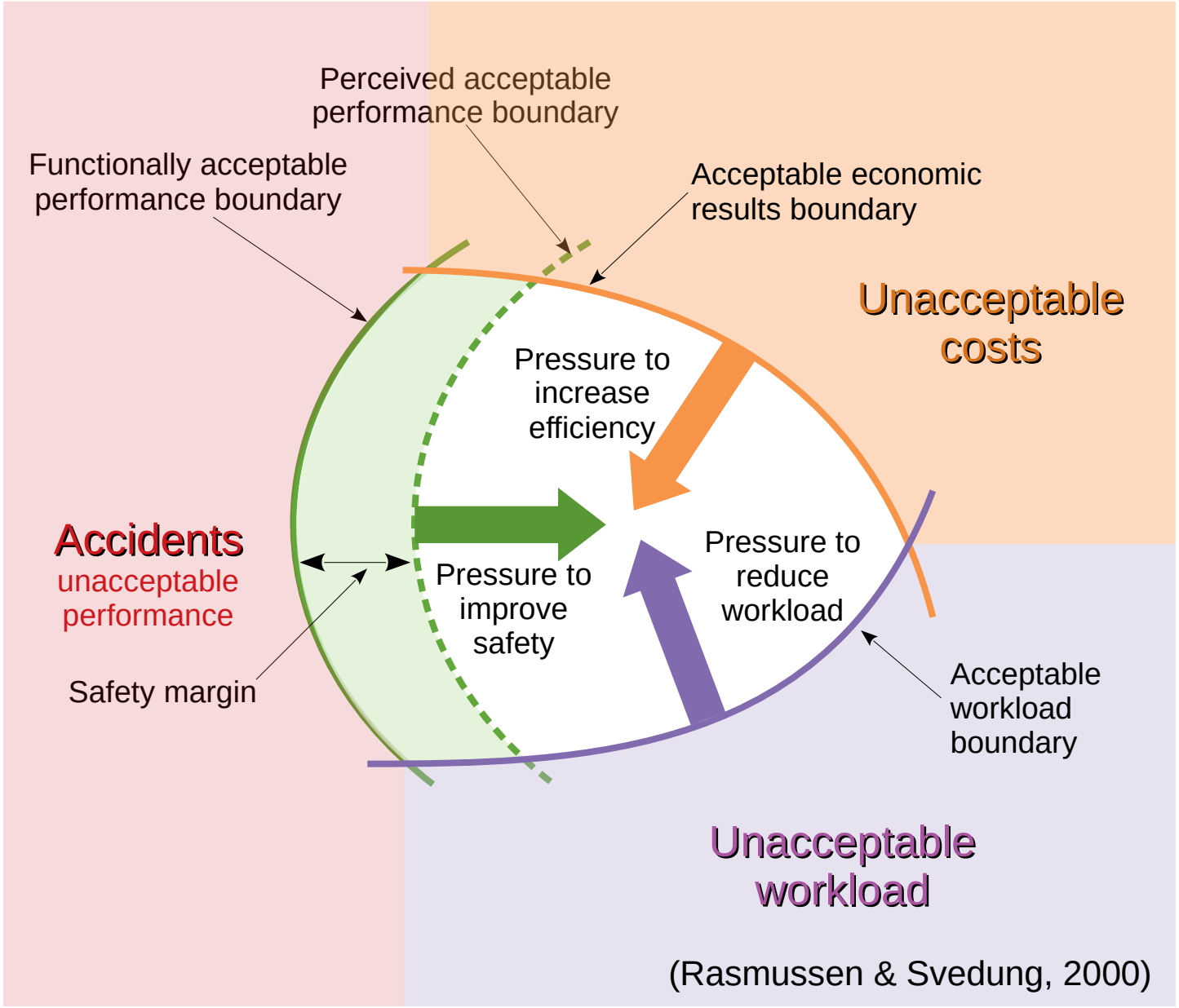
Accident causality



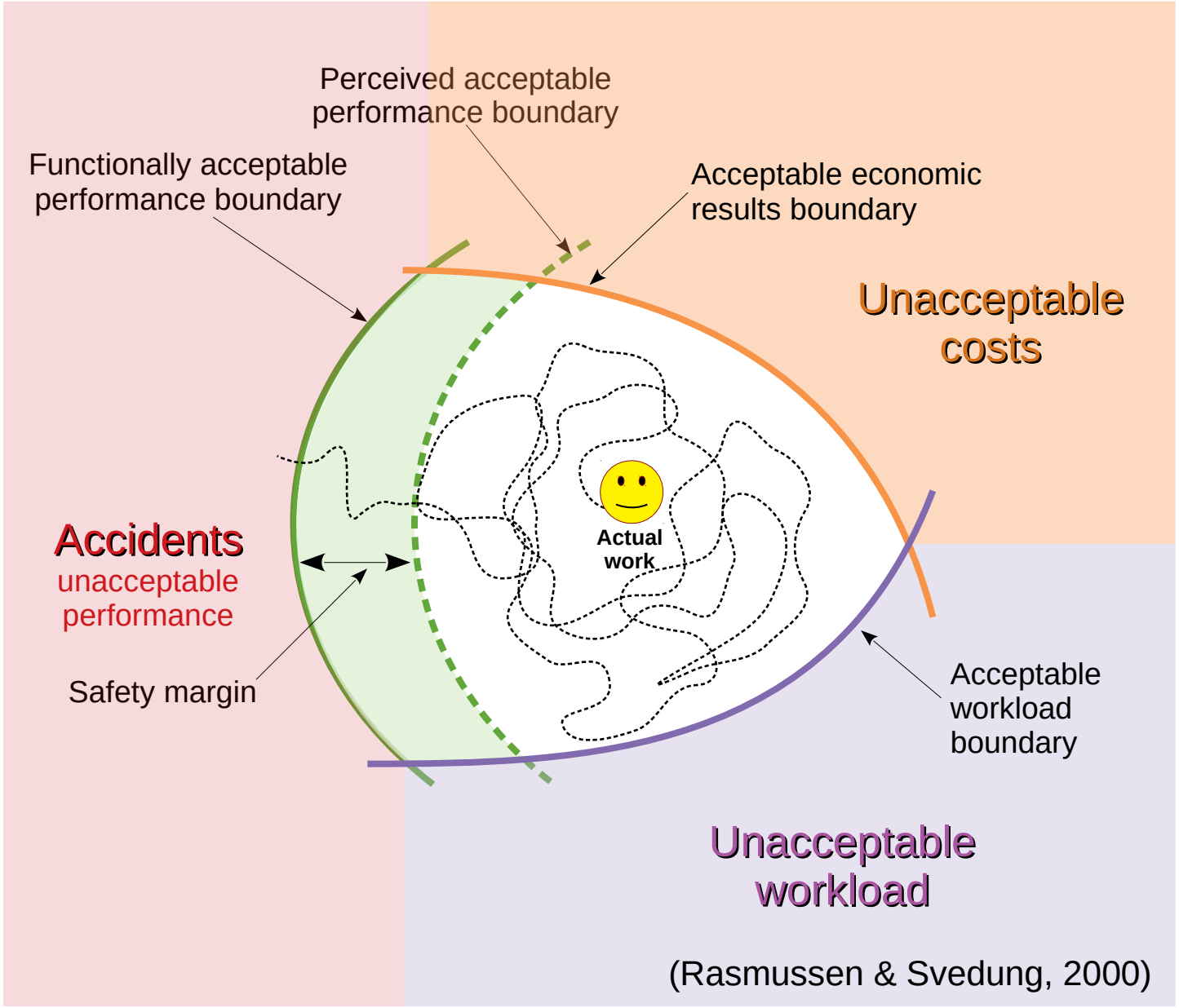
Accident causality



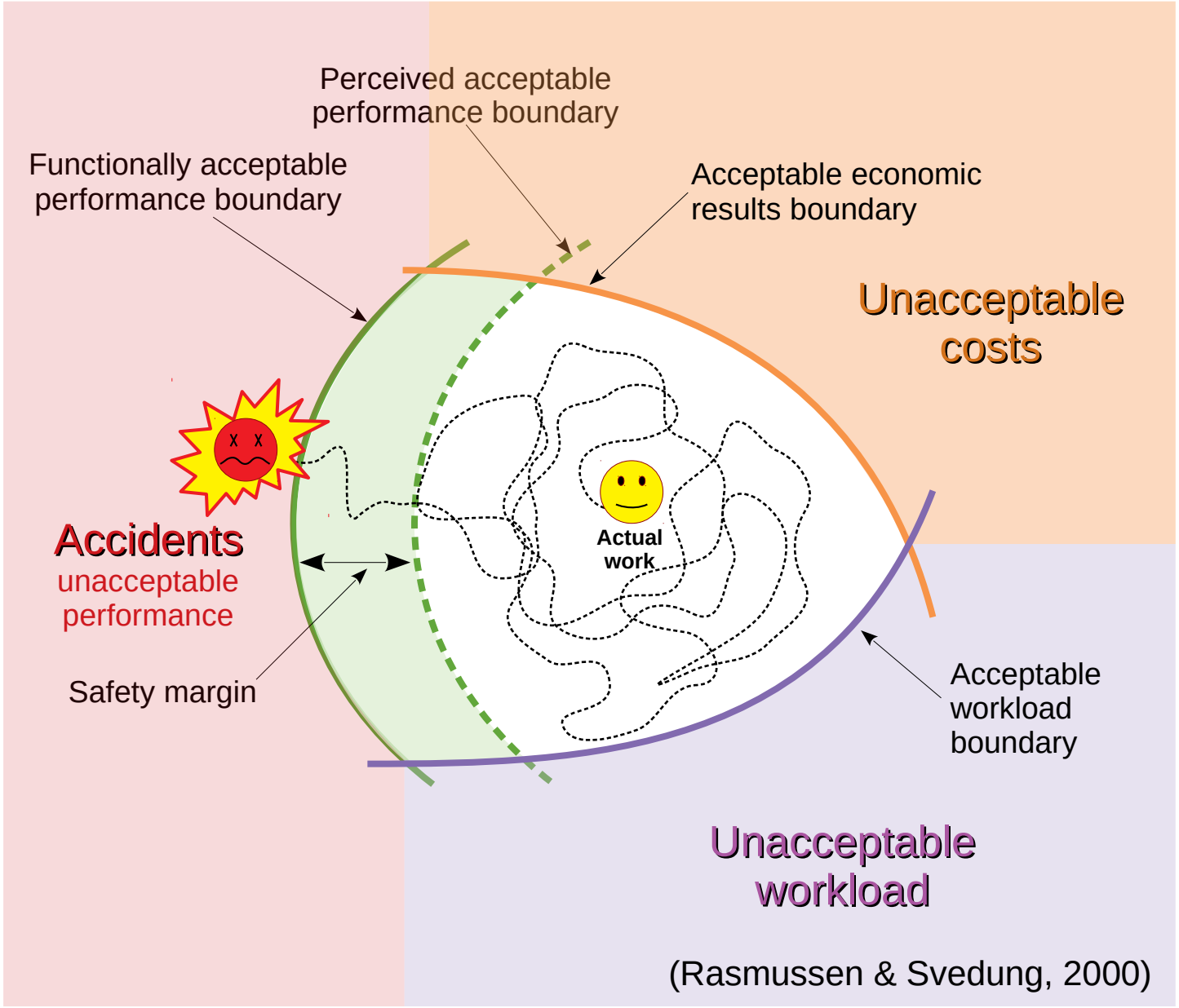
Accident causality



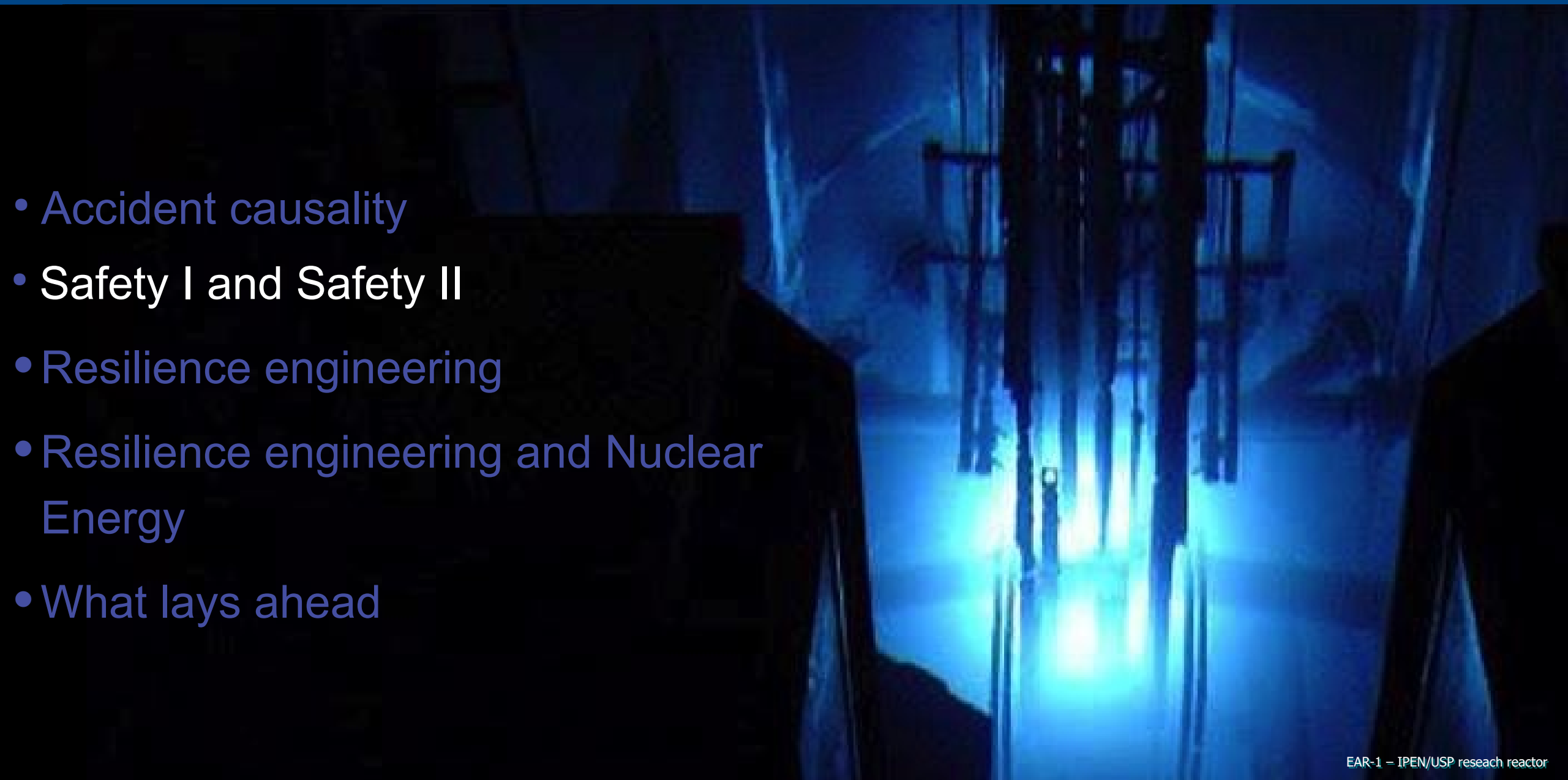
Accident causality



Accident causality



Summary



- Accident causality
- Safety I and Safety II
- Resilience engineering
- Resilience engineering and Nuclear Energy
- What lays ahead

EAR-1 – IPEN/USP reseach reactor

Safety I and Safety II

SAFETY:

- **Risk assessment**
- **Safety management**
- **Safety culture**
- **Accident investigation**

Freedom from unacceptable risk

SAFETY I

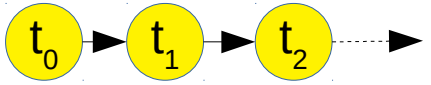
<u>The Causality Credo</u>:

- **Undesirable events happen when something has gone wrong, they have causes;**
- **Through analysis, these causes may be identified, isolated, eliminated, fixed, etc…**
- **Identifying and eliminating all causes, it is possible to prevent accidents from happening (zero accidents goal).**

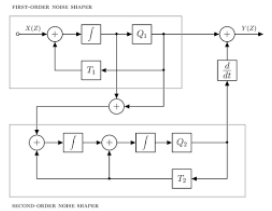
SAFETY I

- Decomposition: analytical approaches to reach individual meaningful elements….

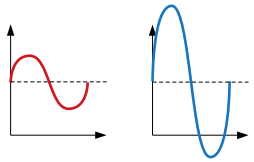
- Binomial performance: something either works or fails:



- Events occur following a certain order or sequence.



- Events combine following a certain logic to produce results.



- Outputs are proportional to inputs.

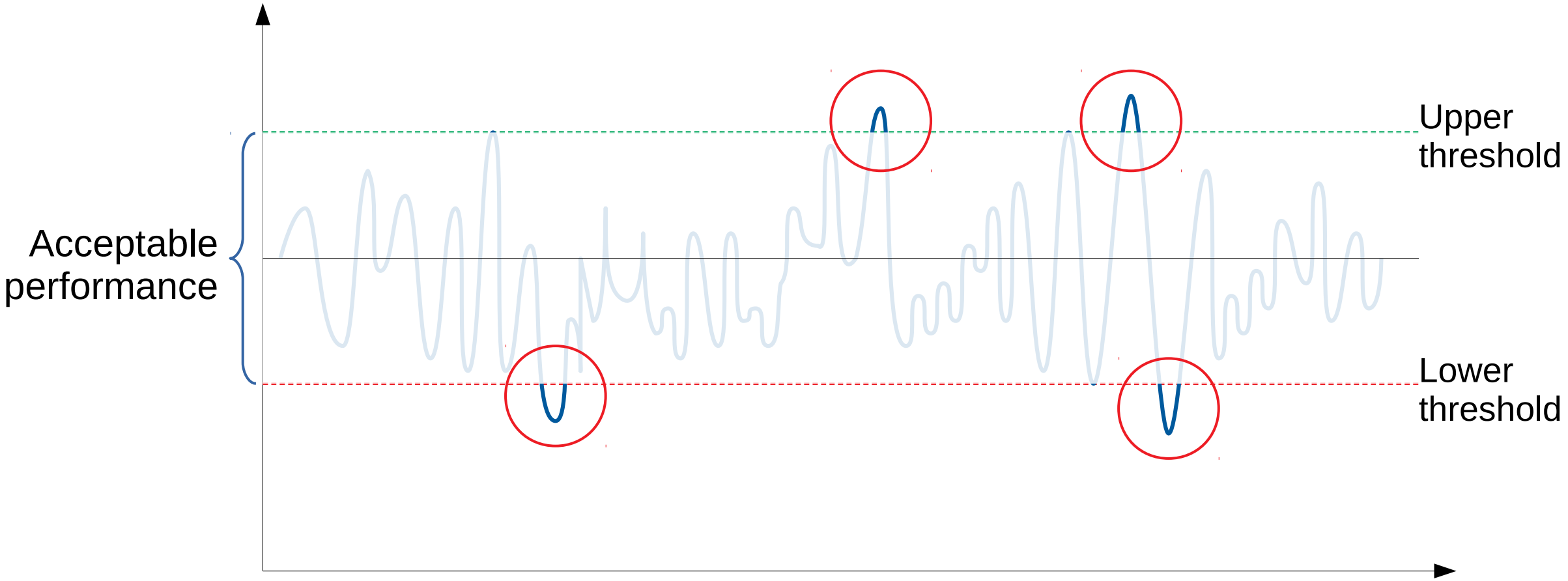
Safety I and Safety II

SAFETY I

- Learns from situations where safety is absent.
- Absence of accidents does not necessarily translate to safety.
- The “safer” the system is, less opportunities to improve (?!).
- Prevention considering past events, but what about the next event?
- Deterministic and stochastic approaches.

Safety I and Safety II

SAFETY I



System tractability

	Tractable	Intractable
Details	Few. Easy to describe.	Many. Elaborate descriptions.
Comprehensibility	Known principles.	Partly, or completely unknown principles.
Stability	Static, does not change while being described.	Dynamic, changes before one is able to describe it.
Relationship to other systems	Independent.	Interdependent.
Control	Easy.	Difficult.

Safety I and Safety II

System tractability

Technology changes fast

New type of hazards: new materials, organisms, populations, systems, networks etc...

Chances to learn from experience are ever more limited

Humans and technology interact in ever more direct and complex relationships

Hardware, software, peopleware etc. fail in new and unexpected ways

Growing complexities and couplings make predicting a system's behavior practically impossible to predict

Growing societal intolerance to accidents and aversion to risk

Very dynamic business may impair the ability the maintain an effective regulatory framework

Instantaneous and global communication bring global dimension the government's and regulatory bodies' responsibilities for safety.

SAFETY II

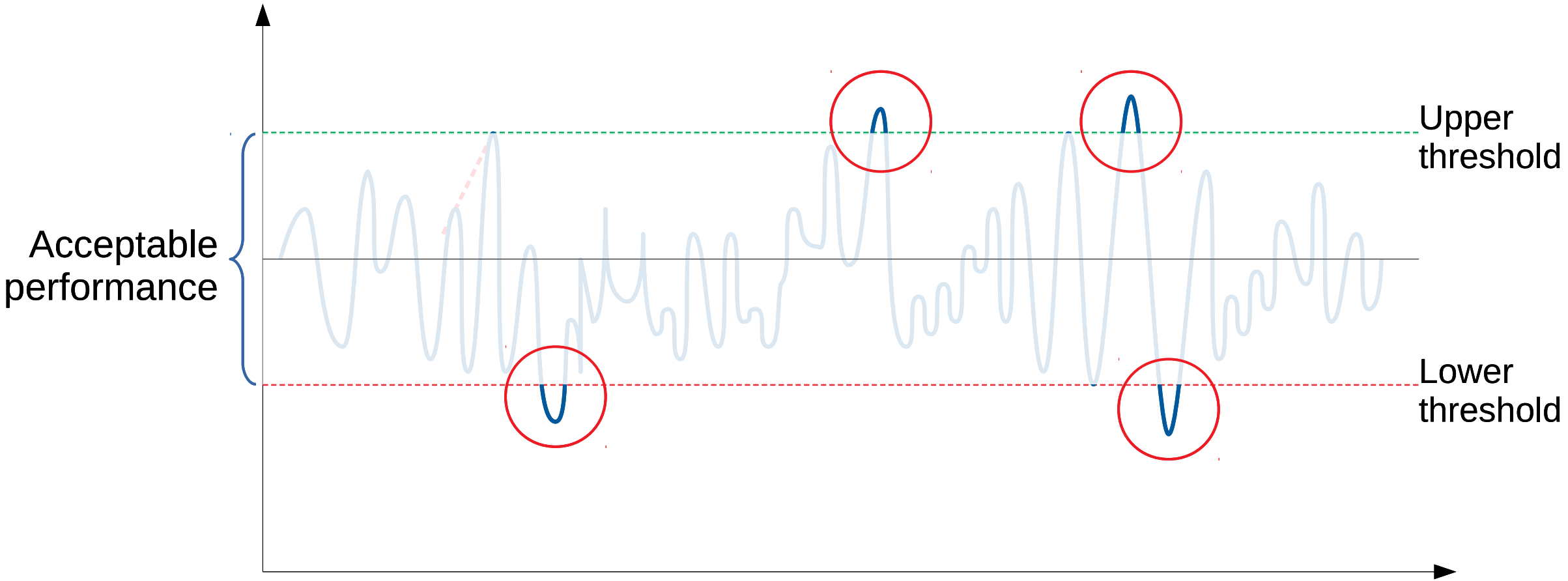
- Success and failures are equivalent.
- Outcomes are emergent, not resultant.
- Resonance: non-linearity of outcomes.
- Dependencies and descriptions must reflect reality, not design.
- Human capability to adjust to the unexpected is key to safety.

SAFETY II

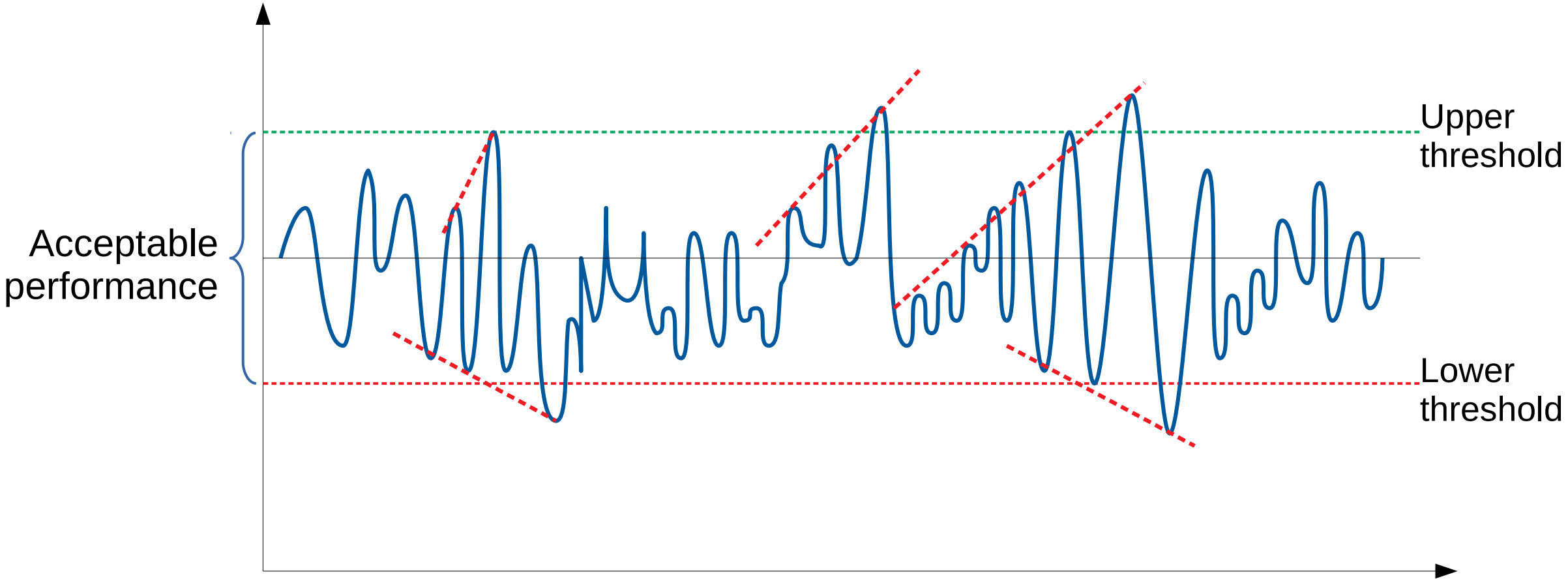
- Learning from everyday successful performance.
- Safety may be translated into meaningful indicators.
- Continuous improvement is measurable.
- Performance assurance, not prevention, to face the unexpected.
- Functional resonance approach

Safety I and Safety II

SAFETY I



SAFETY II



SAFETY II:

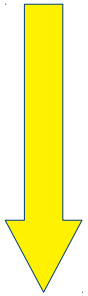
- **Anticipate;**
- **Monitor;**
- **Respond; and**
- **Adapt.**

Ensure performance

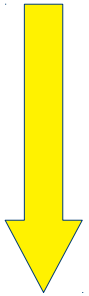
Safety I and Safety II

SAFETY I ≠ SAFETY II

Avoiding failures



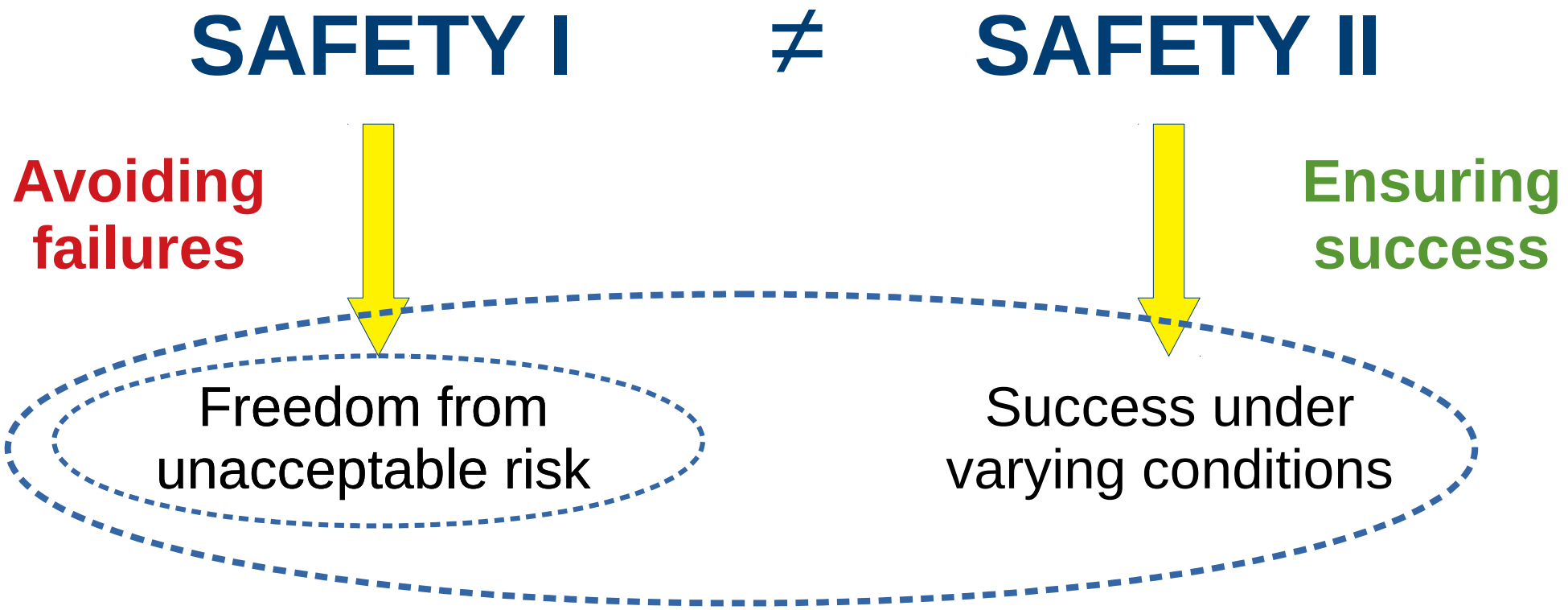
Freedom from unacceptable risk



Ensuring success

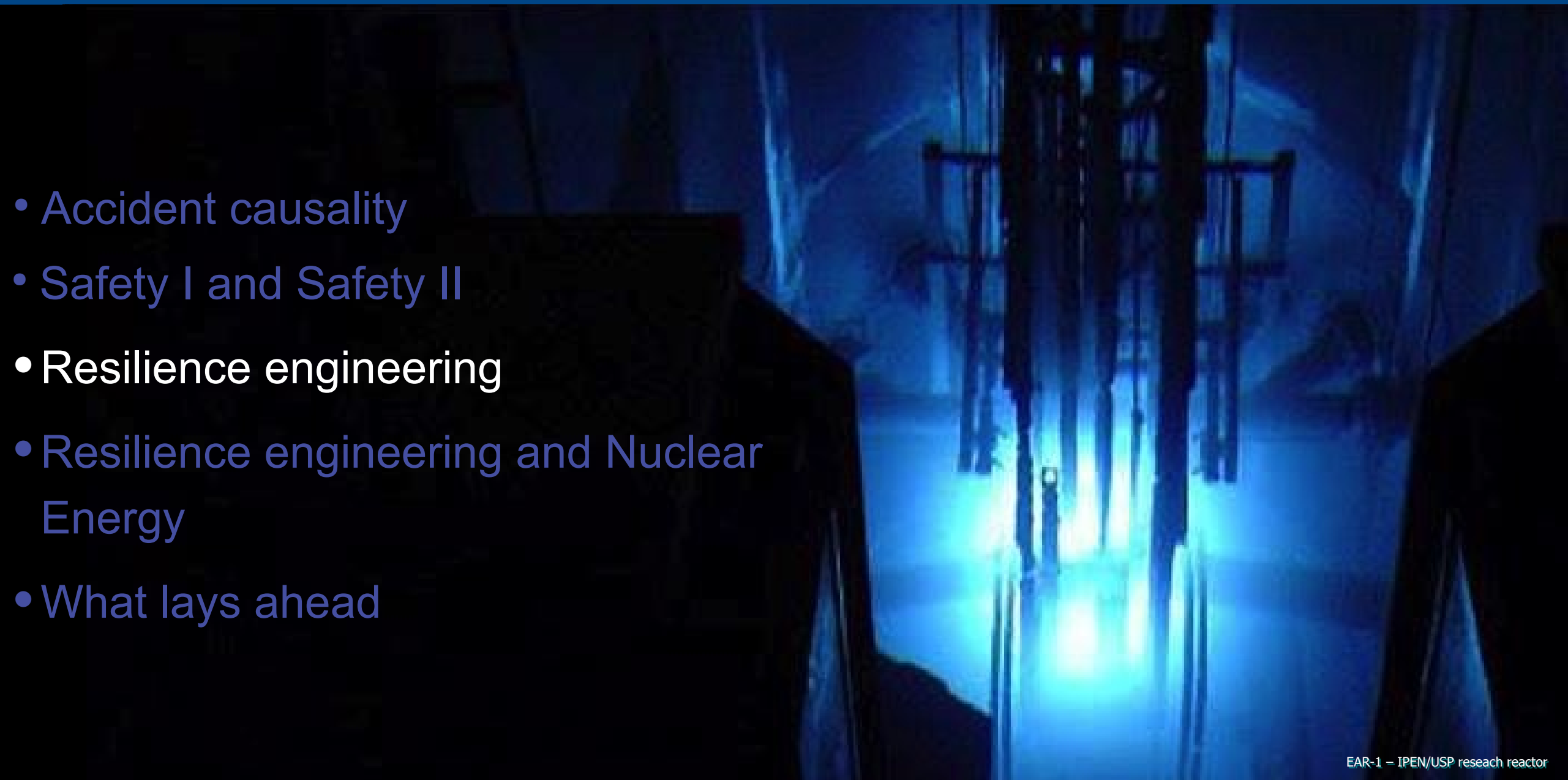
Success under varying conditions

Safety I and Safety II



Summary

- Accident causality
- Safety I and Safety II
- Resilience engineering
- Resilience engineering and Nuclear Energy
- What lays ahead



EAR-1 – IPEN/USP reseach reactor

Resilience?

- Supply chain resilience
- Societal resilience
- Coastal systems resilience
- Critical infrastructure resilience
- Network resilience
- Cybersecurity resilience
- Structural resilience
- Disaster resilience
- Flood resilience
- Material resilience
- Fiber resilience
- Economic resilience
- Business resilience
- Psychological resilience
- Biological resilience
- Microbial resilience
- Ecological resilience
- Socio-ecological resilience
- Urban resilience
- Smart-grid resilience
- Software resilience
- Nanomaterial resilience
- Energy resilience
- Coral resilience
- Seismic resilience
- Cryptologic resilience
- Communication resilience
- Educational resilience

Resilience?

General concept:

Capacity the deal with disturbances.

4 R's: Robustness, Redundancy, Resourcefulness, and Rapidity

Resilience: according to resilience engineering

The intrinsic ability of a system to adjust its functioning prior to, during, or following chances and disturbances, so that it can sustain required operations under both expected and unexpected conditions.

Resilience engineering

Resilience!

Essential characteristics: (Woods, 2006)

- Buffering capacity;
- Flexibility;
- Margin; and
- Tolerance.

Resilience engineering:

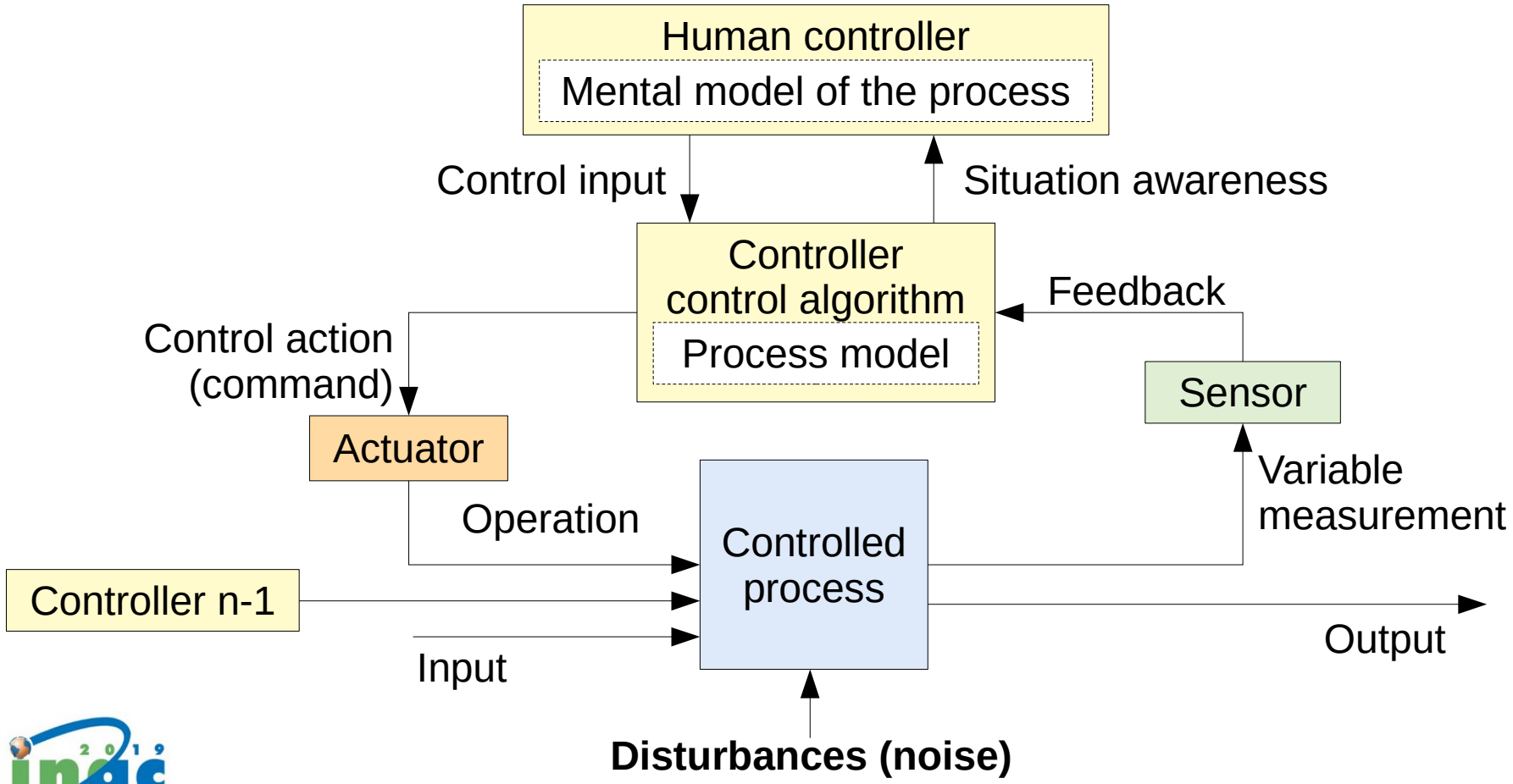
- Methodologies for the design or development of resilient systems.
- Enhance to ability to prevent system performance variability beyond acceptable limits when facing changes, disturbances or uncertainties.
- Development of resilient performance potentials.

Resilience engineering

The System-Theoretic Accident Method and Process - STAMP: Untoward performance emerges from failures in controlling the system. System Theoretic Process Analysis (STPA) model: (Nancy Leveson, 2011)

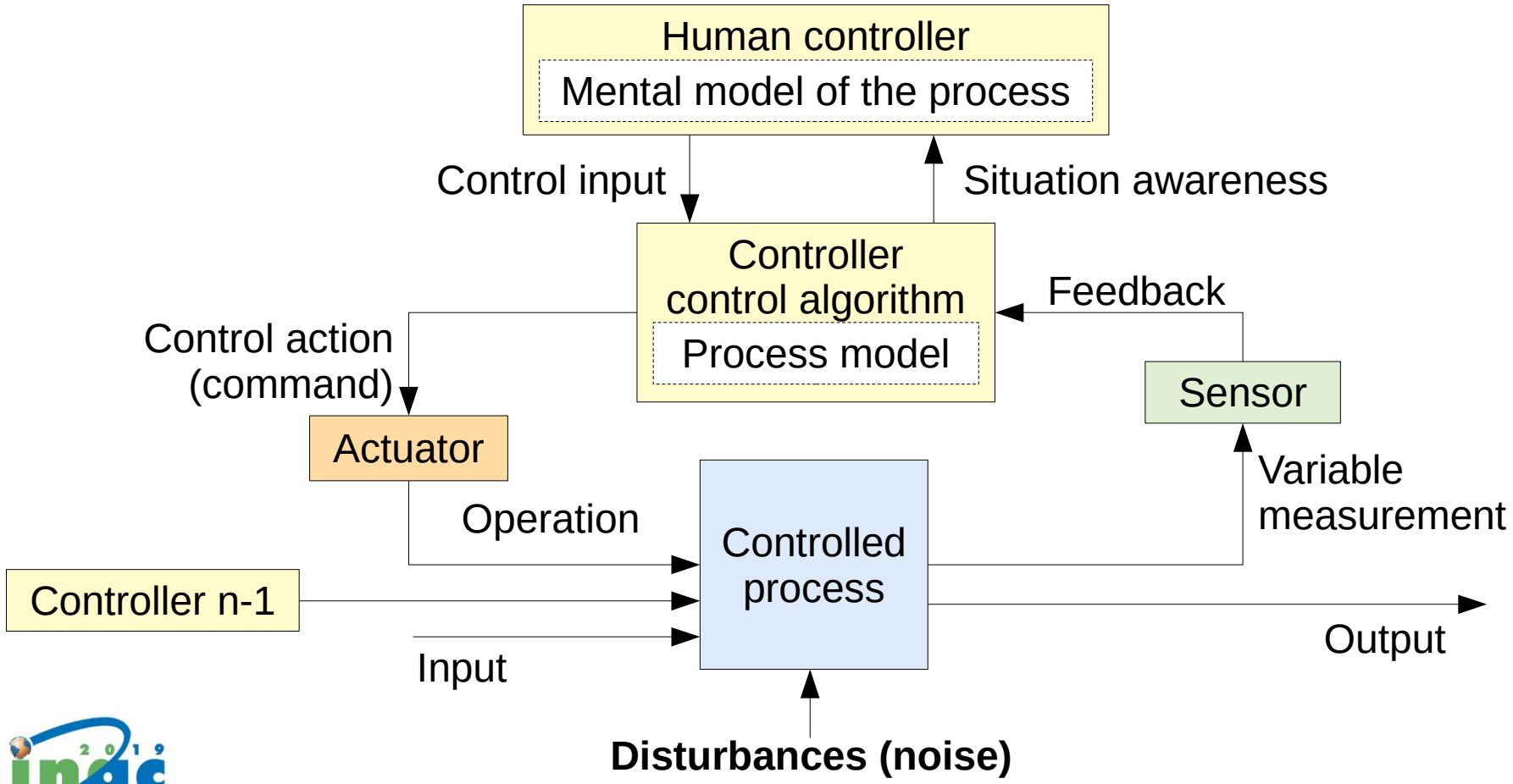
Resilience engineering

The System-Theoretic Accident Method and Process - STAMP: Untoward performance emerges from failures in controlling the system. System Theoretic Process Analysis (STPA) model: (Nancy Leveson, 2011)



Resilience engineering

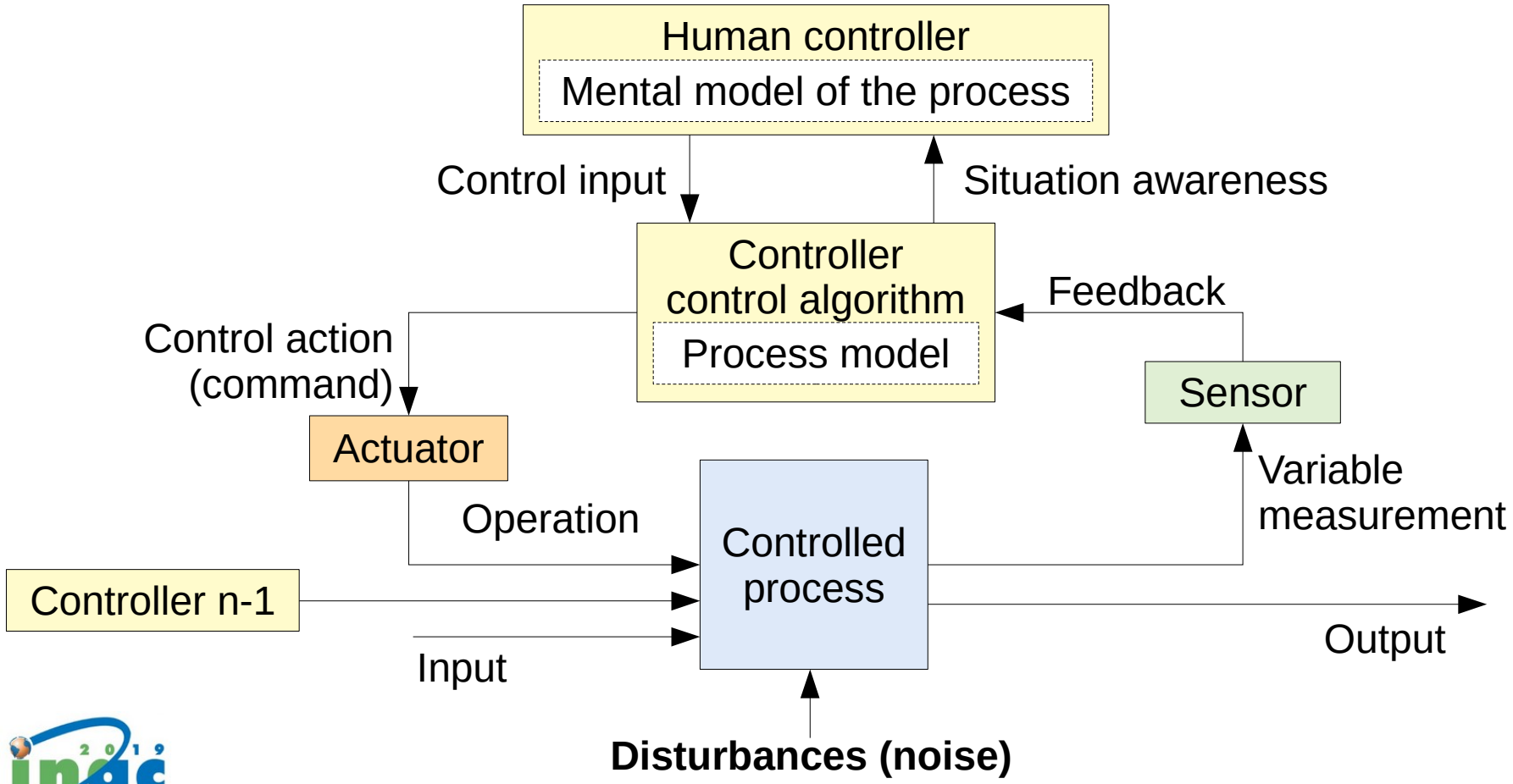
The System-Theoretic Accident Method and Process - STAMP: Untoward performance emerges from failures in controlling the system. System Theoretic Process Analysis (STPA) model: (Nancy Leveson, 2011)



Focus on system process dynamics, not individual human actions

Resilience engineering

The System-Theoretic Accident Method and Process - STAMP: Untoward performance emerges from failures in controlling the system. System Theoretic Process Analysis (STPA) model: (Nancy Leveson, 2011)

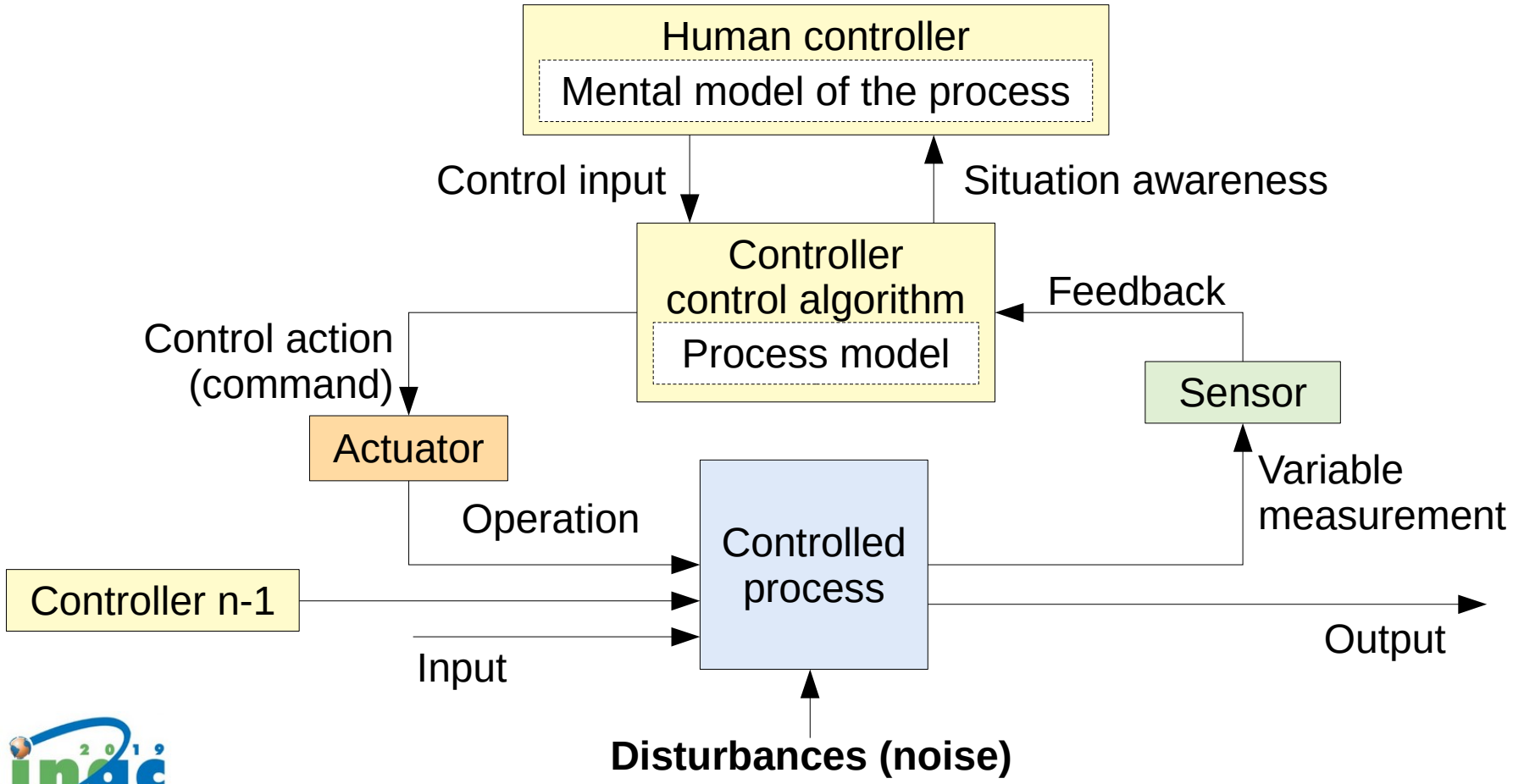


Focus on system process dynamics, not individual human actions

Unrestricted interactions may give rise to emergent properties and system behavior

Resilience engineering

The System-Theoretic Accident Method and Process - STAMP: Untoward performance emerges from failures in controlling the system. System Theoretic Process Analysis (STPA) model: (Nancy Leveson, 2011)



Focus on system process dynamics, not individual human actions

Unrestricted interactions may give rise to emergent properties and system behavior

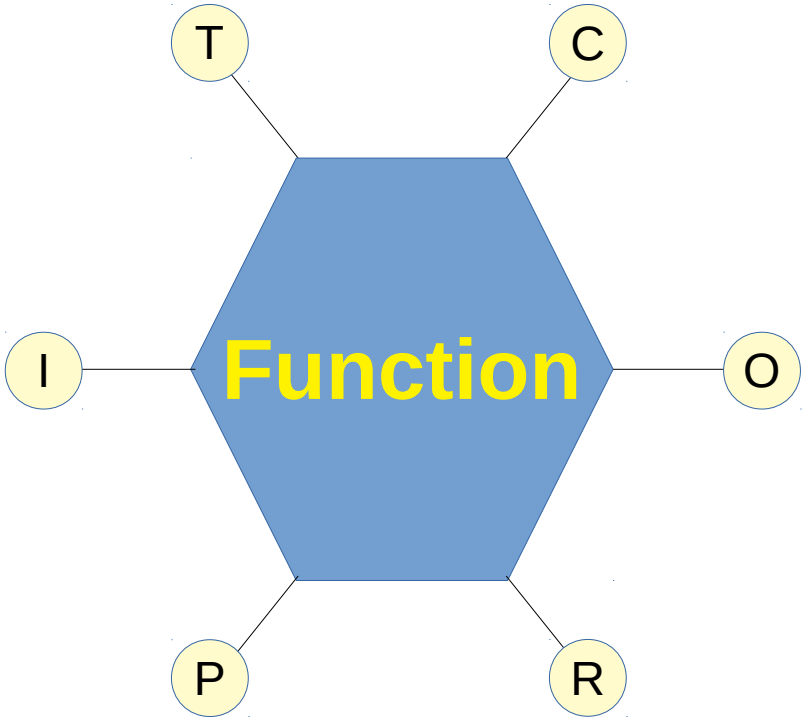
Proper function allocation to impose suitable constraints to systems is paramount

Resilience engineering

The Functional Resonance Analysis Method - FRAM: Untoward performance emerges from performance variability functional resonance: (Erik Hollnagel, 2012)

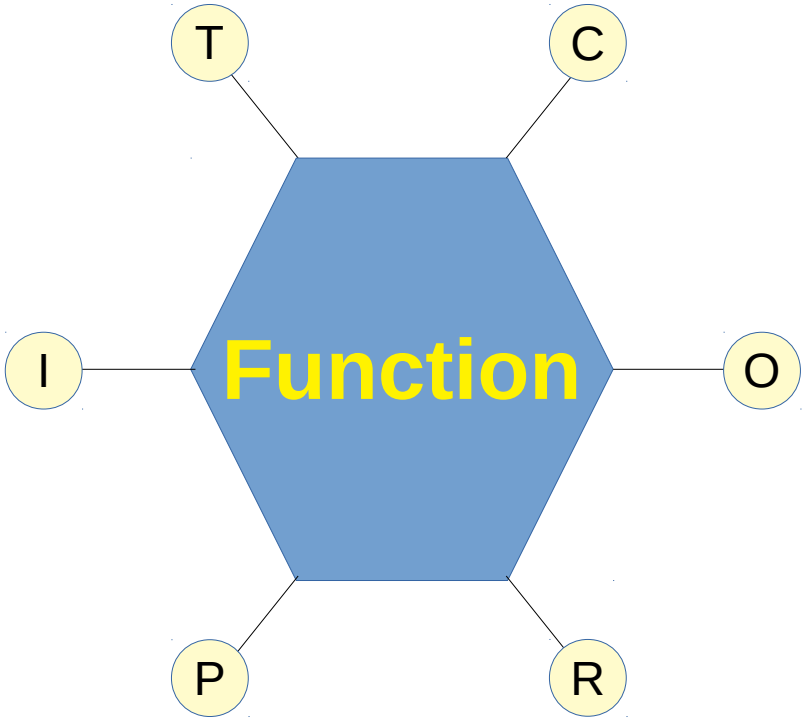
Resilience engineering

The Functional Resonance Analysis Method - FRAM: Untoward performance emerges from performance variability functional resonance: (Erik Hollnagel, 2012)



Resilience engineering

The Functional Resonance Analysis Method - FRAM: Untoward performance emerges from performance variability functional resonance: (Erik Hollnagel, 2012)



Function: relationship between a goal, objective or purpose and the means necessary to achieve them.

Functional aspects: relationships or couplings among functions (**not flows**)

T – **Time**: temporal aspects;

C – **Control**: oversees or regulates the function;

P – **Precondition**: must be met or present before the function is executed;

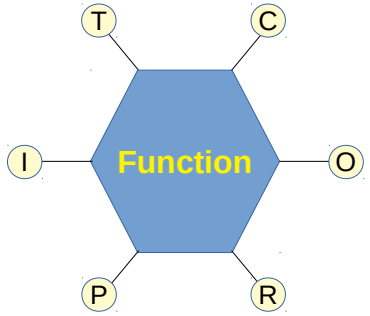
R – **Resources**: necessary, or consumed by the function;

I – **Input**: activates, is used, or transformed to produce the output; and

O – **Output**: result of functional performance. Connection to downstream functions.

Resilience engineering

The Functional Resonance Analysis Method - FRAM: Untoward performance emerges from performance variability functional resonance: (Erik Hollnagel, 2012)



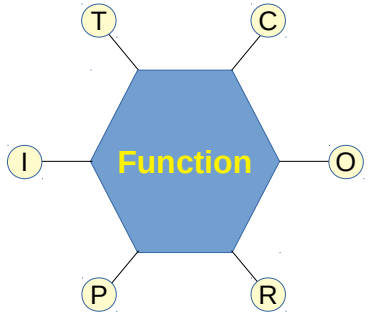
The six aspects connect functions to each other, but do not represent flows, but relationships or couplings.

The study of how variabilities in these six couplings influence the function performance. Varibility and functional resonance may arise from:

- Intrinsic or endogenous variability;
- Extrinsic or exogenous variability due to the environment;
- Upstream-downstream functional coupling variability originated in one or more of functions that provide any of the aspects of a downstream function

Resilience engineering

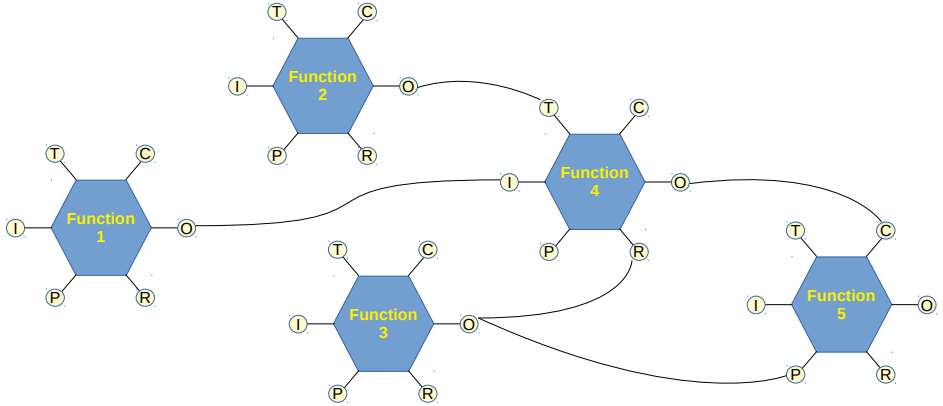
The Functional Resonance Analysis Method - FRAM: Untoward performance emerges from performance variability functional resonance: (Erik Hollnagel, 2012)



The six aspects connect functions to each other, but do not represent flows, but relationships or couplings.

The study of how variabilities in these six couplings influence the function performance. **Variability and functional resonance** may arise from:

- Intrinsic or endogenous variability;
- Extrinsic or exogenous variability due to the environment;
- Upstream-downstream functional coupling variability originated in one or more of functions that provide any of the aspects of a downstream function



Resilience engineering

The Resilience Analysis Grid - RAG: Assessment of an organization's potentials for consistent resilient performance: (Erik Hollnagel, 2018)

The four potentials for resilient performance:

I. Potential to **anticipate**: identify trends, changes, threats and opportunities.

II. Potential to **monitor**: measure performance, conditions and environment.

III. Potential to **respond**: perceive and react in a timely manner.

IV. Potential to **adapt** (learn): identify, capture and apply knowledge to continuously ensure performance.

Resilience engineering

The Resilience Analysis Grid - RAG:

Assessment of eight aspects for the assessment of each of the four potentials.

(Erik Hollnagel, 2018)

Indicators...

- Exist?
- Are they verified?
- Are they validated?
- Are the delays in the sampling process adequate?
- Is their sensitivity adequate?
- Is the collection frequency adequate?
- Are they directly meaningful?
- Are they used to initiate or plan actions?

Resilience engineering

The Resilience Analysis Grid - RAG:

Assessment of eight aspects for the assessment of each of the four potentials.

Specific statements are developed to address each of the eight aspects of the four potentials.

Assessment of these statements are collected using a 5 point Likert scale and plotted on a radar-type diagram.

1. Strongly disagree
2. Disagree
3. Neither agree or disagree
4. Agree.
5. Completely agree.

(Erik Hollnagel, 2018)

Resilience engineering

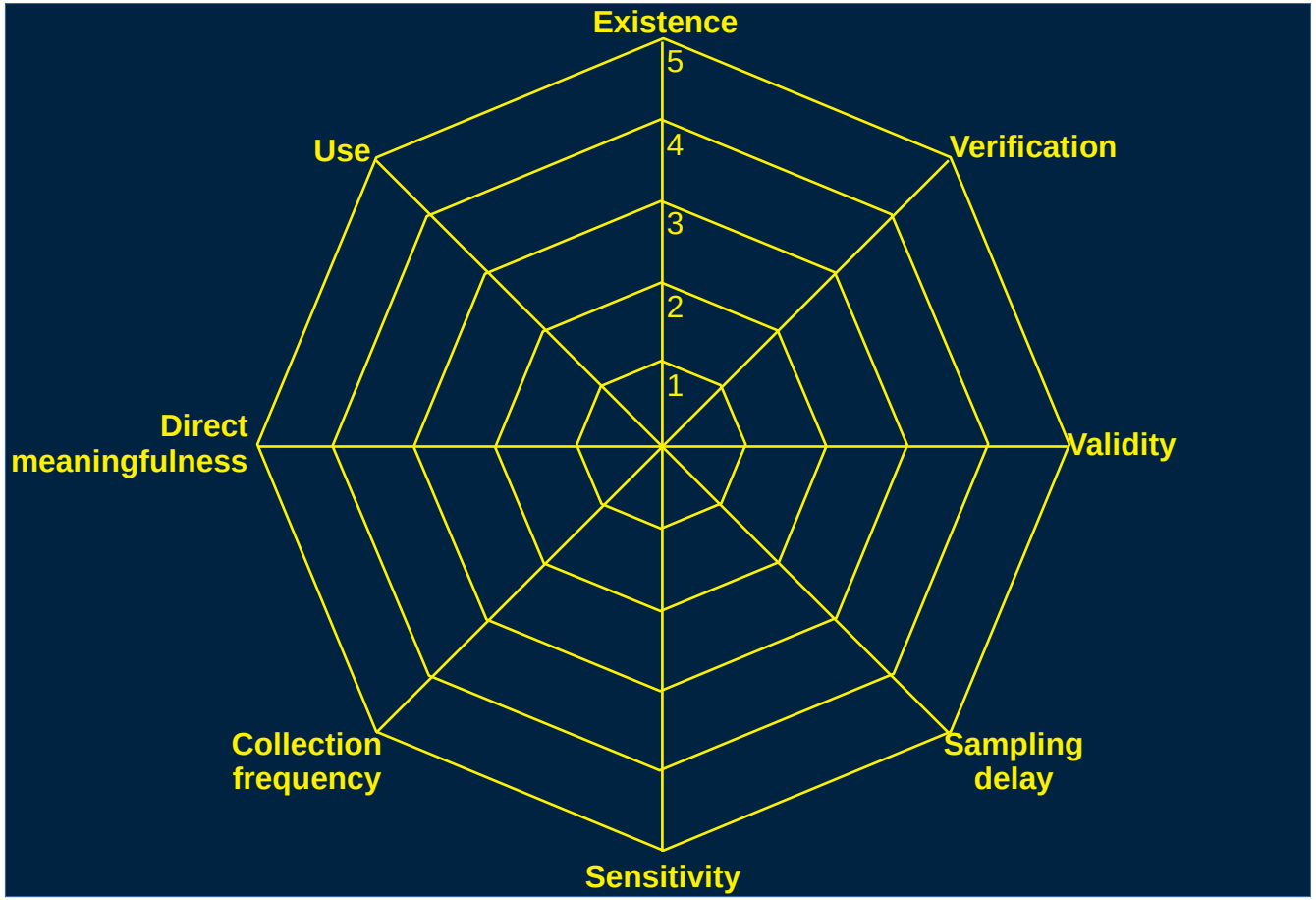
The Resilience Analysis Grid - RAG:

Assessment of eight aspects for the assessment of each of the four potentials.

Specific statements are developed to address each of the eight aspects of the four potentials.

Assessment of these statements are collected using a 5 point Likert scale and plotted on a radar-type diagram.

1. Strongly disagree
2. Disagree
3. Neither agree or disagree
4. Agree.
5. Completely agree.



(Erik Hollnagel, 2018)

Resilience engineering

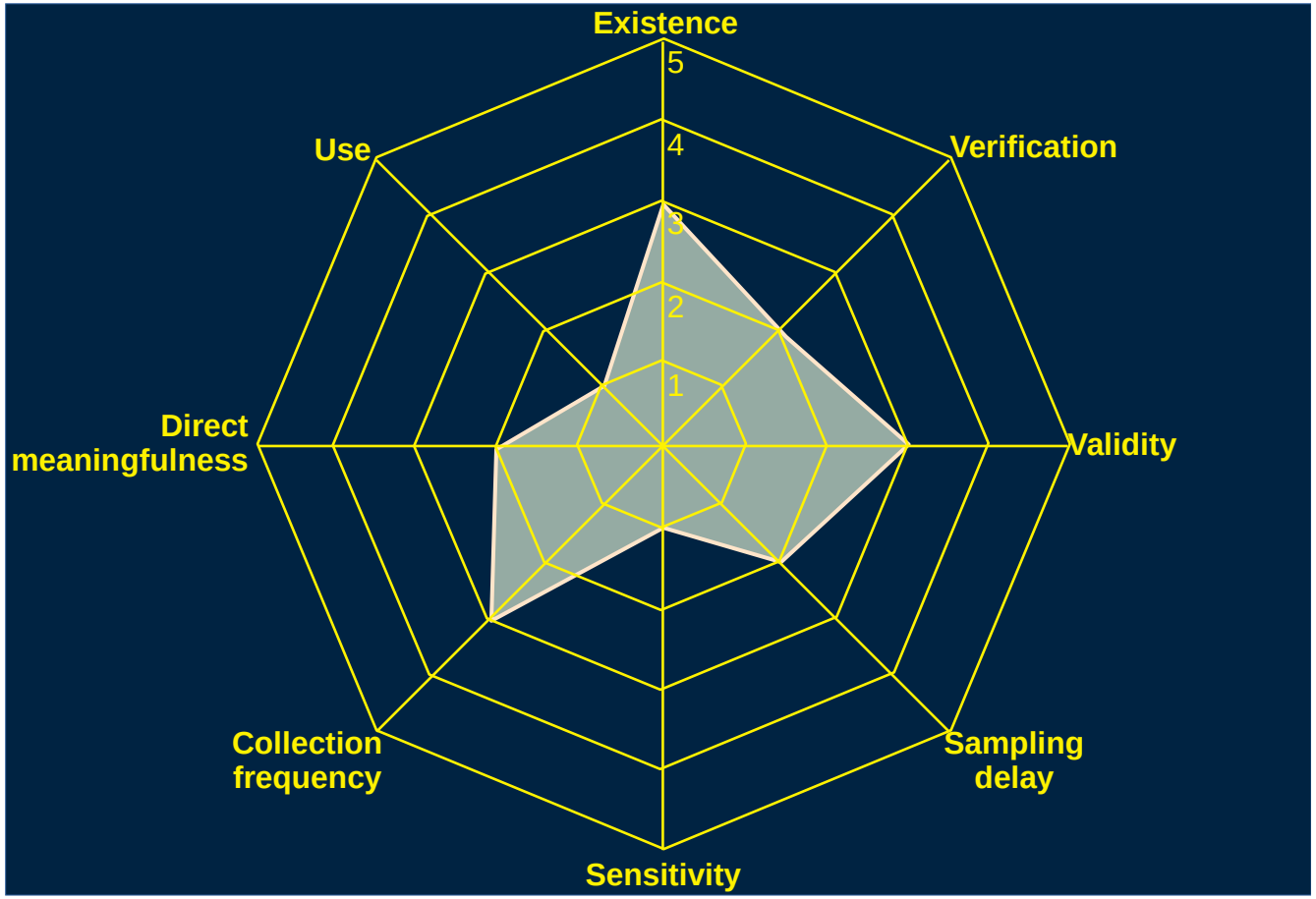
The Resilience Analysis Grid - RAG:

Assessment of eight aspects for the assessment of each of the four potentials.

Specific statements are developed to address each of the eight aspects of the four potentials.

Assessment of these statements are collected using a 5 point Likert scale and plotted on a radar-type diagram.

1. Strongly disagree
2. Disagree
3. Neither agree or disagree
4. Agree.
5. Completely agree.



(Erik Hollnagel, 2018)

Resilience engineering

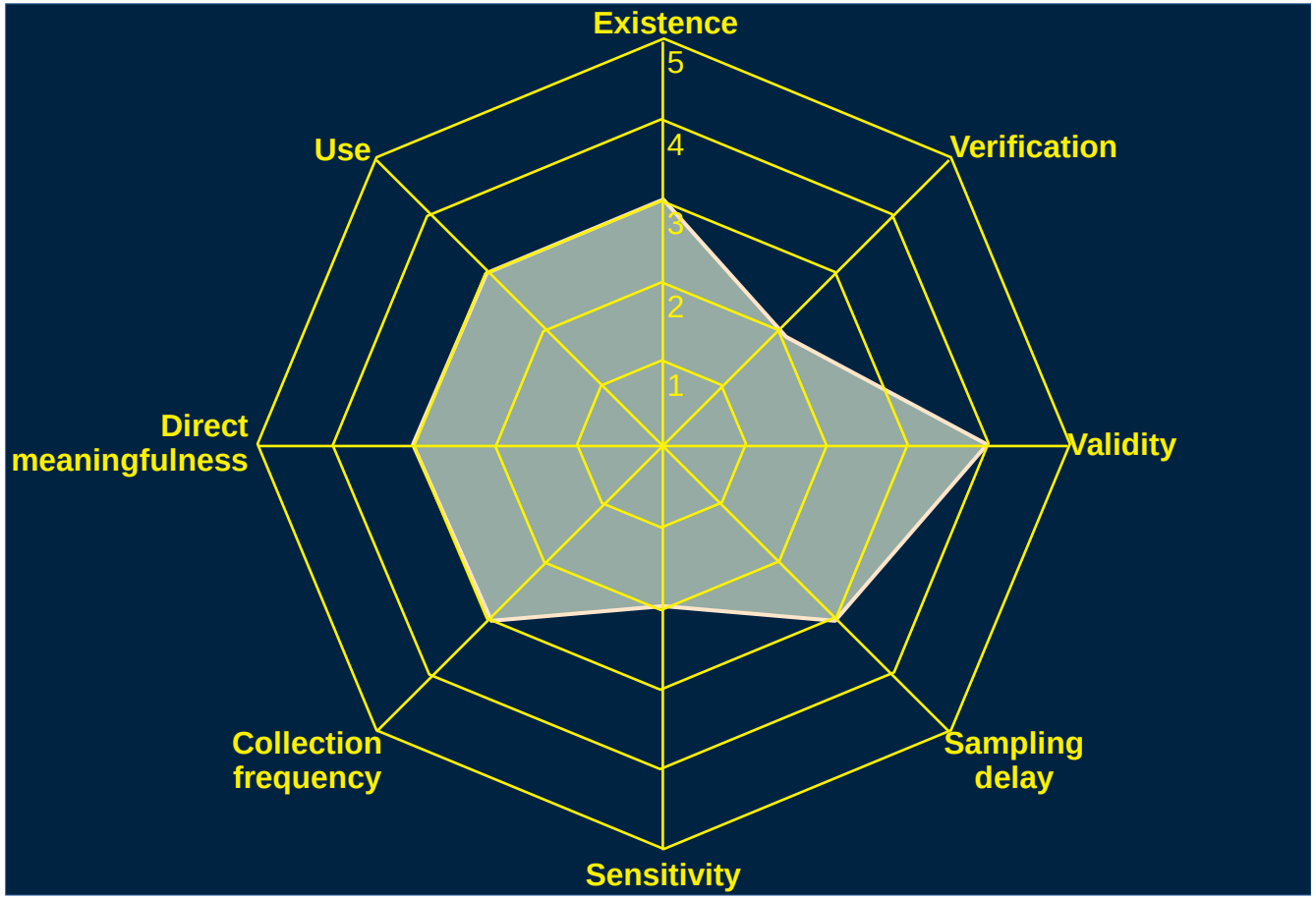
The Resilience Analysis Grid - RAG:

Assessment of eight aspects for the assessment of each of the four potentials.

Specific statements are developed to address each of the eight aspects of the four potentials.

Assessment of these statements are collected using a 5 point Likert scale and plotted on a radar-type diagram.

1. Strongly disagree
2. Disagree
3. Neither agree or disagree
4. Agree.
5. Completely agree.



(Erik Hollnagel, 2018)

Resilience engineering

The issue of a quantitative approach.

Resilience engineering methods are, currently, limited to qualitative approaches.

STAMP: transfer functions for the elements of a STAMP model.

FRAM: mathematical representation of functions and couplings, quantification of functional resonance.

RAG: reducing subjectivity in capturing perceptions.

(Erik Hollnagel, 2018)

Summary

- Accident causality
- Safety I and Safety II
- Resilience engineering
- Resilience engineering and Nuclear Energy
- What lays ahead

EAR-1 – IPEN/USP reseach reactor

Resilience engineering and nuclear energy

Resilience engineering has been applied to several different activities, especially those where safety is critical.




However, there are few cases of its application to nuclear energy.

Resilience engineering and nuclear energy

SYSTEMATIC BIBLIOGRAPHIC REVIEW

Search criteria

Term: “ **RESILIENCE . AND. ENGINEERING**”

In: Title, abstract, author keywords and topics.

Period: From 2015 to 2019.

Publication types: Journals and conference papers.

Resilience engineering and nuclear energy

SYSTEMATIC BIBLIOGRAPHIC REVIEW

7615 unique entries

7409 rejected

- Ecological resilience;
- Psychological resilience;
- Material resilience;
- Societal resilience;
- Network resilience;
- ...

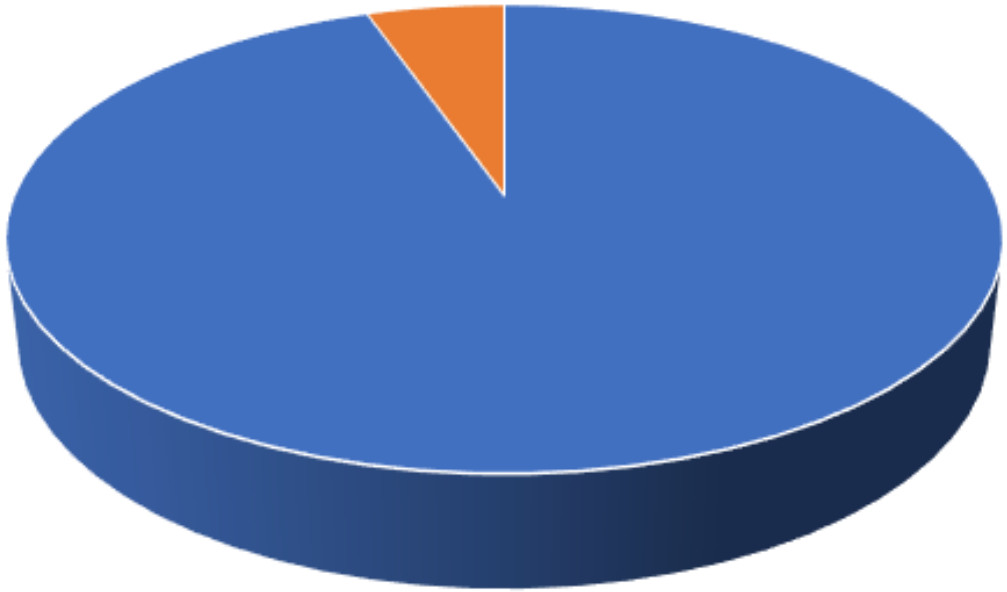
206 accepted

- Transport: 46;
- Industry & energy: 42
- Healthcare: 31
- Human factors & HSW: 28
- Management: 26
- Theory & methods: 22
- **Nuclear: 11**

Resilience engineering and nuclear energy

SYSTEMATIC BIBLIOGRAPHIC REVIEW

Nuclear: 5%

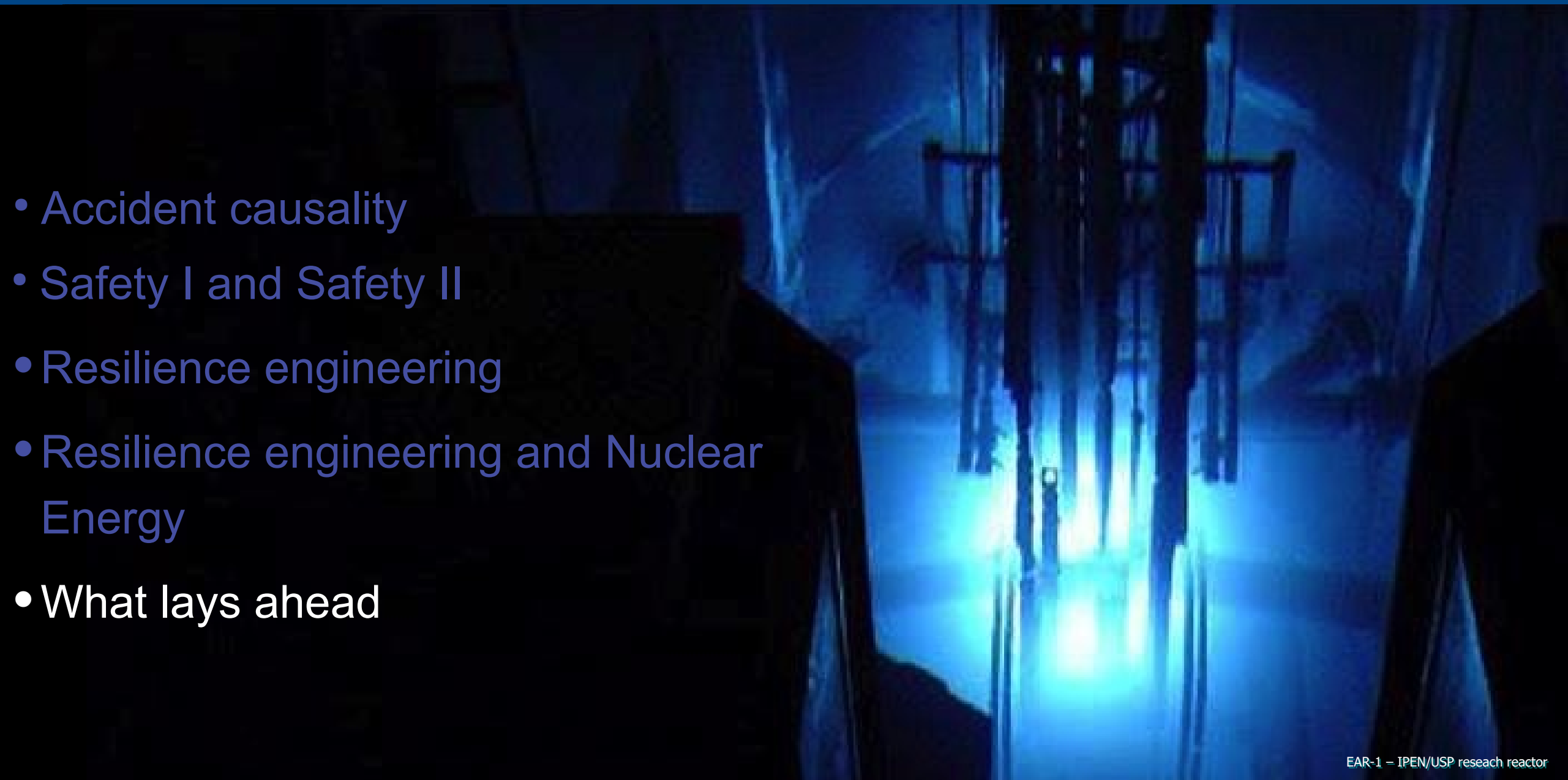


Other: 95%

- Healthcare,
- Transportation,
- Energy (not nuclear),
- ….

Summary

- Accident causality
- Safety I and Safety II
- Resilience engineering
- Resilience engineering and Nuclear Energy
- What lays ahead



EAR-1 – IPEN/USP reseach reactor

What lays ahead

SYNESIS: SAFETY I + SAFETY II and more…

Synesis is the unification of activities that is necessary in order that today's socio-technical systems can function as intended and desired. (Hollnagel, 2019)

Holistic and multidisciplinary approach.

Resilient culture? Resilient regulation?

THANK YOU.

Tuxaua Q. de Linhares, M.Sc.
tlinhares@nuclear.ufrj.br