Risk-based design of technical facilities

Doc. RNDr. Dana Procházková, DrSc.

CONTENT

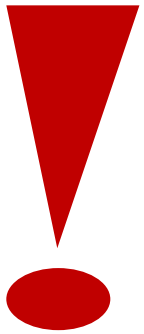
1. Introduction
2. Summary of knowledge on technical facilities
3. Data for risk-based design of technical facilities
4. Risk causes in designing the technical facilities
5. Risk management plan at designing
6. Procedure of generation of risk-based design of technical facilities
7. Conclusion

1. INTRODUCTION

In presentation we will follow technical facilities created by humans, which facilitate their lives; no military ones.

However, all positive consequences of technical progress on the humans are redeemed by existence of a much larger number of risks that lead to:

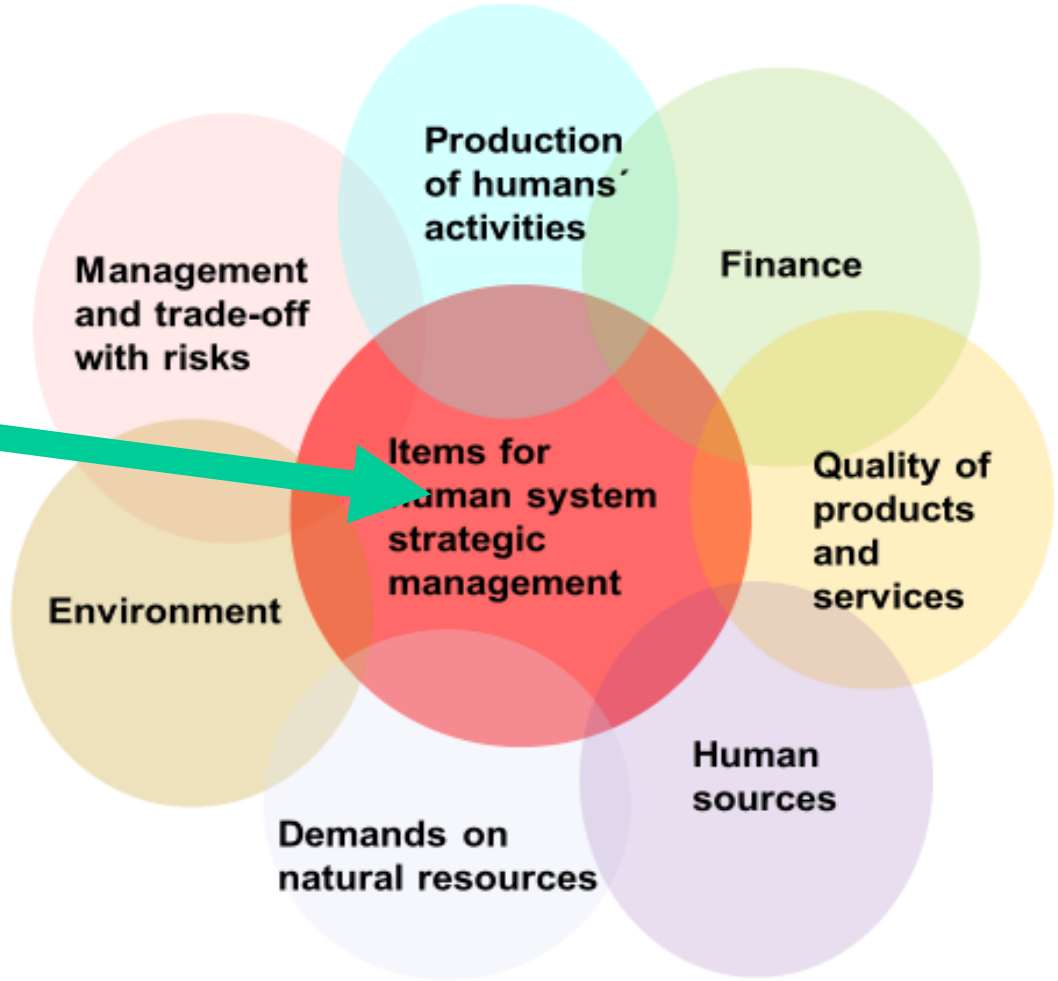
- **the failure of the State basic functions,**
- **safety level reduction,**
- **disruption of coexistence of technical facilities with their surroundings,**
- **loses on humans lives and health.**



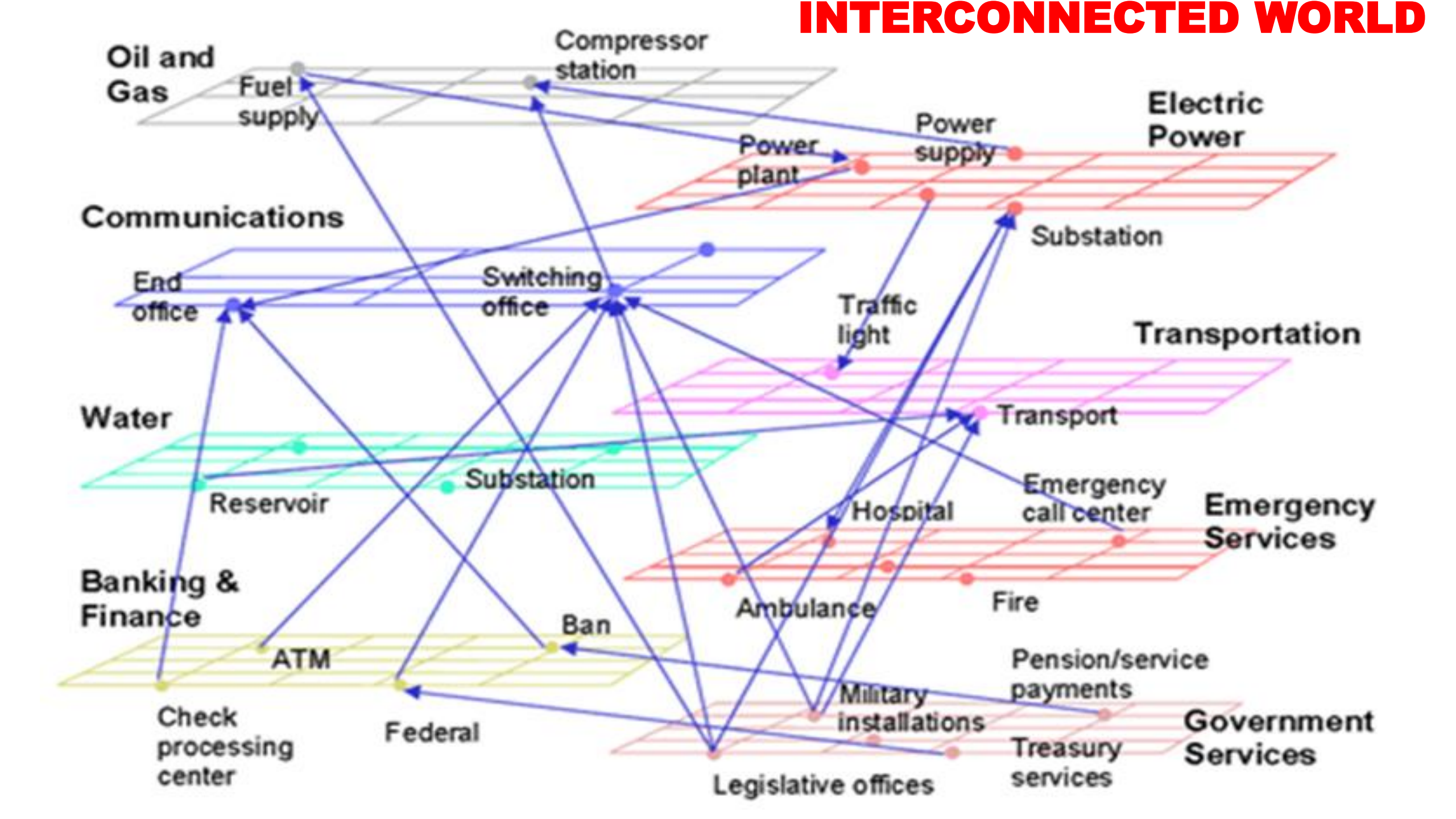
The risk expresses the probable size of unacceptable impacts (losses, damages and harms) of disasters with size of normative hazard on entity assets or subsystems in a given time interval (e.g. 1 year) in a given site, i.e. risk is always site and time specific).

For safety and coexistence of technical facilities with vicinity, we need:

- **to consider strategic management,** i.e. many different aspects**,**
- **to manage risks during all stages of their lives, i.e.:**
  - sitting,
  - designing,
  - building,
  - construction,
  - operation,
  - decommissioning.



We further concentrate to designing.


INTERCONNECTED WORLD
Oil and Gas
Fuel supply
Compressor station
Power plant
Power supply
Electric Power
Substation
Communications
End office
Switching office
Traffic light
Transportation
Transport
Water
Reservoir
Substation
Emergency call center
Hospital
Emergency Services
Ambulance
Fire
Banking & Finance
ATM
Ban
Pension/service payments
Military installations
Government Services
Treasury services
Check processing center
Federal
Legislative offices

Tools supporting the technical facilities safety are:

1. **Standards and norms for sitting, designing,** building and operation.
2. **Risk management at sitting, designing,** building and operation.
3. **Risk management plans.**
4. **Emergency plans.**
5. **Continuity plans.**
6. **Crisis plans.**

The lessons learned from practice show that respecting the present standards and good practice principles:

- **averts to repeat mistakes from the past,**
- **but it covers only 68.4 % of possible cases.**

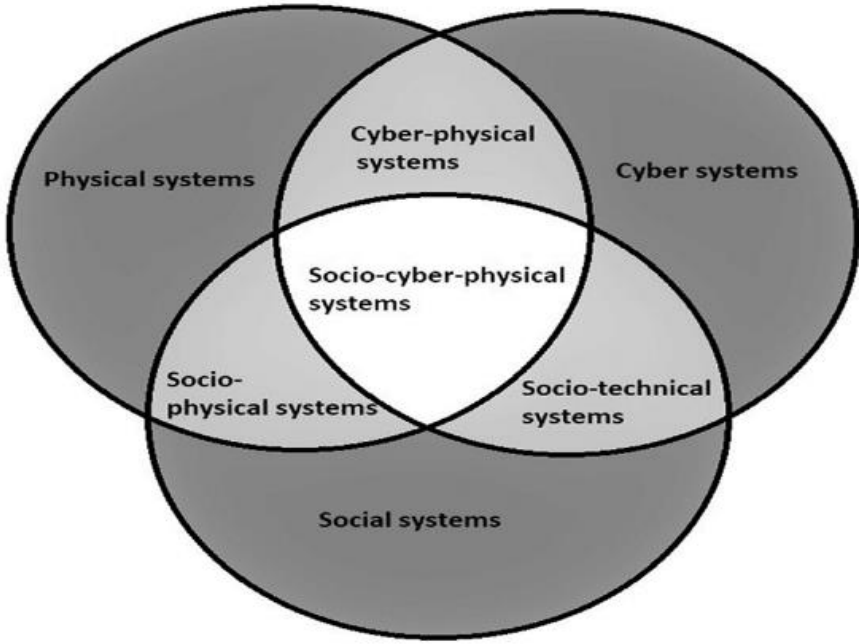
Risk management is necessary – novella ISO 9000 from 2015

I WILL SHOW HOW TO REALIZE RISK MANAGEMENT IN DESIGN.

2. SUMMARY OF KNOWLEDGE ON TECHNICAL FACILITIES

According to recent knowledge technical facilities:

- **are systems of systems** (open set of mutually interconnected open systems),
- **have natures socio-cyber-physical (technical).**



A system according to its core means more than only a sum of parts, and therefore, the stress is put on:

- study of the interactions and associations,
- **non-linear thinking, interactions**,
- inductions,
- feedbacks,
- experiments or realistic simulations.

E.g. feedbacks cause non-linearity's in the system behaviour that is not predictable, and therefore, it is not possible to use the common prognostic methods for the identification of the possible states of a system.

The characteristics of a system thinking are:

- to see both, the whole and the details at the same time,
- to focus on the dynamics of processes,
- to pay attention to relations, associations and interactions,
- to take into account the roles of feedback,
- to consider the relativity of possible situations,
- to think in a long-term way.

Each system is characterized by elements, linkages and flows. Linkages and flows cause interdependences.

Flows of energy, information, material, finances etc. among the system elements cause couplings that are causes of vulnerabilities are also .

These couplings create **interdependences** that are often the causes of failures at extreme disasters.

Interdependences are required and non-demanded and their natures are physical, cyber, organisational and territorial.

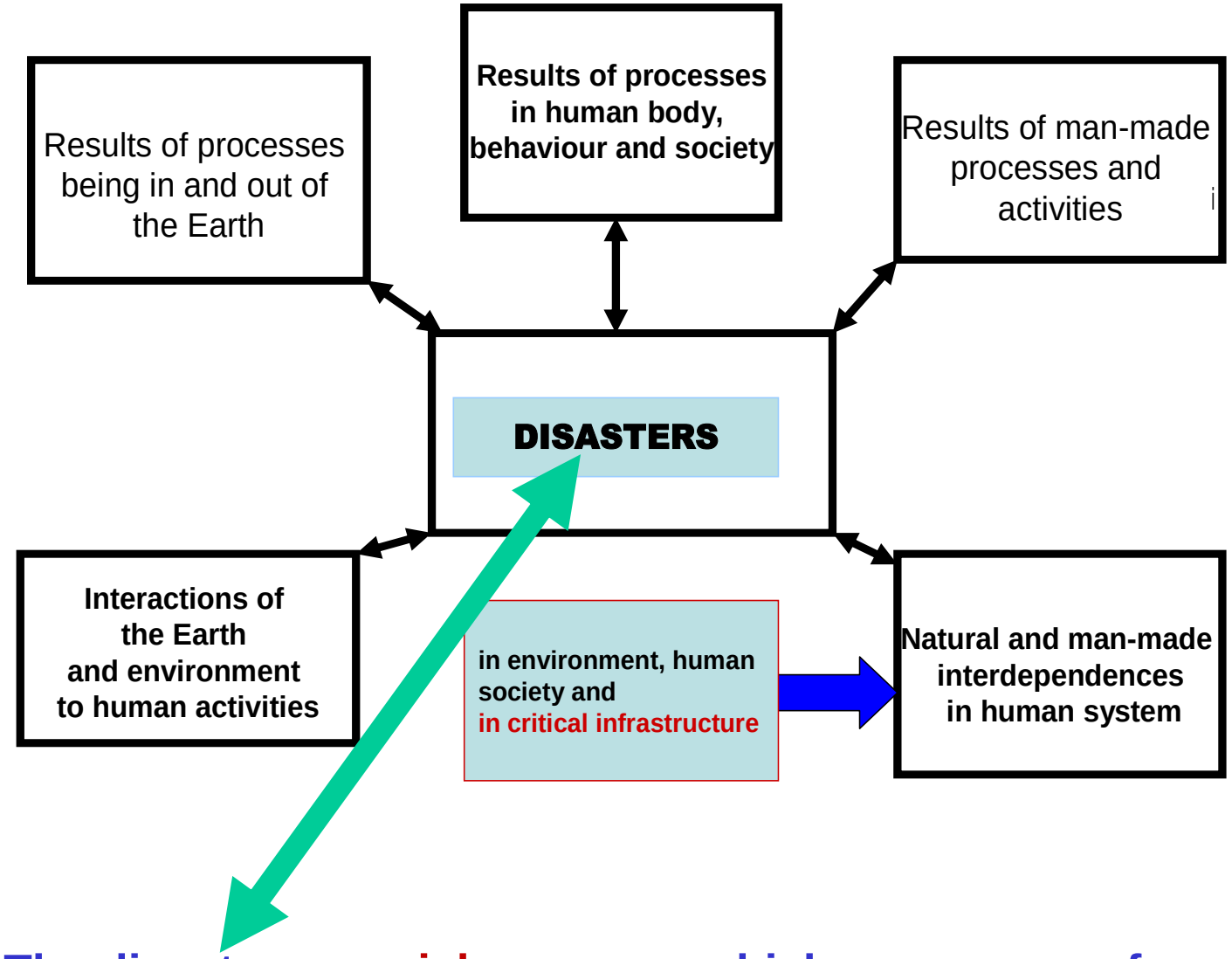
For the characteristic and management of technical facilities, including the designing, we need to differentiate:

- **simply organized units,** the results of analytic solutions are used,
- **composite systems** (in practice the term construction is used) that are understood as a representation of elements that are organized and connected in a certain way and because of a proper structure they fulfil certain functions, there are used results of statistical solutions based on analytic functions, the parameters of which are variable in a certain interval, which is a reflection of various possible states / variants of the system behaviour,
- **complex systems**, the results of simulations must be used since the given aggregates have many components (often systems too) those interact together and are organized in several levels, which causes that we observe:
  - **suddenly emerged behaviour** features that is not possible to obtain from the knowledge of components' behaviour, it is the so-called emergence,
  - **hierarchy,**
  - **self-organization,**
  - **various management structures, which all together seems as a chaos.**

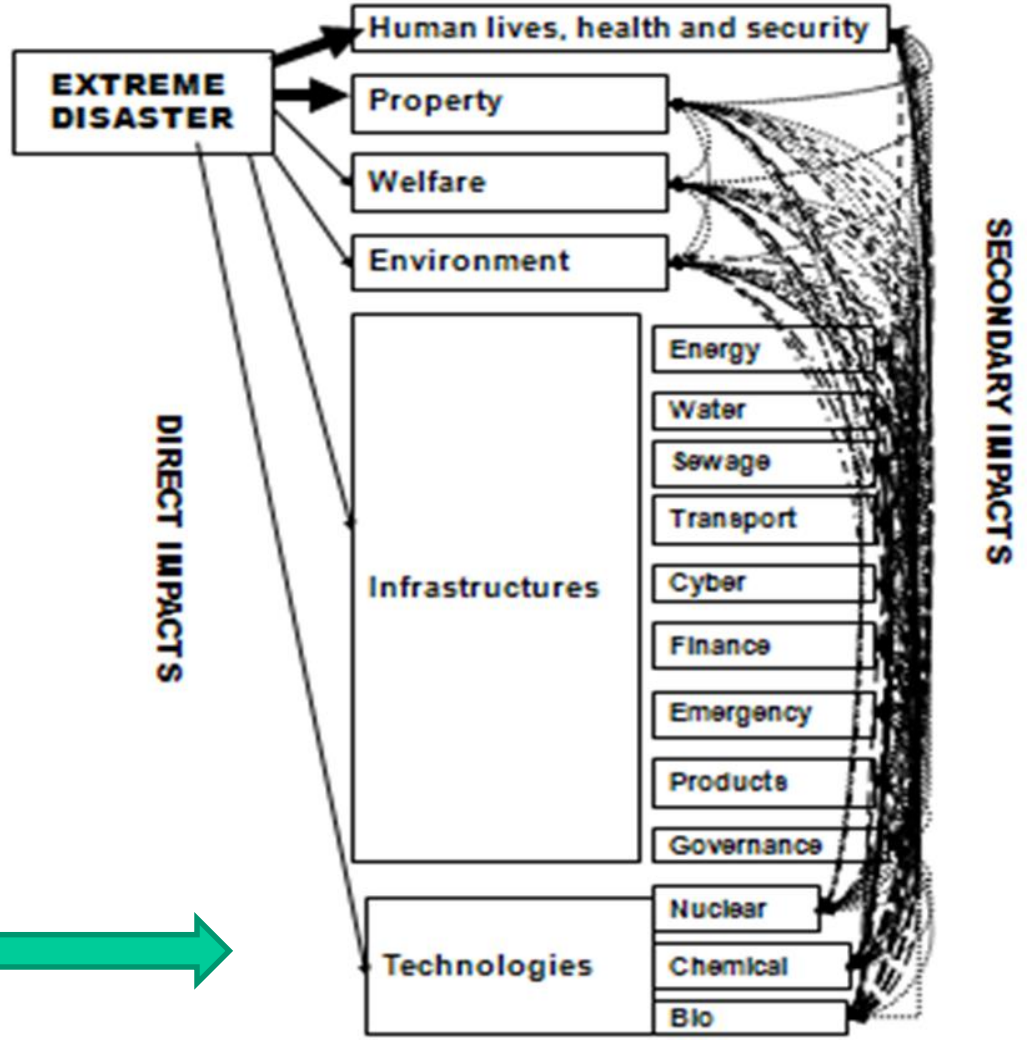
Special type is system of systems.

All important technical facilities with object or network structures are complex.

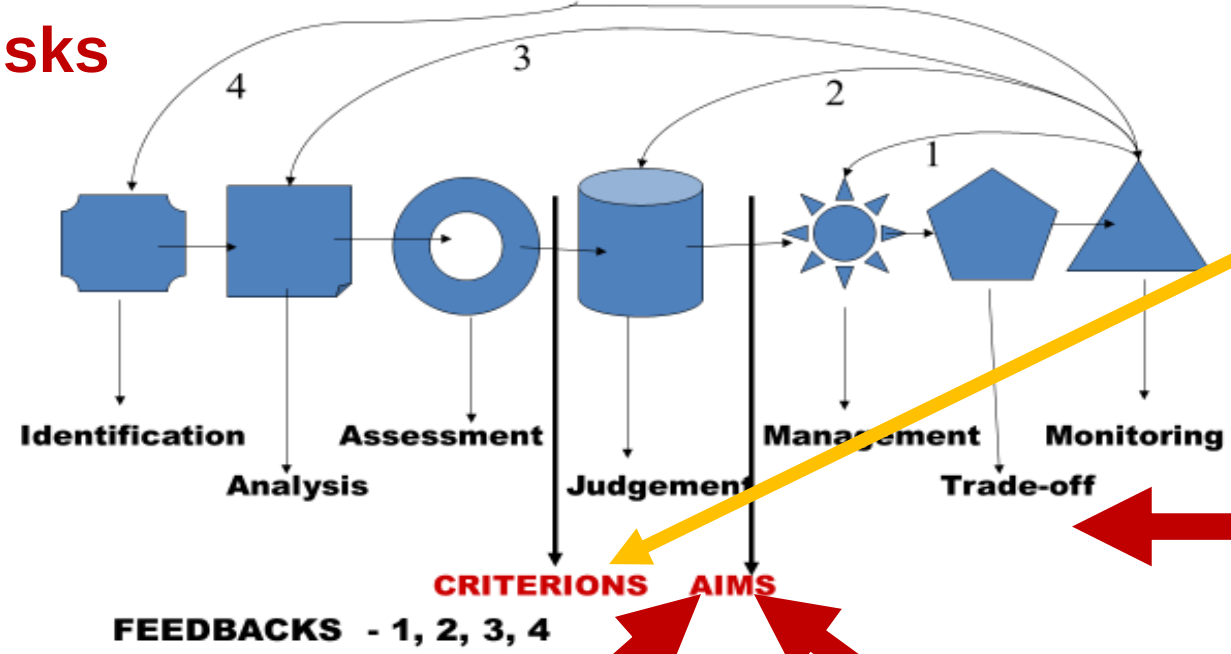
All-Hazard-Approach



The disasters are risk sources, which are causes of emergency situations, the severity of which substantially increases if cascade impacts occur.



Work with risks

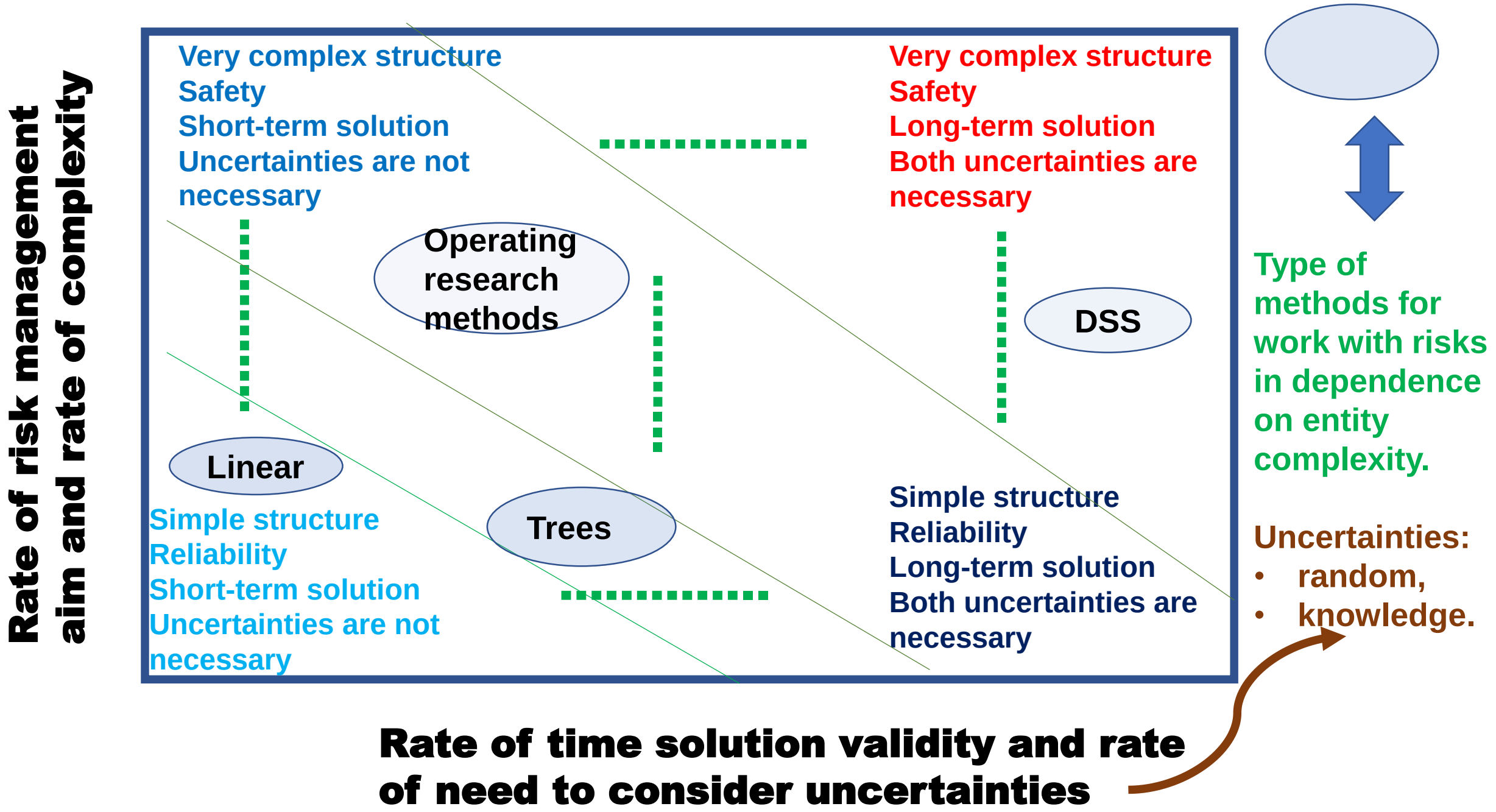


Risk:
- **acceptable**
- **ALARA**
- **unacceptable**

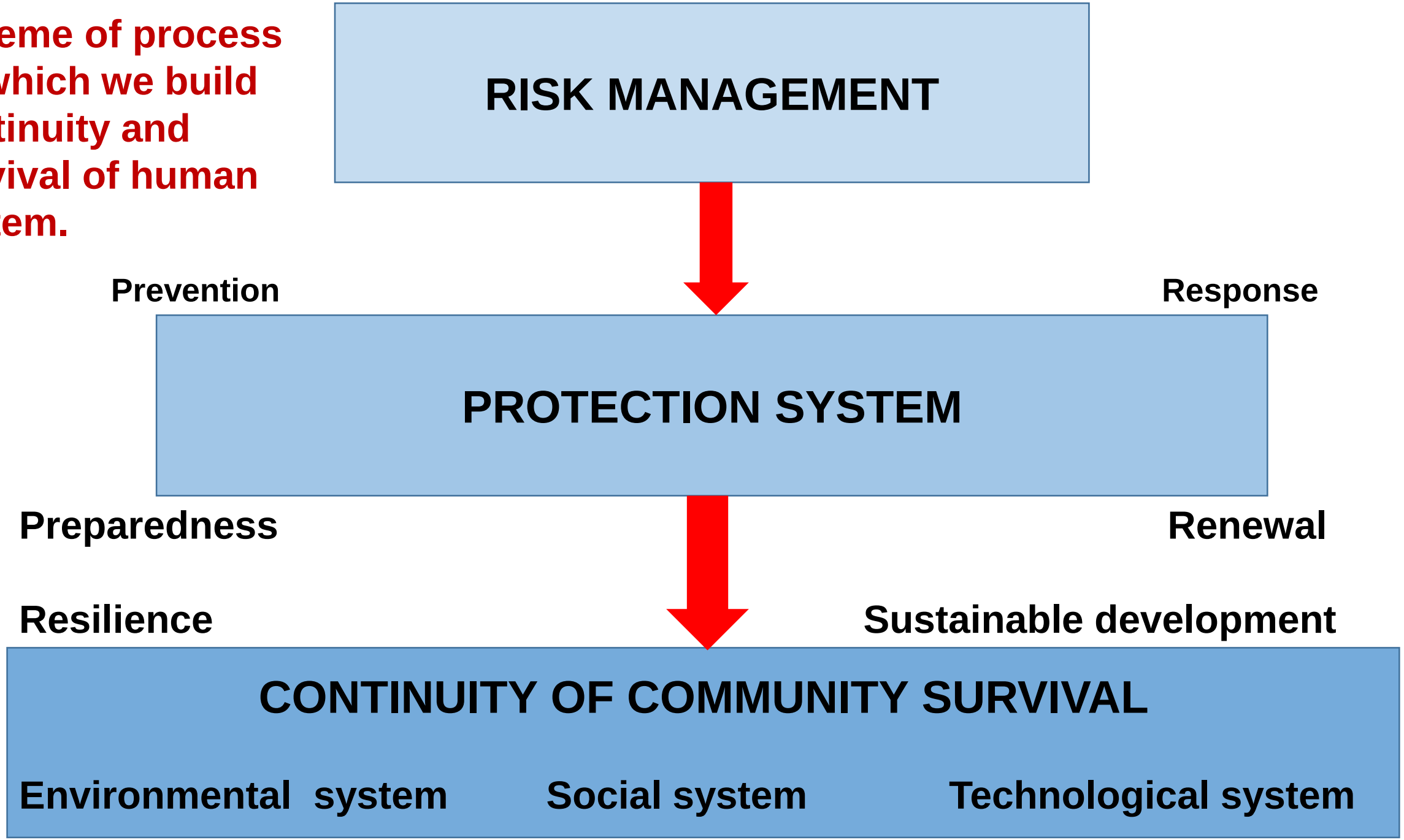
Tools for trade-off with risks:
- **prevention,**
- **preparation** (tools for mitigating, procedures, technique…..),
- **response,**
- **renovation.**

1. **Safe asset – human, environment, machine …**
2. **Safe fittings – tool, machine, component…**
3. **Save personnel**
4. **Safe complex of machines, production line**
5. **Safe set of product lines**
6. **Safe network**
7. **Safe set of infrastructures**
8. **Safe process**
9. **Safe operation**
10. **Safe system of systems**

It predetermines tools of work with risks.


Rate of risk management aim and rate of complexity
Very complex structure
Safety
Short-term solution
Uncertainties are not necessary
Very complex structure
Safety
Long-term solution
Both uncertainties are necessary
Operating research methods
DSS
Linear
Trees
Simple structure
Reliability
Short-term solution
Uncertainties are not necessary
Simple structure
Reliability
Long-term solution
Both uncertainties are necessary
Type of methods for work with risks in dependence on entity complexity.
Uncertainties:
• random,
• knowledge.
Rate of time solution validity and rate of need to consider uncertainties

Scheme of process by which we build continuity and survival of human system.



RESILIENCE

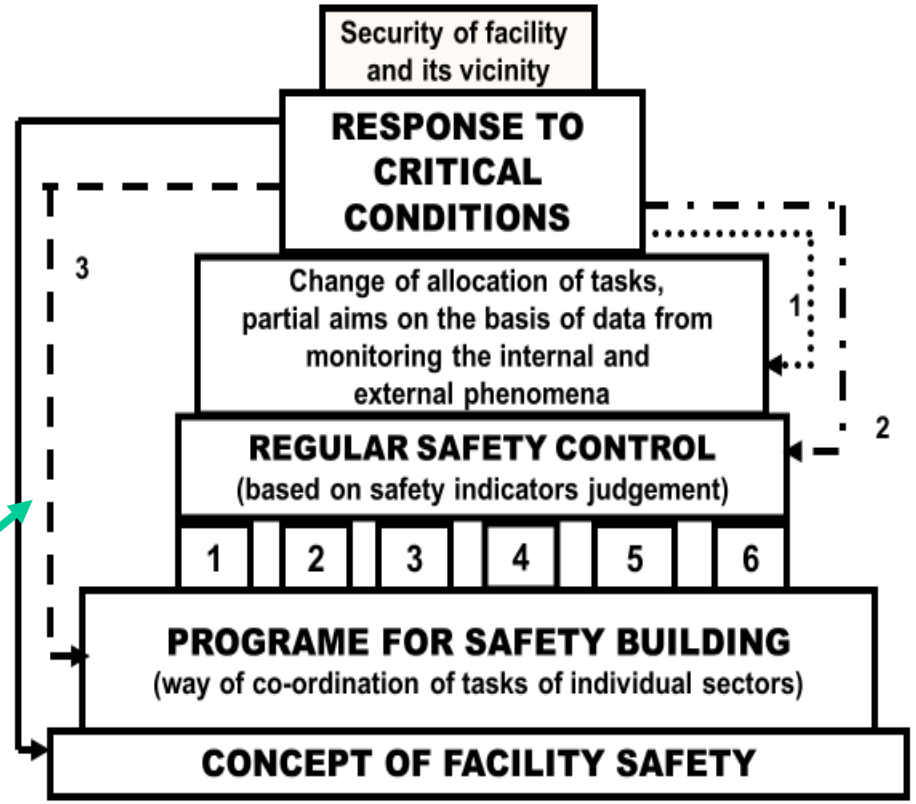
ROBUSTNESS
System withstand outer load without loss of functionality.

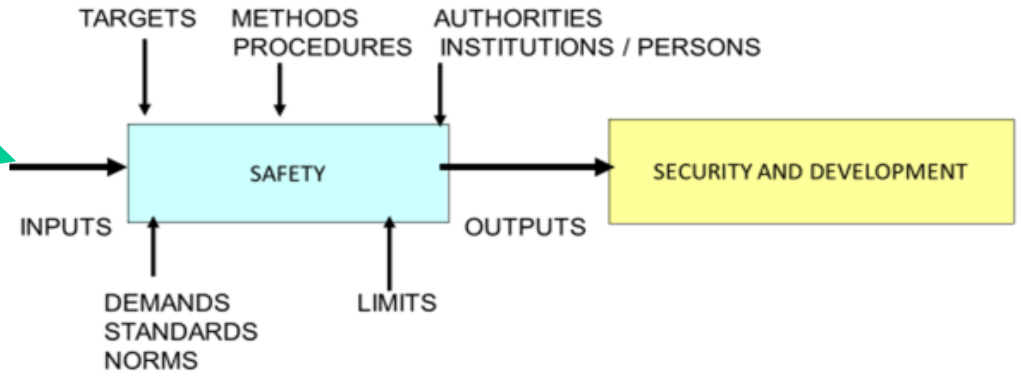
REDUNDANCY
System works during the break. System is due to back up functional during the break.

INVENTIVENESS
System is capable to identify problem and to mobilise sources.

SPEED
System is capable to reach the target and so to avert future damages.

Examples of tools for safety building.





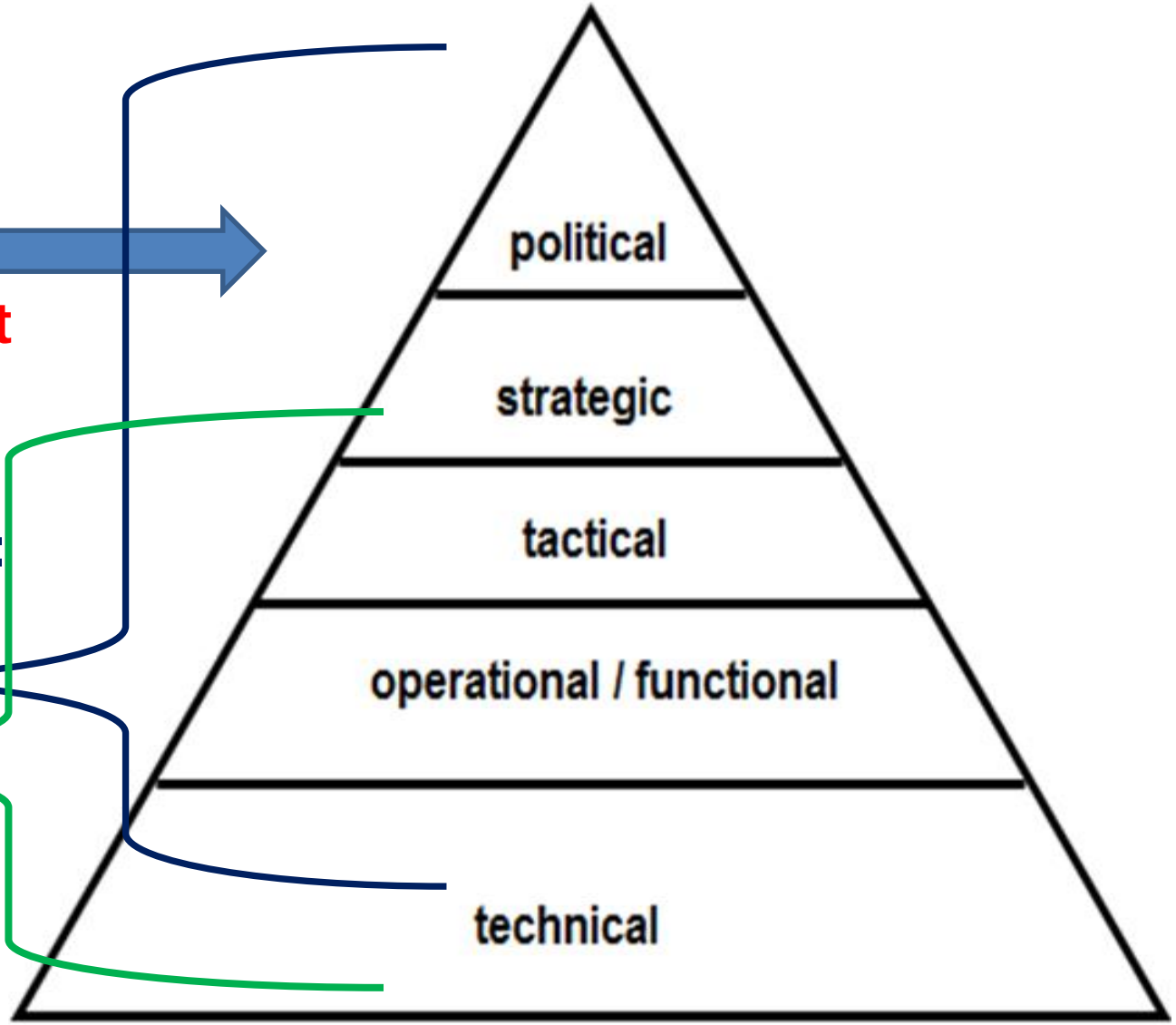
Process of ensuring the safety and security and its factors.

RESPONSIBILITIES FOR THE RISK MANAGEMENT OF THE TECHNICAL FACILITIES

Because the technical facilities are critical assets of each State, the technical facilities safety and the technical facilities protection need to be ensured at all management levels.

Responsibilities for risk management:

A. The territory administration
B. The technical facility



Human cognition contains a lot of knowledge and experiences with risks.
Generally, from safety reasons it is necessary:

1. **To control the processes that lead to significant risks.**
2. **To reduce the vulnerabilities of public assets.**
3. **To rise the human society resilience.** Resilience is the combination of asset capability „withstanding" and "recovering" from disaster.

The aim of our research, the results of which will be presented, was the judgement how in practice connected with complex technological facility safety it is used the present human cognition.

I.e.

How they are used pieces of knowledge on:

- **risk sources,**
- **ways of work with risks that have potential to ensure:**
  - **human security,**
  - **safe technical facility and its safe vicinity.**

3. DATA FOR RISK-BASED DESING OF TECHNICAL FACILITIES

Tasks of designing:

- **theoretical analysis of:**
  - **critical processes,**
  - **equipment and places** and design of practical implementation of technically and financially available countermeasures,
- **selection of:**
  - **materials,**
  - **technical principles**, construction procedures, determination of critical construction and mounting processes etc.,
- **experimental verification** of installed fittings and their operability under normal, abnormal and critical conditions,
- **ensuring the:**
  - **durability,**
  - **tractability of equipment and processes**, required service life; quality and sufficient human resources, costs in the required amount, technical services; services etc.; and realization of buildings, structures and equipment under given conditions, etc.

For humans security and technical facilities safety, it is needed, so that environment reactions throughout technical facility lifetime would be adequate and its coexistence with surrounding may exist.

Ensuring these aims needs to be inserted in designing.

Firstly, it is necessary to consider sources of all risks – All-Hazard-Approach – i.e. not only phenomena that damaged fittings, components and other physical elements, but also destructive phenomena that are results of all mutual reactions inside and outside technical facilities under, normal, abnormal and critical conditions.

The identification of risk sources is critical activity for ensuring the technical facilities safety at operation.

Terms of references are the base for future safety.

At terms of references creation, it is necessary to have:

- **knowledge of:**
  - regulations,
  - risks in the site to which the technical facility is placed,
  - technical system, which constitutes a technical facility; models and theories associated with accidents; methods of analysis, management and settlement of risks; and management of enterprise (finance, human resources, organization, technology, innovation...),
- **competencies for:**
  - the application of results of methods of risk analysis and evaluation,
  - implementation of methodology of analysing and assessing the risks adapted to the problem,
  - emergency and crisis management; analysis of situations / activities / accidents; transformation of policy into real actions; the conversion of accident statistics into action plans; strategic planning; hierarchy of problems; capability to find right information and lesson learned; critical analysis; designing the right solutions; communication; carrying out the synthesis and adapting the wording intended for the public; and ethics.

In terms of reference creation, it is necessary to:

- **specify: for each relevant disaster, size of threat according to given standards; identify critical tasks of technical facility from integral safety viewpoint,**
- **understand tasks and causes of their criticality,**
- **identify possible human failures,**
- **propose measures for safety ensuring with regard to variable conditions.**

Their critical tasks from integral safety creation viewpoint are physical activities, by which operator contributes to:

- **triggering the non-committed and unacceptable phenomenon,**
- **detection and prevention of phenomenon in question,**
- **management and mitigation of phenomenon in question,**
- **response to emergency situation.**

The aim of technical facility design is to create a production process that is profitable, economic, safe and does not threaten public assets, especially humans and environment.

This can be achieved by optimizing the safeguard, economic and functional criteria.

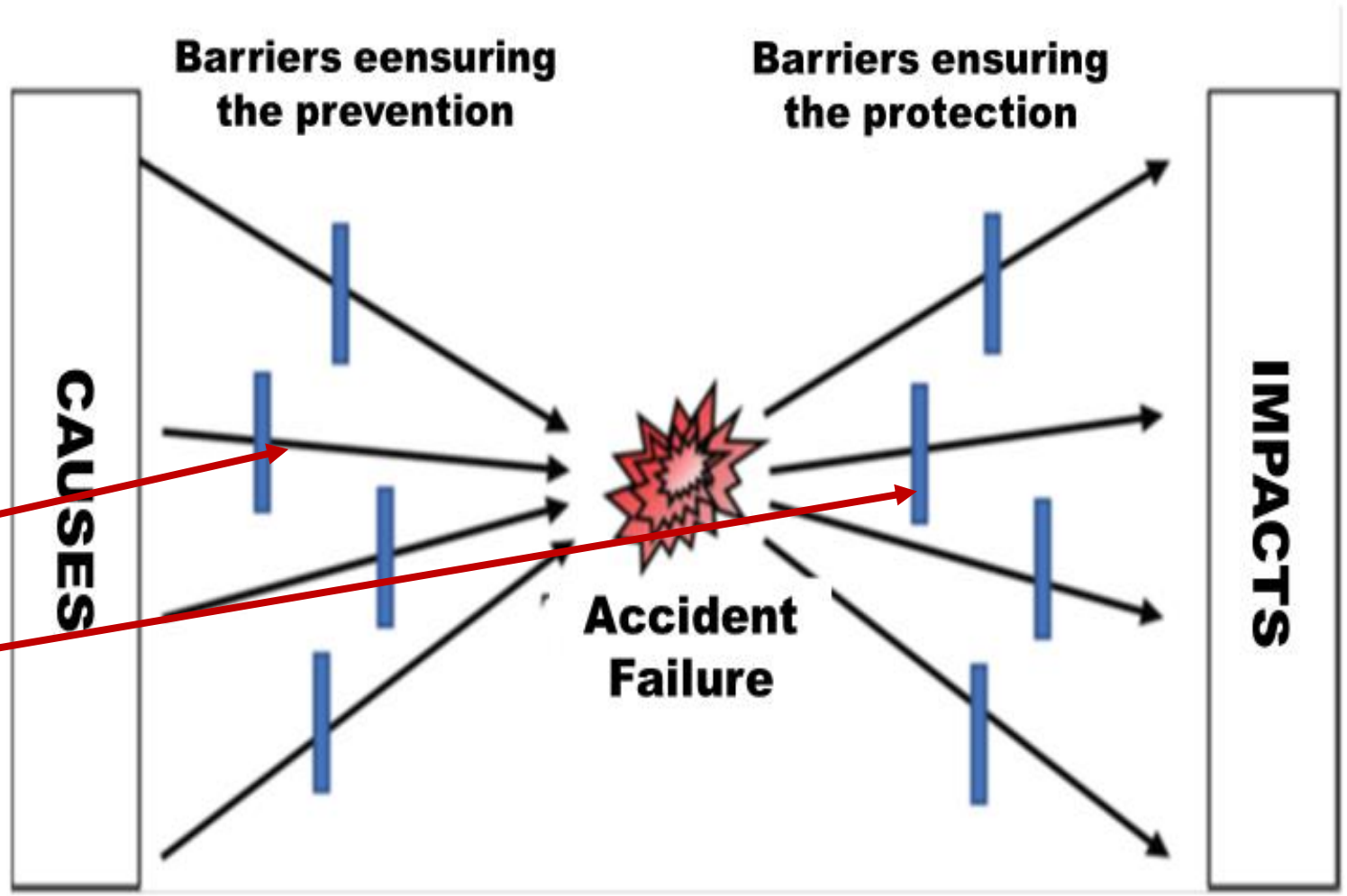
Therefore, the design covers a wide range of problems, for example, it goes on selection of:

- materials,
- technical principles,
- construction procedures,
- framework procedures,
- determination of critical construction and framework processes,
- protection ways in domains physical, cyber etc.

In designing, it is very important how the designer divides the risk mastering:

- in design by preventive measures,
- only at response.

designer in design must prepare qualified measures for response.



Bow-tie diagram

From safety perspective, it is necessary to follow in the design the requirements for:

- durability,
- manageability of equipment and processes,
- lifespan,
- human resources,
- costs,
- technical services,
- other service,
- safety of employees, humans in surroundings and environment.

Big roles play LIMITS AND CONDITIONS for technical facility, which are a set of clearly defined conditions for which it is proven that the operation of the technical facility is safe.

They are tools for managing the safety.

Their observance guarantees the safe operation.

From safety viewpoint, the main goal of designing process is to avert unwanted combinations of incidents that have potential to cause accidents accompanied by major damages.

To do this, it is necessary to use:

- proactive indicators or **safety functions** for control safety under border conditions, thereby the occurrence possibility of unlikely severe accident is reducing,
- **seven principles of resilience:**
  - backup,
  - to insert ability of sleek and controlled degradation,
  - to insert ability to return from degraded state,
  - flexibility in both, the system and the organization,
  - to insert ability to control limit conditions close to the performance interface,
  - to insert optimal management models,
  - to reduce complexity,
  - to reduce possible non-demanded couplings.

In design, it is necessary to include program for safety increase that ensures:

- safety and functionality of all fittings that corresponds to their missions,
- identification, evaluation, elimination or regulation of potential risks at acceptable level for important installations, systems and their various parts,
- risk management, which includes all possible disasters with resources inside and outside the technical facility that cannot be eliminated,
- protection of personnel, people in the vicinity, environment, facilities and property,
- use of new materials or products and test techniques only in a way that is only associated with minimal risk,
- insertion of safety factors that ensure corrective measures that lead to improvement,
- consideration of all appropriate historical data.

At designing, it is necessary to consider at each critical process the problems connected with:

- given process,
- designing a process,
- process management,
- operational staff and signalling its condition,
- safety management system,
- other technical systems promoting the safety,
- external active and passive systems for mitigating the risks leaded to process failure,
- technical facility emergency response,
- technical facility surrounding response.

The processes risk management strategy need to use:

- **principles of inherent safety,**
- **passive safety systems,**
- **active safety systems,**
- **different barriers types,**
- **procedural procedures that are proven or thoroughly tested in such a way that they do not contain latent sources of danger under possible conditions,**
- **in important technical facilities, the Defence-In-Depth principle.**

From a professional viewpoint, safety document shall contain answers to questions:

- **what may break down,**
- **what may not work (hazard identification and its analysis),**
- **how serious consequences (risk assessment) can be; what measures need to be taken to avoid this (risk management),**
- **what needs to be done when this occurs (emergency measures).**

For research, in which we formulated risk management at design we firstly compiled original database of technical facilities´ accidents and failures from world data; several case studies were analysed in great details.

The database contains 7829 events from the whole world sources that were accessible in last 35 years to authors; 521 events originated due to mistakes in designing.

Methods and their results

BY CRITICAL ANALYSIS OF DATABASE, i.e.:

- **causes of accidents and failures, we separated causes in categories – fishbone diagram,**
- **lessons learned from responses to accidents and failures, we determined the risk mitigation measures for designing – risk management plan for designing.**

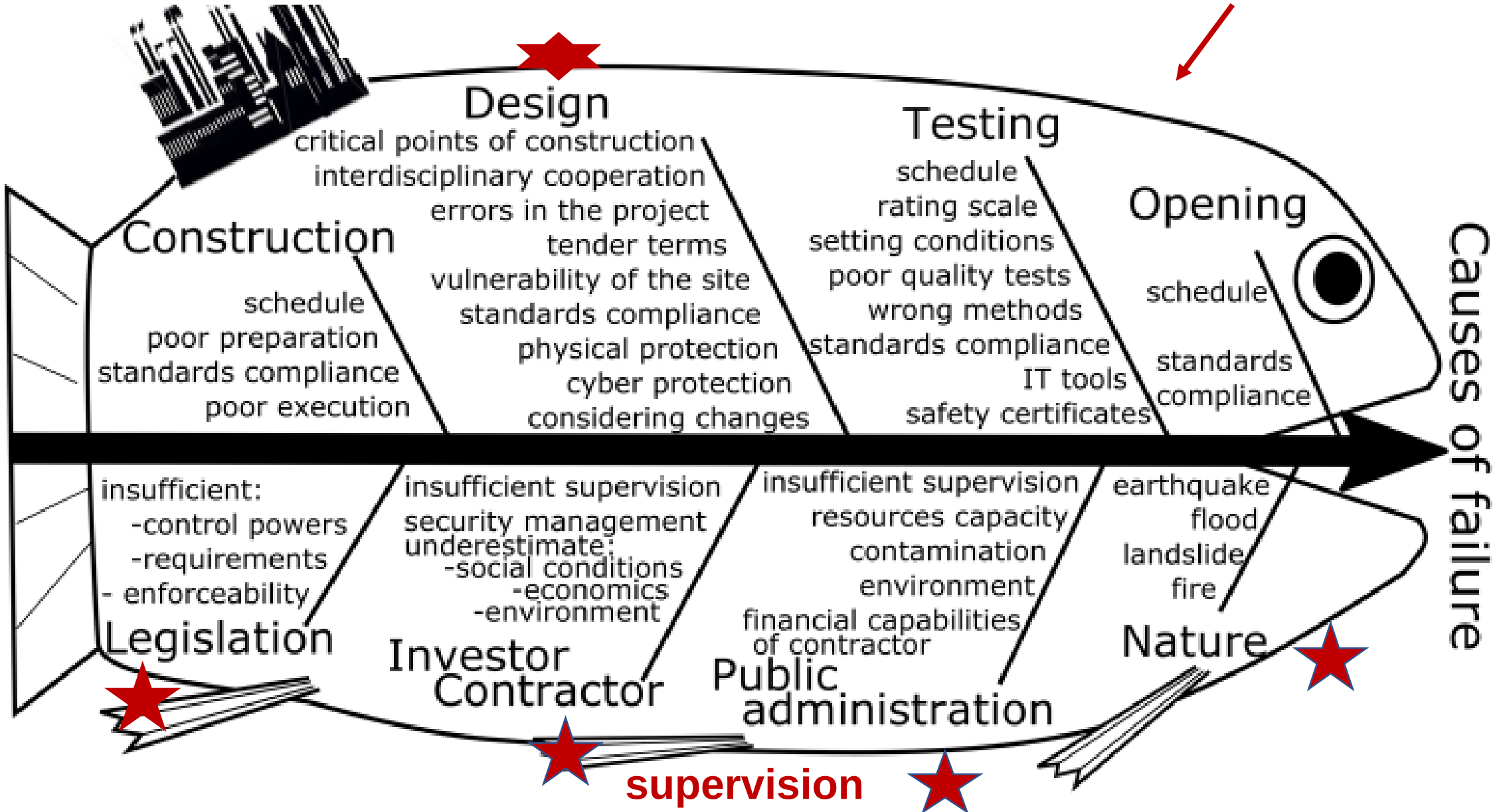
BY CONSIDERATION OF:

- **knowledge on design process compilation,**
- **knowledge on work with risks,**
- **experiences from practice,**

we determined the risk based design procedure.

4. RISK CAUSES IN DESIGNING THE TECHNICAL FACILITIES

Fishbone diagram



The sources of accidents or failures of technical facilities are:

- **one big phenomenon (natural or technological disaster or human failure),**

- **occurrence of minor errors, realization of which in short time period is dangerous,** although the impacts of separate individual errors are manageable by prepared response measures**.**

The second case is more frequent

The combination of dangerous events in design must be also considered.

5. RISK MANAGEMENT PLAN

The risk management plan for design process is after prevention principles the second important tool for technical facility design.

Risk area	Risk description	Probability of occurrence Risk impacts size	Risk mitigation measures
Authorized designer	.....		
	As a result of a poor quality or non-cooperative team of project processors, the project is of poor quality and it leads sooner or later to disruption of construction or operation, enormous expenditure, citizens safety and problems with public administration……..	**Probability:** Medium **Impacts:** Large	**Measures:** To introduce rules for team cooperation **Execute:** Authorized designer team worker **Responsibility:** Authorized designer team director

EXAMPLE

Risk management plan shows measures for removing the usual errors of designers.

Duties have all participants: designer, investor, state administration, future operator, public.

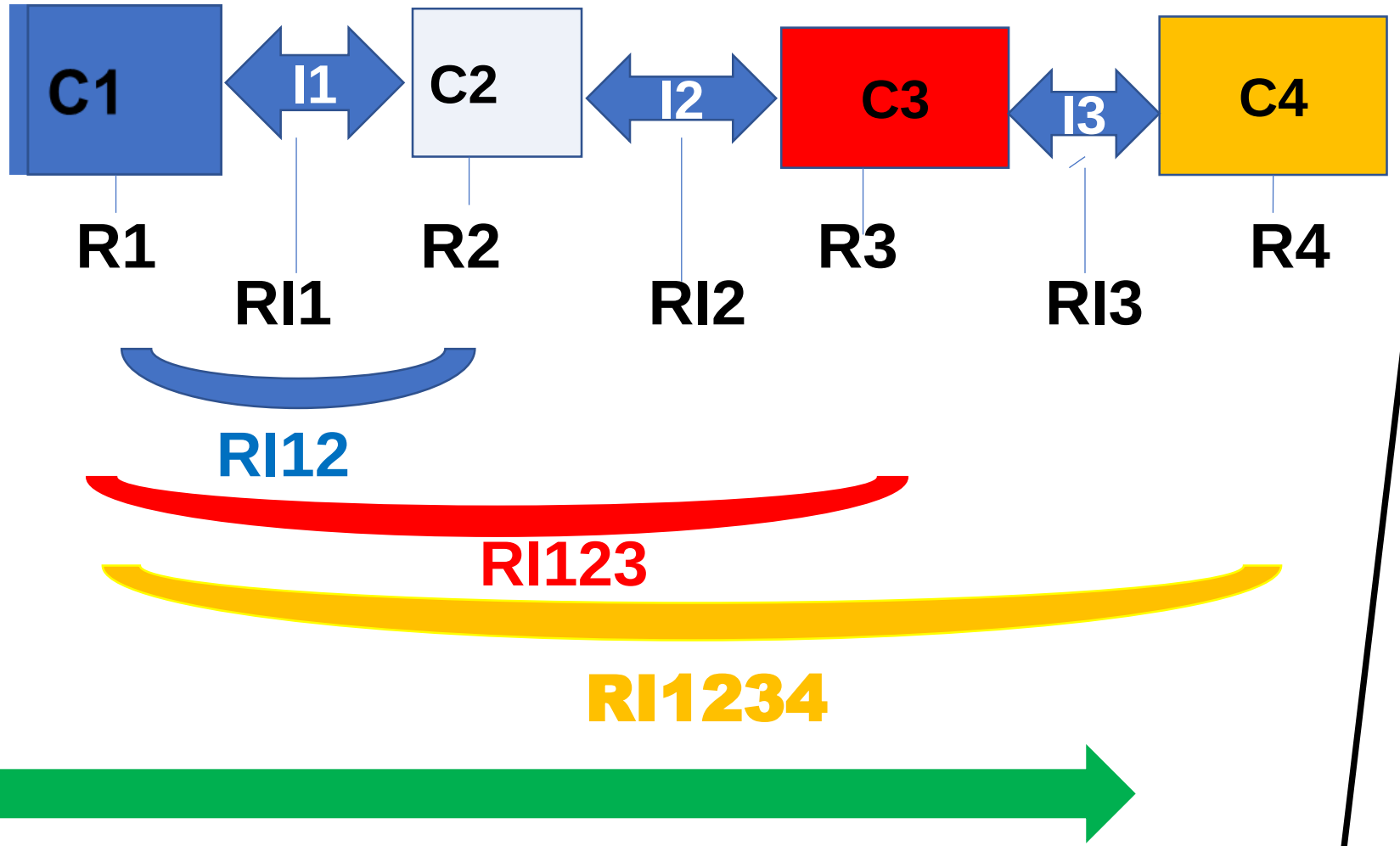
6. PROCEDURE OF GENERATION OF RISK-BASED DESIGN OF TECHNICAL FACILITIES

Based on the above facts, the technique for compilation of a risk-based design we propose by such way:

1. **To establish a list of components and systems that comply with the standards and will be combined into sub-units.**
2. **For all items in the list of components and systems (point 1), to determine the limits and conditions from the point of view of their operation in a particular territory with regard to: the material from which they are made; demands on uptime; the working mode in which they will work; human factor; and possible other risks (internal fire or explosion and external risks).**
3. **For all items in the list of components and systems (point 1), to determine for the site-specific sources of risks determined by considering the All-Hazard-Approach, the sizes and characteristics of the partial risks.**

4. **For all risk sources (point 3) to determine impact scenarios; and when some risk impacts are not acceptable, it is necessary to increase the material and construction requirements so that these risks may be acceptable.**
5. **To establish the component interconnections and model of their interconnections, which meets standards and inherent safety requirements.**
6. **For all interconnections (point 5) to determine the limits and conditions from the point of view of their material composition, method of execution (loose, tight, or complex), methods of interconnection (welds, screws, rivets, seals, etc.) and the realization of possible other risks (internal fire or explosion, human factor and external risks).**
7. **For the risk sources (point 3) to determine impacts scenarios of partial risks for all interconnections and integrated risk for whole made up from jointed components; when the partial risks and integrated risk of whole made up from jointed components are not acceptable, it is necessary to increase requirements on material and construction of components interconnections so that these risks may be acceptable.**

8. **For the risk sources (point 3) to determine for the entire production process the process impact scenarios showing the integrated risk manifestation. In the case that the integrated risk is not acceptable, to increase the demands on design of: components of production process; working regime; and operators, so that the risks may be acceptable.**
9. **For the risk sources (point 3) to determine integral risk. If the risk is only conditionally acceptable (ALARP), then make modifications to the technology that will allow an immediate quality response that will ensure a return to normal state. In case of unacceptable risk, it is necessary to return to the adjustment of partial risks of components, systems and their interconnection (planned and even those that arise in the realization of sources of major risks) and the introduction of the principle of fail safely.**
10. **Considering the risk sources (point 3) to specify requirements for the steering system, that is for both, the I&C and the operators under normal, abnormal and critical conditions.**



Direction of design process.

1. C1, C2, C3, C4, I1, I2, I3 proposed according to norms
2. **Determination of risks connected with disasters possible in site.** R1,R2,R3,R4, RI1, RI2,RI3 - risks of components and interfaces; RI12, RI123, RI1234 – integrated risks

3. PROCEDURE for risk mitigation:

- judgement R1, R2, R3, R4,..
- corrections of C1,C2,C3,C4, RI1,RI2…..if necessary,
- judgement RI12,
- corrections of C1,I1,C2, if necessary
- judgement RI123,
- corrections of C1,I1,C2,I2,C3, if necessary
- judgement RI1,2,3,4
- corrections of C1,I1,C2,I2,C3,I3,C4, if necessary

Rules for judgement are in next slide.

For each technical facility and its vicinity it is necessary**:**

- **to construct site-specific Decision Support System (DSS) for determination of risks of all components and for their interfaces,**
- **to use value scale for risk judgement.**

Risk rate	n/N [%]
Negligible – 0	More than 95 %
Low – 1	70–95 %
Medium – 2	45–70 %
High – 3	25–45 %
Very high – 4	5–25 %
Extremely high – 5	Less than 5 %

Rules for risk judgement:

Risk is acceptable – categories 0 and 1

Risk is ALARA - categories 2 and 3

Risk is unacceptable – categories 4 and 5

FURTHER PROCEDURE

If risk is:

- **acceptable – no corrections are needed,**
- **ALARA – it is necessary to insert in design measures enabling the response,**
- **unacceptable – it is necessary to change material, way of interconnections of components, technology of interfaces etc. + again to judge risk.**

7. CONCLUSION

The above-summarized knowledge and results of study of technical facilities´ accidents and failures **show that basis for ensuring the facilities safety at required life cycle is knowledge of:**

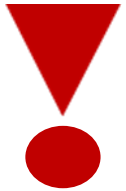
- **regulations** (legislation, norms, standards) in context,
- **risks in the site** to which the technical facility is placed,
- **technical system**, which constitutes a technical facility,
- **models and theories** associated with accidents,
- **methods of** analysis, management and settlement of risks,
- **way of management that operator might use after commissioning** (finance, human resources, organization, technology, innovation...).

It is necessary for all involved:

- **to respect the public interest,**
- **to participate in building the safety culture**

and for managers to motivate employees to do quality work, even by their own example, as shown by the so-called "golden rules of safety".

The grounds need to be inserted into the design.

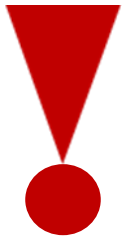


The research showed that:

- **each technical facility design has a certain danger. The designer art is to select such solution that is optimal,** i.e. it is sufficiently safe and it is possible to realize with regard to investor and public administration options. The near the same holds for manufacturer´ skill (craftsmanship) at realization**,**
- **impressive and low robust designs with insufficient safety margins often fail sooner or later,**
- **wrongly determined limits and conditions for critical technical facility parts lead to frequent disturbances up to serious accidents; they are not able to react to condition changes.**

The analysis of accessible legislations revealed that rules in force do not require to follow operation process safety in designing, and this occasionally leads to problems at operation.

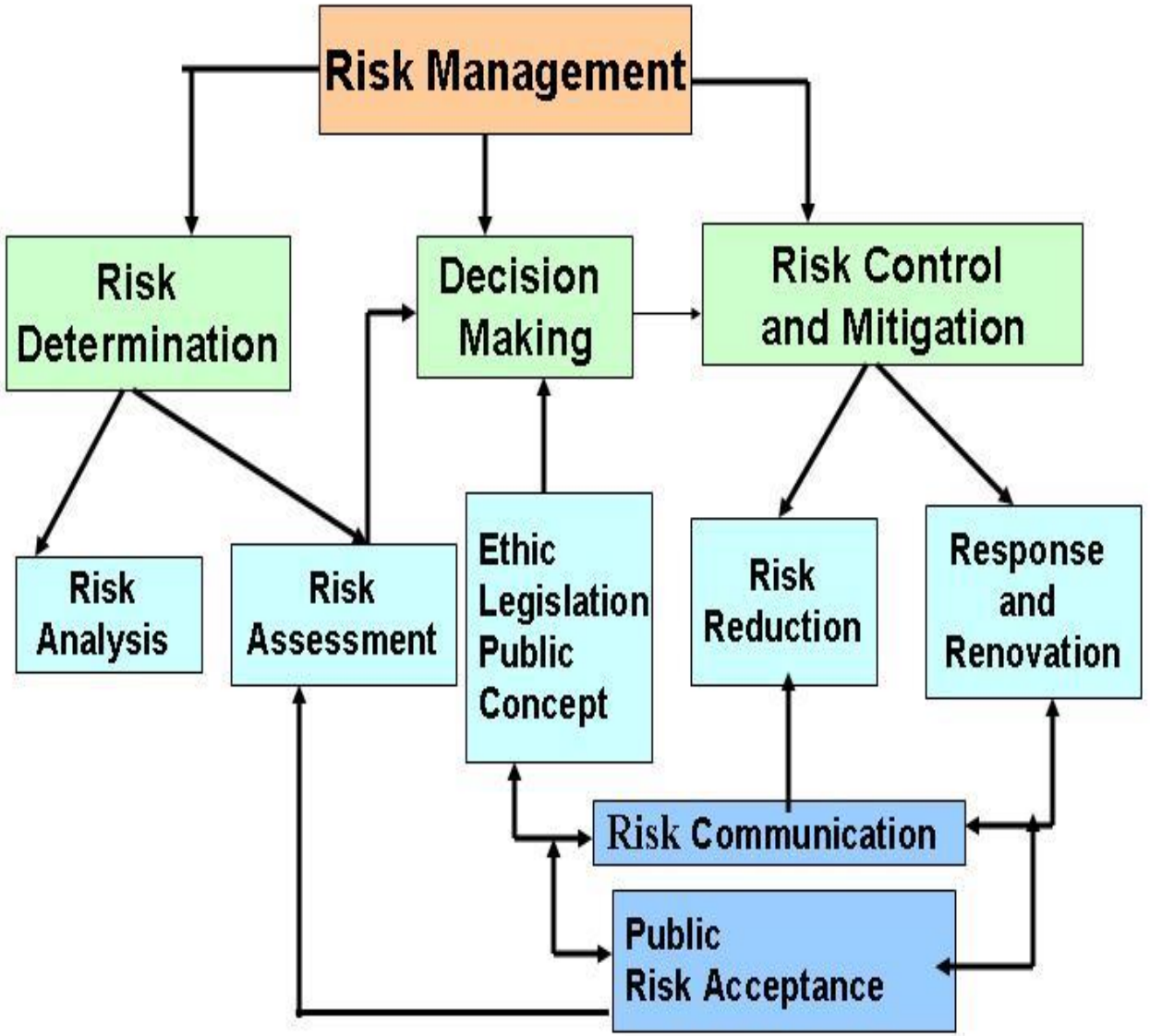
The analysis of accessible legislations revealed that rules in force do not require to consider in design the combination of dangerous events in short time interval.



The procedure of generation of technical facility risk-based design was tested with success at seven medium technical facilities. It was published in prestige foreign journals.

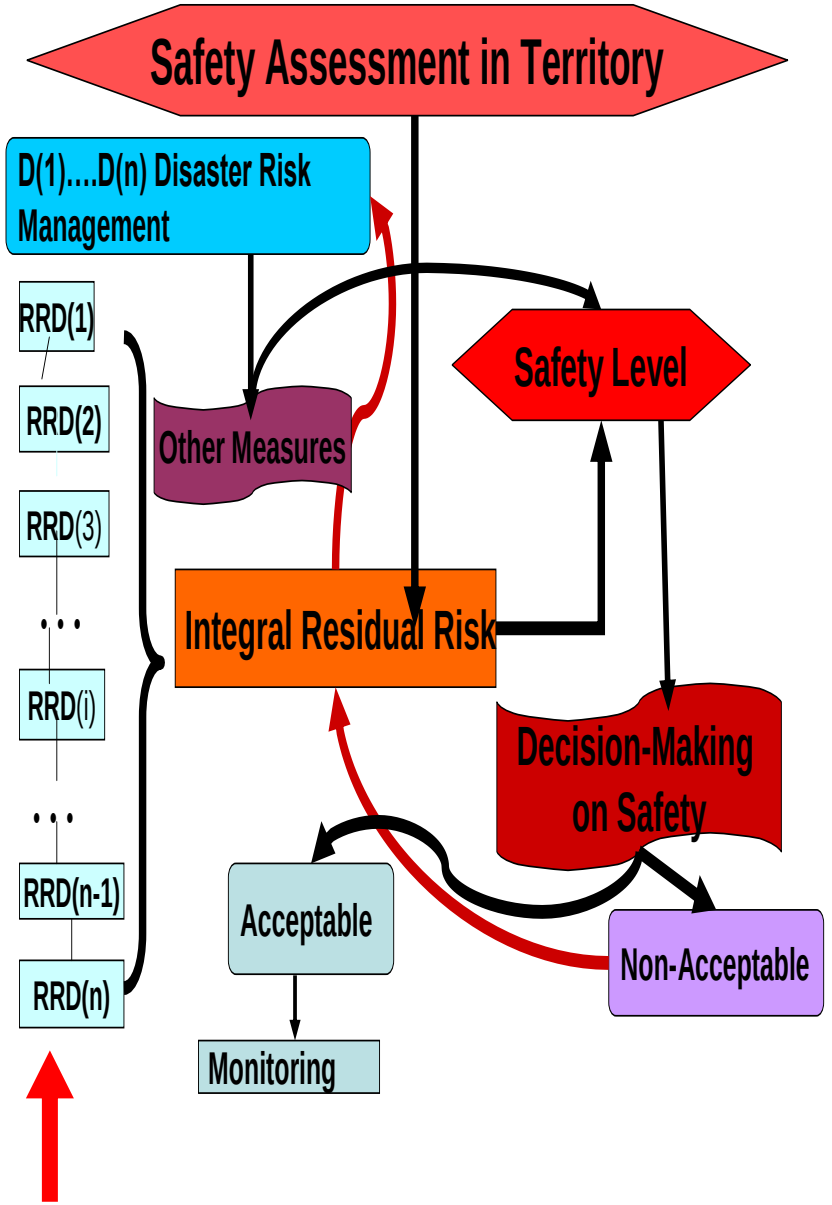
Now, it is continued the procedure implementation in practice and its improvement.

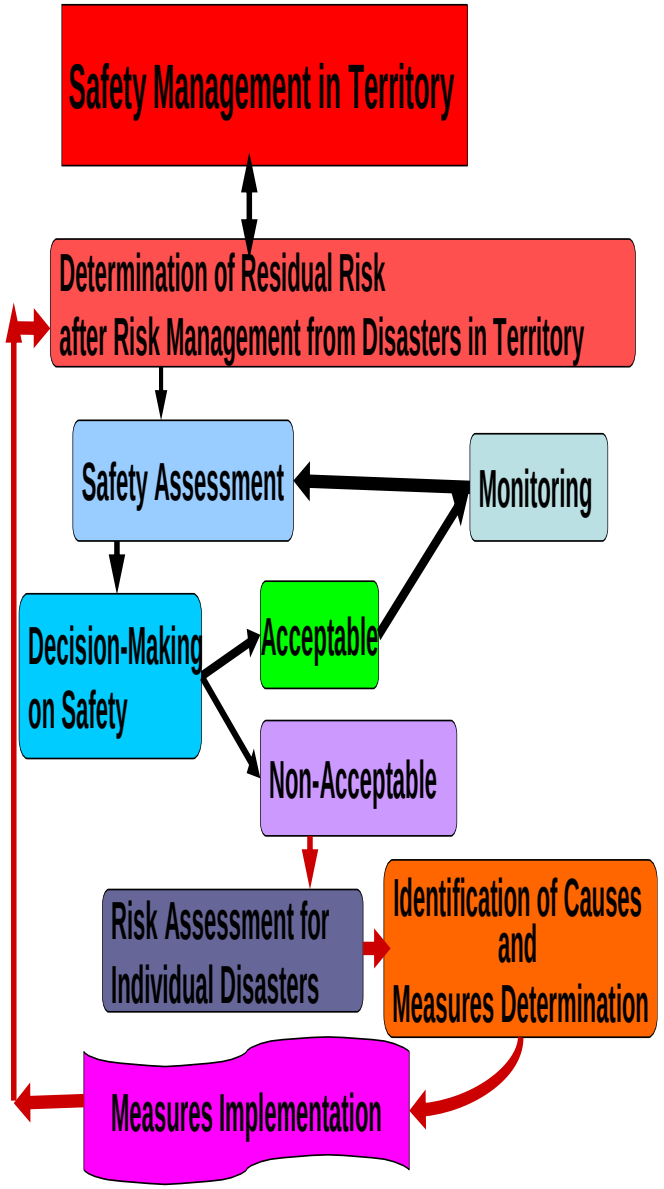
THANK YOU VERY MUCH FOR ATTENTION !!!



Model of risk management

- how to negotiate with one disaster





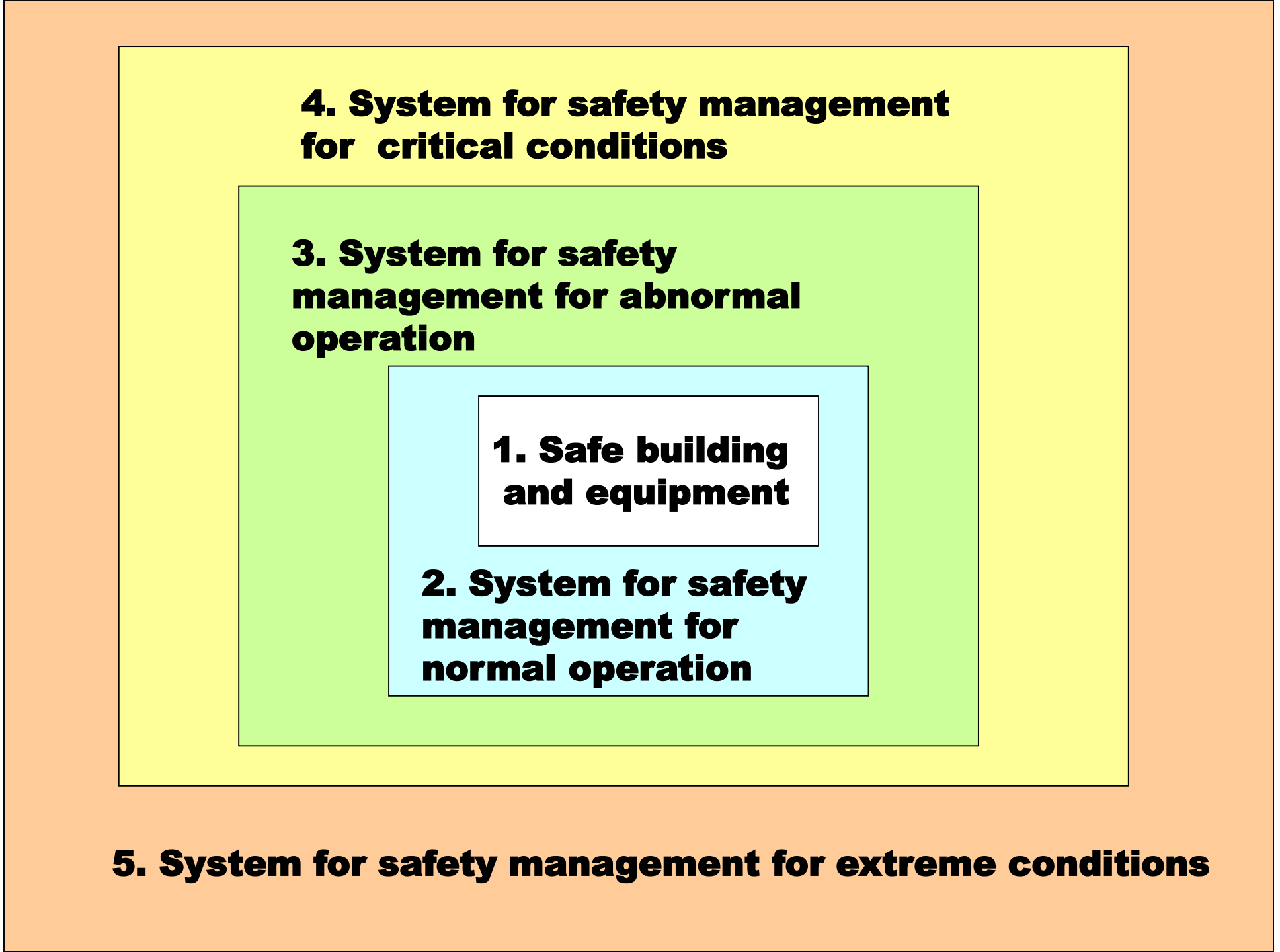
You see that aim is optimum for all possible disasters.

Strategy of management for ensuring the security and sustainable development of managed subject consists in negotiation with risks. In its frame according to present possibilities of human society we apply several ways of deal with risk:

- **part of risk is reduced**, i.e. by preventive measures the risk realisation is averted,
- **part of risk is mitigated**, i.e. by preventive measures and by preparedness (warning systems and another measures of emergency and crisis management) there are reduced or averted non-acceptable impacts,
- **part of risk is re-insured**,
- **part of risk for which there are prepared resources for response and renovation**,
- **part of risk for which there is prepared** contingency plan, i.e. for part of risk that is non-controllable or too expensive or low frequent.

To this it is joined the distribution of risk defeating among all stakeholders. The distribution in good governance is performed according to rule that:

- all stakeholders have responsibility for risk defeat,
- the defeat of real risk is assigned to subject, the preparedness of which is the best.


4. System for safety management for critical conditions
3. System for safety management for abnormal operation
1. Safe building and equipment
2. System for safety management for normal operation
5. System for safety management for extreme conditions