ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

Risk Analysis of Highly-integrated Systems

Fundamentals II

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

More ‚Risk' Terms

Maximum acceptable risk (Grenzrisiko)

- Highest degree of justifiable risk regarding a specific action or state.

Residual or remaining risk (Restrisiko)

- Descriptive: risk which remains after implementation of all planned safety measures, arising from
  - consciously accepted risks,
  - mis-assessed risks, and
  - unrecognized risks.
- Normative: Admissible risks following risk acceptability assessments.

Elements of Risk: Damage

- General: negative effects of an undesirable event or procedure or an undesirable impairment of an object to be protected as a consequence of harmful events.
- In a narrow sense: degradation or impairment of the integrity of an object of concern resulting in a reduction of reliability, safety or capability.
- Damage quantification is not always well defined: depending on context, we may obtain different results.
- Example: counting the severely injured people after an accident.

Common Damage Measurements with [Measuring Units]

- Impact of undesired event affects following:

Inside installation	**Outside installation**
Employees, Persons [number] • Death: immediate, possible • Injuries: light, heavy • Health damage: temporary, permanent	The public [number] • Death: immediate, possible • Injuries: light, heavy • Health damage: temporary, permanent • Evacuations: temporary, permanent
Installation [quantity of released substances, energy] • Undesired dangerous state of installation (nuclear meltdown, “runaway” reaction)	Environment [quantity of released substances, energy, etc.] • Released substances [quantity, toxicity, energy units] • Concentration [mass and volume units] • Contamination [area and mass units]
Cost/Investment [monetary units] • microeconomic • management	Cost [monetary units] • macroeconomic
Loss of production [time, currency units]	Loss of area utilization [area and time units]

Elements of Risk: Frequency

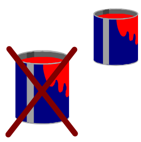
Frequency of an event: frequency is often used wrongly instead of other terms, although there are clear definitions:

- **Frequency (Häufigkeit)**: a frequency denotes a number.
- **Relative frequency (relative Häufigkeit)**: number of cases in which an event happened, divided by the number of cases in which the event could have happened (dimensionless)
- **Rate**: mathematical construct, which measures the actual change of a number in units of change of another number (usually time). Empirically, it can be done by estimating an average (relative frequency) over a long time interval.
- **Frequency (Frequenz)**: can also be time related.
- **Probability (Wahrscheinlichkeit)**: "a real number in the scale 0 to 1 attached to a random event."(ISO 3534:1993). Defined by the axiom system of Kolmogorov.

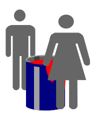
Definition of Vague Terms: Safety

- **absolute sense**: attribute defined by the absence of any danger (ultimately unobtainable).

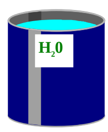
- **relative sense**: attribute defined by (a) the absence of a specific danger, (b) involving a comparatively low and thus acceptable risk or (c) complying with normative requirements.



- **subjective**: perceived certainty of danger protection.



- **intrinsic**: attribute which mandatorily limits to a predetermined or acceptable extent or excludes a danger to a state, process or product.



Conclusion

In risk analysis we find standardized, but also „vague“ terms that can be defined or understood in different ways, depending on the context. The interdisciplinary approach in risk analysis requires Definitions. Without an agreement on terminology “expensive” misunderstandings can occur.

Risk management

- Coordinated activities to direct and control an organization with regard to risk (ISO/IEC Guide 73, 2002)
- A systematic approach for identification, quantification, assessment, optimization, monitoring and communication of risks, which can affect the health or security of people or the environment and are related to an activity, a function or a process. It is a stepwise process that allows a continuous enhancement in the context of decision making. It can be applied at any stage of an activity to minimize losses and take advantage of possibilities:
  - R & D
  - Design, planning and site selection
  - Construction
  - Operation
  - Emergency preparedness and planning
  - Accident management and emergency measures
  - Decommissioning, removal.
- Risk management has to be highly integrated in the continuous operation of any organisation.

Relationship between terms: "Risk Analysis" and "Risk Management" (ISO/IEC Guide 73, 2002)

- Risk Management *…coordinated activity to direct and control*
  - Risk Assessment
    - Risk Analysis
      - Source Identification… *potential for a consequence (= hazard)*
      - Risk Estimation *…events, prob., consequences*
    - Risk Evaluation *…against given risk criteria*
  - Risk Treatment *… selection and implementation of measures to modify risks*
    - Risk Avoidance *…decision not to become involved, or action to withdraw*
    - Risk Optimization *… process*
    - Risk Transfer *…burden sharing*
    - Risk Retention *…acceptance of burden/benefit … unidentified risks*
  - Risk Acceptance *…decision (by whom?)*
  - Risk Communication *…sharing info between decision maker and other stakeholders*

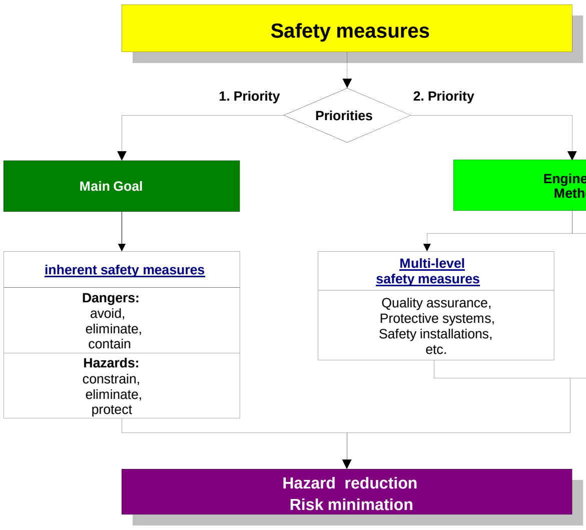
Risk management approaches for technical systems

- **Trial-and-error** with organized feedback of experience; Design and adherence to a body of rules and regulations
  - Can only be applied, if a failure does not lead to extreme high damage
- **Risk-based approach (analysis and minimization of Risks)**
  Systematic identification of hazards and scenario analysis. Identification of weak spots and optimization possibilities using experience / know-how
  ⇒ requires detailed description and knowledge of the system
- **Precautionary principle**
  Extraploratory analysis of negative and positive implications and the comparison to alternatives
  - Useful when the degree of uncertainty is high; protects against "unpleasant surprises"

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

Safety oriented approach as basis for Risk Management



ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

Questions in risk analysis

- What can go wrong? (accident sequences, scenarios)
- What is the probability of these scenarios?
- What are the consequences?

Set of multiple threats disclosing vulnerabilities

- **Natural events** such as earthquakes, hurricanes, tornados, severe flooding, or other (increasing) extreme weather conditions
- **Accidents or technical factors** leading to the debilitation of plants, networks and operations
- **Human factors** such as unintended and intended failures, malicious physical or cyber-attacks
- **Market factors** e.g. economic pressure trading-off security factors
- **Policy factors** such as misusing “energy” for political purposes

Structural vs. functional analysis

- The structural approach answers the question: "what is the system made of?", the functional approach answers the question: "how is it working?"
- The **structural analysis** consists first of identifying the boundary between the system and its environment. The system's environment refers to fixed constraints, i.e. what lies outside the system.
  The second step is to identify the elements (components, sub-systems or black boxes) of the system; the last step is to identify existing channels of "communication" allowing exchanges between elements, i.e. the organization of the system.
- The preliminary task of the **functional analysis** is to identify the system's objectives: they refer to the goal and the services a given system has to fulfill or provide.
  The performances of the system can then be measured, with respect to the required level of expected output or service.
  Most of functional approaches are called input-output approaches or efficiency approaches, having the objective to identify the weak points and especially the places where there is waste and then proceed to remove the inefficiency.

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

Deterministic vs. probabilistic approach

Deterministic (postulating)

- Events completely determined by cause-effect-chains (causality)
- Analyse of the effects of assumed causes

Statistic (retrospective)

- Rules can be derived from a large number of similar events (based on experience)
- Directly applicable observations can be transferred to the system or to the event level

Probabilistic (prognostic)

- Events can be identified by the probability of occurrence
- Use of observations on the level of components (Axiom-system of Kolmogoroff)

Probabilistic risk analysis (key terms)

Events (examples):

- Pump fails within a specific time interval
- Wind speed exceeds a specified value
- A set of events triggers a physical reaction

Probabilities:

- Classic (Laplace): Probability as the number of times a specific event takes place divided by the total number of (discrete) events
- Based on frequency (Mises): Probability as the limit value of the relative frequency, in which an event takes place under constant conditions
- Subjective: Probability as the degree of expectation of an individual based on some information, that a possible event will take place

Frequency:

- Time dependent frequency (e.g. events per year, ≥ 0)

Risk Calculation Examples

statistically	probabilistically
Risk = expected value ≥ 0	Risk = related probability
Example: throwing a coin ("heads" = „0" and "tails" = „1")	
$E(X) = \sum_{i=1}^{2} x_i \cdot \hat{P}r(X = x_i)$ E(X): Expected value X: Probability variable "heads"/"tails" $\hat{P}r(\bullet)$: Relative frequency Observation: $x_i = \begin{cases} 1 & \hat{P}r(X = x_i) = \frac{550}{1000} = 0{,}55 \\ 0 & \hat{P}r(X = x_i) = \frac{450}{1000} = 0{,}45 \end{cases}$ ⇒ E(X) = 0,55 The „expectation" for „1" is closer to 100%	Risk = Pr(X) = Pr(X|E)·Pr(E) Pr(E): Probability that a coin will be thrown Pr(X): Probability that "1" occurs Pr(X|E): Probability of "1" under the condition that a coin has been thrown Pr(X) = Pr(X|E)·Pr(E) = 0,5·1 = 0,5 The probability of heaving "1" is 0.5 Axiom system of Kolmogoroff: 1. 0 ≤ Pr(x) ≤ 1 2. Pr(sure event) = 1 3. $Pr\left(\bigcup_{i=1}^{n} x_i\right) = Pr\left(\sum_{i=1}^{n} x_i\right)$

Analysis Preparation

Determination of the objectives of the analysis, suitable methods, available resources

- Framing of the problem
- Building the analysis team, responsibilities, method of operation, etc.
- Provision of methods/tools, resources

Definition of the protection goals

- Protection of persons, environment, vicinity and other assets
- Limits for certain event frequencies, risk goals/targets

Definition of the objects to be analysed

- Documentation of the objects to be analysed and the system boundaries
- Optionally: Front-end and back-end („life cycle“)

Analysis Preparation (cont.)

Specification of the system states and system modes

- Normal operation, startup and shutdown procedures, faults and failures, decommissioning
- Production, transport, storage

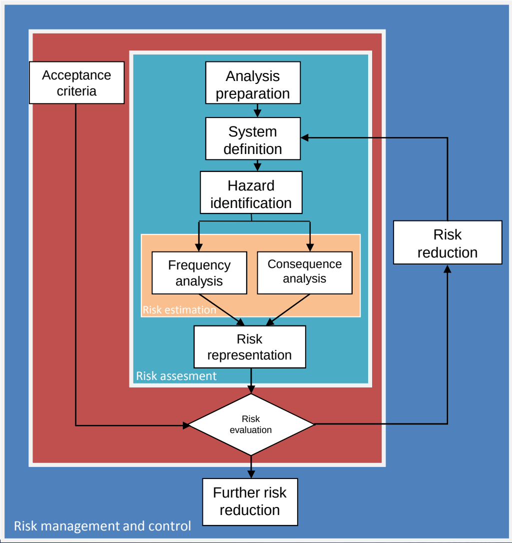
Specification of the analysis breadth and depth

- Truncation criterion: Definition of a threshold (frequency of occurrence) limiting event chains

Specification of effects

- System inherent/internal:
  technical failure/breakdown and/or human factors
- External factors:
  natural (e.g. earthquake) and civilization causes (e.g. airplane crash)

Risk analysis procedure



ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

Scope of Probabilistic Risk Assessment (PRA)

- Both accident initiating events and the unavailability of safety equipment or measures needed to handle accidents are assumed.
- The technical system and specific chains of events (scenarios) including their frequencies of occurrence and resulting system states are modelled.
- Physical phenomena of the postulated scenarios are modeled, and respective consequences are assessed – inside and outside the system.
- The risk of the analysed system is the sum of the products of realistically identified consequences x and their frequencies h(x)

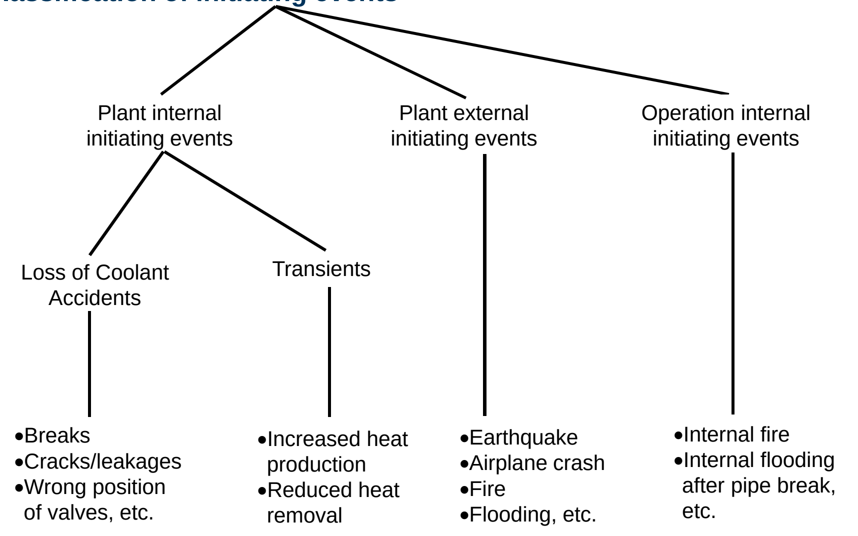
  $R = x_1 \cdot h(x_1) + x_2 \cdot h(x_2) + ...$

  for a representative number of exclusive initiating events and event chains.

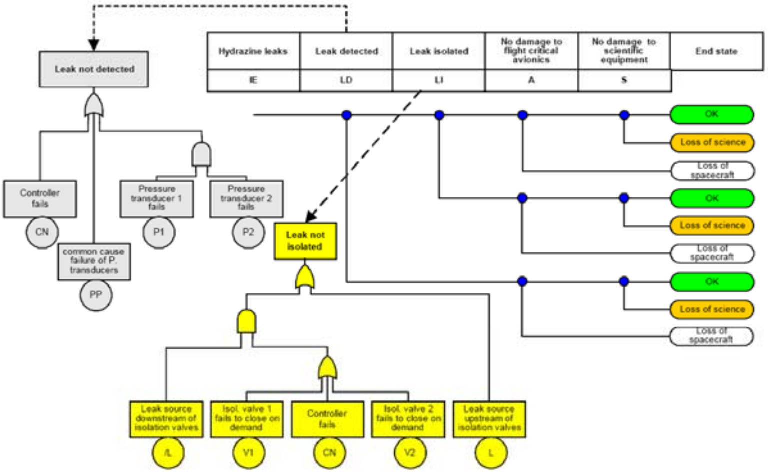
Structure and "Levels" of a PRA for Nuclear Power Plants

Plant response to initiating events	→ **Level 1**	Frequency of core damage (CDF)
Physical effects, containment response	→ **Level 2**	Frequency and amount of radionuclides released (source term, PDF)
Athmospheric dispersion, potential and expected doses, dose-effect/risk relation	→ **Level 3**	Frequency and quantities of environmental and health effects

Classification of initiating events



Combination of Fault Trees and Event Trees



Source: Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. 2002

Information requirement

Frequency of triggering Events

- Generic data (Publications)
- Plant specific knowledge

System response / System reliability

- Reliability data of single components
- Human factors (reliability of Operator)
- Common cause mechanisms

Renewal processes / Maintenance

⇒ Actual plant / system description, operating handbooks

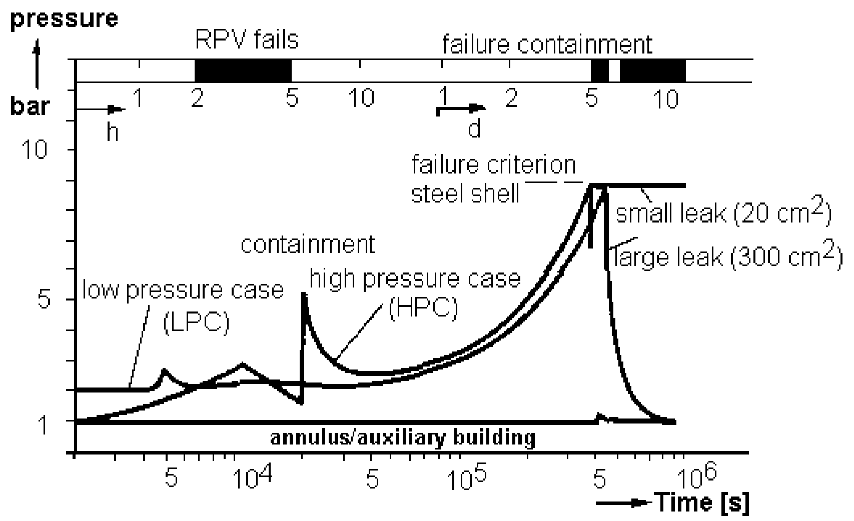
GRS-Results Level 1 PRA, German NPP GKN-II, Full Power

Initiating Events	System damage state	Core damage state
Loss of main feed water	26%	<5%
Loss of main heat sink	20%	<5%
Loss of preferred power	17%	10%
Very small primary leaks	16%	53%
SBLOCA via stuck-open SRV	5%	15%
Steam generator tube rupture	4%	7%

Total expected frequency of system damage state without AM: $8.5x10^{-6}$/year
Total expected frequency of core damage state with AM: $2.5x10^{-6}$/year

--	Expected frequency of system damage state / year	Expected frequency of core damage state / year
Mean	$8.5x10^{-6}$	$2.5x10^{-6}$
5% Fractile	$1.6x10^{-6}$	$4.4x10^{-7}$
50% Fractile (median)	$4.6x10^{-6}$	$1.5x10^{-6}$
95% Fractile	$2.1x10^{-5}$	$7.3x10^{-6}$
„Point Value“*	$5.0x10^{-6}$	$1.7x10^{-6}$

Pressure Curve in the Containment after a Core Melt Accident



Sources

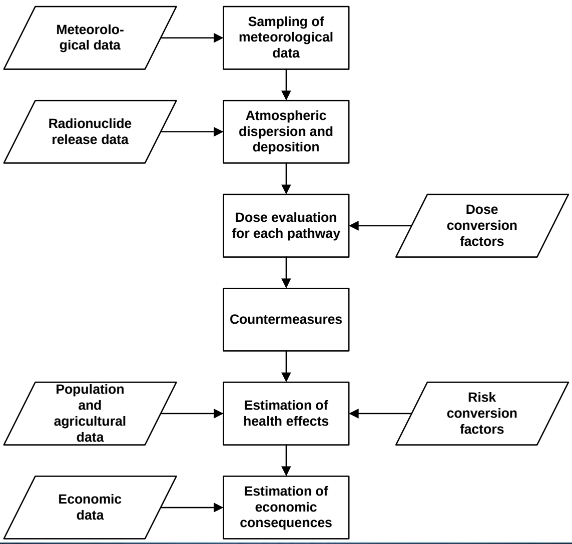
- The source term is defined by the amount, the physical and the chemical properties of each isotope released, thermal energy in the release plume/cloud, release rate over time and release height.
- The source term depends on the accident sequence.

Examples of various source terms

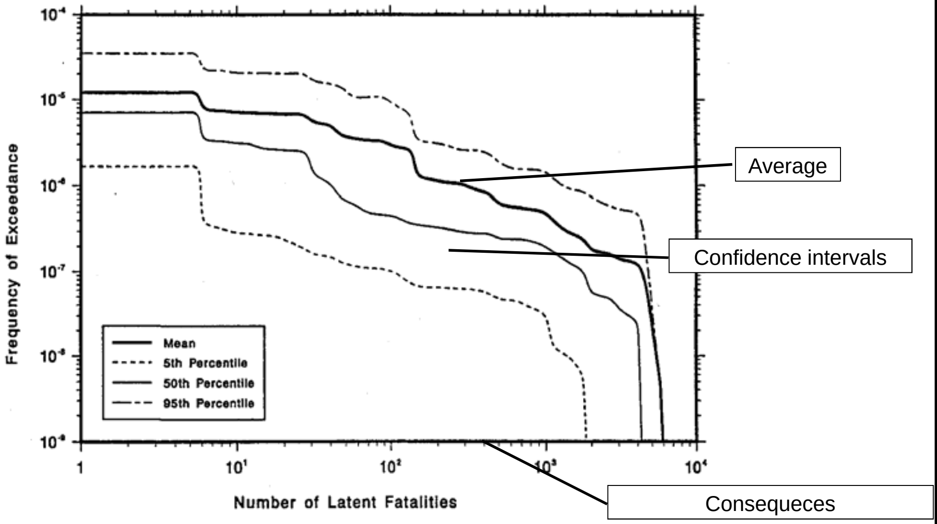
Source term	Time before release [h]	Duration of release [h]	Release rate [MW]	Release height [m]	Time of alarm [h]	Released quantity						
						Xe-Kr	Org-I	I	Cs-Rb	Te-Sb	Ba-Sr, Ru	La
QT1	2.0 3.0	1.0 5.0	2.0 0.2	10 10	1.0 -	1.0 -	0.001 -	0.1 -	0.1 -	0.05 0.05	0 0.01	0 0.001
QT2	2.0	1.0	0	10	1.0	1.0	0.001	0.1	0.1	0.1	0.01	0.001
QT3	2.0	1.0	0	10	1.0	0.1	0.00001	0.001	0.001	0.001	0.0001	0.00001
QT4	2.0 3.0 5.0	1.0 1.0 1.0	0 0 0	10 10 10	1.0 - -	1.0 - -	0.00033 0.00033 0.00033	0.033 0.033 0.033	0.033 0.033 0.033	0.033 0.033 0.033	0.0033 0.0033 0.0033	0.00033 0.00033 0.00033
QT5	2.0	24.0	0	10	1.0	1.0	0.001	0.1	0.1	0.1	0.01	0.001

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

Basic Elements of Probabilistic Consequence Assessment



Result Representation



Large-Scale Critical Infrastructures (1/2)

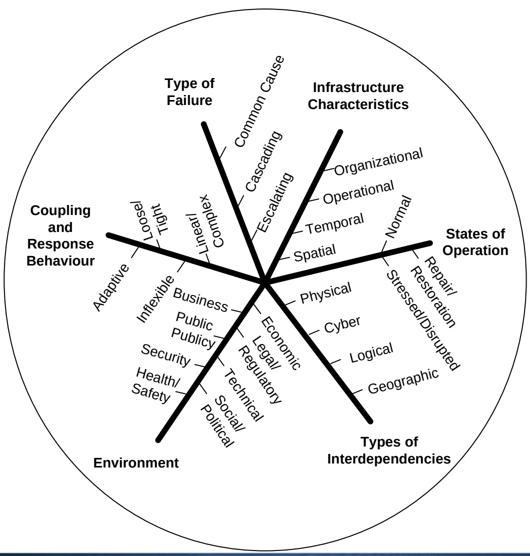
- A network of large-scale human-made systems that function synergistically to produce a continuous flow of essential services
- Designed to satisfy specific social needs but shape social change at a much broader and complex level
- Subject to multiple threats (technical-human, physical, natural, cyber, contextual; unintended or malicious) and pose risks themselves
- Highly complex, inter-dependent, both physically and through a host of industrial ICT (“system of systems”); subject to rapid changes
- Disruptions may cascade (recall “blackouts”), even “normal” service interruptions cost industrialized countries a few percent of GDP
- No single owner / operator / regulator; based on different goals / logics

Large-Scale Critical Infrastructures (2/2)

Include (according to the Commission of the European Communities):

- Energy installations and networks (e.g. electrical power, oil and gas production, storage facilities and refineries, transmission and distribution system)
- Communications and Information Technology (e.g. telecommunications, broadcasting systems, soft- / hardware and networks including Internet)
- Finance (e.g. banking, securities and investment)
- Health Care (e.g. hospitals, health care and blood supply facilities, laboratories and pharmaceuticals, search and rescue, emergency services)
- Food (e.g. safety, production means, wholesale distribution and food industry)
- Water (e.g. dams, storage, treatment and networks)
- Transport (e.g. airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems)
- Production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials)
- Government (e.g. critical services, facilities, information networks, assets and key national sites and monuments)

Dimensions of interdependencies



Source: Rinaldi, et al 2001

Baltimore Howard Street Tunnel

Broken 40-inch-diameter water main (© National Transportation Safety Board)

The interrelationship among infrastructures and its potential for cascading effects were evident on July 19, 2001, when a 62-car freight train carrying hazardous chemicals derailed in Baltimore's Howard Street Tunnel.

In addition to its expected effects, this disaster caused a cascading degradation of infrastructure components not previously anticipated. For example, the tunnel fire caused a water main to break above the tunnel, shooting geysers 20ft into the air. The break caused localized flooding which exceeded a depth of three feet in some areas.

Impact on Infrastructure Sectors