# Handout for Students

# Basic safety&security and crisis management terminology


Safety

By **safety**, we mean the protection of people and the environment from industrial and occupational safety incidents arising from passive hazards and risks, such as accidents, fires, the release of dangerous goods and other unwanted conditions that have their origin in unintended human and/or technical shortcomings, including the limitation and control of these events.

Security

**Security** is protection against events (criminal offences, threats and other unwanted conditions) carried out by persons with malicious intent against employees, customers, physical and intellectual property or SBB's reputation.

Cyber Security

By **cybersecurity**, we mean the protection of information and communication systems from threats such as attacks and manipulations, the prevention of damage and the minimization of risks related to information processing. This also includes the protection of intellectual property. Protection goals are the confidentiality, availability and integrity of systems and data.

Continuity Mgmt

**Continuity management** is the systematic planning and control of measures to maintain essential business processes even in the event of disruptions,

Crisis Mgmt.

**Emergency and crisis management** covers the immediate response and coordination in an emergency to limit damage and ensure the ability to act.

# Protection against hazards – dealing with risks

Frameworks such as the NIST Cybersecurity Framework (CSF) exemplify how risks can be managed in a structured way and how the resilience of organizations can be increased – an approach that can be applied not only to IT systems, but also to other security-relevant processes and infrastructures


**Identify**
The goal is to develop an understanding of the relevant resources, processes and risks. This includes systematically identifying critical systems, dependencies and potential threats.

**Protect**
On the basis of the analysis, suitable measures are implemented to ensure safe operation. This includes technical protection mechanisms as well as organizational regulations and training.

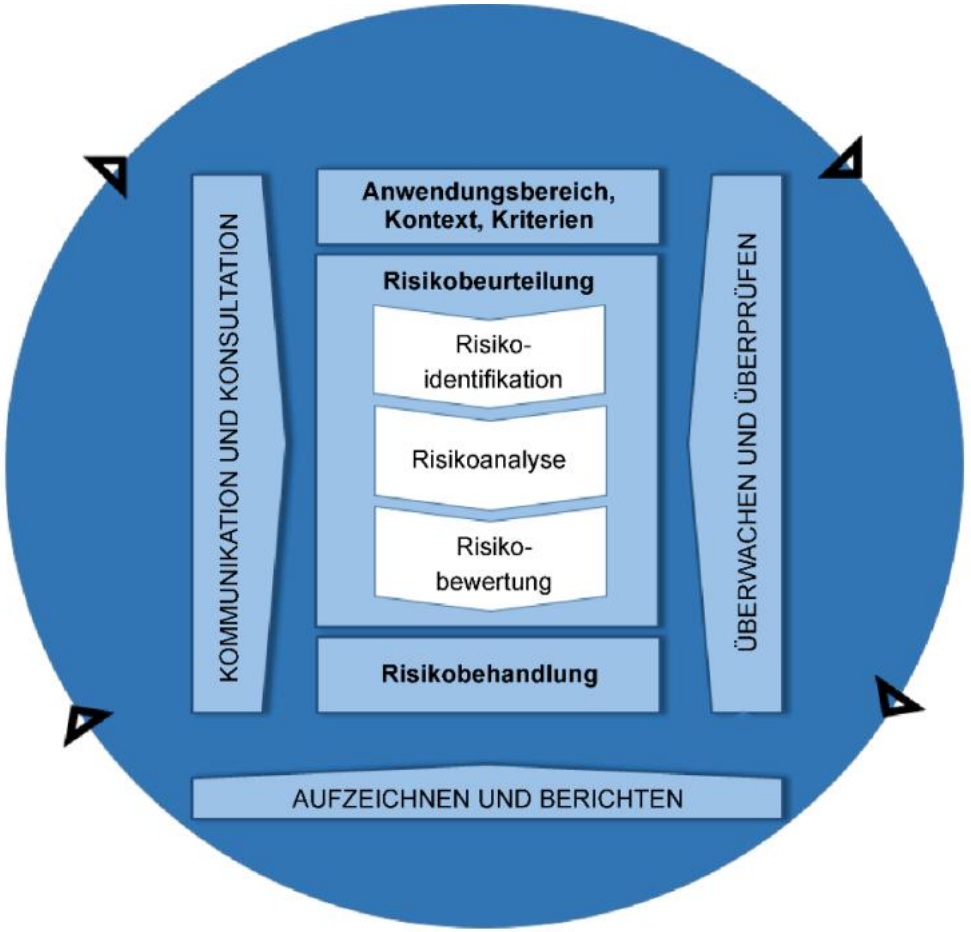
**Detect**
The capability is developed to detect safety-relevant events at an early stage. This is achieved through monitoring, sensors, reporting and clear escalation paths.

**Respond**
After a disruption or an attack, a fast, coordinated response is crucial. Response plans define responsibilities, communication channels and concrete courses of action.

**Recover**
The focus is on returning to a safe, stable operating state. This also includes improving resilience and learning from incidents for future prevention.

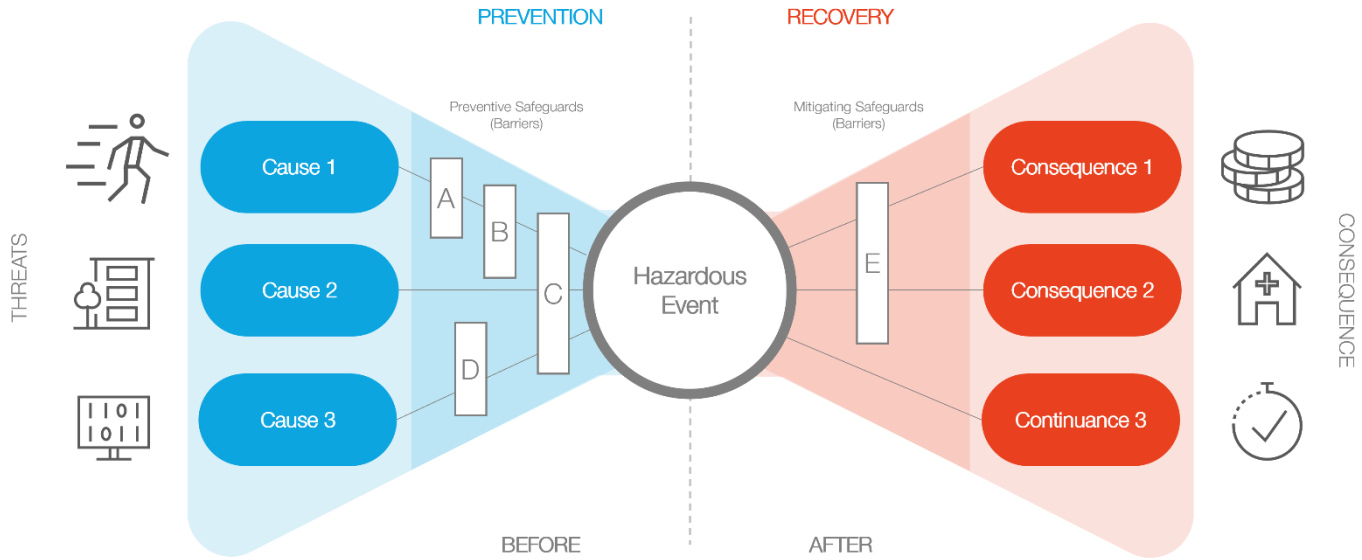
# Risk management SBB.

- SBB's risk management system is based on the SN ISO 31000:2018 guideline in accordance with the owner's goals and in the same way as all other federally affiliated companies.
- Risks are assessed and treated according to the situation in everyday business.
- The risk management process includes activities for the systematic management of risks such as regular risk assessment, ongoing risk treatment, monitoring and communication.
- Twice a year, a structured risk process is carried out by Corporate Risk Management. Depending on the risk potential, the risks are further reported and consolidated via the next higher instance.



# Bow-tie risk analysis serves as a visualization tool.

**A bow-tie diagram** is created by combining two established risk-analysis tools: the fault tree and the event tree. The left side shows the causes that can lead to a hazardous event; the right side shows the consequences.




**Important**: simple, linear cause-and-effect chains are the exception, we live in a complex world: several causes can influence and accumulate each other and feedback effects are also possible.
One of its strengths, however, is the clarity and clarity that supports a discussion on risks.

Threats
can be human, organizational, or technical in nature

List of possible causes for a hazardous event

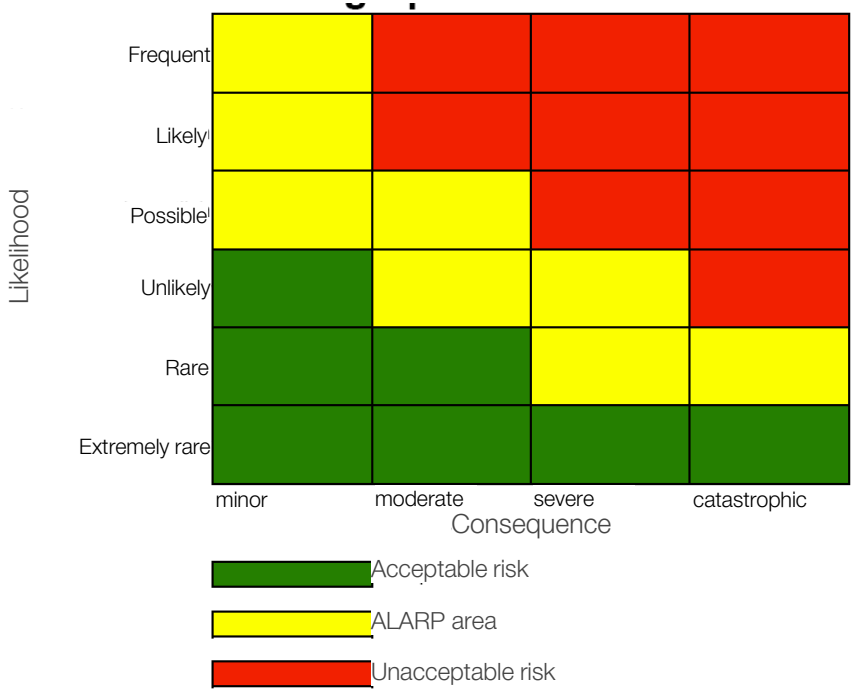
Preventive measures that reduce the probability of the occurrence of the event.

Top event or the "Oh-no!" Moment

Recovery measures that mitigate the consequences of the event once it has occurred.

Consequences that result from the occurrence of the event, typically damage (e.g. financial loss, injuries/fatalities, reputational damage, availability, etc.)

# Risk assessment and ALARP principle.




Risk assessment:

- In order to make different risks comparable, companies define criteria to evaluate them in terms of probability of occurrence and extent of damage
  - Probability of occurrence in number of cases per unit of time
  - Extent of damage > injured/dead, financial damage, damage to image, etc.

ALARP principle in risk management

- The basic idea: Risks should be reduced to such an extent that they are "as low as reasonably achievable". ALARP = as low as reasonably practicable
- Consideration: It is a matter of striking a balance between the safety gain and the effort (costs, time, technical feasibility).
- Limit: A residual risk remains – zero risk is neither possible nor required.
- Proof: Organisations must be able to demonstrate that additional measures would be disproportionate
- Risk appetite: The accepted residual risk range depends on the organization's risk appetite – that is, how much risk it is willing to bear in terms of safety, cost, and performance.

# An overview of the main legal and normative requirements regarding safety.

## Operational safety in the railway environment (excerpt)

- Railway Act (EBG, SR 742.101) – regulates the construction, operation and safety of railways.
- Ordinance on the Construction and Operation of Railways(AB-EBV, SR 742.141.1) – specifies safety requirements in railway operations.
- Ordinance on the safety of railways(SEV, SR 742.141.2) – regulates safety management systems and safety certifications.
- BAV-Richtlinien – specific requirements of the Federal Office of Transport
- EN series of standards 50126/50128/50129 (RAMS, Software, Approval) – International standard, also binding for Switzerland in approval processes.

## Occupational safety (excerpt)

- Labour law (ArG, SR 822.11) – regulates working and rest periods, health protection.
- Accident Insurance Act (UVG, SR 832.20) – Prevention and accident insurance obligations
- Labour law (OR, Art 328) – equires employers to respect and protect the personality of employees; this includes safeguarding life, health and personal integrity (including protection against psychological stress).
- EKAS-Guidelines (Federal Coordination Commission for Occupational Safety) — sector-specific occupational safety requirements.

# An overview of the main legal and normative requirements regarding security and cybersecurity.

## Cybersecurity (Excerpt)

- Federal Act on Information Security at the Confederation (ISG, SR 120) – Principles for information and cyber security in federal agencies, orientation for critical infrastructures.
- Data Protection Act (DSG, SR 235.1) – Protection of personal data.
- Railway Cybersecurity Guideline (RL CySec-Rail) – Specification of the AB-EBV regarding the minimum design of the Information Security Management System (ISMS)
- EU-NIS-Guideline / NIS2 – ybersecurity level, relevant for cross-border systems in the rail environment.
- Cyber Resilience Act (CRA) and EU data protection legislation (GDPR)
- ISO/IEC 27001 ff. – International standard for information security management systems.
- IEC 62443, IEC 63452 (formerly: TS50701): security for OT

## Security (Excerpt)

- Railway Act (EBG, SR 742.101) – obliges railway undertakings to ensure safe operation and to protect facilities and infrastructure against deliberate interference
- Ordinance on the safety of railways (SEV, SR 742.141.2) – regulates security management systems including aspects of security (access controls, property protection)
- BAV and fedpol requirements – specific measures for physical security in rail transport, cooperation with fedpol and cantonal/transport police
- EU requirements on critical infrastructures (CIP, CER Directive) — relevant for internationally operating railway operators.

# An overview of the main legal and normative requirements continuity / crisis management

Continuity and Crisis Management (excerpt)

- Railway Act (EBG, SR 742.101) - Obliges railway undertakings to ensure safe operation at all times. This includes the obligation to ensure minimal operation even in the event of disruptions or crises.
- Ordinance on safety in the railway sector(SEV, SR 742.141.2) - Safety management systems must include plans for emergencies and crisis situations; includes requirements for risk assessment, crisis organisation and restart processes.
- VKOVA (SR 742.161) - Regulates the coordination in the event of extraordinary events (e.g. major disruptions, disasters, terrorist situations) in public transport. Specifies how energy supply companies must cooperate with authorities and other partners (FOT, fedpol, cantons, emergency services) and coordinate their emergency organisation accordingly.
- Federal Act on Civil Protection and Civil Defence (BZG, SR 520.1) - governs the cooperation of railway undertakings with authorities on civil protection. The emergency and crisis management of railway undertakings must be embedded in national protection and emergency planning.
- ISO 22301 (Business Continuity Management) - International standard for setting up and operating a Business Continuity Management System (BCMS).

# The development of safety continues to be positive.

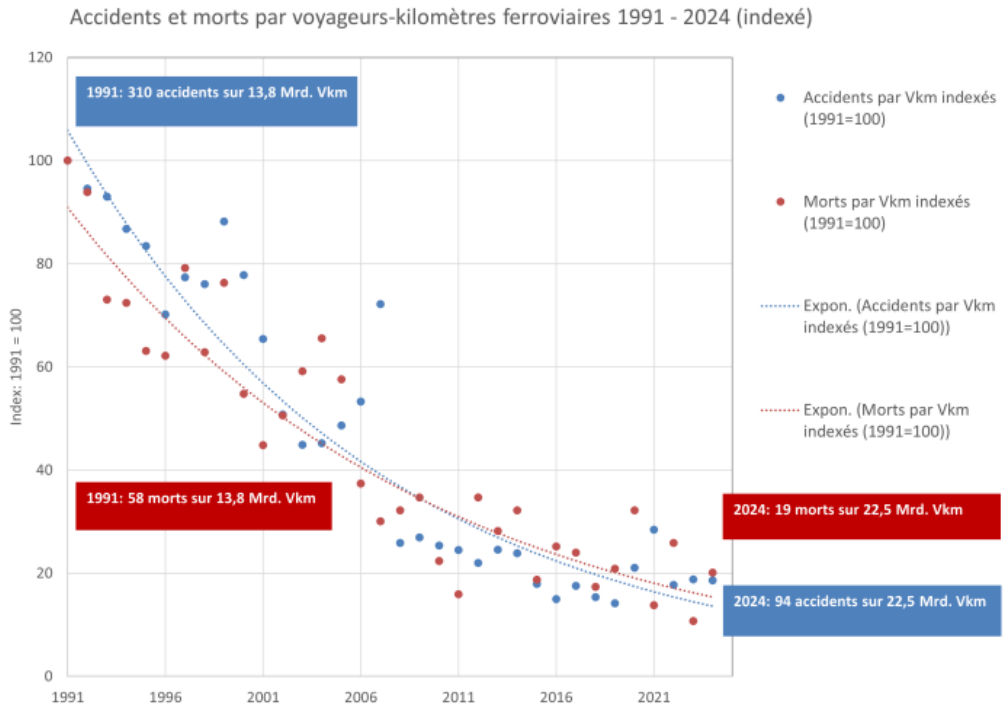
## Comparaison des risques des moyens de transport terrestres (sélection), de 2013 à 2022

| | Un décès pour: | Risque de mourir en fonction de la distance parcourue, mesuré par rapport au moyen de transport le plus sûr, le chemin de fer (=1) |
|---|---|---|
| Chemin de fer | 190,86 mrds de personnes-km | 1 fois |
| Voiture de tourisme | 1,13 mrd de personnes-km | 169 fois |
| Vélo (sans vélo électrique) | 0,10 mrd de personnes-km | 1 985 fois |
| Motocycle | 0,04 mrd de personnes-km | 4 732 fois |

Les risques ont été calculés en rapportant, pour chaque moyen de transport considéré, le nombre de passagers ou d'usagers tués aux personnes-kilomètres effectués en Suisse. Pour réduire l'influence des variations à court terme sur les résultats, une période de 10 ans a été prise en considération (de 2013 à 2022).

gr-f-11.06.01.02
© OFS 2024

Source: OFS – Prestations du transport de personnes (PV-L); OFROU, OFS – Accidents de la circulation routière (SVU); OFT – Nouvelle base de données d'événements © OFS




Railway remains the safest mode of transport in Switzerland. The development of accidents and deaths over time is also positive (Source: Sicherheitsbericht 2024, BAV)