Railway systems and their transition
Lecture 11

Safety and Security.

Peter Kummer
EPFL, Autumn Semester 2025
December 9, 2025

Preparatory reading for the lecture.

Preparatory reading:
Handout with basic safety&security and crisis management terminology, risk management framework, bow-tie analysis.

Please refer to the document on moodle

Agenda.

1. What is "integral safety and security"?
2. The derailment in the Gotthard Base Tunnel – a lesson from multiple perspectives
3. Challenges of the railway system
4. Discussion
5. Exercise

WHAT IS SAFETY AND SECURITY?

What does safety mean for the railways...

Safety is absolutely key.

For accident-free and punctual rail operations.

To bring customers and goods safely from A to B.

After work, all employees go home healthy.

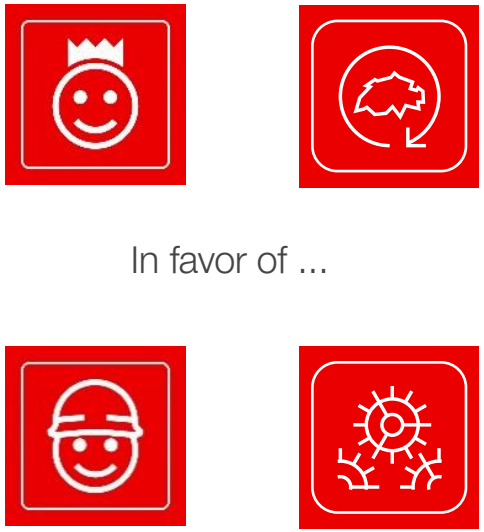
1

Why is safety and security not easy to achieve ?

It often appears different from what it is.

Image-Source: http://markelikalderon.com/wp-content/uploads/2008/06/trojan-horse.jpg

Modern, integral security consists of various subject areas.



1

Dealing with risks

Source: https://www.risknet.de/wissen/risknet-cartoons

1

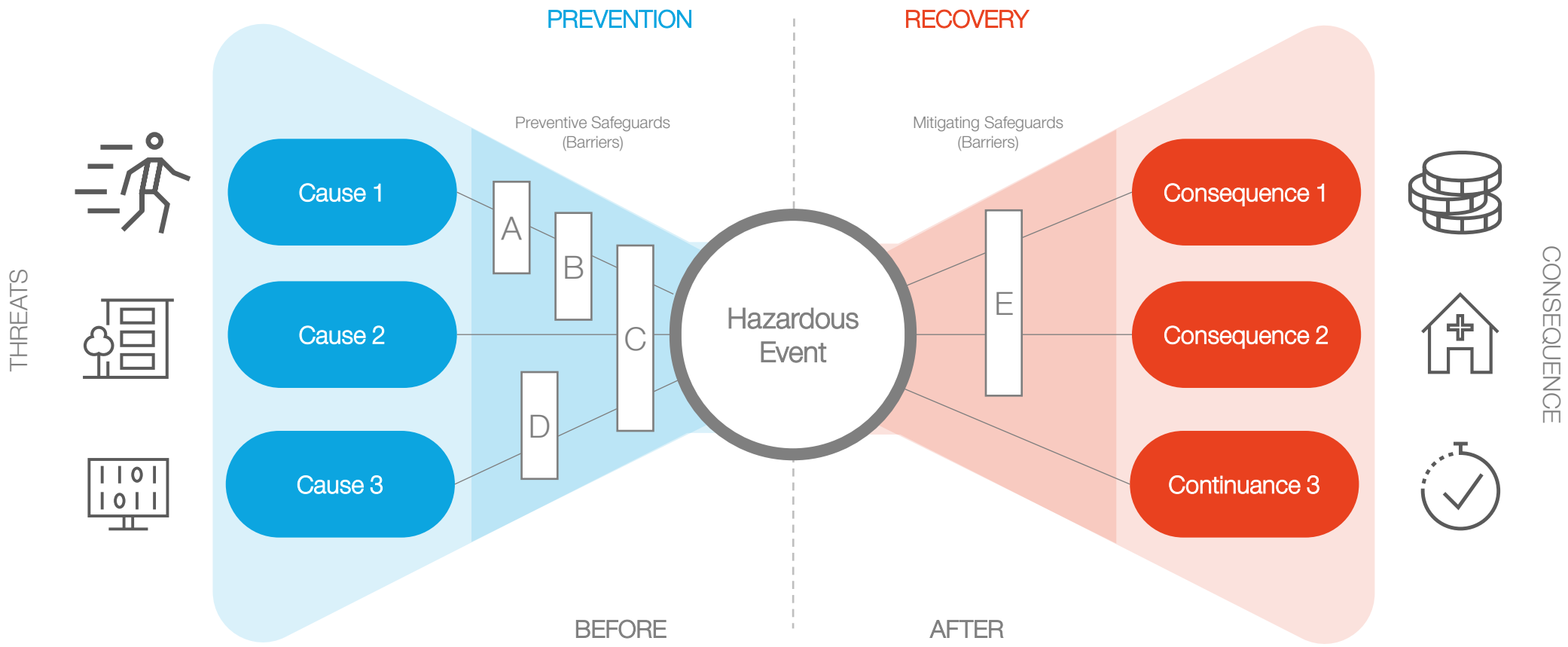
Dealing with risks is central to security.

- **Difference between hazard and risk:**
  A hazard is the potential source of harm; risk assesses how likely and how severe that harm would be.
- Risk factors & causal chains:
  Safety incidents often arise from a combination of factors, not just a single cause.
- **Prevention vs. response:**
  Safety management includes both preventive measures to avoid incidents and reactive measures to limit harm.
- **Systemic perspective:**
  Risks typically affect technology, people, processes and organisation simultaneously; safety analyses must cover all levels.
- **Transparent visualization:**
  Methods like bow-tie help present complex risk processes clearly and make them tangible for decision makers.
- **Guidance:**
  SBB uses the SN ISO 31000:2018 guideline

Fundamentals

1

Causes and consequences using a bow-tie risk analysis.



This presentation has been designed using resources from PoweredTemplate.com

Case Study: Event in the Gotthard Base Tunnel

Derailment in the
Gotthard Base Tunnel

Safety

Hypotheses for the lecture
(no connection with the real event of 10.08.2023)

Assumption of the cause

Cybersecurity
(Attack)

Security
(Sabotage)

Crisis-& Continuity
Management

2

Tunnel out of service

Can a single technical defect paralyze a billion-dollar project?

The derailment in the Gotthard Base Tunnel / Event

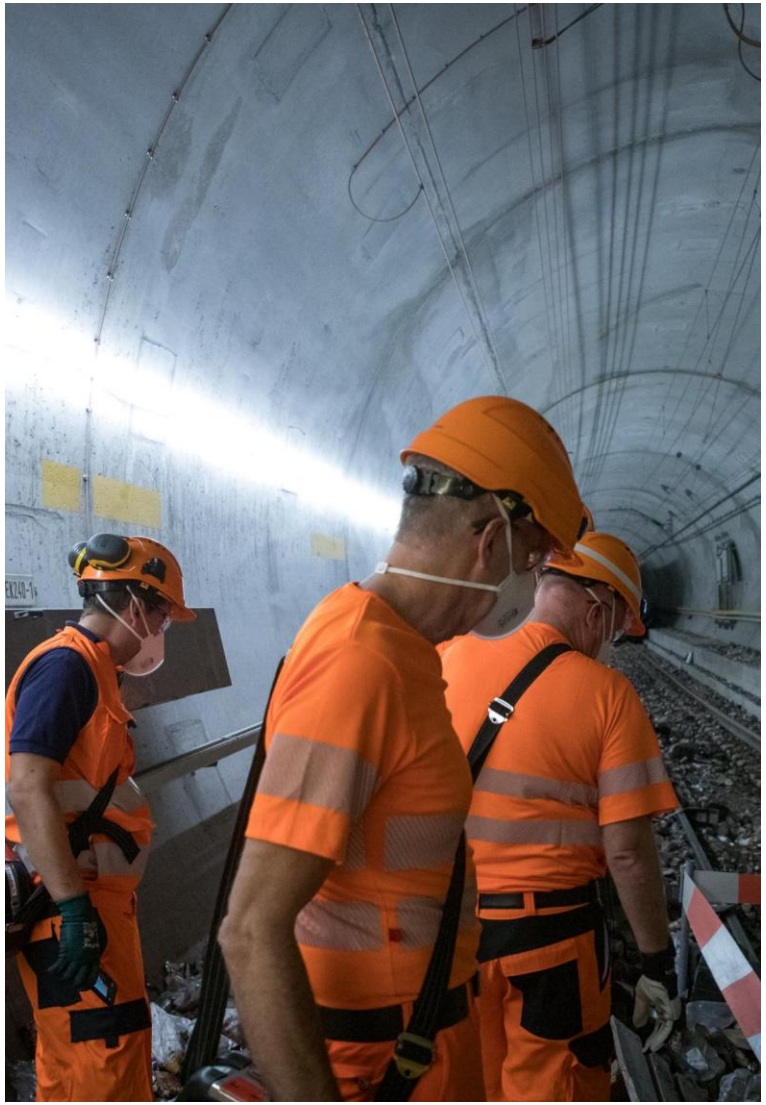
- On 10 August, a freight train starts in Chiasso in the direction of Basel/Mannheim.
- Shortly after entering the Gotthard Base Tunnel, the wheel of a car breaks.
- During the ride, more parts come loose until the wheel fails completely.
- As a result, a switch is severely damaged, which leads to the derailment of the rear part of the train.
- A total of 16 cars derail, the train comes to a standstill after changing lanes.
- Fortunately, there are no injuries, but considerable damage to the infrastructure

2

This is what we found in the tunnel.

Berm at track change

High-speed switch area



The derailment in the Gotthard Base Tunnel / Causes

- **Fatigue cracks in the wheel** disc of a freight car – developed over a long period of time and remained undetected.
- **Wheel breakage due to thermal overload** of the wheel due to high braking energy and material fatigue.
- **Lack of detection by automatic systems such as the ZKE** (train control devices) – hairline cracks can not be detected.
- **Lack of apropriate wheel checks** to detect anomalies that have arisen.
- **Systemic material problems** with certain types of wheel discs in European freight transport.

The **final SUST report does not identify operational or organisational deficiencies as causes of the derailment**, but it does point to structural conditions that increase the complexity of the events.

2 The derailment in the Gotthard Base Tunnel / Consequences

- **Interruption of the main north-south axis:**
  Massive impact on national and European rail traffic, including backlogs of freight trains. Reopening only in Sept. 2024.
- **Diversions:**
  Passenger and freight trains over the old mountain line with loss of capacity and time (approx. +60 min).
- **Operational adjustments:**
  Replanning of the timetable, increased personnel and vehicle requirements, postponement of planned construction work.
- **Social consequences:**
  Limited connections to southern Switzerland, reduced national supply, traffic shifted to road.
- **Financial impact:**
  Damage of around CHF 150 million.
- **Political & organizational factors:**
  Political interventions, proof of limited operation, flexible employees required.

2

Resumption of service

✓ 23.08.23
Restart of freight traffic in the east tube

✓ 29.09.23
Some passenger trains in the east tube

✓ 10.12.23
Start of passenger services on weekends (mixed slots Fri, Sat, Sun) in the east tube

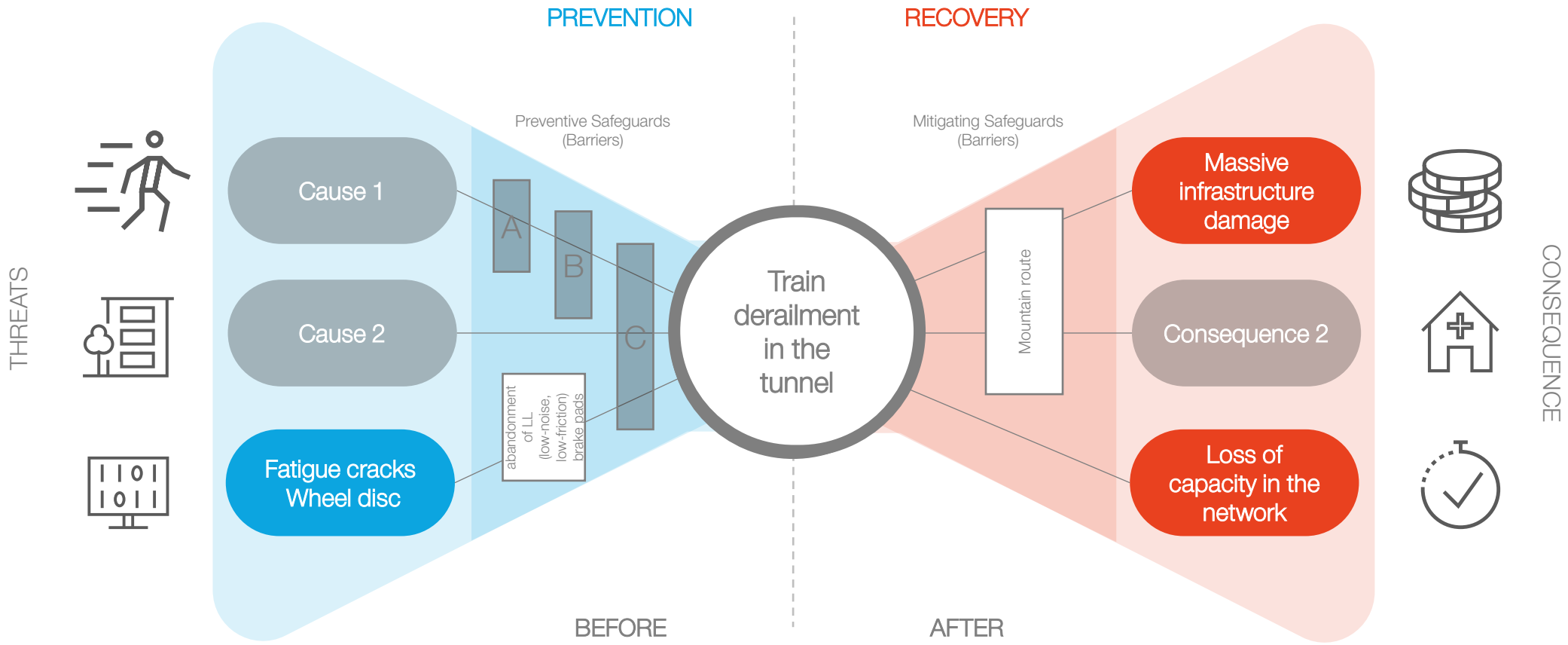
✓ 25.03.24
Early morning south-to-north passenger service,e increased freight capacity (8-wagon blocks), holiday services for Easter, Ascension Day and Pentecost

✓ 02.09.24
Full commissioning with a 30-minute frequency in long-distance services

Full recommissioning on 02.09.2024

2

Excursus: Bow-tie risk analysis for GBT (exemplary).



This presentation has been designed using resources from PoweredTemplate.com

2

Operational/occupational safety

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

2

Operational/occupational safety

Learning from incidents is important!

- **Technical and organizational measures** must interact
- **Data/condition monitoring is becoming increasingly important,** and **near misses are also indicators of risk**
- Observe **human-machine interfaces**, both for operational and occupational safety

Safe behaviour requires a positive safety culture

2 Operational/occupational safety

Incendie à Faido (TI)

Tunnel du Gothard: un véhicule prend feu, 29 personnes évacuées

Un feu de voiture a entraîné l'interruption du trafic ferroviaire pour une durée indéterminée lundi dans l'importante galerie.

Publié: 29.01.2024, 12h44
Mis à jour: 29.01.2024, 12h44

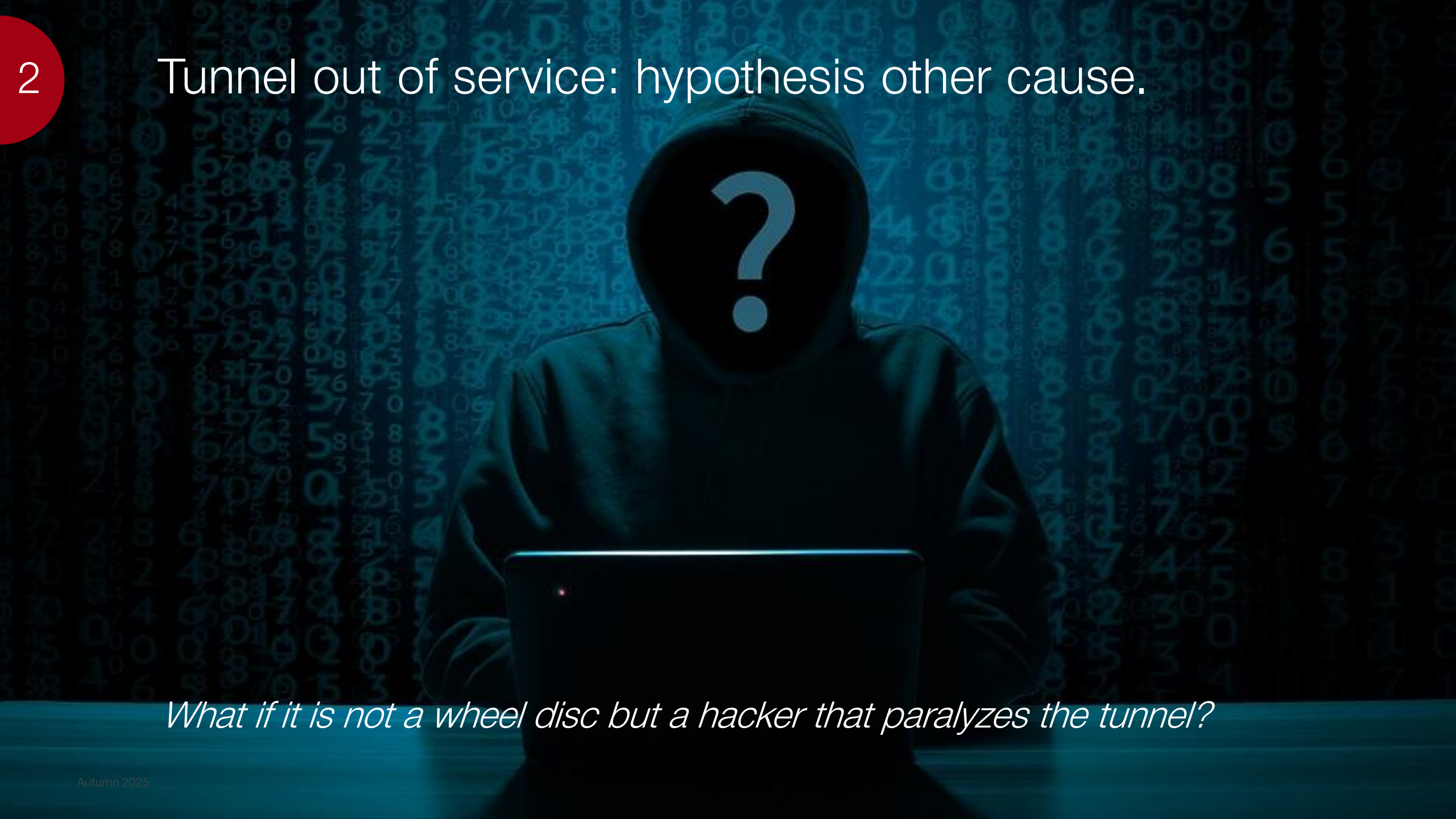
8

L'incident est survenu vers 08h20, selon la police tessinoise.
KEYSTONE/Urs Flueeler

Un véhicule d'une entreprise de sécurité a pris feu lundi matin à la sortie du tunnel de base du Gothard près de Faido (TI), entraînant l'interruption du trafic ferroviaire pour une durée indéterminée. Une trentaine d'ouvriers ont dû être évacués.

2

Tunnel out of service: hypothesis other cause.



What if it is not a wheel disc but a hacker that paralyzes the tunnel?

Information Security / Cybersecurity

- Cybersecurity means 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.
- **Information security and cybersecurity** are often **used synonymously**, whereby information security also includes different data and media (e.g. paper documents or the knowledge of employees).

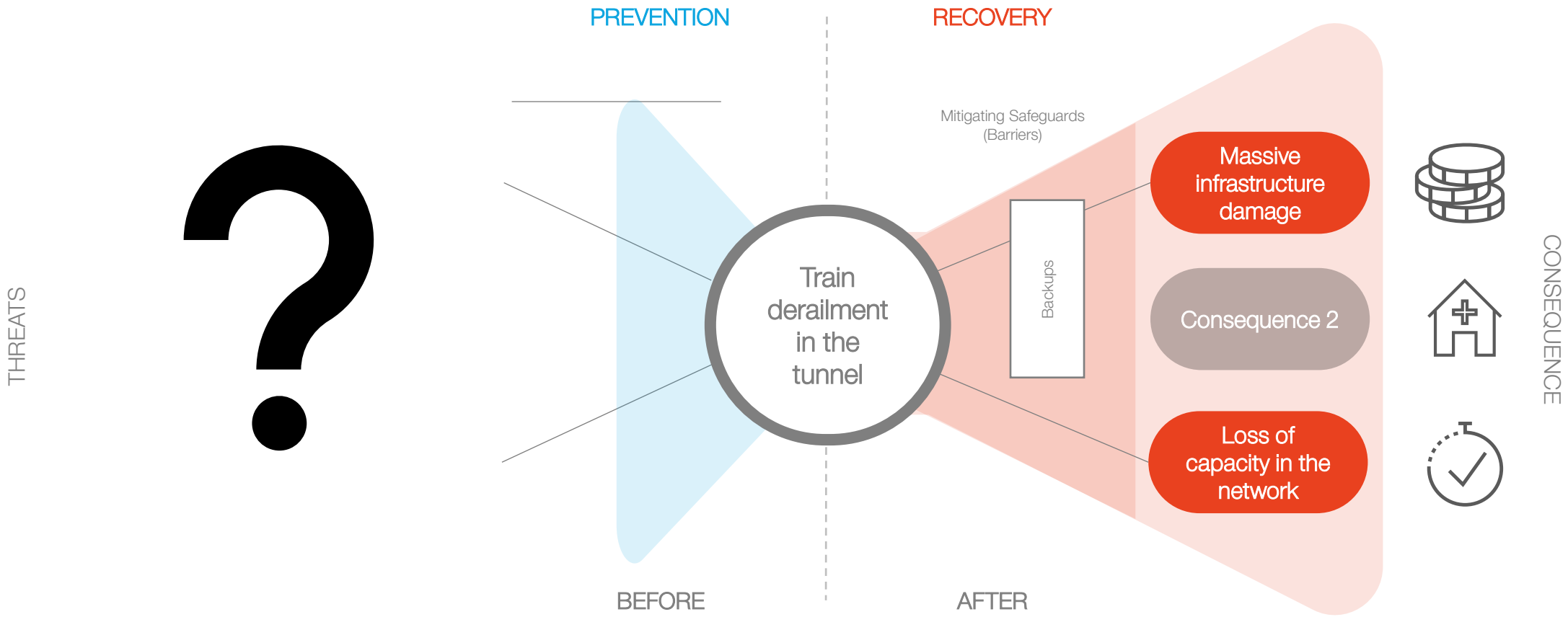
The protection objectives are the **confidentiality, availability and integrity** of systems and data.

Information Security / Cybersecurity

- **Rail operations are highly digitalized**
  Interlockings, ETCS, maintenance systems, logistics – everything runs via IT / OT.
- Data integrity and availability are just as critical as physical security.
- **Cyber risks can trigger physical risks**
  Manipulation or data loss can cause miscontrol (points, signals, timetables) and thus have similar consequences as a technical defect
- **Resilience also means cyber resilience**
  Backups, emergency IT, redundant control centers are just as important as physical spare parts.

2

A bow-tie analysis of GBT from a cybersecurity perspective will identify other causes and suggest measures.



This presentation has been designed using resources from PoweredTemplate.com

Tunnel out of service: hypothesis

How do you protect critical infrastructure from deliberate physical attacks?

2 Security

Security is **protection against events** (criminal offences, threats and other undesirable conditions) committed by persons with **malicious intent against employees, customers, physical and intellectual property**.

2

Security

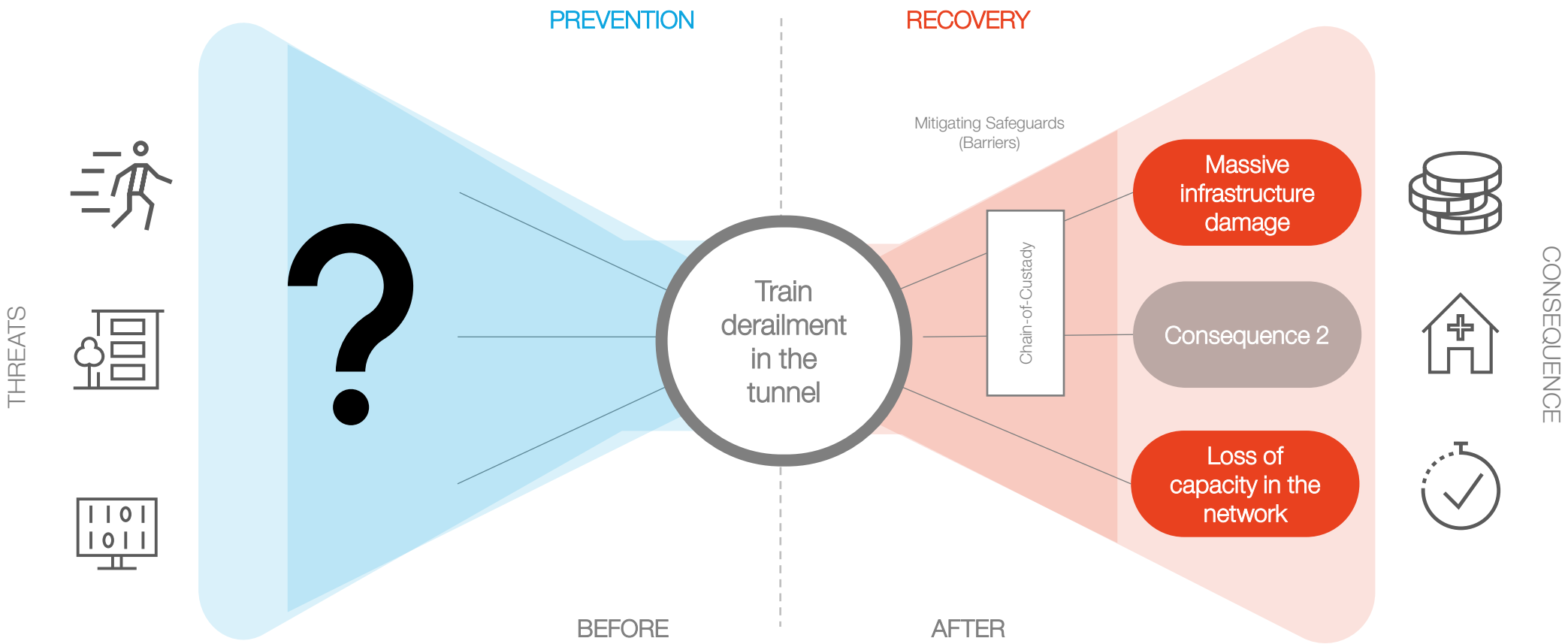
- **The railway system is an open and freely accessible system.**
  This means that important infrastructure elements are freely accessible (e.g. cable ducts)

- **Focus on critical infrastructures / highly frequented customer areas**
  Signal boxes, operations centres, railway stations, events, energy supply

- **Social changes have an impact on the railways**
  Cooperation with authorities important for joint work for public safety

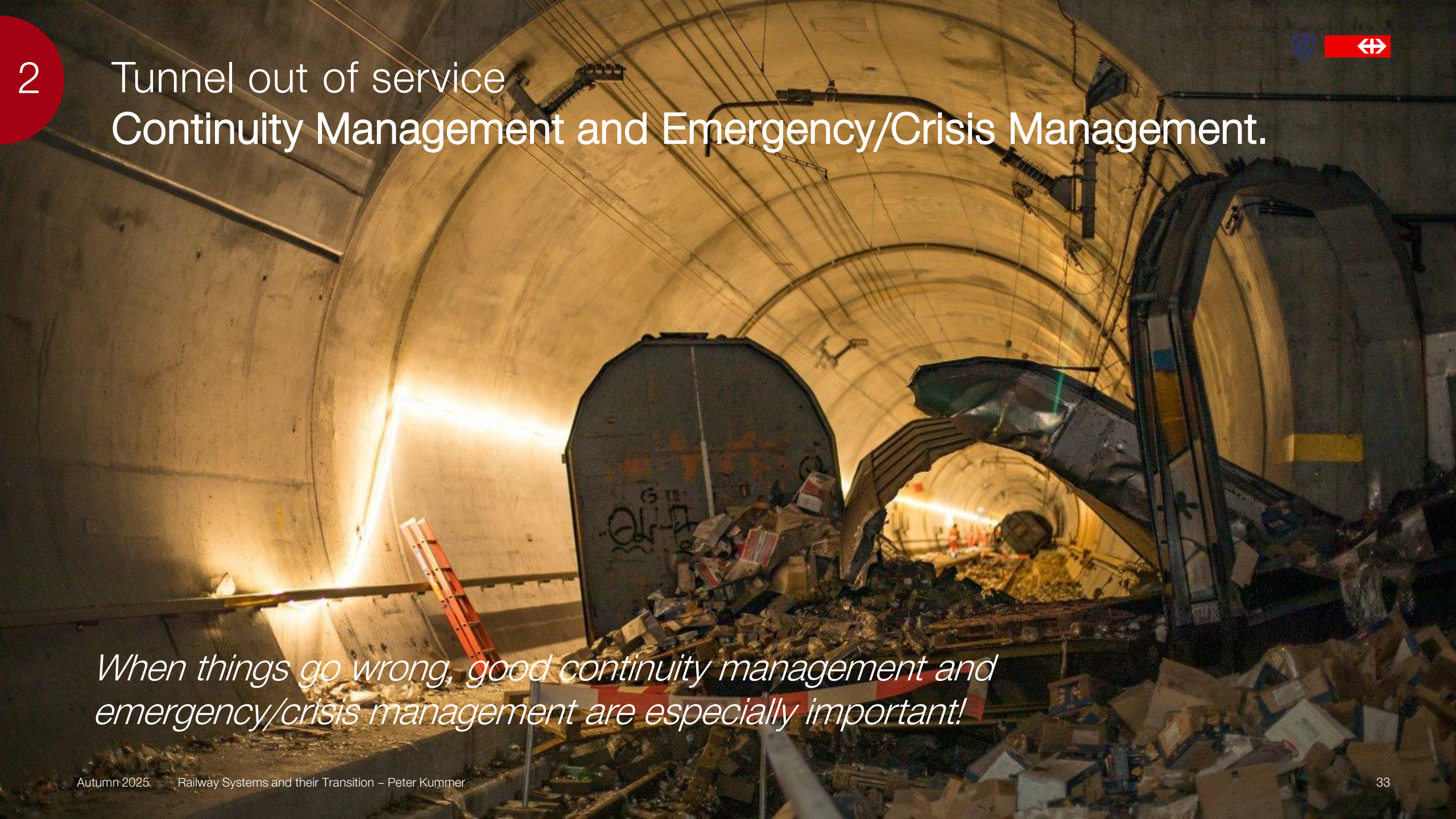
2

A bow-tie analysis from a security perspective requires malice on the part of an attacker



2

Tunnel out of service
Continuity Management and Emergency/Crisis Management.



When things go wrong, good continuity management and emergency/crisis management are especially important!

2

Continuity-and Crisis Management.

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

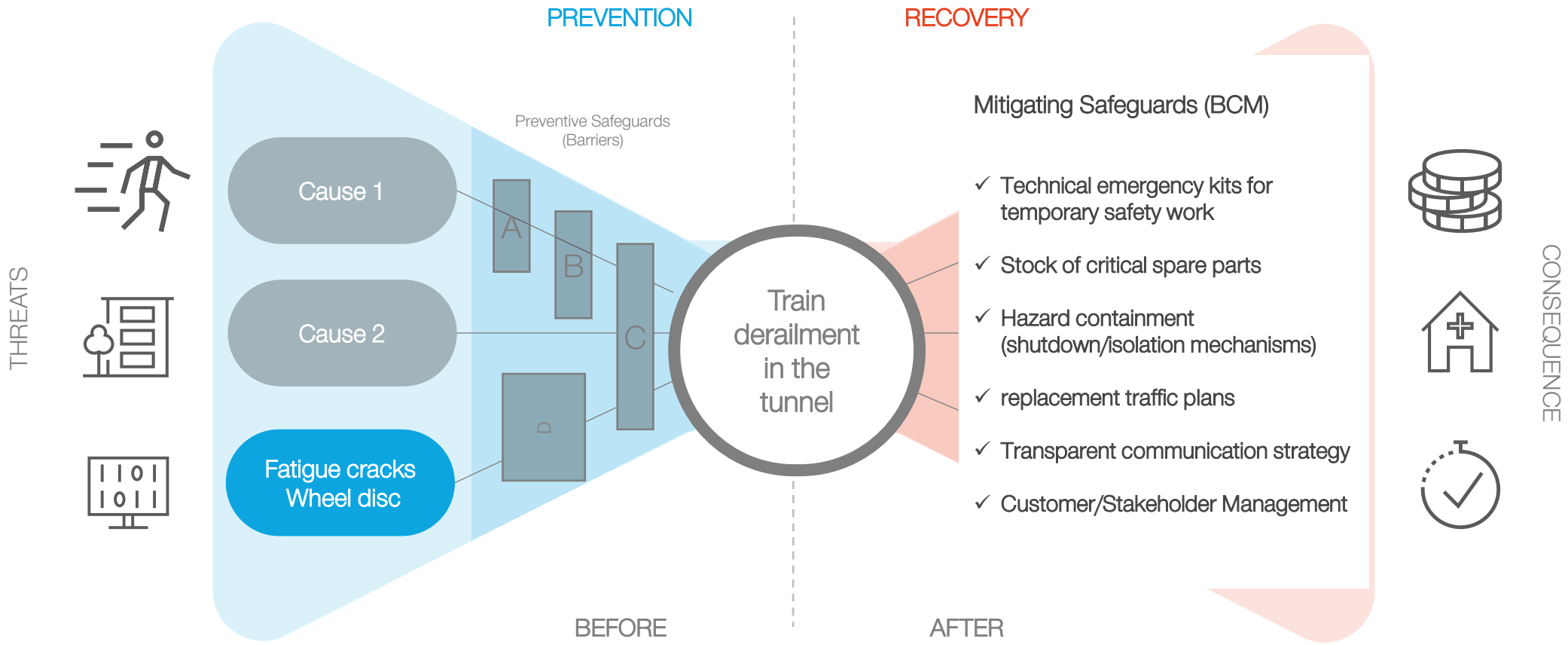
while the

emergency or crisis management, which includes immediate response and **coordination in an emergency to limit damage and ensure the ability to act.**

Continuity- and Crisis Management.

- **Business continuity is more than crisis response**
  BCM not only plans the emergency, but also the **structured restart** and the **maintenance of operations during a malfunction.**
- **Identify critical processes**
  Which assets and processes are indispensable?
- **Redundancies and fallback options**
  Replacement routes or IT backups ensure continuity.
- **Collaboration & Communication**
  BCM affects **operations, engineering, Communications, government and customers** at the same time.
- Communication is key when it comes to crisis management

A Bow-Tie Analysis from the BCM Perspective



Meet the challenges of the rail system in an integrated way.

3

An integrated railway needs integrated safety

Many future challenges can only be mastered together.

Everywhere there is
increased capacity demand.

Lack of attention / distraction / overload

Digitalisation / networking
continues to increase.

Not all security measures are ...

Equally visible to everyone

Security programs, regulations, audits, awareness campaigns, on-site presence, Safety clothing, etc.

Agreements with partners, operators and national and international bodies

Legal and technology monitoring

A lot of technical measures

Cyber Defence and Darknet Monitoring

3

Security is a process – not a state.

- Interdisciplinarity:
  - engineering, IT, organisational structures and communications must be tightly interconnected.
- Resilience rather than pure prevention:
  - disruptions will occur – what matters is response speed and recovery time.
- Cyber + physical:
  - attacks and technical failures often have similar consequences.
- Critical infrastructure requires redundancy:
- security is a process, not a fixed state.
- Communication is key:
  - without clear information, trust and operational freedom are lost.

Safety Culture

«Safety must be seen by all of us as a positive and important addition to everyday (working) life."

Source: https://pixabay.com/de/photos/bergsteigen-und-klettern-2264698/

«A culture of dealing with errors assumes that mistakes will occur and that they are reported and fixed. Errors are an integral part of learning and development.»

… Mistakes can happen.

Source: https://pixabay.com/de/photos/bergsteigen-frau-sonnenuntergang-6001209/

Questions / Discussion