FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

We know all about Safety – but what is Cyber Safety?

Dipl.-Ing. Gabriele Schedl, CSE

Director Safety Management, Frequentis AG
International Safety Manager of the Year 2014
Regional Vice President Europe, International System Safety Society

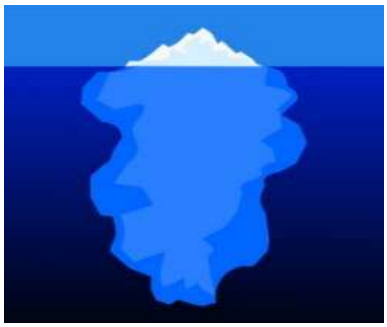
Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Motivation to System Safety

Accidents (reactive)



Hazards (proactive)

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

System Safety – Definitons

"System Safety is the application of special technical and managerial skills to the systematic, forward-looking identification and control of hazards throughout the lifecycle of a project, program or activity."

Harold Roland and Brian Moriarty

"The essence of System Safety is that the system does what it is supposed to do, and does not do what it is not supposed to do."

System Safety Society

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

System Safety – Definitons

What is a System?

A system is a set or group of interacting, interrelated elements, that are organized and integrated to form a collective unity to achieve a common objective.

A system, has a definition of boundaries to which the systematic process of hazard identification, hazard analysis and control is applied.

The system considers people, procedure and the equipment.

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

System Safety – Definitons

What is Safety?

The state in which the possibility of harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and safety risk management.

International Civil Aviation Organization

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Exemplary Hazard Risk Matrix

	Hazard Severity			
Hazard Probability	CATASTROPHIC	HAZARDOUS	MARGINAL	NEGLIGIBLE
Frequent	A	A	B	C
Probable	A	B	B	C
Occasional	B	B	C	D
Remote	B	C	D	D
Improbable	C	D	D	D
Incredible	D	D	D	D

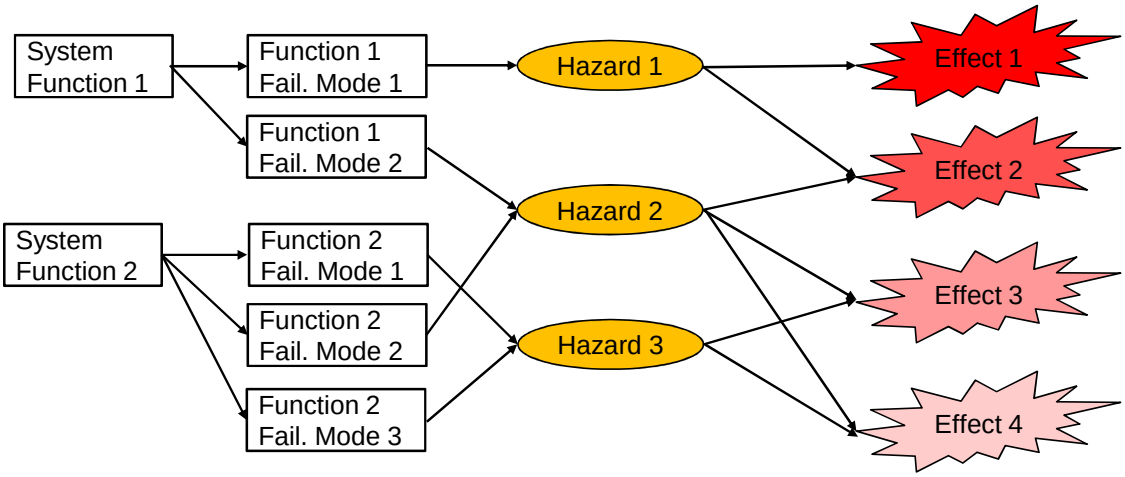
Risk Class	Interpretation
A	Intolerable
B	Undesirable and shall only be accepted when risk reduction is impracticable
C	Tolerable with the endorsement of either the Project Manager together with the internal ordering party or the Safety Director
D	Acceptable with the endorsement of the normal project reviews

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Failure Modes – Hazards – Accidents

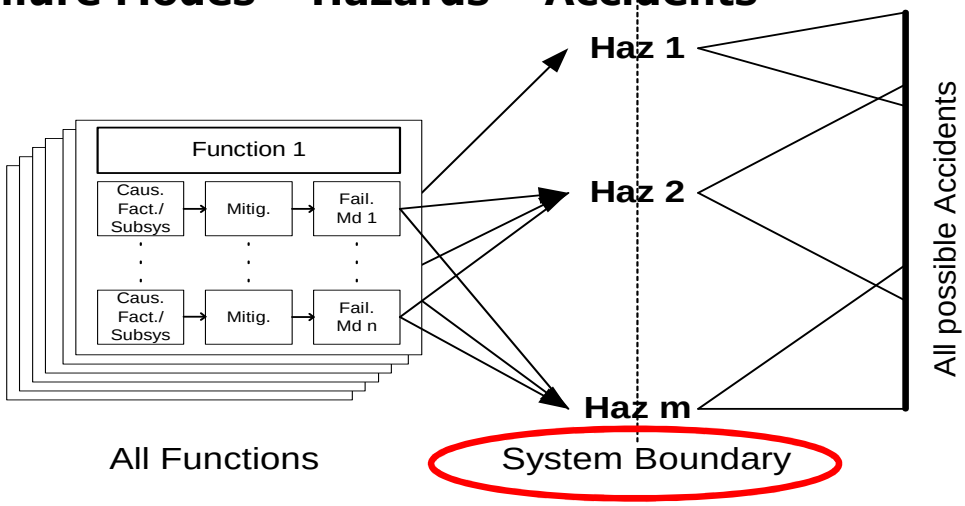


Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Failure Modes – Hazards – Accidents

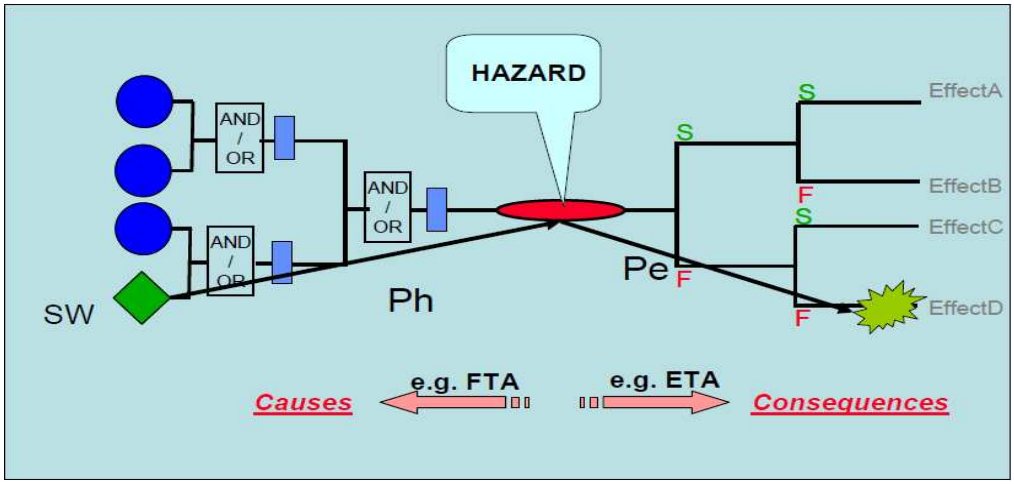


Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Safety/Software Integrity Allocation

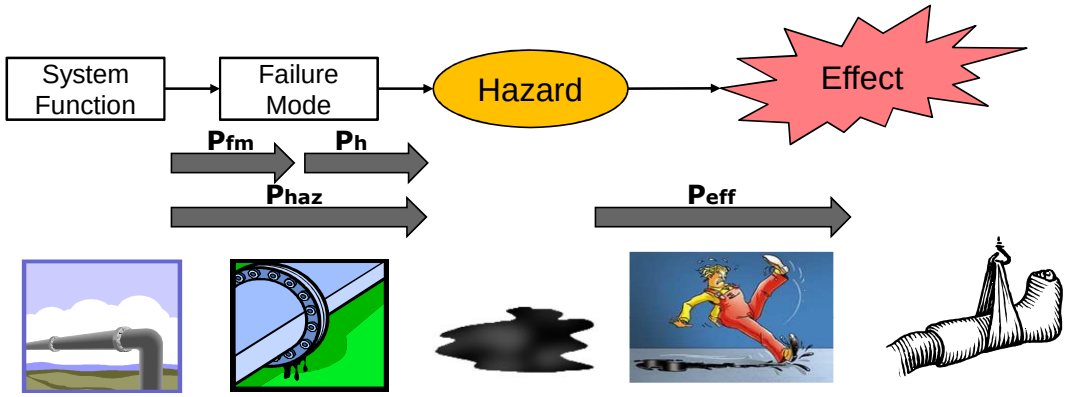


Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Failure Modes – Hazards – Accidents



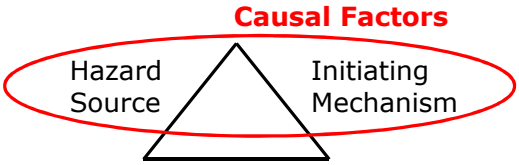
Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Hazard Triangle Model

Hazard Source
Electricity
Fuel
Chemicals
Pressure
Temperature
Radiation …



Target / Threat Outcome (Danger)

Target	Threat
Personnel	Injury
Public	Death
System	Loss
Environment …	Damage …

Initiating Mechanism
Hardware failure
Software failure
Human error
Interface error
Poor design
Poor maintenance …

Erstellt von: Gabriele Schedl

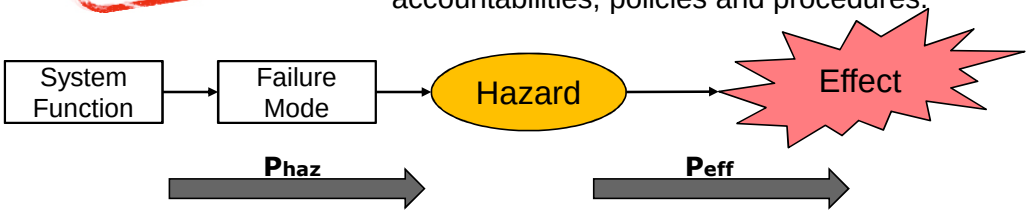
FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Safety Summary

The primary concern of system safety is the management of hazards: their identification, evaluation, elimination, and control through analysis, design and management procedures.

A Safety Management System (SMS) is a systematic approach to managing safety, including the necessary organizational structures, accountabilities, policies and procedures.



Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

(New) Challenge Safety & Security

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Safety Concerns Everywhere

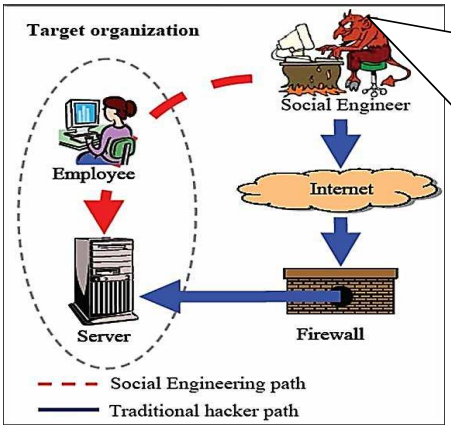
> Huge problems of competence – incl regulators
> Many conflicts between safety and security
> Inconsistent, inapplicable rules (lack of HF input)
> Consistent, known violation of policies

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Social Engineering



Hi, it's Felix from helpdesk, currently we're heavily stressed with that new heartbleed cyber attack, you've heard about it?

It is really really bad, our CEO and CTO are here right now to check the situation.

I need a remote desktop to your computer, but my admin credentials are currently locked in another server, so I need to use yours really quickly.

Okay? Great, so what is your password?

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Background – Security

ICS-CERT (Department of Homeland Security, US)

> 256 reported incidents in 2013
> Majority of incidents detected in networks of **critical infrastructure** organizations
> Energy sector (59%), **critical manufacturing** (20%), transportation (5%)
> **Supply chain** is targeted

Security is a serious concern to safety-critical applications

> Reported malware in **ATM systems** (W32.Stuxnet)
> Sophisticated malware and viruses
> Exploits easily available on the internet

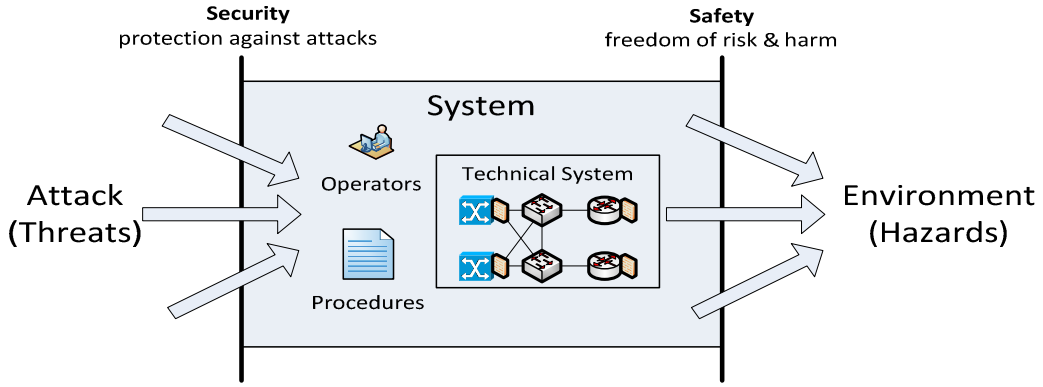
ICS… Industrial Control System
CERT … Computer Emergency Response Team
ATM … Air Traffic Management

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Safety & Security



Strong connection of System Safety & System Security regarding the **availability** of functions for **authorized** parties

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Safety & Security

Commonalities

Process-oriented and life-cycle approach
> Must be considered in early design phase, no „add-on"

Additional expenses (technical and monetary) that pays off
> Long-term benefits

Risk assessment based approach
> Evaluate residual risk
> Categorisation
> Mitigation means

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Safety & Security

Differences

No common international Safety & Security standard
> E.g. IEC61508, ISO27000

Safety requirements may overrule Security requirements
> Conflicting situations, for example:

- Security requires complexe and unique passwords to login
- Safety requires short term login to avoid critical loss of time in stressful situation

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Motivation – Air Traffic Management (ATM)

Former and current Voice Communication Systems (VCS)
> Proprietary hard- and software
> TDM technology
> Sealed off environment inherently given by TDM

Future situation for **ATM-Supplier** industry driven by
> COTS hardware
> 3rd party software libraries
> Virtualization technology
> Shared Voice-over-IP (VoIP) networks
> Fast moving technology
> High security risk

TDM … Time-Division Multiplexing
ATM … Air Traffic Management
COTS … Commercial Off-The-Shelf

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Background – Safety & Security Example

Example: Technical Monitoring and Control System (TMCS)

> Configuration of radio frequencies and roles
> Change may be necessary at a specific point in time
> Depending on daytime and task, rush hours!

Safety

> **Availability** of the Voice Communication System is **critical**
> **Sufficient resources** required to operate airspace **safely**
> Backup system required to clear the sky

Security

> **Unauthorized** access to TMCS is **critical**
> Misconfiguration or sabotage could lead to **safety incidents** (e.g. frequency change)

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Cyber Space

Cyber Space

> Systems and services connected directly or indirectly to the internet or networks
> Border of cyberspace is hard to describe
> Non-physical events

Typical Situation in ICSs

> Data is transmitted through shared IP networks
> Trustful and sealed-off environment is hard to archive
> Air-gap may be bypassed (e.g. by USB thumb drive, weakest link)
  > Maintenance done with devices which had direct access to the internet?

USB … Universal Serial Bus
IP… Internet Protocol

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Driving Factors

Increasing complexity in software networks
> Leads to more complex failure modes.

Increasing use of COTS products
> Leads to new security threats.

Increasing use of sub-contractors

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Driving Factors

Changes in Safety-Related Systems
> Increasing interconnection of systems through IP networks
> COTS and 3rd party software
  > IT Hardware (e.g. Servers, Switches, Routers)
  > Common Operating Systems (e.g. Linux)
  > Frameworks (e.g. Java Runtime Environment)
> Claims for state of the art

Challenges
> COTS vulnerabilities widley known (e.g. OpenSSL heartbleed bug)
> Patch Management
> Growing IT security awareness & interest

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

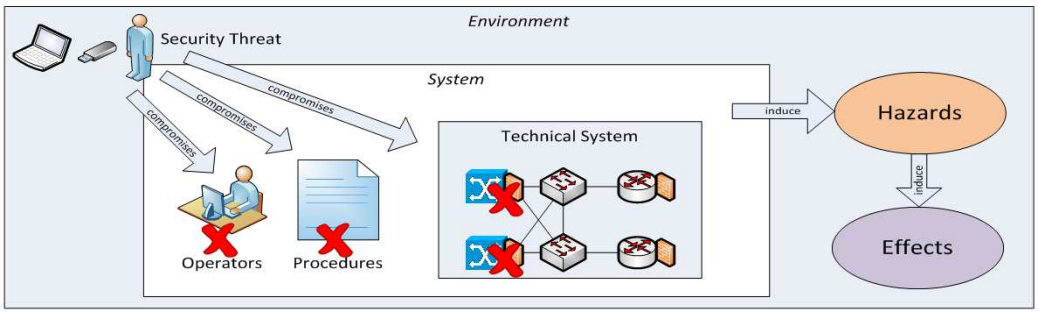
FREQUENTIS

Example

Non-physical security events in cyberspace may have **real implications**

> Denial of Service (**non-physical**)

> Disruption of safety-related ATM procedures (**reality**)



Sara Sadvandi, Nicolas Chapon, Ludovic Piètre-Cambacédès, "Safety and Security Interdependencies in Complex Systems and SoS: Challenges and Perspectives"

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Conflict between Safety & Security

- Existing safety standards eg ED153
  - Focus on verification and validation
  - In proportion to SWAL/criticality
- Anti-viral systems violate ED-153
  - Updated every 24-48 hours
  - could themselves bring down ACC
  - Cannot test anti-virus definiitons
  - Without increasing security exposure
- Do you want safety or security
  - Can have both eg banking approach

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Connection between Safety & Security

Security affects Safety

> Risks must be considered globally

Both areas aim to improve the availability and reliability

> Common cutting point in it's mission

Awareness, Culture and Training

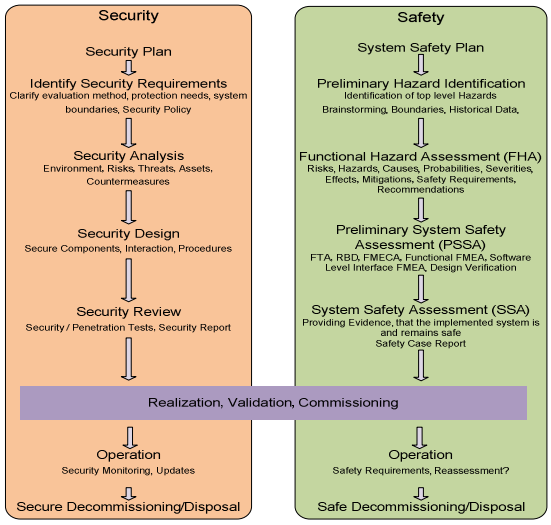
> Unlike safety, cyber security needs to become part of daily operations

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Life Cycle Integration



Processes independent, but cooperation is possible!

Activities may differ depending on requirements

Different focus in operation
(Software Update versus Software Assurance)

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Benefits of Integration

Including security threats into Functional FMEA

> Identification of safety & security relevant functions
> Mapping of threats to failure modes and hazards
> Security Risk Assessment for critical subset (if necessary)

Outcome and Benefit

> Identification of safety functions where security is important
> Definition of common mitigations and requirements
> Harmonization of safety & security contradictions
> Systematic analysis of threats and hazards
> More safe and secure systems

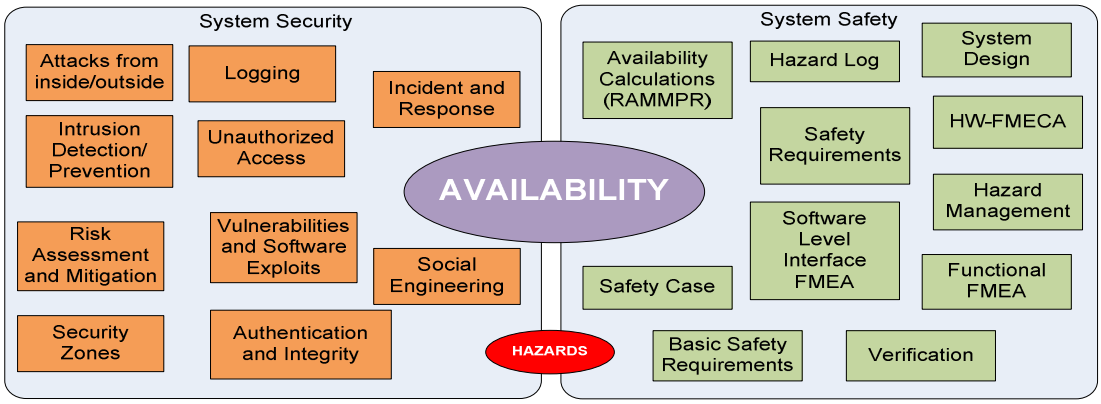
Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Summary Safety & Security

Availability is a main principle of both domains



Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

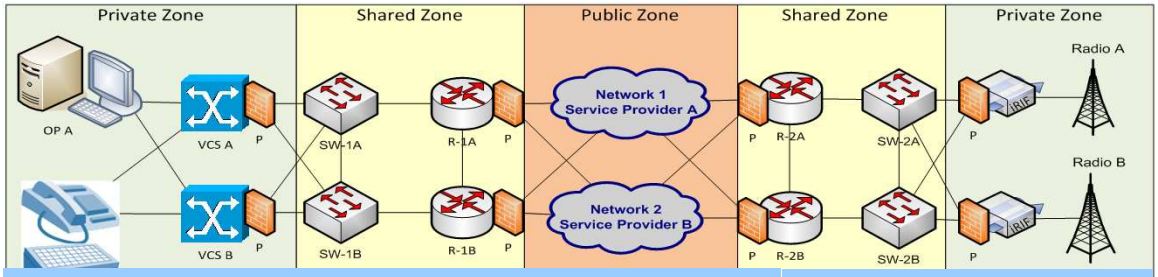
FREQUENTIS

Cybersafety & Security Assessment

Exemplary assessment of a Voice Communication System

> Taking into account the **safety impact** of cyberspace related **security threats**

> Voice connections may be across **different parts** of cyberspace



VCS … Voice Communication System
OP … Operator Position
SW … Layer 2 Switch
R … Layer 3 Router
P … Perimeter
iRIF … IP Radio Interface

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Cybersafety & Security Assessment

Security zones through perimeter functions necessary

> Classifying network zones is a great instrument in the course of security analysis

> Physical and logical separation of parts of cyberspace by perimeters

> Shared and public zone are of **special interest**

> Private zone is the most protected because of the security measures of other zones

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Security Zones

Security Zones	Assumptions	Security Risk
Public	Non-trusted environment (e.g. Service Provider, 3rd party) No control over technology No dedicated resources available (worst case is best effort)	High
Shared	Trusted environment but not under full control Resources are shared with other (e.g. radar devices) Increased risk of insider attacks	Middle
Private	Control over technology Dedicated resources (bandwidth, quality of service) Devices and personnel fully trusted	Low

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Cybersafety & Security Assessment

Functional Failure Modes and Effects Analysis (FMEA)

1. Analysis of safety-related functions
2. Assignment of **assets** (operational value)
3. HAZOP guidewords used for finding failure modes
4. Failure modes identified through HAZOP guidewords
5. Deviation of **theoretical** hazards

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Example FMEA

Id	Function	Asset	HAZOP Guideword	Failure Mode	Hazard
1	IP based audio transmission (RTP, RTSP, SIP)	Information in transport	No/Not	No audio transmission possible	Loss/degradation of telephone functionality

FMEA… Functional Failure Modes and Effects Analysis
HAZOP … Defense Standard 00-58
RTP … Real-Time Transport Protocol
RTSP … Real-Time Streaming Protocol
SIP … Session Initiation Protocol

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Cybersafety & Security Assessment

Security analysis

> Definition of assets (e.g. information, data, service availability)

> Identification of **predictable** security threats by best practice

> Predictable threats like DoS are generaly known

> Zero-day exploit is non-predictable

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Example Security Analysis

Id	Threat	Example
1	Denial of Service (DoS)	RTP flooding, SIP Proxy DoS, SIP invite flooding

Mapping of security threats to safety analysis

Link between security threat and safety hazard established

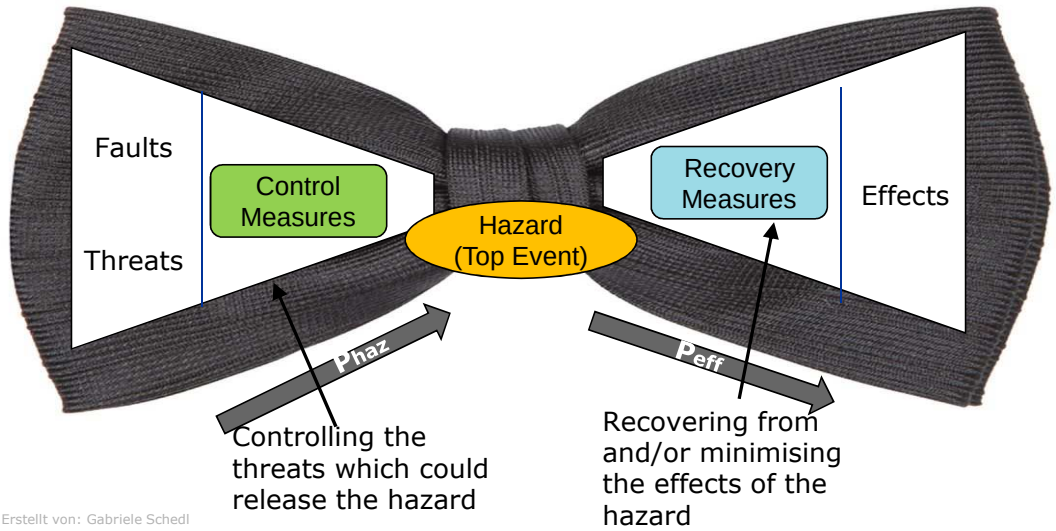
RTP … Realtime Transport Protocol
SIP … Session Initiation Procotol
DoS … Denial of Service

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Bow-Tie Diagram



Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING
FREQUENTIS

Mitigations – Security Mechanisms

Secure tunneling of network traffic (e.g. IPsec VPN)

> Connects areas of the **same security zone** level
> Protects **information in transport** by cryptographic measures
> Avoids network related attacks like sniffing or MITM
> Hides network traffic for attackers
> Fail-over redundancy is a challenge because of secure tunnel setup

MITM … Man in the Middle
IT … Information Technology
VPN … Virtual Private Network

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING
FREQUENTIS

Mitigations – Security Mechanisms

Perimeter functions (e.g. firewall, access control lists)

> Controlled communication **between different security zones**
> Forward only allowed network traffic and refuse any other access
> Blocking or logging of malformed messages to secure a safety system
> **Logging** is important for IT forensics
  > Absolutely required for investigations

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Recommendations

Detailed knowledge of physical and logical system parts required
> System boundaries must be clear
> Transition **between security zones** are of special interest

Golden rule
> **Security measures** should not compromise safety related functions
> Security functions need proper documentation to analyse the safety impact

Common mindset
> Understanding of safety and security is essential
> Gathered information can be used for **joint analysis**

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Further Effort Needed

Some problematic areas remain currently unresolved:

Software Assurance vs. Security Updates in the field of ATM
> Comprehensive verification and validation activities mandatory by standards
> Software related **security updates** would require re-certification by authorities
  > Security updates on a daily bassis, but assurance activities last for weeks

Focus of interest
> Safety requirements overrule security features **and vice versa**

Speaking the same language between project members
> Comprehensive understanding and clear definitions required

ATM … Air Traffic Management

Erstellt von: Gabriele Schedl

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

FREQUENTIS

Conclusion

Awareness for Cybersafey must be raised
> Security threats may lead to safety hazards
> Safety requirements may overrule security claims, but security affects safety

Risks of cyberspace must be taken into account
> Security threats should be considered within safety analysis for transparency

FMEA method has been extended for **security**
> Information can be shared between safety & security analysis

Cybersafety has high value for safety systems and thus for our **society**
> Cooperation with security professionals for combined assessments recommended

Erstellt von: Gabriele Schedl