System Safety Part 3: Cyber Safety and Security
ISSC 2016, Orlando, USA
Open Brainstorming

If you think about **Security**, what comes into your mind?
Highly reliable communication and information solutions for a safer world
More than 65 years of innovation in safety-critical applications
Frequentis group 2015
Global market leader

Headquarters Vienna

Solutions partners and regional offices in over 50 countries

95% Export

228 M EUR turnover 2015

1,309 Employees

12% R&D

1947 Established

80% STEM*

*) Science, Technology, Engineering, Math
Frequentis product portfolio – driven by know-how, experience and synergies
Communication and information solutions for a safer world

- **ATM Civil**
  - Voice communication systems
  - Remote tower
  - ATM systems
  - Intelligent networks
  - Aeronautical information management

- **Defence**
  - Red/black communications
  - National air policing
  - Last minute briefing system
  - Joint forces command

- **Public Safety**
  - Call handler and radio dispatcher
  - Network components and emergency applications
  - ECO system

- **Public Transport**
  - Fixed terminal systems - GSM-R and bearer independent
  - Incident management

- **Maritime**
  - Integrated maritime solutions and networks
  - smartVTS
  - GMDSS /SAR
  - Tactical communication

**Safety critical solutions**

**Common products**
- Voice communication
- Information management
- Networking

**R&D: Leveraging cross-industry heritage in product development**
Frequentis – a strong network around the world

- 90% of all passengers worldwide are served by Frequentis customers
- 25,000 working positions using Frequentis solutions
- 120+ countries
- 33% of the world safer with Frequentis networks
- #1 in GSM-R dispatcher terminals
- 200,000km protecting the largest maritime coastline

Status: E01/2016
Projects in 120 countries around the world

More than 300 customers

#1 VCS ATM market share

Largest public safety control centre in Europe

#1 GSM-R dispatcher terminal market share

Largest maritime coastline safer - 200,000km
Agenda

- TBD
What is Security?

- Security is a composite of:
  - Confidentiality: Absence of unauthorized disclosure of information
  - Integrity: Absence of improper system alterations
  - Availability: Readiness for correct service
### Terminology

- **Asset**
  - anything that has value to the organization

- **Threat**
  - a potential cause of an unwanted incident, which may result in harm to a system or organization

- **Vulnerability**
  - a weakness of an asset or group of assets that can be exploited by one or more threats

- **Security Risk**
  - a security risk is the loss potential to an organization’s asset(s) that will likely occur if a threat is able to exploit a vulnerability
Security Awareness is a Mindset!

- Lack of security awareness might compromise all other dependability attributes
- Take it personal!
  - When have you last changed your passwords?
  - Where do you store your passwords?
  - Are your passwords secure?
  - Do you use different passwords for all services?
  - Do you ever transmit passwords in plain text?
  - Do you ever check e-mail via POP, IMAP, http? (i.e. without SSL/TLS)
  - Do you read the permissions for Smartphone apps?
  - Do you have a virus scanner? On all your computers?
  - How do you weigh usability vs. security?
  - Do you regularly install all critical updates?
  - Do you use Adobe Flash Player, Java Applets,…?
  - Do you use public WLAN Hotspots?
  - What about your camera on your laptop? Microphone?
  - …
Security Mindset? ;-)
Motivation & Background
Motivation – Driving Factors

- Reliance on electronic systems
  - Hardware, software, networks, …

- Cyber-Security has become a global economic and social concern
  - Threats and vulnerabilities harm humanity and society

- Safety critical infrastructures are attractive targets
  - Increasing use of Commercial Off The Shelf (COTS) components
  - Net-centric approach (e.g. SWIM)
## Motivation – Change of Environment

<table>
<thead>
<tr>
<th>Current systems</th>
<th>Future systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>„Closed“ System</td>
<td>Service Oriented Architecture (SOA)</td>
</tr>
<tr>
<td>Point-to-Point connections</td>
<td>Net-centric</td>
</tr>
<tr>
<td>„Monolithic“ system</td>
<td>Interconnected sub-systems, and extended to include airports, pilots and data providers</td>
</tr>
<tr>
<td>Proprietary interface definition</td>
<td>Standard protocols with published vulnerabilities</td>
</tr>
<tr>
<td>Diversity of suppliers and systems</td>
<td>Fewer suppliers</td>
</tr>
<tr>
<td>Lots of redundancy</td>
<td>Efficiency</td>
</tr>
<tr>
<td>Existing users have security management systems in place</td>
<td>Some new end-users have little security management (e.g. general aviation)</td>
</tr>
</tbody>
</table>
Motivation – New Vulnerabilities

- Increased inter-connection and propagation vectors
  - Between safety-critical area and others (e.g. remote access)

- Increased level of exposure
  - Change of point-to-point to net-centric communication architecture

- Use of standard components (COTS, TCP/IP, …)
  - Publication of vulnerabilities, e.g. Heartbleed

- Varying levels of cyber-security maturity
  - Maturity levels may vary and create weak links in cyber-security chain

...
Motivation – Security News-Ticker 2015/16

- 15,435 vulnerabilities across 3,870 applications were recorded in 2014
  - Pasted from <http://www.net-security.org/secworld.php?id=18132>

- European Aviation Safety Agency – Airplane hacking is reality
  - Pasted from http://securityaffairs.co/wordpress/40975/hacking/easa-airplane-hacking.html

- ConnectedDrive: Der BMW-Hack im Detail

- Stromausfall in der Ukraine augenscheinlich durch Hacker ausgelöst

- BSI-Sicherheitsbericht: Erfolgreiche Cyber-Attacke auf deutsches Stahlwerk
Motivation – Threats to Safety

- Harm of environment
- Disruptive attacks reduce operational capacity
- Financial and reputational damage
- Loss of confidence
Motivation – Cyber Attacks

- Cyber-attacks against the ATM Cyber Space can be defined as an offensive activity executed against the confidentiality, integrity and availability of the ATM cyber space elements. Cyber-attacks are designed to:
  - Deny
  - Degrade
  - Disrupt
  - Manipulate or Destroy

- A cyber-attack may lead to the malfunction of the ATM/ANS operations, e.g. safety, confidentiality and business degradation/continuity

- The implementation of the new Air-Ground Data links based on IP protocols will increase the risks of a cyber-attack on avionics systems such as Flight Management Systems
Motivation – Things are happening NOW

Cybercrime

- Malware (Viruses, Ransomware, Trojan Horses, Adware, Spyware,…)
- (D)DoS Attacks
- Website Defacements
- Phishing, Spear Phishing
- Doxing
- Spam
- …
CWEs and CVEs

- CWE = Common Weakness Enumeration (https://cwe.mitre.org)
- CVE = Common Vulnerability and Exposure (https://cve.mitre.org)

- A CWE is a generic weakness in a software system that can lead to a CVE
- A CVE is a concrete vulnerability in a specific software version
- e.g. the Heartbleed bug has ID CVE-2014-0160, and is caused due to CWE-130, CWE-119 and CWE-201
## Top 10 CWEs

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-89</td>
<td>Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')</td>
</tr>
<tr>
<td>CWE-78</td>
<td>Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')</td>
</tr>
<tr>
<td>CWE-120</td>
<td>Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')</td>
</tr>
<tr>
<td>CWE-79</td>
<td>Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')</td>
</tr>
<tr>
<td>CWE-306</td>
<td>Missing Authentication for Critical Function</td>
</tr>
<tr>
<td>CWE-862</td>
<td>Missing Authorization</td>
</tr>
<tr>
<td>CWE-798</td>
<td>Use of Hard-coded Credentials</td>
</tr>
<tr>
<td>CWE-311</td>
<td>Missing Encryption of Sensitive Data</td>
</tr>
<tr>
<td>CWE-434</td>
<td>Unrestricted Upload of File with Dangerous Type</td>
</tr>
<tr>
<td>CWE-807</td>
<td>Reliance on Untrusted Inputs in a Security Decision</td>
</tr>
</tbody>
</table>
## "Monster" Mitigations

<table>
<thead>
<tr>
<th>ID</th>
<th>Mitigation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>M1</td>
<td>Establish and maintain control over all of your inputs.</td>
<td></td>
</tr>
<tr>
<td>M2</td>
<td>Establish and maintain control over all of your outputs.</td>
<td></td>
</tr>
<tr>
<td>M3</td>
<td>Lock down your environment.</td>
<td></td>
</tr>
<tr>
<td>M4</td>
<td>Assume that external components can be subverted, and your code can be read by anyone.</td>
<td></td>
</tr>
<tr>
<td>M5</td>
<td>Use industry-accepted security features instead of inventing your own.</td>
<td></td>
</tr>
<tr>
<td>GP1</td>
<td>(general) Use libraries and frameworks that make it easier to avoid introducing weaknesses.</td>
<td></td>
</tr>
<tr>
<td>GP2</td>
<td>(general) Integrate security into the entire software development lifecycle.</td>
<td></td>
</tr>
<tr>
<td>GP3</td>
<td>(general) Use a broad mix of methods to comprehensively find and prevent weaknesses.</td>
<td></td>
</tr>
<tr>
<td>GP4</td>
<td>(general) Allow locked-down clients to interact with your software.</td>
<td></td>
</tr>
</tbody>
</table>
Bugs and Exploits

- Security bug
  - Serious fault (flaw, defect) in the software that might compromise security

- Exploit
  - Code or systematic mechanism which takes advantage of the bug ("a way to 'use' the bug")

- Zero-day exploit:
  - Exploit which is available *before* the bug is patched
  - ("after zero days")

- A (new) security bug and exploit is very valuable
Selling bugs and exploits?

- Various companies specialise in dealing with bugs and exploits
- There is a big (partly black, partly official) market for such bugs

Vupen: "Access to this service is thus highly restricted, and is only available to approved government agencies (Intelligence, Law Enforcement, and Defense) in approved countries."
How many are there?

Common Vulnerabilities and Exposures
A BUG’S LIFE
ALL SOFTWARE HAS FLAWS. WHAT HAPPENS WHEN YOU FIND ONE? IT CAN BE FIXED—OR SOLD

1. ANALYZE SOME SOFTWARE
   Finding flaws takes high-level skills. You’re looking for major errors that creators missed.

2. FIND A VULNERABILITY
   A true zero-day has to be 1) serious enough that it’s a security problem and 2) previously unknown.

3. SELL THE BUG TO...
   Once you’ve nagged your bug, you’ve got a few options.
   - The software maker
     • Many companies will pay cash for bugs in their products.
   - The government
     • Intelligence agencies often purchase bugs covertly for use in espionage.
   - Criminals
     • They buy bugs on the black market and use them to steal trade secrets or personal info.
   - Foreign governments
     • So for the trade in bugs is largely unregulated, so the market is global.

THANKS!

4. COLLECT YOUR RICHES!
   Serious vulnerabilities in popular applications and operating systems can be worth five- or six-figure sums.

Time, July 21, 2014
# Price-list of a zero-day in black market

<table>
<thead>
<tr>
<th>Software</th>
<th>Price Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADOBE READER</td>
<td>$5,000–$30,000</td>
</tr>
<tr>
<td>MAC OSX</td>
<td>$20,000–$50,000</td>
</tr>
<tr>
<td>ANDROID</td>
<td>$30,000–$60,000</td>
</tr>
<tr>
<td>FLASH OR JAVA BROWSER PLUG-INS</td>
<td>$40,000–$100,000</td>
</tr>
<tr>
<td>MICROSOFT WORD</td>
<td>$50,000–$100,000</td>
</tr>
<tr>
<td>WINDOWS</td>
<td>$60,000–$120,000</td>
</tr>
<tr>
<td>FIREFOX OR SAFARI</td>
<td>$60,000–$150,000</td>
</tr>
<tr>
<td>CHROME OR INTERNET EXPLORER</td>
<td>$80,000–$200,000</td>
</tr>
<tr>
<td>IOS</td>
<td>$100,000–$250,000</td>
</tr>
</tbody>
</table>


High monetary reward for zero-days attracting more hackers to find them -> organisations need to invest for zero-day discovery and harden their infrastructure.
Some Quotes

- "Cybercriminals will buy so-called zero-day vulnerabilities in the black market, while government agencies and corporations purchase them from brokers and exploit clearinghouses, such as VUPEN Security, ReVuln, Endgame Systems, Exodus Intelligence, and Netragard."

- "Endgame sold 25 zero-day exploits a year for $2.5 million."

- "average vulnerability sells from around $35,000 to $160,000."

all from
Hacking Techniques and Attacks

- Social Engineering
- Brute-force attacks
- Viruses, Trojan Horses, Worms,…
- (Distributed) Denial of Service (DoS, DDoS)
- Spoofing
- Man-in-the-middle

or – most effectively – any combination of the above
Cyberterrorism, Cyberattacks, Cyberwar

- Hostile acts against governments, countries, certain groups,…
- E.g. "Sony Hack", attributed to North Korea
Cybersecurity

- Google search trends for term "cybersecurity" (2006-2015)
  - http://www.google.com/trends/
Many (legacy) Embedded Systems were designed without security in mind

Embedded Systems are increasingly interconnected ("Internet of Things")

SCADA Systems:
- Supervisory Control and Data Acquisition Systems: control and monitor technical processes
-  → highly vulnerable, consequences may be dramatic (safety-related!)

Not easy to retrospectively build-in security into embedded systems

Embedded systems are more vulnerable than larger computer systems
- because they often do not have the same amount of security measures
- because they are not updated frequently (or never)

Embedded systems are less vulnerable
- because they are often not based on operating systems with known vulnerabilities
- because tailored attacks would be needed, which are more expensive
Motivation – Easy Targets


- Shodan finds computers
  - Webservers, critical-infrastructure, refrigerators, webcams,…
  - Shodan indexes the "banners" the servers return

- Many devices still have their default passwords set…
Motivation – Easy Targets

A swimming pool acid pump
Air Gap

- Air Gap: Physical separation between networks
- Air Gap = Security Protection?

- Good hackers can circumvent an air gap:
  - Removable Media (e.g. USB Sticks)
  - Malware in Hardware (e.g. graphics card)
  - Compiler, Build chain
  - Malicious Updates
  - Social Engineering, use of subcontractors,…

- Best-known example to overcome air gap: Stuxnet
Is there an Air Gap in modern aircraft?

No!

Jeep Hack (July 2015)

- Wireless controlling Jeep Cherokees over the Internet
  - Radio, ventilation, windshield wipers, wiper fluid, cut transmission, disable brakes,…
- How does it work?
  - Fiat Chrysler cars have a system called Uconnect
  - Each car has an IP adress for convenience functions…
  - From here, malware accesses CAN bus
- Patch can only be applied via USB (not remotely)
  - Many cars will stay vulnerable…
The
Reaction

FCA US LLC Releases Software Update to Improve Vehicle Electronic Security and Communications System Enhancements

July 16, 2015, Auburn Hills, Mich. - The security and confidence of our customers is important. As part of its ongoing software security and quality efforts, FCA has an Embedded System Quality Engineering team dedicated to identifying and implementing software best practices across FCA globally. The team's responsibilities include development and implementation of cybersecurity standards for all vehicle content, including on-board and remote services. A number of best practices, procedures, standards, and policies govern FCA's cybersecurity program. Generally, there are many tools and techniques that are utilized throughout the vehicle lifecycle.

Today, this group at FCA released a Technical Service Bulletin (TSB) for a software update that offers customers improved vehicle electronic security and communications system enhancements.

Similar to a smartphone or tablet, vehicle software can require updates for improved security protection to reduce the potential risk of unauthorized and unlawful access to vehicle systems. Today's software security update, provided at no cost to customers, also includes Uconnect improvements introduced in the 2015 model year designed to enhance customer convenience and enjoyment of their vehicle. Customers can either download and install this particular update themselves or, if preferred, their dealer can complete this one-time update at no cost to customers.

Customers with questions may call Vehicle Care at 1-877-855-8400.
"New features via free software updates – as with every Model S, the 60 and 60D will receive free over-the-air software updates that add functionality and continue to improve the driving experience for years to come."
Background – Safety & Security

Security
protection against attacks

Safety
freedom of risk & harm

System

Attack
(Threats)

Operators

Procedures

Environment
(Hazards)

Technical System

Strong connection of System Safety & System Security regarding the availability of functions for authorized parties
Background – Safety & Security Example 1

- **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)
Example: Car to Car Communication

Benefits for Safety
- Warning messages
- Regulated speed and distances
- Traffic control to avoid risks

Security Risks
- Fake safety messages could cause safety risk
- Vulnerabilities in the software (Threats!)
- Driving information (speed, location, daytime)

© DaimlerChrysler
Commonalities and Overlapping

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

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

- Risk assessment based approach
  - Evaluate residual risk
  - Classification and prioritization of risks
Background – Safety & Security

Differences

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

- Safety requirements overrule security requirements
  - Conflicting situations, for example:
    - Security requires complex and unique passwords to login
    - Safety requires short term login to avoid critical loss of time in stressful situation


Safety first
Connection between Safety & Security

- Security affects Safety
  - Risks must be considered globally

- Both areas aim to improve the reliability and availability
  - Reduction of "Bugs"
  - Common cutting point is Availability (and Hazards)
  - Commonalities in hazard and threat management (process based)

- Awareness, Culture and Training
  - Unlike safety, cyber security needs to become part of daily mindset
Background - Cyberspace

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

- **Typical situation for Frequentis Systems**
  - Data is transmitted through **shared IP networks**
  - Trustful and sealed-off environment is hard to archive
  - Air-gap can be bypassed (e.g. by USB thumb drive, weakest link)
    - Maintenance done with devices which had direct access to the internet?
    - Infected hardware, compilers, upgrades,…

- **Cyberspace concerns other safety-related areas**
  - Energy, Defense, Automotive, Public Transport, Health …
Background – Cyber Safety & Security

- **Non-physical** security events in cyberspace may have **real implications**
  - Denial of Service attack (**non-physical**)
  - Disruption of safety-related ATM procedures (**reality**)

Scenarios & Mitigation
Scenarios - Attackers

- Individual hackers
- (H)activists
- Insiders
- Business competitors
- Terrorists
- Organised crime
- State cyber-forces

_motivation and capabilities of attackers vary, readiness for diverse attacks required_

ENISA 2013 Threat Landscape
CANSO 2014 Cyber Security and Risk Assessment Guide
Scenarios - Impact

- Existing methods for estimating impact of a cyber-attack
  - Security Risk Assessment (e.g. ISO27005, NIST.SP.800-30)
  - Impact Areas (Personnel, Capacity, Performance, Economic, Brading, Regulatory and Environment)

- Comparable event to a Cyber-Attack: Eruption of Eyjafjallajokull in Iceland, April 2010
  - Closure of majority of European airspace for 6 days
    - ~ 10 million passengers
    - ~ 100,000 flights
  - IATA estimated $ 1.8 billion in lost revenue
  - ACI Europe estimated cost to airport € 250M
  - CANSO estimated costs for ANSPs €25M a day

Scenarios – ATM Cyber Space

- Collateral damage from external cyber-attack

1) A highly capable organized crime group targets the energy sector
2) Malicious software is introduced into a frequently used third party library
3) Meanwhile in ATM a developer uses the same library for an ATM system update
4) A (software) safety - but not security - assessment is done on the library update and the system goes live
5) The malicious software leads to a Denial of Service of the ATM system
German Steel Mill Incident, Dec 2014

- A malicious actor had infiltrated a steel facility
- Used a spear phishing email to gain access to the corporate network and then moved into the plant network
- Caused multiple components of the system to fail
- Massive physical damage due to furnace shutdown

Targeting
- People & Procedure
- Spear phishing email to gain access to the corporate network

1st Stage Delivery
- Applications
- Compromised host on corporate network

2nd Stage Delivery
- Network
- Moved into the plant network (unknown technique)

Exploitation
- Ability to cause multiple components of the system to fail

Annual Report 2014 of German government’s Federal Office for Information Security (BSI)
SANS ICS Defense Use Case (DUC) Dec 30, 2014
Heartbleed Vulnerability, April 2014

- Serious vulnerability in popular OpenSSL crypto software library
  - Cryptographic library used to secure connections in popular server products including Apache and Nginx (market share of both about 66%)

- Weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet

- This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users

- Mitigation: Patch with fixed version
  - OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
Mitigation – What do to?

What about a short break?
Mitigation – Some ideas for response

General Ideas

- Integrate Security into Safety Risk Assessment (e.g. FHA)
  - Probability of Security Threats? (almost 1?)

- Security & Penetration Tests (Safety Case)

- Information Security Management System (ISMS)
  - e.g. ISO27001 (BS EN 16495:2014 is an ATM adaption), NIST.SP.800-53

- Computer Security Incident Response Team (CSIRT)

- Partnership & Exchange of Information (CERT)

- Security Operation Center (SOC)

- Patch & Configuration Management
Mitigation – Two Examples

1. Keep critical infrastructure physically separated by design
   – If physical separation is not possible, apply Security Zones (perimeters)

2. Patch Management
   – Software Safety Assurance Issue!
Mitigation – Security Zones 1/2

- Exemplary assessment of a Voice Communication System
  - Voice connections may cross **different parts** of cyberspace
*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

<table>
<thead>
<tr>
<th>Security Zones</th>
<th>Assumptions</th>
<th>Security Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Public</strong></td>
<td>Non-trusted environment (e.g. Service Provider, 3rd party) No control over technology No dedicated resources available (worst case is best effort)</td>
<td>High</td>
</tr>
<tr>
<td><strong>Shared</strong></td>
<td>Trusted environment but not under full control Resources are shared with other (e.g. radar devices) Increased risk of insider attacks</td>
<td>Middle</td>
</tr>
<tr>
<td><strong>Private</strong></td>
<td>Control over technology Dedicated resources (bandwidth, quality of service) Devices and personnel fully trusted</td>
<td>Low</td>
</tr>
</tbody>
</table>
ENISA Recommendations for Europe on SCADA patching, Dec 2013
SCADA … Supervisory Control and Data Acquisition
Mitigation – Patch Management 2/2

- Current situation: No security patches applied
- The plan: Provide patches to equipment
- Test in non-operational environment before rolled out to operational machines
- After testing, apply in two phases
  - The first phase will involved half of the intended operational clients for verification of correct functionality over the course of 2-3 days of normal operations
  - The second phase will apply the patch package to all operational clients
- As usual: keep risk of patching in mind!
  - Have a backup!
- Prerequisite: Configuration Management
  - Which version are in the operational environment running?
Mitigation – More ideas

- Redundancy and diversity in (backup) systems
  - Primary system is safe, secondary system is secure (software updates)

- Black / Whitelisting
  - Communication Matrix

- System Hardening & Fault Tolerance
  - Sandboxing, Virtualization, Isolation

- Logging and Monitoring
  - Important for forensic analysis, false positives are a problem

- Reporting of security incidents will become mandatory
  - European General Data Protection Regulation (GDPR)
Summary

Safety & Security
Summary Safety & Security

- Availability is a main principle of both domains
- Risk assessments are common for both areas
- Life-cycle processes considered from the very beginning
- Awareness and mindset for both areas are essential
Summary Safety & Security

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 basis, 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
Security Facts & Problems

- Software has bugs (vulnerabilities, security holes)
  - Operating Systems, Frameworks, Libraries, Open Source, … are affected
  - Median number of vulnerabilities per application = 14
  - Heartbleed, Shellshock, BadUSB, Poodle, goto fail, … just in 2014

- People search for vulnerabilities (or introduce them)
  - Nation States, Government Agencies, Foreign Intelligence Services, Hackers, Insiders, Political Activists, Terrorists, Organized Crime, Investigative Journalists, Industrial Competitors, …

- Safety-critical systems are open to security threats
  - Long-term in operation, outdated software, no (security) updates allowed
  - More and more inter-connection or access to internet, remote access
  - Safety needs Security Safeguards