Karlsruher Institut für Technologie

ENERGY LAB 2.0 Security Lab

GESELLSCHAFT FÜR INFORMATIK

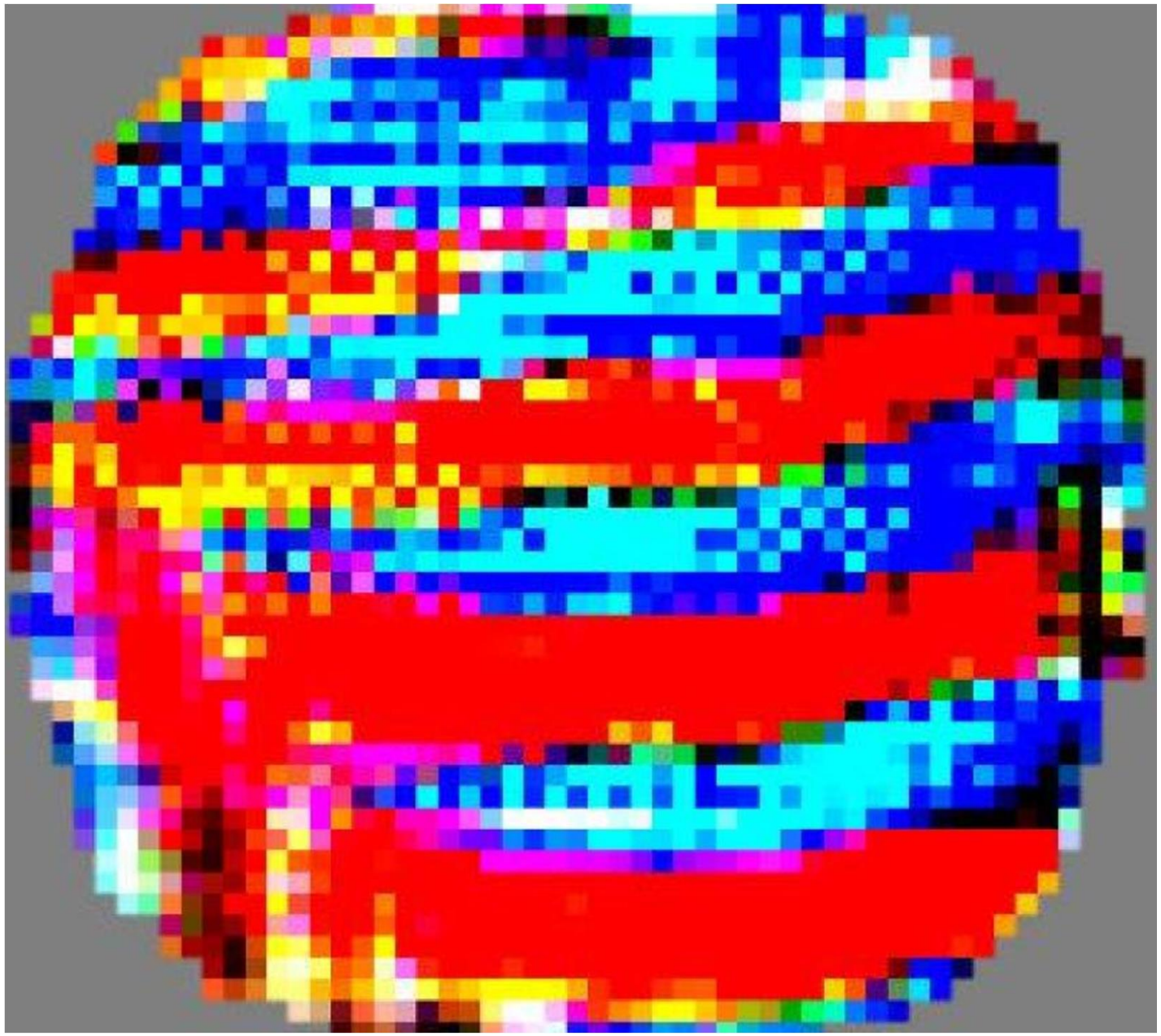
KASTEL

Lessons learned – PISEA Ergebnis in Safety und IT-Security

(*PISEA - Programme for International Science and Engineering Assessment*)

safeware engineering
safe and secure software

Hubert B. Keller, Karlsruher Institut für Technologie (KIT)
Leiter Fachgebiet Advanced Automation Technologies (A2T)
Leiter Arbeitsgruppe Reliable, Safe and Secure Software and Systems (RS4)
Institut für Automation und angewandte Informatik (IAI)



Agenda

Lessons learned – PISEA Ergebnis in Safety und IT-Security
(PISEA - Programme for International Science and Engineering Assessment)
oder
Wie sicher sind kritische Infrastrukturen, Automatisierungslösungen,
Smart Grids, Home Automation, smarte Geräte, …?

- Zur Person
- Angriffsszenarien
- Schwachstellen und Einfallstore
- Informatik Erkenntnisse aus den Jahren 1970 und folgende
- Entwicklungen anhand ausgewählter Beispiele
- Stakeholder für die Entwicklung sicherer Systeme
- Resümee

Zur Person

- **Dr. Hubert B. Keller**
  - Leiter Fachgebiet „Advanced Automation Technologies“
  - Seit 1984 Forschung in Sichere Software, Echtzeitsysteme, Maschinelle Intelligenz
  - Dozent Technische Informatik, Cyber Security in der Energieinformatik, Echtzeitsysteme
  - Mitbegründer GI Fachbereich Sicherheit – Schutz und Zuverlässigkeit
  - Mitautor „Technical Safety – An Attribute of Quality. Springer 2018
  - Autor von „Maschinelle Intelligenz“, Vieweg Verlag, 2000
  - Autor von „Echtzeitsysteme“, Springer Verlag, 2019
  - Mit-Initiator Berliner Sicherheitskonferenz
  - Co-Chair Sicherheitstagung GI 2003
  - Co-Chair Reliable Software Technologies Europe Konferenz 2000 und 2013

Verantwortlich für das SecurityLab Energie

Principal Investigator im Kompetenzzentrum für angewandte Sicherheitstechnologie

Mitbegründer des Fachbereichs Sicherheit der Gesellschaft für Informatik

Vorsitzender von Ada Deutschland e.V. (Verein für sichere Software)

Angriffsszenarien

Polen: Teenager hackt Straßenbahn mit Fernbedienung

- Infrarotes Licht als Steuersystem - 14-Jähriger Teenager hackt Straßenbahn mit Fernbedienung
- „Die Weichen werden anscheinend per Infrarot gesteuert. Das bedeutet, dass er nur die Codes, vielleicht noch die Lichtfrequenz und die Amplitude, herausfinden musste.“

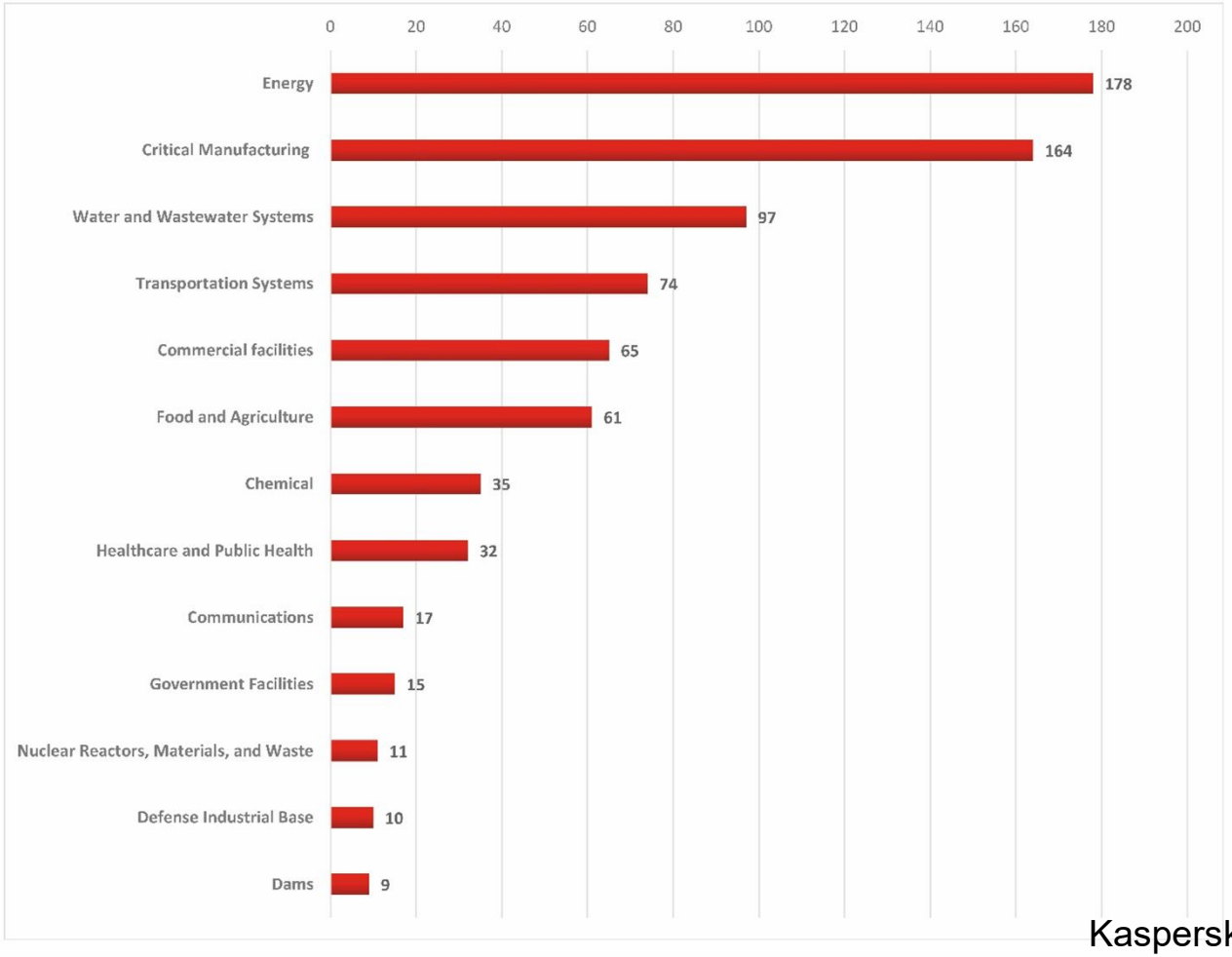
https://www.tecchannel.de/a/polen-teenager-hackt-strassenbahn-mit-fernbedienung,1744101

Ursachen?

- Transport command and control systems are commonly designed by engineers with little exposure or knowledge about security using commodity electronics and a little native wit.
- The apparent ease with which Lodz's tram network was hacked, even by these low standards, is still a bit of an eye opener.

https://www.theregister.co.uk/2008/01/11/tram_hack/

Angriffsziele

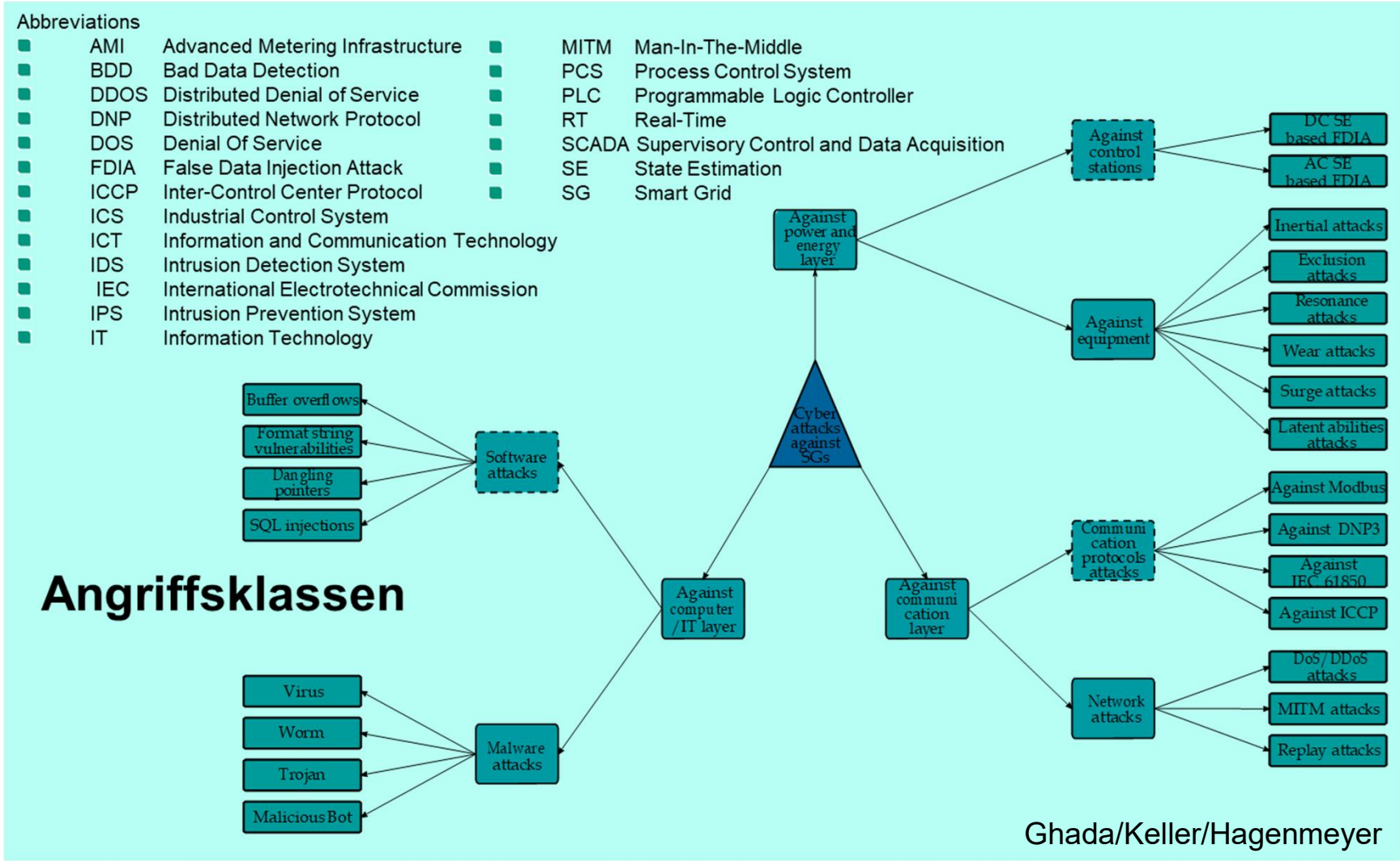


Kaspersky Lab, 2017

Angriffsvektoren klassisch und im Energiesystem der Zukunft

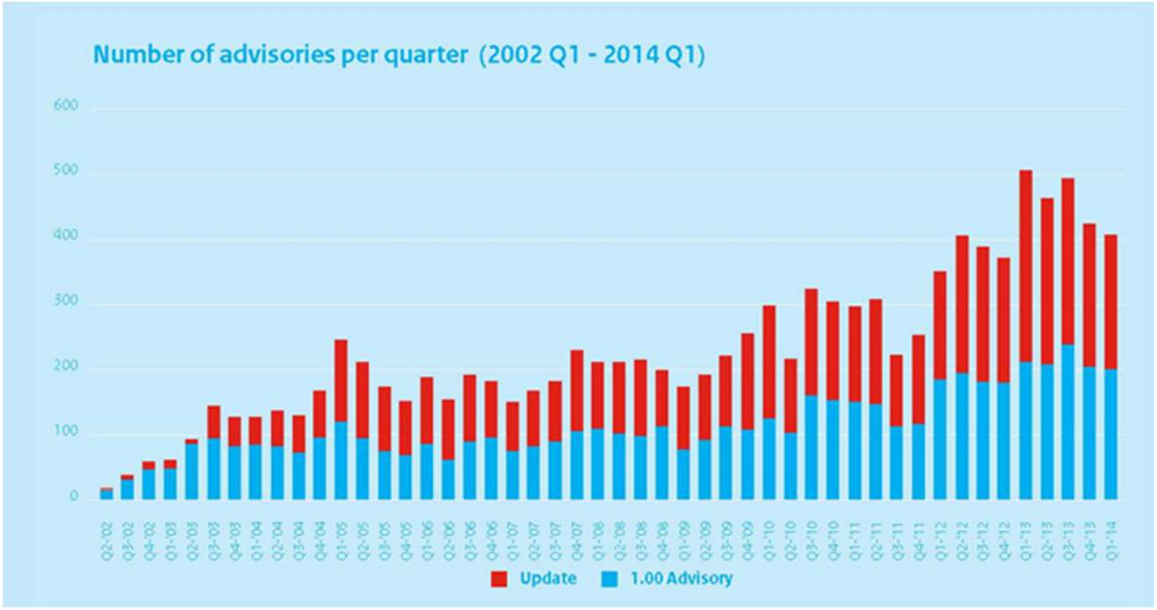
Abbreviations

AMI	Advanced Metering Infrastructure	MITM	Man-In-The-Middle
BDD	Bad Data Detection	PCS	Process Control System
DDOS	Distributed Denial of Service	PLC	Programmable Logic Controller
DNP	Distributed Network Protocol	RT	Real-Time
DOS	Denial Of Service	SCADA	Supervisory Control and Data Acquisition
FDIA	False Data Injection Attack	SE	State Estimation
ICCP	Inter-Control Center Protocol	SG	Smart Grid
ICS	Industrial Control System		
ICT	Information and Communication Technology		
IDS	Intrusion Detection System		
IEC	International Electrotechnical Commission		
IPS	Intrusion Prevention System		
IT	Information Technology		



Realität

- IoT Attacken in 2017: Anstieg um 600% (gegenüber 2016)
- Erwarteter Schaden in 2019: 2 Billionen US Dollar
- Schaden in Deutschland: 2016: 51,6 Mio. €, 2017: 71,8 Mio. €
- Erfasste Cyberkriminalität in Deutschland: 85.960 Fälle in 2017
- Hackerangriffe: alle 39 Sekunden weltweit
- Internetfähige Geräte: 20 Milliarden, steigend



Update = wiederholte gleiche Schwachstelle

Aus: Cyber Security Assessment Netherlands - CSAN-4

Angriff Tools

- Overview of integrated exploits for products in 60 **exploit kits (Hack Tools)**.
- Other sources also report the dominant presence of Java in the exploit market.
- Together with Java, Microsoft Internet Explorer and Adobe Flash and Adobe Reader/Acrobat account for 80 percent of the integrated exploits in exploit kits.

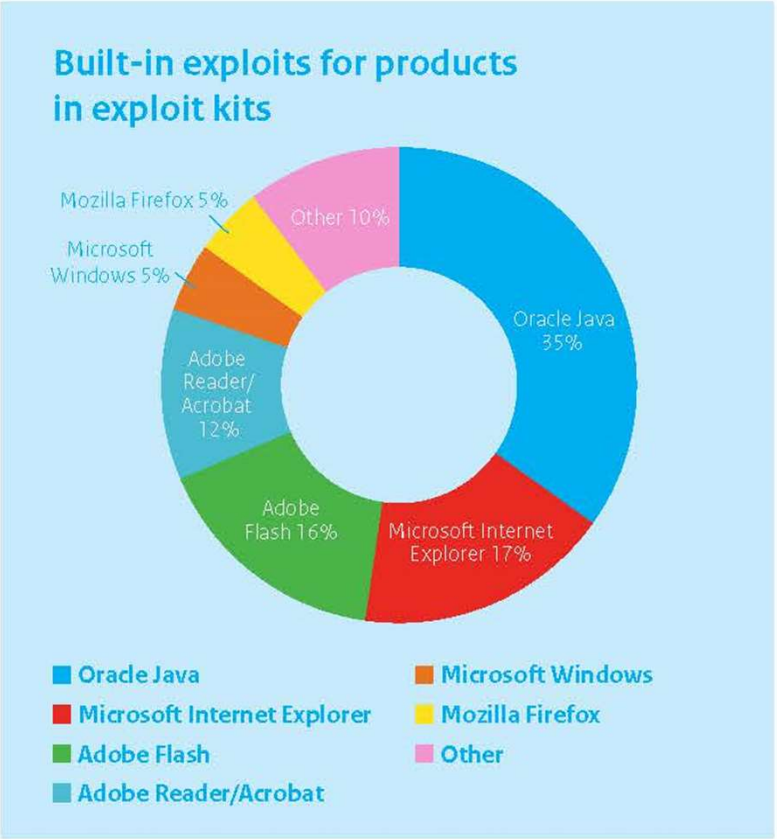


Figure 11. Software abused by exploit kits [71]

Aus: Cyber Security Assessment Netherlands - CSAN-4

DDoS

- 21 October 2016:
  - cyber-attack occurred at Dyn, switch-board operator company as part of the Domain Name System (DNS)
  - many websites were inaccessible
  - reason was a massive Dedicated Denial of Service (DDoS) attack by actors taken control of thousands of internet-enabled devices
  - Attackers took advantage of strategic choices of companies on the hardware side: manufacturers adopted a → speed-to-market strategy rather than a → security-by-design strategy
    → releasing a significant number of vulnerable devices that hackers could co-opt for DDoS attacks

Future of Digital Economy and Society System Initiative, January 2017
Advancing Cyber Resilience Principles and Tools for Boards. In collaboration with The Boston Consulting Group and Hewlett Packard Enterprise

Critical infrastructure

- The protection of cyber assets within the critical infrastructure domain such as oil and gas, power generation and transmission, smart cities and other classifications continue to be a topic of concern for global cybersecurity stakeholders.
- As more critical cyber assets and SCADA systems are interconnected, the concern for human safety remains at the forefront.

- Researchers at the University of Michigan demonstrated how weaknesses in wireless radio communications can be exploited in order to → take control of several traffic lights in an undisclosed Michigan municipality.
- This research highlights the risk associated with the wireless connections and the potential for catastrophic consequences if attackers are able to perform similar feats.

Future of Digital Economy and Society System Initiative, January 2017
Advancing Cyber Resilience Principles and Tools for Boards. In collaboration with The Boston Consulting Group and Hewlett Packard Enterprise

Gefahren für Supply-Chains der Industrie 4.0

- Today, organizations increasingly rely on an array of suppliers to support their critical functions.
- Suppliers have their own suppliers who, in turn, have their own suppliers, creating extended supply chains and entire supply ecosystems.
- All organizations rely on acquiring products and services, and most organizations also supply products and services to other organizations.
- Besides increasingly complex supply chains and cyber threat actors → targeting supplier and acquirer networks, other external events such as severe weather and geopolitical unrest continue to threaten supply chains.
- Together, these threats increase the importance of supply chain resiliency, business continuity, and disaster recovery planning.

Draft NISTIR 8276
Key Practices in Cyber Supply Chain Risk Management:
Observations from Industry

...

Operation ShadowHammer

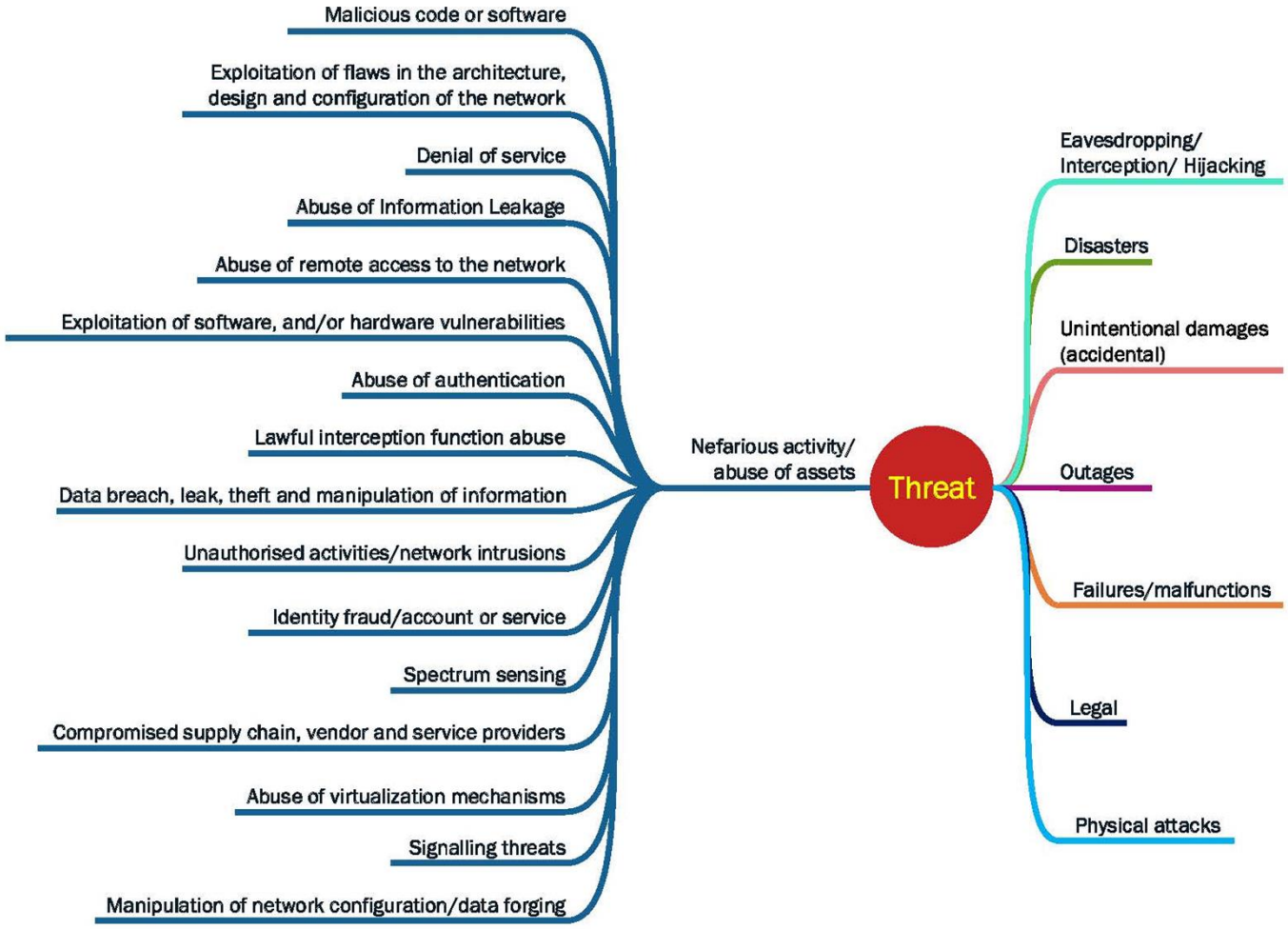
In January 2019, Kaspersky Lab discovered that a server for a live software update tool for users of **ASUS products** had been compromised by attackers and that an estimated 500 000 Windows machines had received a compromised file that effectively acted as a backdoor to the devices for the attackers.

The **malicious file was signed with legitimate ASUS digital certificates** to make it appear to be an authentic software update from the company.

However, the malware was designed to only activate on about 600 unique machines, based on their MAC addresses, indicating that despite the number of affected machines, the attack was extremely targeted.

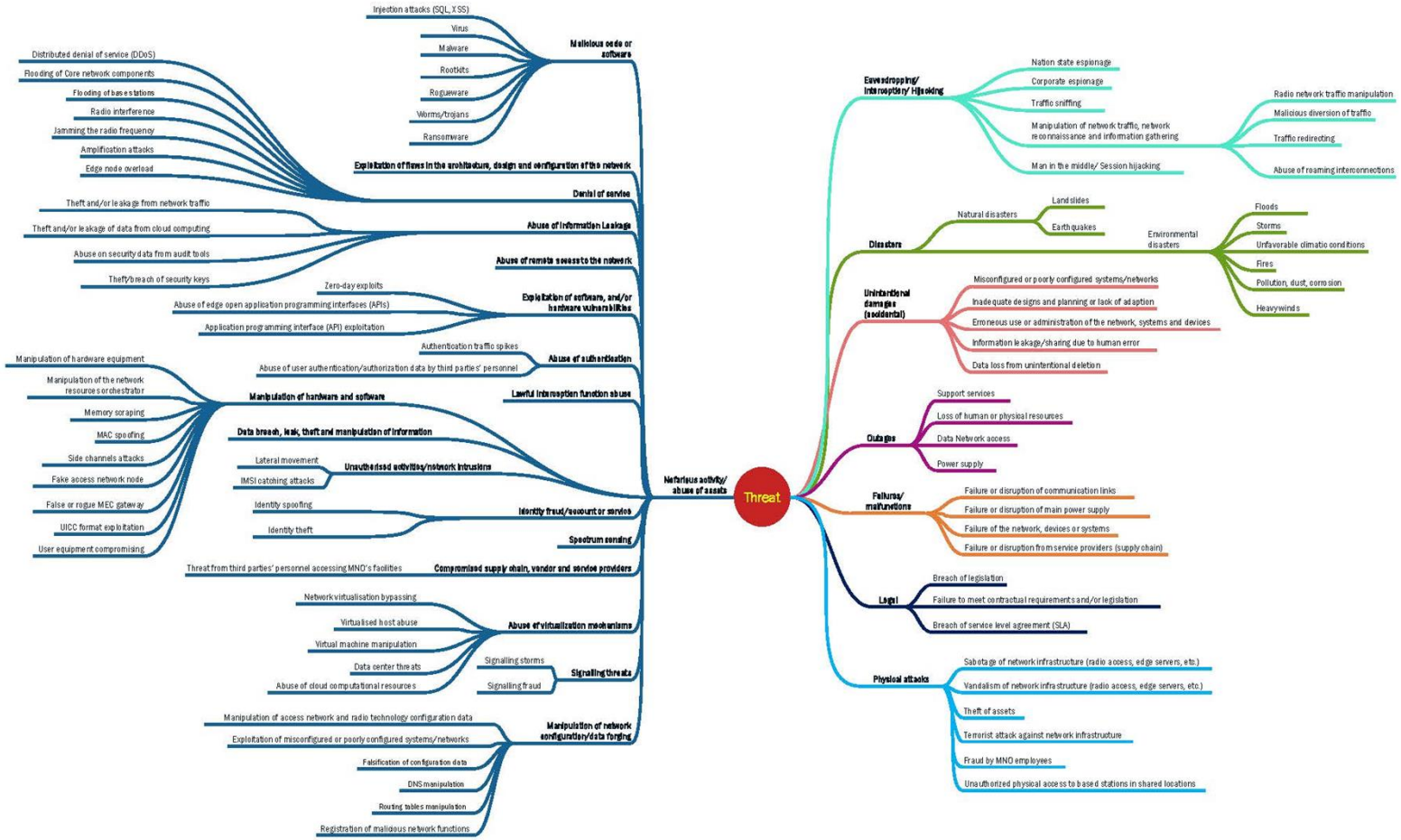
INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2019
09 October 2019, Europol
https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

5G → Threats in der Kommunikation der Zukunft



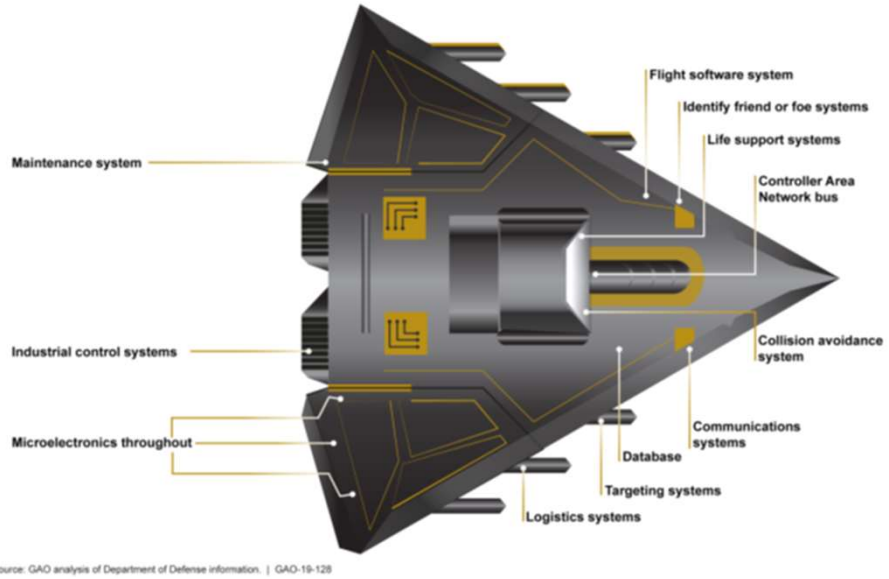
ENISA THREAT LANDSCAPE FOR 5G NETWORKS, November 2019
Threat assessment for the fifth generation of mobile telecommunications networks (5G)

ANNEX B: THREAT TAXONOMY MAP (FULL)



Militärischer Bereich

- DOD weapon systems are more software dependent and more → networked than ever before (see figure).
- DOD routinely found mission-critical → cyber vulnerabilities in systems tha were under development.
- Using relatively simple tools and techniques, testers were able to → take control of systems and largely operate undetected.



- WEAPON SYSTEMS CYBERSECURITY, DOD Just Beginning to Grapple with Scale of Vulnerabilities, Report to the Committee on Armed Services, U.S. Senate, October 2018, GAO-19-128

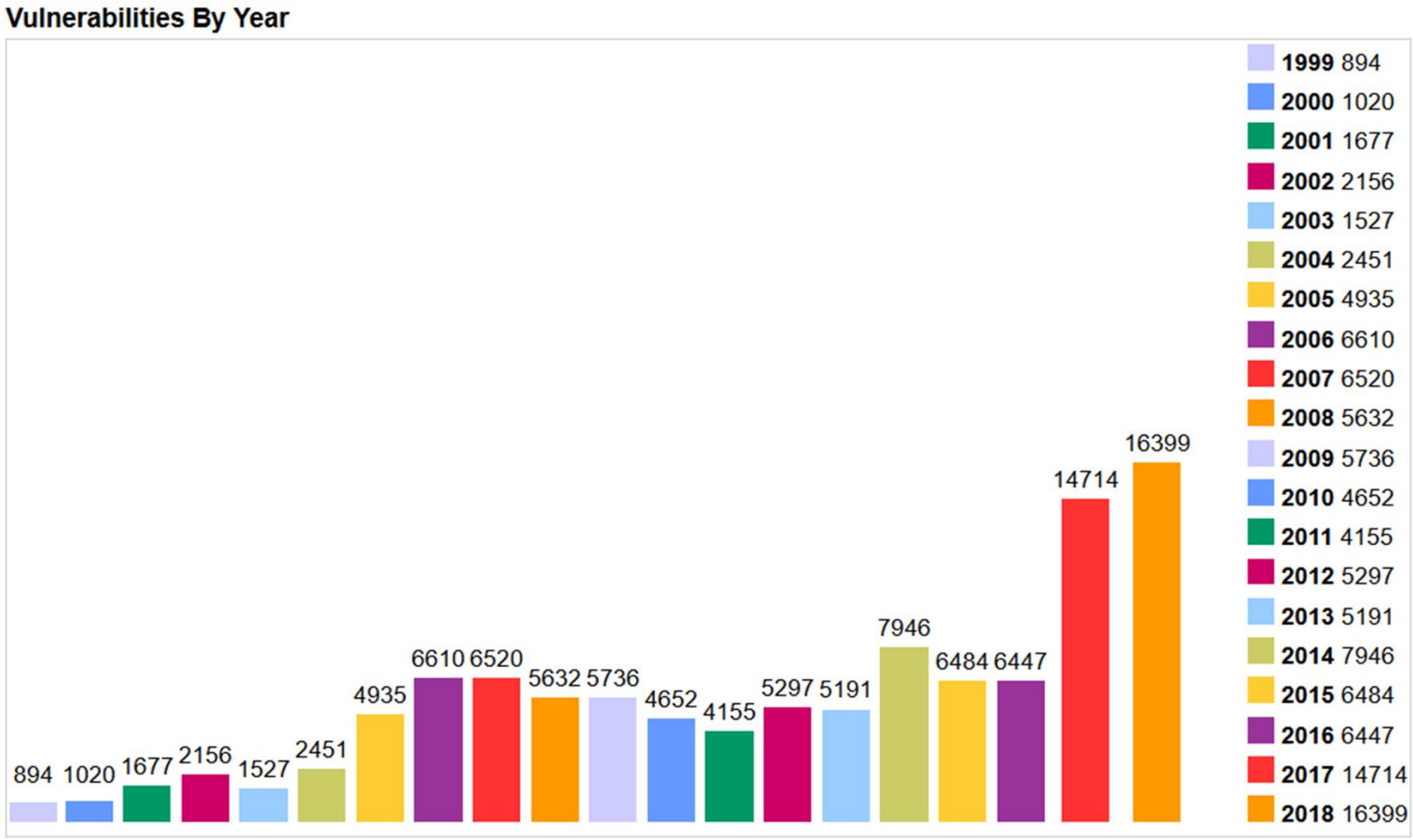
Source of the threat	Targets: Governments	Targets: Private organisations	Targets: Citizens
State actors	Digital Espionage	Digital Espionage	Digital Espionage
	Offensive cyber capabilities	Offensive cyber capabilities	
Terrorists	Disruption of IT/takeover	Disruption of IT/takeover	
Professional criminals	Theft and publication or selling of information ↓	Theft and publication or selling of information	Theft and publication or selling of information ↑
	Manipulation of information ↓	Manipulation of information ↓	Manipulation of information
	Disruption of IT ↑	Disruption of IT ↑	Disruption of IT ★
	IT takeover ↓	IT takeover ↑	IT takeover
Cyber vandals and Scriptkiddies	Information theft ↓	Information theft ↓	Information theft
	Disruption of IT ↓	Disruption of IT	
Hacktivists	Theft and publication of information obtained	Theft and publication of information obtained	Theft and publication of information obtained
	Defacement	Defacement	
	Disruption of IT	Disruption of IT	
	IT takeover ★	IT takeover	
Internal actors	Theft and publication or selling of information	Theft and publication or selling of information	
	Disruption of IT	Disruption of IT	
Cyber researchers	Receiving and publishing information	Receiving and publishing information	
Private organisations		Information theft (industrial espionage) ↓	Commercial use/abuse or 'resale' of information ★
No actor	IT failure	IT failure	IT failure

Angreifer vers Ziele

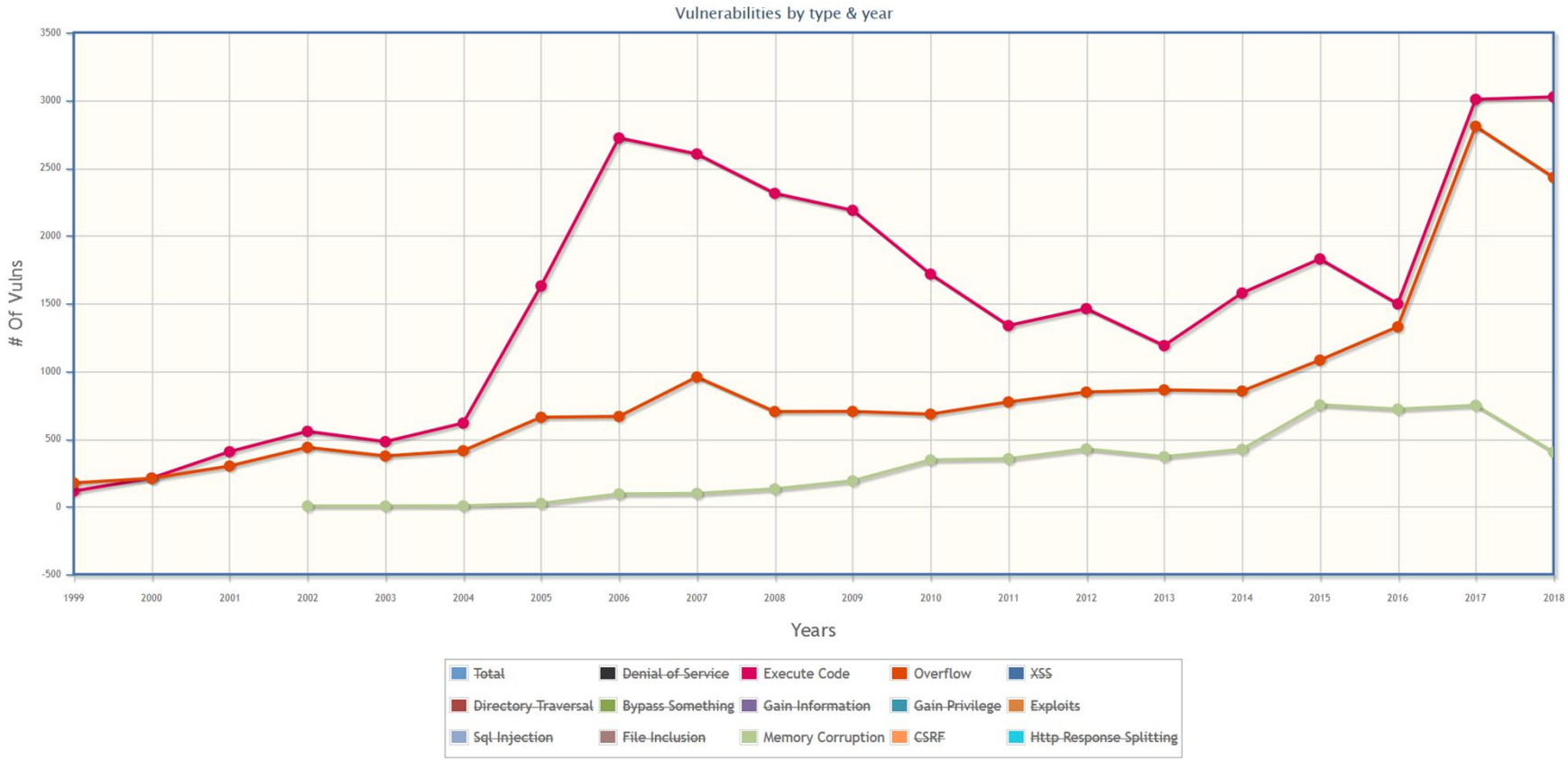
Aus: Cyber Security Assessment Netherlands - CSAN-4

Schwachstellen und Einfallstore

Schwachstellenentwicklung



Index-, Speicher- und Ausführungsschwachstellen

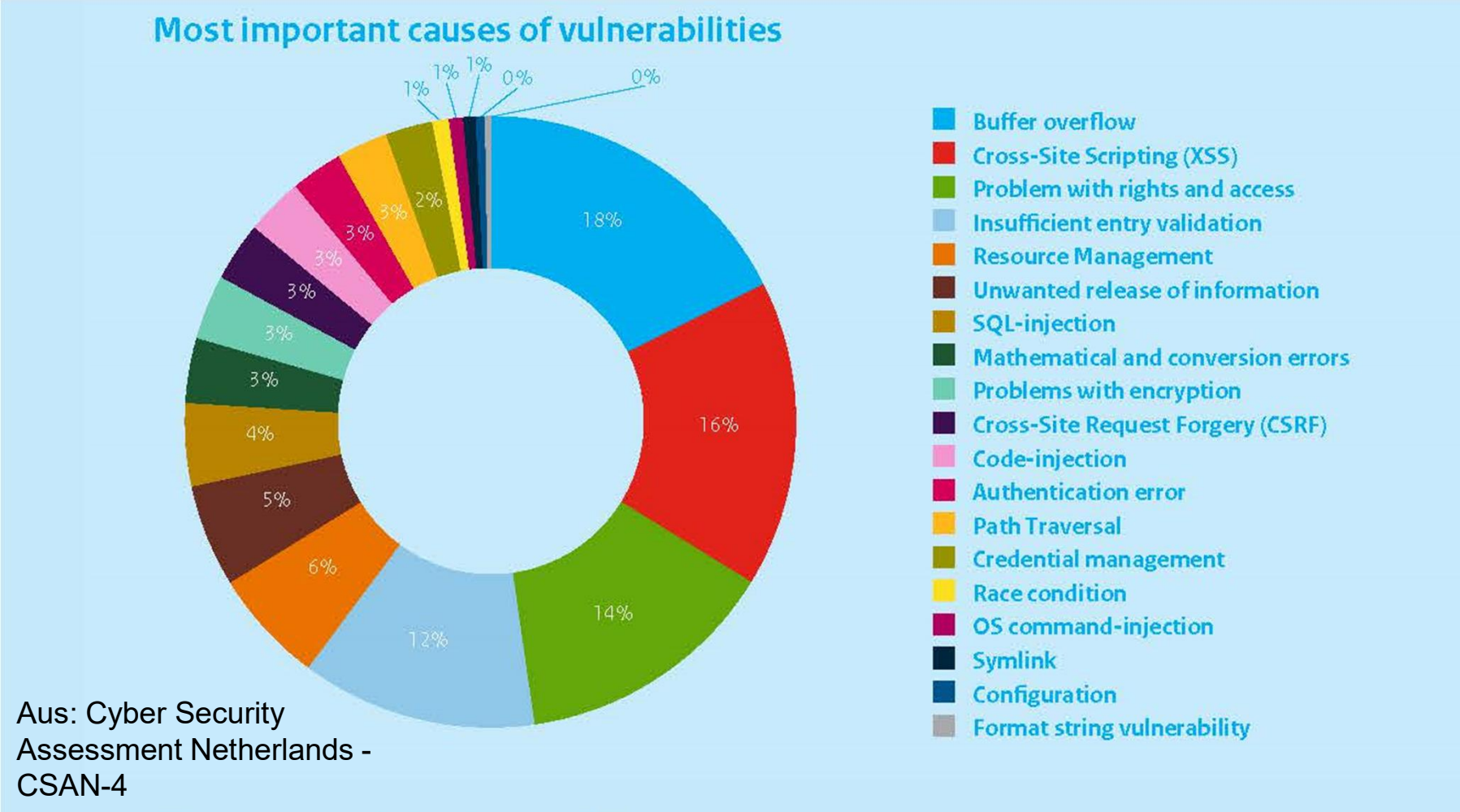


Software Schwachstellen

- Vulnerabilities in software remain the Achilles' heel of cyber Security
- The vulnerability of software and systems → remains relentlessly high. This does not seem to change.
- This is the technical Achilles' heel when it comes to guaranteeing cyber security, certainly where it concerns the popular standard software which is used in many systems.
- At present there is no solution for this issue. More attention for concepts such as security-by-design and secure software development, can possibly restrict the extent of the problem, but error-free software is highly improbable, now and in the future.
- Vulnerabilities in → Java are the most abused.
- Exploit kits → bundle ready-made exploits for vulnerabilities, making it easy to infect large quantities of systems in a short space of time.
- Java is widely used as → embedded software in cars, mobile telephones (also non-smartphones) and television sets.

Aus: Cyber Security Assessment Netherlands - CSAN-4

Ursachen von Schwachstellen



Aus: Cyber Security Assessment Netherlands - CSAN-4

NIST Aussagen zu Java, C, C++

NIST – National Institute of Standards and Technology 2011, Source Code Security Analysis Tool, Functional Specification Version 1.1
(siehe auch: Seacord. R. C. et al.: A Structured Approach to Classifying Security Vulnerabilities. TECHNICAL NOTE, CMU/SEI-2005-TN-003, January 2005)

- "… many software security weaknesses are introduced at the implementation phase …"
- "…identify code weaknesses that significantly affect the security of software applications …"
- **"… C, C++ and Java, because they are the languages in which most of today's vulnerabilities have been identified …"**
- "There are languages that are, by design, more suitable for secure programming. … Such languages entirely preclude many common weaknesses …. Choosing such languages mitigates many security risks." (→ Ada, Rust, Spark)

Remote Desktop Protocols - RDP

- Use of vulnerable RDPs grow (brute force access or buy access on criminal forum)
- May 2019: Microsoft security vulnerability CVE-2019-0708 (BlueKeep)
  - An attacker can exploit this vulnerability by connecting via RDP to the target machine and sending **specifically crafted requests**.
  - This particular vulnerability does → not require either victim interaction nor user authentication, allowing any attacker who succeeds in exploiting the vulnerability to execute arbitrary code on the compromised machine.
  - The exploit works completely filelessly, providing full control of a remote system **without → having to deploy** any malware.
  - In addition, it also does not require an active session on the target.
  - Almost one million devices may be vulnerable to this exploit.

INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2019
09 October 2019, Europol
https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

Cyber Security Architekturen in der Automatisierung

ISA99
jetzt
IEC 62443

Konzept:

Segmentierung des Netzwerks

Einsatz von Secure Router

Einsatz von VPNs

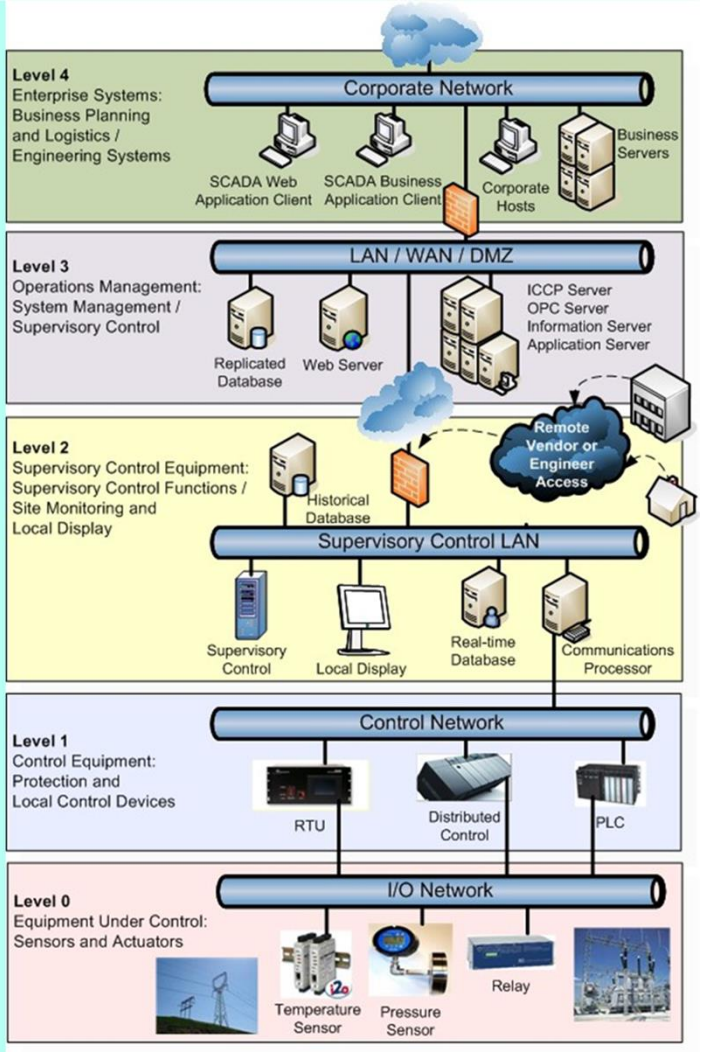
Monitoring-Systeme

Ausreichend?

ISA SCADA architecture (for security)

ISA SCADA architecture by functional-level reference model

International Society of Automation
ISA99 - Industrial Automation and Control Systems Security



Automatisierung als Rückgrat

Advisory (ICSA-18-226-01) - http://ics-cert.us-cert.gov
Siemens SIMATIC STEP 7 and SIMATIC WinCC
Original release date: August 14, 2018

Beispiel SPS Konfiguration

1. EXECUTIVE SUMMARY

- **CVSS v3 8.6**
- **ATTENTION:** Exploitable locally/low skill level to exploit
- **Vendor:** Siemens
- **Equipment:** SIMATIC STEP 7 (TIA Portal) and SIMATIC WinCC (TIA Portal)
- **Vulnerabilities:** Incorrect Default Permissions

2. RISK EVALUATION

Successful exploitation of these vulnerabilities may allow an attacker … to manipulate files and cause a denial-of-service-condition, or **execute code** ….

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

Siemens reports these vulnerabilities affect the following SIMATIC STEP 7 products:
SIMATIC STEP 7 (TIA Portal) and WinCC (TIA Portal) v10, v11, v12: All versions, v13: All versions, v14: All versions < v14 SP1 Update 6, and v15: All versions < v15 Update 2.

3.2 VULNERABILITY OVERVIEW

3.2.1 INCORRECT DEFAULT PERMISSIONS CWE-276

Improper file permissions in the default installation of TIA Portal may allow an attacker … to **insert specially crafted files**, which may prevent TIA Portal startup (denial-of-service) or **lead to local code execution**. **No special privileges are required**, ….
CVE-2018-11453 has been assigned to this vulnerability. A CVSS v3 base **score of 7.8** has been calculated; the CVSS vector string is ….

3.2.2 INCORRECT DEFAULT PERMISSIONS CWE-276

Improper file permissions in the default installation of TIA Portal may allow an attacker with local file system access to **manipulate resources**, which may be transferred to devices and executed there by a different user. **No special privileges are required**, but the victim needs to transfer the manipulated files to a device. Execution is caused on the target device rather than on the PG device.
CVE-2018-11454 has been assigned to this vulnerability. A CVSS v3 base **score of 8.6** has been calculated; the CVSS vector string is …..

3.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Chemical, **Energy**, Food and Agriculture, and Water and Wastewater Systems
- **COUNTRIES/AREAS DEPLOYED:** Worldwide

Siehe: https://ics-cert.us-cert.gov/advisories/ICSA-18-226-01

Unsichere Sicherheitssysteme in der Automatisierung

- **Siemens SIPROTEC 4** and **SIPROTEC Compact** (Update B), 07/27/2017
  Advisory contains mitigation details for **improper input validation**, **missing authorization**, and **improper authentication** vulnerabilities in the Siemens SIPROTEC 4 and SIPROTEC Compact devices.

- **Statement Siemens:**
  Digital transformation will only be successful if we succeed in → ensuring the security of data and networked systems. Digitalization and cybersecurity are two sides of the same coin.

- Handelsblatt:
  Siemens, Daimler, Airbus, Telekom, TÜV: Allianz für Cyber-Sicherheit findet immer mehr Mitglieder
  Hackerangriffe kosten Konzerne jedes Jahr **Milliarden** – und die Risiken steigen weiter.
  Ein Bündnis von 16 Konzernen hat nun Standards für die → Sicherheit in ihren Lieferketten definiert.

Permanenz in Schwachstellen von Routern

Juni 2019

Cisco Releases Security Updates for Multiple Products

Original release date: June 05, 2019

Cisco has released security updates to address vulnerabilities in multiple Cisco products. A remote attacker could exploit some of these vulnerabilities to take control of an affected system.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review the following Cisco advisories and apply the necessary updates:

- Industrial Network Director Remote Code Execution Vulnerability cisco-sa-20190605-ind-rce
- Unified Communications Manager IM&P Service, Cisco TelePresence VCS, and Cisco Expressway Series Denial of Service Vulnerability cisco-sa-20190605-cucm-imp-dos
- Webex Meetings Server Information Disclosure Vulnerability cisco-sa-20190605-webexmeetings-id
- TelePresence Video Communication Server and Cisco Expressway Series Server-Side Request Forgery Vulnerability cisco-sa-20190605-vcs
- Unified Computing System BIOS Signature Bypass Vulnerability cisco-sa-20190605-ucs-biossig-bypass
- IOS XR Software Secure Shell Authentication Vulnerability cisco-sa-20190605-iosxr-ssh
- Industrial Network Director Stored Cross-Site Scripting Vulnerability cisco-sa-20190605-ind-xss
- Industrial Network Director Cross-Site Request Forgery Vulnerability cisco-sa-20190605-ind-csrf
- Enterprise Chat and Email Cross-Site Scripting Vulnerability cisco-sa-20190605-ece-xss

...

Cisco Releases Security Updates for Multiple Products

August 2019

Original release date: August 29, 2019

Cisco has released security updates to address vulnerabilities in multiple Cisco products. **A remote attacker could exploit some of these vulnerabilities to take control of an affected system.**

The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review the following Cisco advisories and apply the necessary updates:

- REST API Container for IOS XE Software Authentication Bypass Vulnerability *cisco-sa-20190828-iosxe-rest-auth-bypass*
- Unified Computing System Fabric Interconnect root Privilege Escalation Vulnerability *cisco-sa-20190828-ucs-privescalation*
- NX-OS Software Remote Management Memory Leak Denial of Service Vulnerability *cisco-sa-20190828-nxos-memleak-dos*
- NX-OS Software IPv6 Denial of Service Vulnerability *cisco-sa-20190828-nxos-ipv6-dos*
- NX-OS Software Cisco Fabric Services over IP Denial of Service Vulnerability *cisco-sa-20190828-nxos-fsip-dos*
- FXOS and NX-OS Software Authenticated Simple Network Management Protocol Denial of Service Vulnerability *cisco-sa-20190828-fxnxos-snmp-dos*
- NX-OS Software SNMP Access Control List Configuration Name Bypass Vulnerability *cisco-sa-20190828-nxos-snmp-bypass*
- NX-OS Software Network Time Protocol Denial of Service Vulnerability *cisco-sa-20190828-nxos-ntp-dos*
- NX-OS Software NX-API Denial of Service Vulnerability *cisco-sa-20190828-nxos-api-dos*
- Nexus 9000 Series Fabric Switches ACI Mode Border Leaf Endpoint Learning Vulnerability *cisco-sa-20190828-nexus-aci-dos*

VPN und virtuelle Maschinen

- Juniper Networks Releases Security Updates
  Original release date: January 09, 2020
  Juniper Networks has released security updates to address → multiple vulnerabilities in various Juniper products. A remote attacker could exploit some of these vulnerabilities to take control of an affected system.

- VMware Releases Security Updates
  Original release date: November 12, 2019
  VMware has released security updates to address vulnerabilities in ESXi, Workstation, and Fusion. An attacker could exploit some of these vulnerabilities to take control of an affected system.

Siemens (→ kleine Liste, nur als Beispiel, gilt analog für andere!)

- ICSA-19-162-01 : Siemens Siveillance VMS
- ICSA-19-162-02 : Siemens SIMATIC Ident MV420 and MV440 Families
- ICSA-19-162-03 : Siemens LOGO!8 Devices
- ICSA-19-134-04 : Siemens LOGO!8 BM
- ICSA-18-317-02 : Siemens S7-400 CPUs (Update A)
- ICSA-19-134-02 : Siemens SIMATIC WinCC and SIMATIC PCS 7
- ICSA-19-134-03 : Siemens LOGO! Soft Comfort
- ICSA-19-134-05 : Siemens SINAMICS PERFECT HARMONY GH180 Drives NXG I and NXG II
- ICSA-19-134-06 : Siemens SINAMICS PERFECT HARMONY GH180 Fieldbus Network
- ICSA-19-134-07 : Siemens SCALANCE W1750D
- ICSA-19-134-09 : Siemens SIMATIC Panels and WinCC (TIA Portal)
- ICSA-19-099-02 : Siemens Spectrum Power 4.7

..2

- ICSA-19-099-01 : Siemens SIMOCODE pro V EIP
- ICSA-19-099-05 : Siemens RUGGEDCOM ROX II
- ICSA-19-099-04 : Siemens SINEMA Remote Connect
- ICSA-17-318-01 : Siemens SCALANCE, SIMATIC, RUGGEDCOM, and SINAMICS Products (Update F)
- ICSA-18-226-02 : Siemens OpenSSL Vulnerability in Industrial Products (Update E)
- ICSA-18-067-01 : Siemens SIPROTEC 4, SIPROTEC Compact, DIGSI 4, and EN100 Ethernet Module (Update C)
- ICSA-18-345-02 : Siemens SINUMERIK Controllers (Update A)
- ICSA-18-025-02B : Siemens Desigo PXC (Update C)
- ICSA-18-088-03 : Siemens SIMATIC PCS 7, SIMATIC WinCC, SIMATIC WinCC Runtime Professional, and SIMATIC NET PC Software (Update G)
- ICSA-18-317-05 : Siemens SIMATIC S7 (Update A)

..3

- ICSA-17-129-01 : Siemens devices using the PROFINET Discovery and Configuration Protocol (Update K)
- ICSA-18-023-02 : Siemens Industrial Products (Update A)
- ICSA-18-067-02 : Siemens SIPROTEC 4, SIPROTEC Compact, and Reyrolle Devices using the EN100 Ethernet Communication Module Extension (Update B)
- ICSA-18-282-05 : Siemens SIMATIC S7-1500, SIMATIC S7-1500 Software Controller and SIMATIC ET 200SP OpenController (Update A)
- ICSA-18-347-02 : Siemens EN100 Ethernet Communication Module and SIPROTEC 5 Relays (Update A)
- ICSA-19-043-02 : Siemens EN100 Ethernet Communication Module and SIPROTEC 5 Relays
- ICSA-19-043-04 : Siemens SIMATIC S7-300 CPU
- ICSA-19-043-05 : Siemens Intel Active Management Technology of SIMATIC IPCs

..4

- ICSA-19-038-01 : Siemens SICAM A8000 RTU Series
- ICSA-19-038-02 : Siemens EN100 Ethernet Module
- ICSA-19-036-04 : Siemens SIMATIC S7-1500 CPU
- ICSA-17-243-01 : Siemens Discovery Service of OPC UA Protocol (Update C)
- ICSA-18-352-05 : Siemens TIM 1531 IRC Modules
- ICSA-18-317-01 : Siemens IEC 61850 System Configurator, DIGSI 5, DIGSI 4, SICAM PAS/PQS, SICAM PQ Analyzer, and SICAM SCC
- ICSA-18-317-03 : Siemens SIMATIC Panels and SIMATIC WinCC (TIA Portal)
- ICSA-18-317-04 : Siemens SCALANCE S
- ICSA-18-317-06 : Siemens SIMATIC STEP 7 (TIA Portal)
- ICSA-18-317-07 : Siemens SIMATIC IT Production Suite
- ICSA-18-317-08 : Siemens SIMATIC Panels
- ICSA-18-282-02 : Siemens SCALANCE W1750D

..5

- ICSA-18-282-03 : Siemens ROX II
- ICSA-18-282-04 : Siemens SIMATIC S7-1200 CPU Family Version 4
- ICSA-18-226-01 : Siemens SIMATIC STEP 7 and SIMATIC WinCC (Update A)
- ICSA-18-128-01 : Siemens Medium Voltage SINAMICS Products (Update A)
- ICSA-18-109-01 : Siemens SIMATIC WinCC OA Operator IOS App (Update A)
- ICSA-18-137-03 : Siemens SIMATIC S7-400 CPU (Update A)
- ICSA-18-254-03 : Siemens TD Keypad Designer
- ICSA-18-254-04 : Siemens SIMATIC WinCC OA
- ICSA-18-254-05 : Siemens SCALANCE X Switches
- ICSA-14-035-01 : Siemens SIMATIC WinCC OA Multiple Vulnerabilities
- ICSA-11-361-01 : Siemens Automation License Manager Vulnerabilities
- ICSA-12-030-01A : Siemens SIMATIC WinCC Vulnerabilities (UPDATE A)

..6

- ICSA-14-073-01 : Siemens SIMATIC S7-1500 CPU Firmware Vulnerabilities
- ICSA-14-079-01 : Siemens SIMATIC S7-1200 Improper Input Validation Vulnerabilities
- ICSA-14-098-03 : Siemens Ruggedcom WIN Products BEAST Attack Vulnerability
- ICSA-14-107-01 : Siemens SINEMA Vulnerabilities
- ICSA-14-114-02 : Siemens SIMATIC S7-1200 CPU Web Vulnerabilities
- ICSA-11-091-01A : Siemens Tecnomatix FactoryLink Vulnerabilities (Update A)
- ICSA-14-105-03B : Siemens Industrial Products OpenSSL Heartbleed Vulnerability (Update B)
- ICSA-14-051-03B : Siemens RuggedCom Uncontrolled Resource Consumption Vulnerability (Update B)
- ICSA-14-087-01A : Siemens ROS Improper Input Validation (Update A)
- ICSA-11-223-01A : Siemens SIMATIC PLCs Reported Issues Summary (Update A)

..7

- ICSA-14-205-02A : Siemens SIMATIC WinCC Vulnerabilities (Update A)
- ICSA-14-135-03A : Siemens RuggedCom ROX-based Devices Certificate Verification Vulnerability (Update A)
- ICSA-13-338-01 : Siemens SINAMICS S/G Authentication Bypass Vulnerability
- ICSA-15-013-01 : Siemens SIMATIC WinCC Sm@rtClient iOS Application Authentication Vulnerabilities
- ICSA-15-020-01 : Siemens SCALANCE X-300/X408 Switch Family DOS Vulnerabilities
- ICSA-15-022-01 : Siemens SIMATIC S7-1200 CPU Web Vulnerability
- ICSA-15-034-01 : Siemens SCALANCE X-200IRT Switch Family User Impersonation Vulnerability
- ICSA-15-034-02 : Siemens Ruggedcom WIN Vulnerability
- ICSA-14-329-02D : Siemens SIMATIC WinCC, PCS7, and TIA Portal Vulnerabilities (Update D)

..8

- ICSA-14-198-03G : Siemens OpenSSL Vulnerabilities (Update G)
- ICSA-15-048-02 : Siemens SIMATIC WinCC TIA Portal Vulnerabilities
- ICSA-15-048-01 : Siemens SIMATIC STEP 7 TIA Portal Vulnerabilities
- ICSA-13-347-01 : Siemens COMOS Privilege Escalation
- ICSA-13-254-01 : Siemens SCALANCE X-200 Web Hijack Vulnerability
- ICSA-15-064-05 : Siemens SPCanywhere App Vulnerabilities
- ICSA-15-064-03 : Siemens SPC Controller Series Denial-of-Service Vulnerability
- ICSA-15-064-02A : Siemens SIMATIC ProSave, SIMATIC CFC, SIMATIC STEP 7, SIMOTION Scout, and STARTER Insufficiently Qualified Paths (Update A)
- ICSA-15-064-01A : Siemens SIMATIC HMI Basic, SINUMERIK, and Ruggedcom APE GHOST Vulnerability (Update A)
- ICSA-15-176-01 : Siemens Climatix BACnet/IP Communication Module Cross-site Scripting Vulnerability

..9

- ICSA-15-195-01 : Siemens SICAM MIC Authentication Bypass Vulnerability
- ICSA-15-202-02 : Siemens Sm@rtClient Password Storage Vulnerability
- ICSA-15-202-01 : Siemens SIPROTEC Denial-of-Service Vulnerability
- ICSA-15-050-01A : Siemens SIMATIC STEP 7 TIA Portal Vulnerabilities (Update A)
- ICSA-15-239-02 : Siemens SIMATIC S7-1200 CSRF Vulnerability
- ICSA-15-244-01 : Siemens RUGGEDCOM ROS IP Forwarding Vulnerability
- ICSA-12-305-01 : Siemens SiPass Server Buffer Overflow
- ICSA-15-099-01E : Siemens SIMATIC HMI Devices Vulnerabilities (Update E)
- ICSA-15-300-01 : Siemens RuggedCom Improper Ethernet Frame Padding Vulnerability
- ICSA-15-202-03B : Siemens RUGGEDCOM ROS and ROX-based Devices TLS POODLE Vulnerability (Update B)

..10

- ICSA-15-356-01 : Siemens RUGGEDCOM ROX-based Devices NTP Vulnerabilities
- ICSA-11-244-01 : Siemens WinCC Flexible Runtime Heap Overflow
- ICSA-16-019-01 : Siemens OZW672 and OZW772 XSS Vulnerability
- ICSA-16-040-02 : Siemens SIMATIC S7-1500 CPU Vulnerabilities
- ICSA-16-075-01 : Siemens SIMATIC S7-1200 CPU Protection Mechanism Failure
- ICSA-16-103-02 : Siemens SCALANCE S613 Denial-of-Service Vulnerability

Informatik Erkenntnisse aus den Jahren 1970 und folgende

Historie

- Ab 1955: Realisierung kleinster und kleiner Programme (elementare Algorithmen) auf noch wenig leistungsfähigen Rechnern
- Die Programme waren leicht überblickbar, die Problemstellung elementar.
- Leistungsfähigere Prozessoren für größere Problemstellungen und Programme ohne Ingenieur-mäßiges Vorgehen
- Charakteristika:
  vieler Sprachen, je nach Problem bzw. Teilproblem,
  Projekte nicht systematisiert (kein Phasenzyklus),
  Struktur der Programme ergab sich irgendwie,
  Implementierung war höchst individuell und extrem optimiert
- Algorithmus nicht mehr erkennbar,
- Keine Dokumentation

… Historie

- Kollaps der Programmerstellung war vorprogrammiert
- die Kosten im laufenden Betrieb für die Behebung von Fehlern oder die Anpassung an geänderte Anforderungen waren enorm
- Wartbarkeit und Wiederverwendbarkeit von Programmen oder -Teilen war nicht möglich
- Fehlerbehebung produzierte selbst wieder Fehler
- Teilweise wurde auf die Behebung von Fehlern verzichtet, da ein erkannter Fehler besser beherrschbar war, als die durch die Behebung entstehenden neuen Fehler

- Software Krise um ca. 1972

Stand der Informatik

Security Schwachstellen sind überwiegend Implementierungsschwachstellen (You2003)

Schwachstellen betreffen Anwendungssysteme, Betriebssysteme und Security-Infrastruktursysteme wie Security-Router, virtuelle Maschinen etc.

Zuverlässigkeit als durchgehende (ausschließliche) Erbringung der spezifizierten Funktion über einen definierten Zeitraum.

„Funktion" der Mathematik

x→f→y

x ∈ D, y ∈ W
Bildmenge D
Wertemenge W

D ⊂ G, W ⊂ Z
G, Z = ℜ

Funktion f ist **auf D definiert** und **bildet** Bildmenge D **in Wertemenge W** ab

„Funktion" der Informatik

x→f→y
x ∈ D, y ∈ W

x'→f→error
D' = G \ D, W' = Z \ W = error

D ⊂ G, W ⊂ Z
D' = G \ D, W' = Z \ W = error
G, Z = ℜ

Algorithmus f berechnet für jede **Eingabe aus D** die **Ausgabe aus W**.
Für jeden **Wert außerhalb von D** erfolgt **Fehlermeldung (Ausschließlichkeit)!!!**

Stand der Programmierung

„Funktion“ als Ergebnis der Programmierung

x→f→y
x ∈ D, y ∈ W
D ⊂ G, W ⊂ Z

x‘→f→ „undefined behaviour“
D‘ = G \ D
W‘ = Z \ W
G, Z = ℜ

x‘→f→ „undefined behaviour“

D‘ = G \ D = „handcrafted“
W‘ = Z \ W = „gain administrator privileges“

Programm liefert für jede Eingabe aus D korrekte Werte.
Für jeden Wert außerhalb von D erfolgt Stack/Buffer Overflow,
Rücksprungadresse wird überschrieben,
Unbekannter Code ausgeführt und
Der Angreifer erhält Administratorrechte.

Vulnerability :=
Schwachstelle in Programmen, die es einem Angreifer erlauben, durch spezielle Bitmuster die Ausführung von nicht vorgesehenem Code initiieren. Ursache ist die nicht typstrenge Prüfung von Kommandos und Daten und nachfolgend Programmmanipulation.

(siehe: ISO/IEC TR 24772: Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use)

Unsafe programming languages

- One bug affects iPhones, another affects Windows, and the third affects servers running Linux
- At first glance these might → seem unrelated, but in reality all three were made possible because the software that was being exploited was written in programming languages which allow a category of errors called → memory unsafety
- By allowing these types of vulnerabilities, languages such as C and C++ have facilitated a nearly **unending stream** of critical computer security vulnerabilities for years.
- Imagine you had a program with a list of 10 numbers. What should happen if you asked the list for its 11th element?
- …

...

- Most of us would say an error of some sort should occur, and in a memory safe programming language (for example, Python or Java) that's what would happen.
- In a memory unsafe programming language, it'll look at wherever in memory the 11th element would be (if it existed) and try to access it.
- Sometimes this will result in a crash, but in many cases you get whatever happens to be at that location in memory, even if that portion of memory has nothing to do with our list.
- This type of vulnerability is called a → buffer-overflow, and it's one of the most common types of memory unsafety vulnerabilities.
- HeartBleed, which impacted 17 percent of the secure web servers on the internet, was a buffer-overflow exploit, letting you read 60 kilobytes past the end of a list, including → passwords and other users' data.

The Internet Has a Huge C/C++ Problem and Developers Don't Want to Deal With It.
What do Heartbleed, WannaCry, and million dollar iPhone bugs have in common?
by Alex Gaynor
Nov 15 2018
https://www.vice.com/en_us/contributor/alex-gaynor

Entwicklungen anhand ausgewählter Beispiele

USA – Secure Coding

Robert Seacord, https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices

- **Validate input**. Validate input from all untrusted data sources. Proper input validation can eliminate the vast majority of software vulnerabilities.
- Heed compiler warnings. Compile code using the highest warning level available for your compiler and eliminate warnings by modifying the code [C MSC00-A, C++ MSC00-A]. Use static and dynamic **analysis tools** to detect and eliminate additional security flaws.
- Architect and **design** for security policies. Create a software architecture and design your software to implement and enforce security policies.
- Keep it **simple**. Keep the design as simple and small as possible. Complex designs increase the likelihood that errors will be made in their implementation, configuration, and use.
- **Default deny**. Base access decisions on permission rather than exclusion. This means that, by default, access is denied.
- Adhere to the principle of **least privilege**. Every process should execute with the the least set of privileges necessary to complete the job.
- **Sanitize data** sent to other systems. Sanitize all data passed. Attackers may be able to invoke unused functionality in these components through the use of SQL, command, or other injection attacks. Because the calling process understands the context, it is responsible for sanitizing the data before invoking the subsystem.

Informatik: Safe Programming Language Ada

- Ada is an unusual language because it was developed in response to a detailed set of requirements.
- In the early 1970s no suitable language was found to fulfill these requirements.
- A competition was then created for companies to create a language meeting the government requirements: Readability, Efficiency, Provability, Expressiveness
- Winner was a team from France lead by Jean Ichbiah.
- Ada achieved ANSI standardization in 1980, and ISO standardization in 1983.

- Modular and strongly Typed Language:
  Jede Variable hat einen statisch zugewiesenen Typ mit allen (!) Informationen zur Übersetzungszeit (!) und ist damit durch den Compiler prüfbar.

  Zur Laufzeit warden neu zugewiesene Werte automatisch auf Typkorrektheit geprüft.

Es gibt
- keinen falschen Index
- keinen Buffer Overflow
- usw.

John Barnes
Safe and Secure Software - An Invitation to Ada 2012

Roderick Chapman & Yannick Moy
AdaCore Technologies for Cyber Security

Ada

- Die Sprachziele von Ada waren:
  - Unterstützung der Zuverlässigkeit und Wartbarkeit von Programmen,
  - Berücksichtigung des Programmierens als menschliche Tätigkeit (Teamarbeit) und
  - Sicherstellung der Effizienz der Programme
- Lesbarkeit von Programmen hat Vorrang vor einfachen Schreibweise

- Variable müssen explizit mit ihrem Typ deklariert werden, Typ einer Variable ist fest
  - Übersetzer kann falsche Verwendung zur Übersetzungszeit feststellen
  - Laufzeitsystem ebenso bei dynamischer Zuweisung (Array mit Indexgrenzen!)
- Ada betrachtet Variablen und Typen mit mathematischer Präzision

Normen - Konstruktive Security nach der NE153

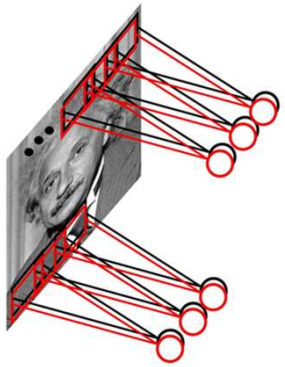
- Im Kern lassen sich diese Anforderungen darauf zusammenfassen, dass IT–Security Konzepte und Funktionen ein integraler Bestandteil der Anforderungsprofile sind und damit auch zum integralen Funktionsumfang automationstechnischer Komponenten und Lösungen gehören.
- Secure by Default
- Secure by Design
- Secure by Implementation
- Secure in Deployment

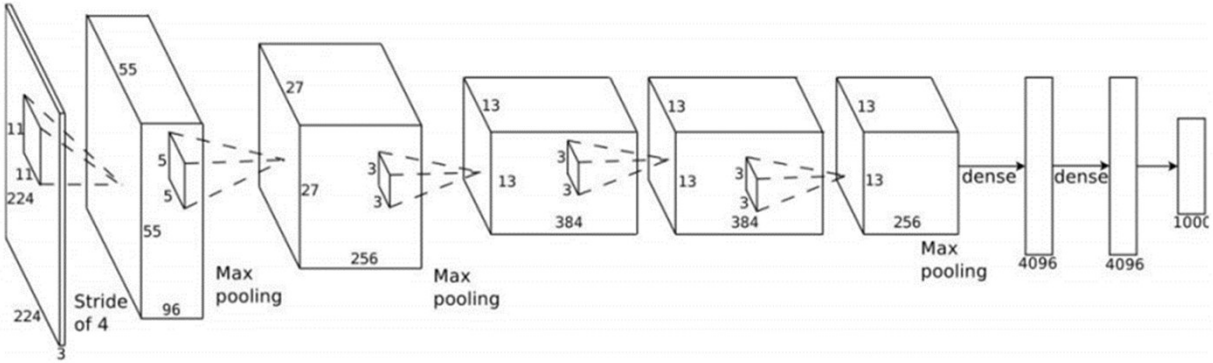
- Normen sind deskriptiv – nicht konstruktiv (vgl. Orientierungsleitfaden für Hersteller zur IEC 62443, ZVEI)
- Security Normen nehmen Wahrscheinlichkeiten an, die nicht existieren
- Normen sind z.B. IEC 62443 (ISA99), ISO 27001
- Richtlinien wie BSI, NIST, EU Direktiven etc.

- KI in der Cyber Security
  - Analyse und Lernen von Normalverhalten
  - Analyse und Erkennung von Anomalien
    (NISTIR Report 8219, Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection)
  - Bitstring / symbolische Elemene zur statischen Analyse
  - Klassifikation im Zugang (Security)
  - Intelligente Hackertools
  - …
- Cyber Security von KI
  - Manipulierbarkeit von KI Verfahren
  - Datenmanipulation (Bilder, Werte, Fake News, …)
  - Fehlleitung von Bilderkennung im autonomen Fahren (siehe Bildverstehen)
  - Provokation falscher Klassifikationen, Handlungsableitungen
  - …

Update in Deep Learning für Autonomous Automotive

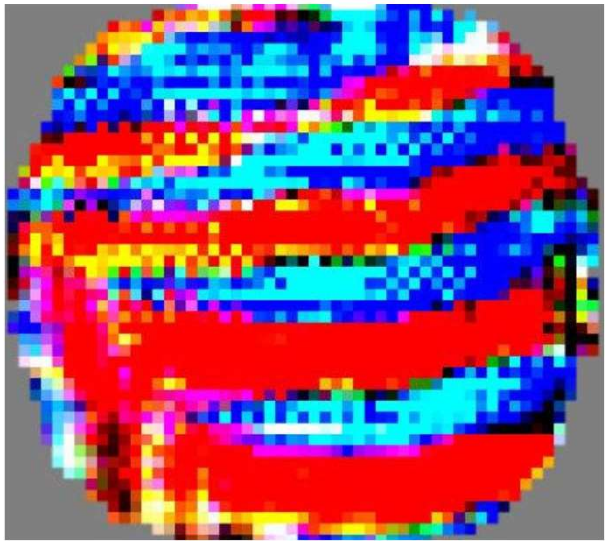
- Deep Learning setzt Rosenblatts Perceptron auf einen neuen Level
- Bildanalysen über neuronale Netze mit vielen Hidden Layern und lokaler Zuständigkeit mit Faltungen (Filter)
- Ziel ist Eigenschaftselemente (**Feature**) von Bildern zu extrahieren, daraus **Objektteile** zusammen zu führen und dann **Objekte** im Bild zu erkennen
- Kann auch für Verhaltensmodellierung eingesetzt werden
- Einsatz für Bildverstehen im autonomen Fahrzeug
- Anwendbar bei definierten Kontexten → Paketverteilanlage
- Komplexe Kontexte → Fahrzeugumfeld → Robustheit kritisch!

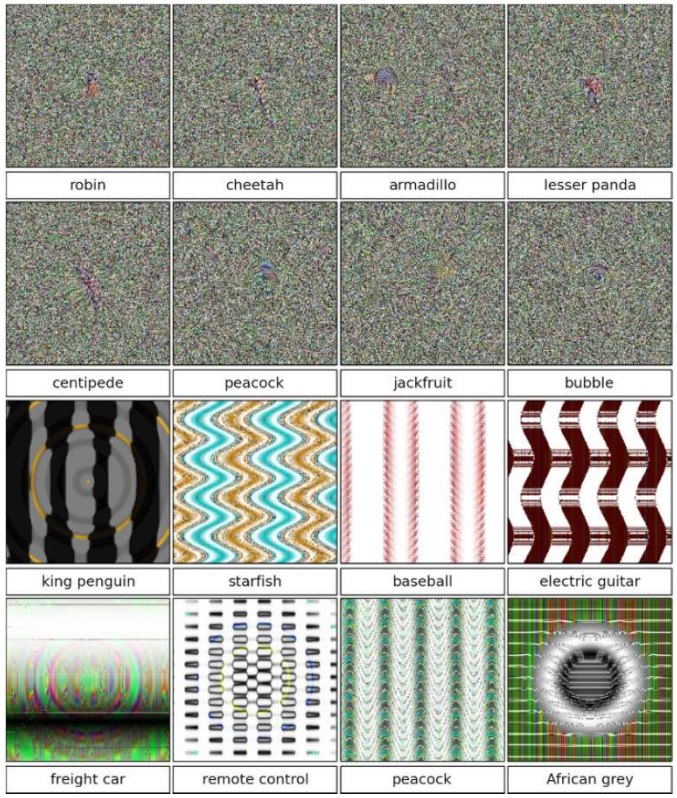


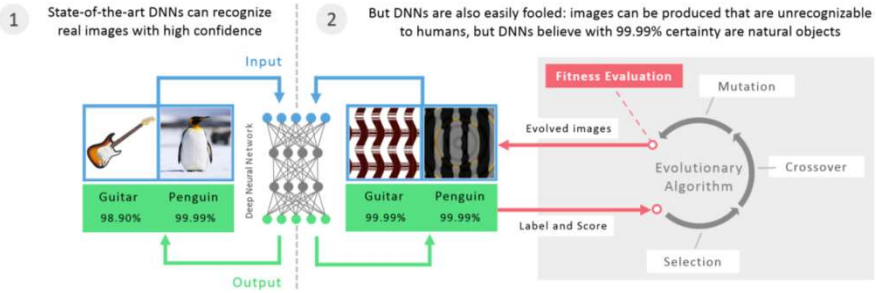


Autonome Fahrzeuge und Sticker

Farbmuster MPI Tübingen, aus: Attacking Optical Flow
Anurag Ranjan, Joel Janai, Andreas Geiger, Michael J. Black
(Max Planck Institute for Intelligent Systems bzw. University of Tübingen)







Nguyen A, Yosinski J, Clune J. Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images. In Computer Vision and Pattern Recognition (CVPR '15), IEEE, 2015.

Stakeholder für die Entwicklung sicherer Systeme

USA

- US CERT
- ICS VERT

- NIST
- Homeland Security

- SWE CMU

- General Electric
  Lässt für deutsches Betriebssystemkern L4 Security Features einbauen!

Niederlande

National Cyber Security Centre

- The National Cyber Security Centre (NCSC), in collaboration with the business community, government bodies and scientists, is working to increase the ability of Dutch society to defend itself in the digital domain.
- The NCSC supports the central government and organisations in fulfilling an essential function for society by providing expertise and advice, response to threats and enhancing crisis management.
- In addition, the NCSC provides information and advice to citizens, the government and the business community relating to awareness and prevention.
- This means that the NCSC constitutes the central reporting and information point for IT threats and security incidents.
- The NCSC is part of the Cyber Security Department of the National Coordinator for Security and Counterterrorism [Nationaal Coördinator Terrorismebestrijding en Veiligheid] (NCTV).

Deutschland?

- BSI
  … soll Schutz bieten, aber gleichzeitig Angriffsoptionen erarbeiten
  (IT-Sicherheitsgesetz 2.0 → Stellungnahme der FG Ada vom 22.5.2019)
  … ICS Richtlinie ohne Implementierungsvorgaben
- Politik
  … keine Ahnung, weiß aber alles

- Gremien
  … VDI, VDE ITG, ZVEI, …
  … alle separat aktiv
- (Automatisierungs-) Industrie
  … Schwachstellen in Serie ohne Ende
- Wissenschaft
  … Wissen, aber keine Ahnung von Realität
  … gut in Akquise von Drittmittel (Problem-Persistenz förderlich)

IT-Sicherheitsgesetz 2.0

Stellungnahme der Gesellschaft für Informatik - Fachgruppe ADA – Zuverlässige Software-Systeme

→ **Mangel an Gewaltenteilung** beim Thema IT Sicherheit → Aufteilung der Verantwortung in voneinander gänzlich unabhängige Entitäten

1. **Hersteller** (Beispiele aus der Luftfahrt: Airbus, Boeing):
- stellen Produkte her, die Sicherheitskriterien erfüllen sollen
- Produkte müssen Sicherheitsstandards genügen und sich einer Zulassung unterziehen

2. **Zulassungsbehörde** (Beispiele aus der Luftfahrt: Luftfahrt-Bundesamt LBA, FAA):
- definiert Standards für Sicherheitszertifikat oder Gebrauchszulassung
- akkreditiert die unabhängigen Gutachter/Testlabore
- Gutachter dürfen in keinem Abhängigkeitsverhältnis stehen

3. **Organisation für die Untersuchung** von IT Sicherheitsvorfällen (Beispiele aus der Luftfahrt: Bundesstelle für Flugunfalluntersuchung BFU, NTSB):
- führt Buch über alle entdeckten IT Sicherheitsvorfälle
- veröffentlicht diese nach gesetzlich zu definierender Vorgabe
- untersucht die Ursachen dieser Vorfälle zur Aufdeckung von Schwächen
- kann Empfehlungen für die Änderung der Standards und Vorschriften ableiten
- ist gänzlich unabhängig von Hersteller und Zulassungsbehörde
- technische Untersuchung soll Erkenntnisse gewinnen, um künftige Vorfälle und Störungen zu vermeiden

Die IT Sicherheitsstandards können gemeinsam von allen interessierten Seiten entwickelt und nach öffentlicher Diskussion als anzuwendende Standards verabschiedet werden.

Resümee

Lessons learned –
PISEA Ergebnis in Safety und IT-Security

(PISEA - Programme for International Science and Engineering Assessment)

- Science and Engineering - Lessons learned:
  … Drittmittelorientiert
  … Industrieorientiert - selling current products
  … Auslieferungsorientiert - time to market
  … Preis orientiert - reducing costs
  … alte Software mit alten Schwächen, neue ebenso (C, C++, …)
  … Ignoranz ohne Ende – Stempel reicht
  … keine Ahnung
- Und nun?
  Berliner Gesamtkonferenz der Sicherheitsinstitutionen als transparente öffentliche Veranstaltung sichern und intensivieren

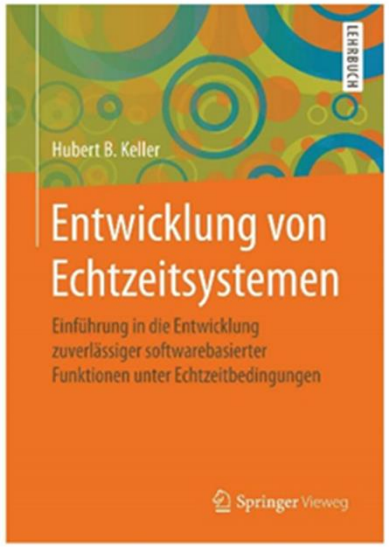
  Unabhängige Experten in einer unabhängigen Institution

  → Deutsche Gesellschaft für Technik und Sicherheit etablieren

Springer

springer.com

Karlsruher Institut für Technologie



1. Aufl. 2019, XIX, 287 S. 184 Abb., 130 Abb. in Farbe.

Gedrucktes Buch
Softcover
[1]32,99 € (D) | 33,92 € (A) | CHF 36,50

eBook
[2]24,99 € (D) | 24,99 € (A) | CHF 29,00

Erhältlich bei Ihrer Bibliothek oder springer.com/shop

Hubert B. Keller

Entwicklung von Echtzeitsystemen

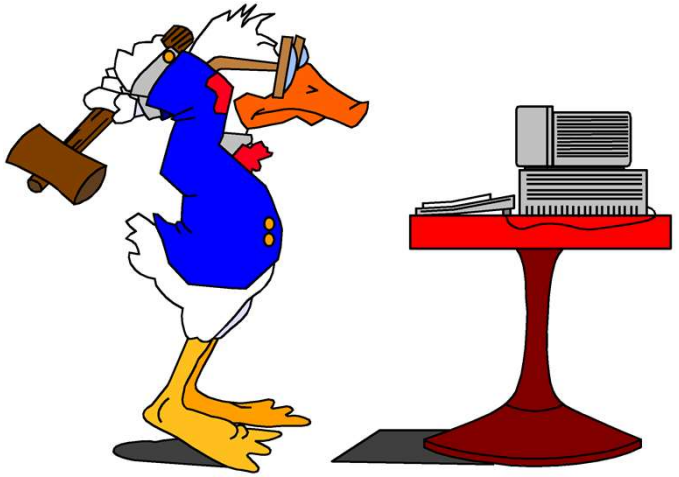
Einführung in die Entwicklung zuverlässiger softwarebasierter Funktionen unter Echtzeitbedingungen

- Entwickeln Sie zuverlässige Realzeitsysteme auf Basis konstruktiver Ansätze
- Klare Darstellung der Anforderungen an Echtzeitsysteme
- Effektive Lösungen für Multitasking mit Zugriffssynchronisation für gemeinsame Daten

Ein hilfreicher Wegweiser zur Entwicklung von Echtzeitsystemen Dieses Buch führt Sie umfassend in die Entwicklung zuverlässiger softwarebasierter Echtzeitsysteme ein. Dazu beleuchtet der Autor Hubert B. Keller alle Entwicklungsaspekte dieser Systeme, nämlich: · Die wichtige Rolle von Automatisierungssoftware · Software-Engineering · Safety- und Security-Aspekte · Scheduling · Implementierung Eignen Sie sich mit diesem Werk konstruktive Ansätze an und erfahren Sie, welche Anforderungen eine erfolgreiche Implementierung an Realzeitsysteme in der Automatisierung stellt. Zudem erhalten Sie mit diesem Buch eine konkrete Anleitung zu einer inkrementellen Vorgehensweise, um mögliche Fehler, Kosten und Risiken bei der Entwicklung von Echtzeitsystemen zu minimieren. Die integrative Darstellung und Bewertung der notwendigen Randbedingungen und die Methoden zur Realisierung von softwarebasierten Funktionen unter Echtzeitbedingungen machen dieses Buch zu einer wertvollen Ergänzung in der Berufspraxis. So konzipieren und entwickeln Sie zuverlässige SystemeZu Beginn erläutert der Autor die Grundlagen.Erfahren Sie in diesem Buch, welche Motivation hinter der Entwicklung von Echtzeitsystemen steht, wie der aktuelle Entwicklungsstand aussieht und welche Rolle Programmiersprachen und die Wertschöpfung durch Software in Unternehmen spielen. In den folgenden Kapiteln stehen u. a. diese weiterführenden Aspekte im Vordergrund: · Herstellungsprozesse für Software · Analyse und Bewertung von Konzepten zur Ereignisbehandlung unter Echtzeitbedingungen · Prozesskonzept und Scheduling als Basis für zuverlässige Echtzeitsysteme · Programmierung von Echtzeitsystemen mit hoher Zuverlässigkeit · Integrative Betrachtung von technischer Sicherheit und Informationssicherheit · Beispielhafte Umsetzung der Entwicklungsmethodik Abschließend gibt Ihnen der Autor konkrete Empfehlungen für die Entwicklung einer zuverlässigen Automatisierungssoftware.

Cyber Security Kosten Konsequenzen ← hohe Eintrittswahrscheinlichkeit
***hoher Schaden**
***hohe Ignoranz**
***Unterschätzung der Angreifer**
***???**

Fragen?



https://www.pngwave.com/png-clip-art-ohqtt

hubert.keller@kit.edu