ISSS BERNER TAGUNG 2019

«SICHERHEITSASPEKTE BEI IT-BESCHAFFUNGEN» | Dec 19th, 2019

Information Security Society Switzerland

Supply Chain Security

Dr. Stefan Frei

Accenture Cyber Defence | Dozent Cyber Security ETHZ

frei@techzoom.net | Twitter @stefan_frei

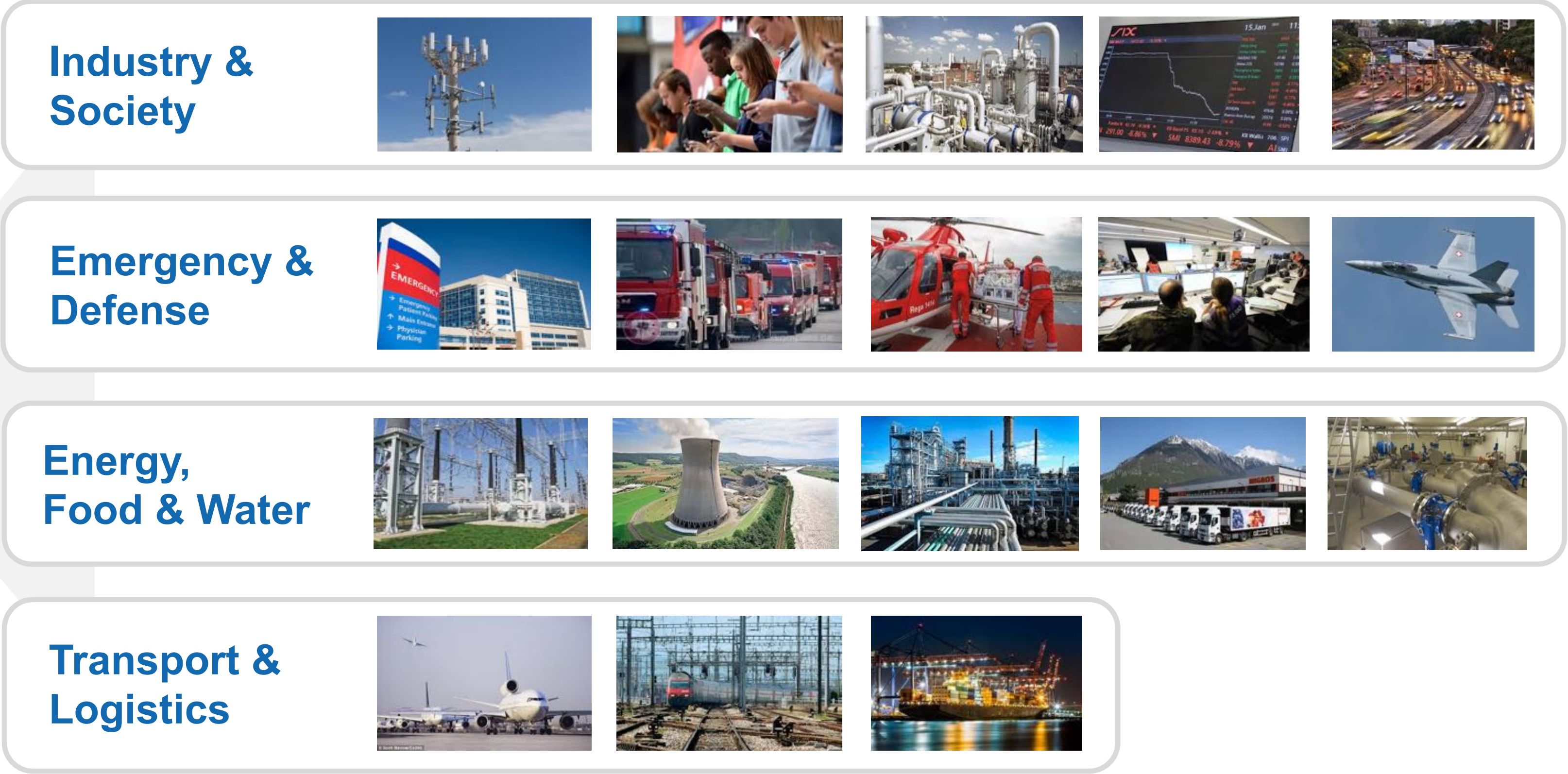
Head of the working group "Supply Chain Security" @ ICT Switzerland

Main Challenge in Cyber Security?

We increasingly depend on digital systems as individuals, society & industry.

75 BILLION

CONNECTED DEVICES
by 2025



How do we assure the security and integrity of critical devices & infrastructure?

HUMANS ARE NEW TO THE MECHANISMS AND ARTIFACTS OF CYBER RISK

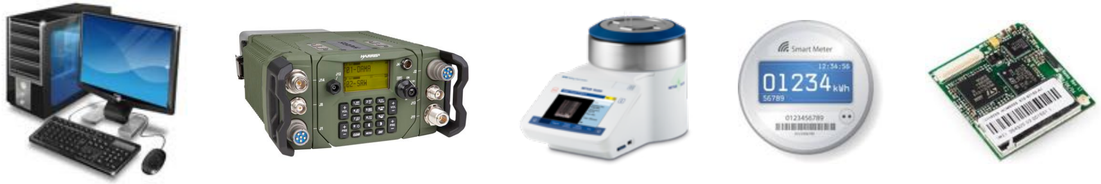
We have no built-in concept to deal with abstract risks

INSTANT
PERCEPTION OF RISKS

No **training needed** to instantly get out of danger

Evolution built us to perceive risks as hunter-gatherer in the wild

LIMITED
PERCEPTION OF RISKS



Security **defects are invisible** without proper testing

Humans are new to technology and abstract risks

NO PERCEPTION OF RISK

People need highly visible incidents before they act

Insecure systems cannot be identified without **extensive testing** ▶ **ILLUSION** OF CONTROL

We face considerable **difficulty to get resources** (e.g. from mngt) to protect **against abstract risks** ▶ **ACCUMULATION** OF RISKS

WHAT COULD POSSIBLY GO WRONG?

Exposures in a complex and ever changing environment

COMPLEXITY

COMPLEX ENVIRONMENT

- Increased **complexity** and coupling
- Emerging properties & bad things happen **for no reason**
- **Unpredictability** of user and social behavior
- Continued discovery of new **vulnerabilities**

ACCIDENT

ATTACKERS

TARGETED ATTACK

NATION STATES

- Have always engaged in **espionage** and **sabotage**
- Have the resources and **a mandate** to do so

ORGANIZED CRIME

- Go where the money is
- Fast **adopters of new technologies**
- Sometimes blurry line between nation state activities

SOFTWARE & HARDWARE

Critical reliance on compiled **code** in **software** and **hardware**, which is **difficult to inspect**.

Attackers Perspective

WHAT WOULD YOU TARGET?

To get the biggest impact with the least effort, stay persistent, and avoid detection?

Lesson from history ..

The majority of mediaeval castles where not taken by direct attack against the enforced walls.

But through ..

.. for todays world

?

WHAT WOULD YOU TARGET?

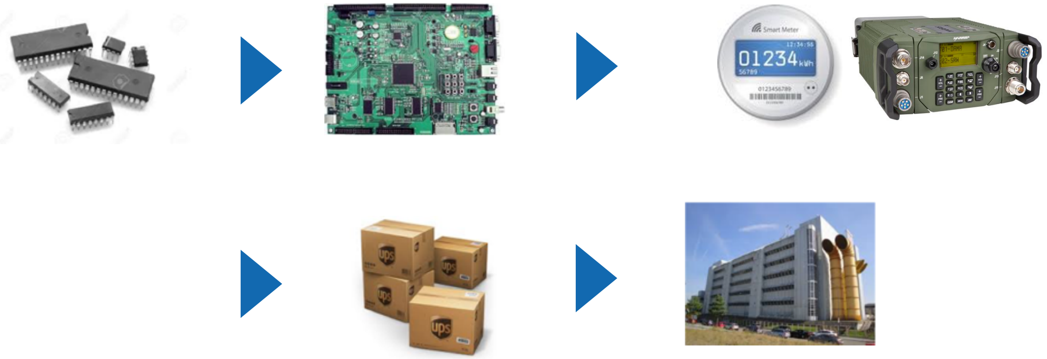
Find the weakest link & attack where they expect it the least!

Lesson from history ..

The majority of mediaeval castles where not taken by direct attack against the enforced walls.

But through treason or marry-in

.. for todays world



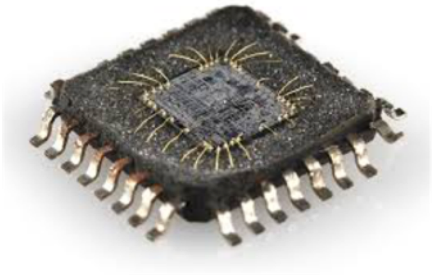
We depend on a **complex supply chain** of numerous sub-systems and various suppliers

.. over which we have limited control at best

SUPPLY CHAIN ATTACK

Scenarios and exposed sectors

- Critical systems and devices are **compromised upon delivery**.
- Functionality of critical systems **changes over time**.
- Operation of critical systems **depend on external services** (cloud, vendor).
- Lack of **update-functionality** results in **loss of control**.



TARGETED ATTACK

INDUSTRY SPECIFIC

Targeting non consumer grade products for specific industries.

A single component has critical implications for a targeted sector.

- Special network equipment (ISP router, GSM)
- Industry Control Systems (ICS)
- Industrial Internet of Things (IIOT)
- Industry specific systems (military, energy, transport, medical, ..)

OPPORTUNISTIC ATTACK

OFF THE SHELF COMMODITY

Targeting off the shelve commodity products for consumers and industry.

Only **a large number of compromised components** become critical.

- Computer, logic boards, processors
- Smart meter, toaster, TV, ..
- Home control systems
- IOT, sensors

History & Examples

LONG HISTORY OF SUPPLY CHAIN ATTACKS

Actor: Nation State - USSR

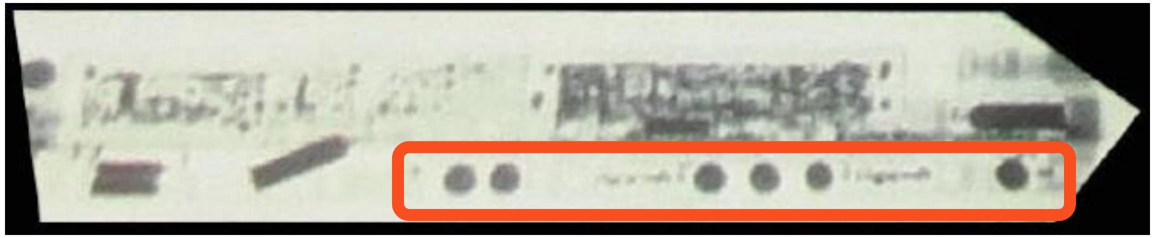
1970 Soviets replaced the comp support bar in IBM typewrites deployed in U.S. embassy in Moscow.

Transmit in plain text whatever was written in the embassy

- *The Selectric Bug was a sophisticated digital eavesdropping device, developed in the mid-1970's by the Soviet Union (USSR).*
- *It was built inside IBM typewriters and was virtually invisible and undetectable.*
- *16 devices found that were in use **at least 8 years.***

Source(s)

- Operation GUNMAN - how the Soviets bugged IBM typewriters
  https://www.cryptomuseum.com/covert/bugs/selectric/



Six black dots in x-ray
Magnetometers that picked up the movements of the six modified latch interposers of the keyboard

LONG HISTORY OF SUPPLY CHAIN ATTACKS

Actor: Organized Crime

2008 Hundreds of card terminals in supermarkets exfiltrate information using mobile network.

The devices were opened, tampered with and perfectly resealed

- *An organized crime syndicate is suspected of having tampered with the chip and pin machines*
- *Tampering either during the manufacturing process at a factory in China, or shortly after they came off the production line.*

Source(s)

- Chip and pin scam 'has netted millions from British shoppers
  https://www.telegraph.co.uk/news/uknews/law-and-order/3173346/Chip-and-pin-scam-has-netted-millions-from-British-shoppers.html

LONG HISTORY OF SUPPLY CHAIN ATTACKS

Actor: Nation State - USA

2012 Hardware and software components can be compromised and with or without the consent or knowledge of the supplier

After years of speculation that electronics can be accessed by intelligence agencies through a back door, an internal NSA catalog reveals that such methods already exist for numerous end-user devices.

- NSA’s backdoor catalog exposed, targets include
  - Cisco 500 series PIX firewalls and most ASA firewalls
  - Juniper Networks firewalls, routers, and netscreen appliances
  - Huawei Eudemon series firewalls and routers
  - Dell PowerEdge 1850, 2850, 1950, 2950 RAID servers

- NSA ANT Product Catalog
  https://nsa.gov1.info/dni/nsa-ant-catalog/index.html

- NSA’s backdoor catalog exposed: Targets include Juniper, Cisco, Samsung, Huawei
  https://gigaom.com/2013/12/29/nsas-backdoor-catalog-exposed-targets-include-juniper-cisco-samsung-and-huawei/
  http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html

Blind Spot

WEAKEST LINK & BLIND SPOT

Hardware is the least protected layer

PRODUCT

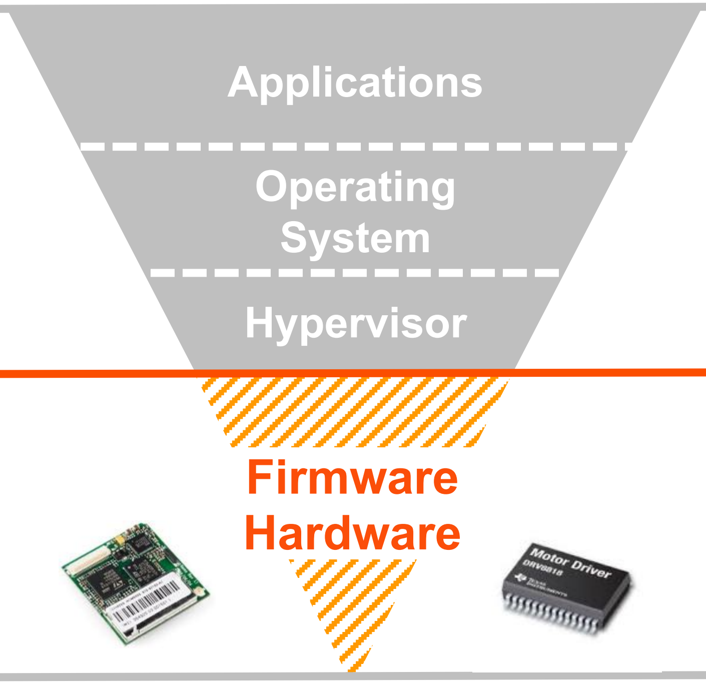
Computer / Device

SOFTWARE

Many layers, lots of security features

HARDWARE

Boards, CPUs, chips, components, designs, ..



KNOWN TERRAIN

(Software)

UNKNOWN TERRAIN

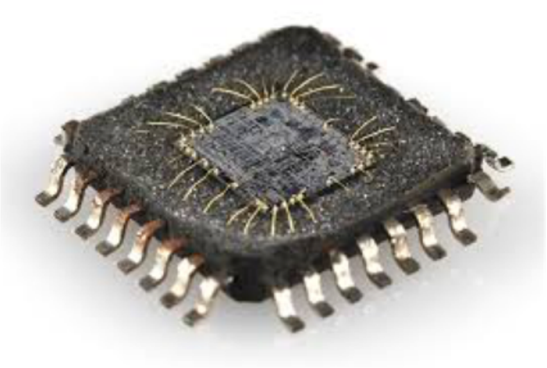
(Hardware)

IMPACT OF COMPROMISED HARDWARE OR FIRMWARE

Cybersecurity remains largely SOFTWARE FOCUSED

- in terms of the techniques employed
- the expertise of the people and companies working in the field

Impact of compromised hardware or firmware



- Remotely access & control the system
- Exfiltrate or leak sensitive information
- Disable/cripple functionality, make incorrect results
- Enforce the use of insecure algorithms
- Physically kill the system

HARDWARE ATTACKS

Harder to conduct than software attacks, since far fewer people have the necessary skills and access.

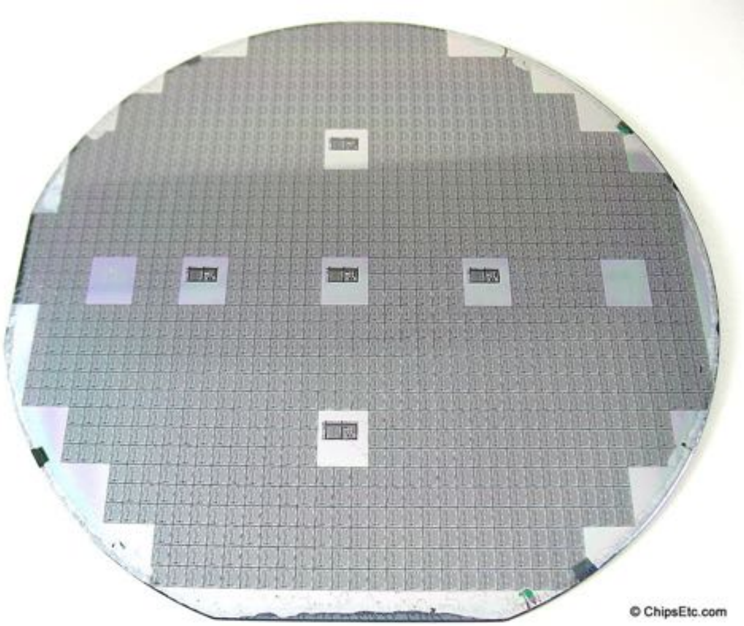
HARDWARE DEFENSE

Harder to defend against, since replacing corrupted hardware can be extremely difficult and expensive.

COMPROMISED HARDWARE OR FIRMWARE NULLIFIES ALL OTHER SECURITY MEASURES

CHIP DESIGN CORRUPTION

Over 5,000 new chips designed each year - involving thousands of companies and hundreds of thousands of chip designers



A skilled attacker could:

- **Compromise a design & minimizing the chance of detection** (chips are so complex that testing is only partial)
- **Introduce a flaw with plausible deniability** (characterizing the back door as a feature to assist in testing prototypes of the chips)

Statistically, there are enough people with the skills, access, and motivation to intentionally compromise a chip design.

Source: Compromised By Design?
https://www.brookings.edu/wp-content/uploads/2016/06/Villasenor_HW_Security_Nov7.pdf

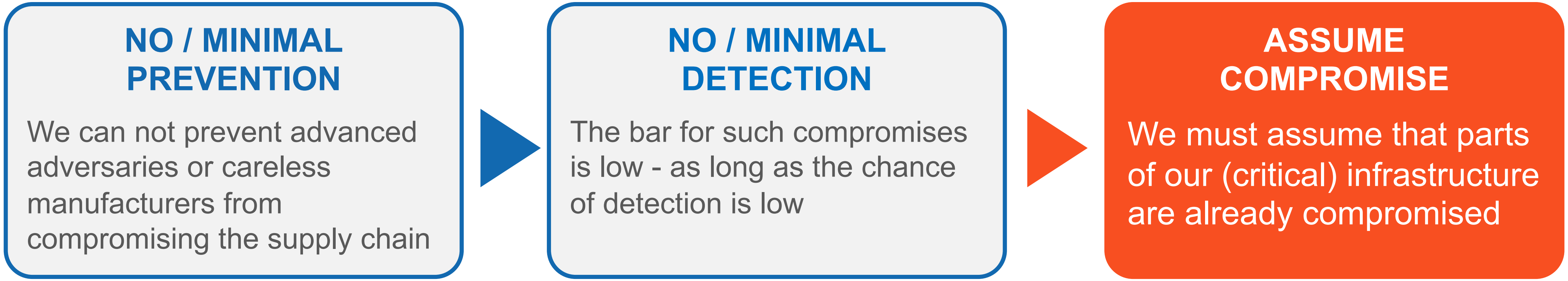
"Frankly, it’s not a problem that can be solved, this is a condition that you have to manage.”

General Michael Hayden

retired head of CIA and NSA

CONCLUSIONS SO FAR

The integrity of digital products has to be challenged and questioned to a greater extent.



NO / MINIMAL PREVENTION

We can not prevent advanced adversaries or careless manufacturers from compromising the supply chain

NO / MINIMAL DETECTION

The bar for such compromises is low - as long as the chance of detection is low

ASSUME COMPROMISE

We must assume that parts of our (critical) infrastructure are already compromised

Change incentive or cost for potential compromise

Systematic testing of the integrity and security

Detection, ongoing testing

We have to systematically verify the integrity & security of critical components.

SOCIETIES ALWAYS DEVELOPED NORMS TO ENSURE THE QUALITY OF CRITICAL GOODS - ENFORCED BY HARSH TESTING

AUTOMOTIVE

- Extensive testing of vehicles before admission
- Periodic inspections
- Minimum quality and safety standards

AVIATION

- Extensive testing of aircraft before admission
- Extensive operations requirements
- Periodic inspections & traceability of components

FOOD MEDICINE

- Extensive testing of new drugs before admission
- Extensive requirements for processing and delivery
- Periodic and surprise inspections & traceability of components

CYBER

- No binding norms or minimum requirements
- Security or the integrity of goods at odds, no systematic testing
- No product liability

PHASES OF INTRODUCING QUALITY REQUIREMENTS

Typically fiercely resisted by the industry with the same arguments

PHASE 1
TECHNOLOGY INTRODUCED

New disruptive technology is introduced, there are yet no quality requirements

- Existing norms do not apply as the innovation is disruptive

PHASE 2
TECHNOLOGY BECOMES CRITICAL

The new technology becomes critical for society, increasing number of accidents / incidents

- Calls for quality standards or norms

PHASE 3
INDUSTRY FIGHTS MIN. REQUIREMENTS

Industry fights introduction with always the same arguments:

- Product is safe - **accidents are the users fault**
- Norms are not necessary - they will **ruin the industry**
- Norms will **stifle innovation**

PHASE 4
NORMS & TESTING INTRODUCED

Eventually, society develops and introduces minimum requirements for critical goods

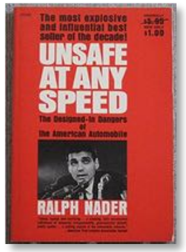
- Minimum safety and security requirements are enforced through harsh testing
- Industry still exists

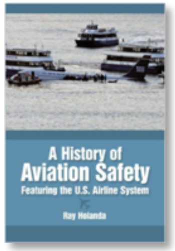
1900
invented & perfected

1950 ..
cars become prevalent

1966
creation of predecessor of
National Highway Traffic Safety Administration

1970 ..
cars tests, seat belts
mandatory, airbags , ..


The most explosive and influential best seller of the decade!
$5.95 $1.00
UNSAFE AT ANY SPEED
The Designed-In Dangers of the American Automobile
RALPH NADER


A History of Aviation Safety
Featuring the U.S. Airline System
Ray Holanda

UNSAFE AT ANY SPEED

Book by Ralph Nader accusing car manufacturers of resistance to the introduction of safety features such as seat belts, and their general reluctance to spend money on improving safety. Ralph's book let to introduction of crash-test dummies and seat belts after disputes. (1965..)

HISTORY OF AVIATION SAFETY

First 50 hour endurance tests for aircraft engines against the protests of the industry: Over half of the engines could not pass the initial test (1920-30). Early philosophy in aviation: fly it, break it, fix it, blame the pilot

Conclusion & Actions

"Plan for the difficult whilst it is easy. Act on the large while it's minute. The most difficult things in the world begin with things that are easy."

Laozi (Lao Tzu), 600 BC

CONCLUSION | TRUST BUT VERIFY

LESSONS
HISTORY

Society has **always developed and introduced:**

- Binding quality norms for **critical goods**.
- Testing **capability to verify required quality**.

FINDINGS
CONCLUSION

Effective testing of cyber products (software & hardware) has to be regarded as a **core competency of the digital society.**

- **An independent and trusted organization** should do that for members.
- Effective cyber testing is a **complex business requiring collaboration** between industry, academia, security community, government)

VISION
OPPORTUNITY

Build Joint Cyber Testing Organization (private / public org) today

- Coordinate tests on **behalf of its members** (industry, nation, ..)
- Tests executed by **trusted testing labs** (own labs & industry partner labs)
- **Document and communicate results** (coordinated disclosure)

Switzerland is well positioned to build or host an internationally trusted organization for testing cyber products

- independent, trusted, competent
- long history of hosting similar organizations (Labor Spiez, Red Cross, ..)

Too often, we wait for catastrophe to spur change.

Thank You

Dr. Stefan Frei

Further reading and acknowledgments to my collaborators

Supply Chain Security

Analysis and measures to secure the digital supply chain

The Supply Chain Security working group of the Cybersecurity Commission of ICTswitzerland

September 2019

ICTSWITZERLAND

DE | FR | EN

WHITE PAPER SUPPLY CHAIN SECURITY

Analyse & Massnahmen zur Sicherung der digitalen Lieferkette

https://ictswitzerland.ch/white-paper-supply-chain-security | Sep 2019

der **Arbeitsgruppe Supply Chain Security** von **ICT**SWITZERLAND

https://ictswitzerland.ch/en/topics/cyber-security/supply-chain/