



Costica Dima

Cyber- & HW- security in IoT World – NTB Buchs

Security Solutions by Avnet Silica - DACH

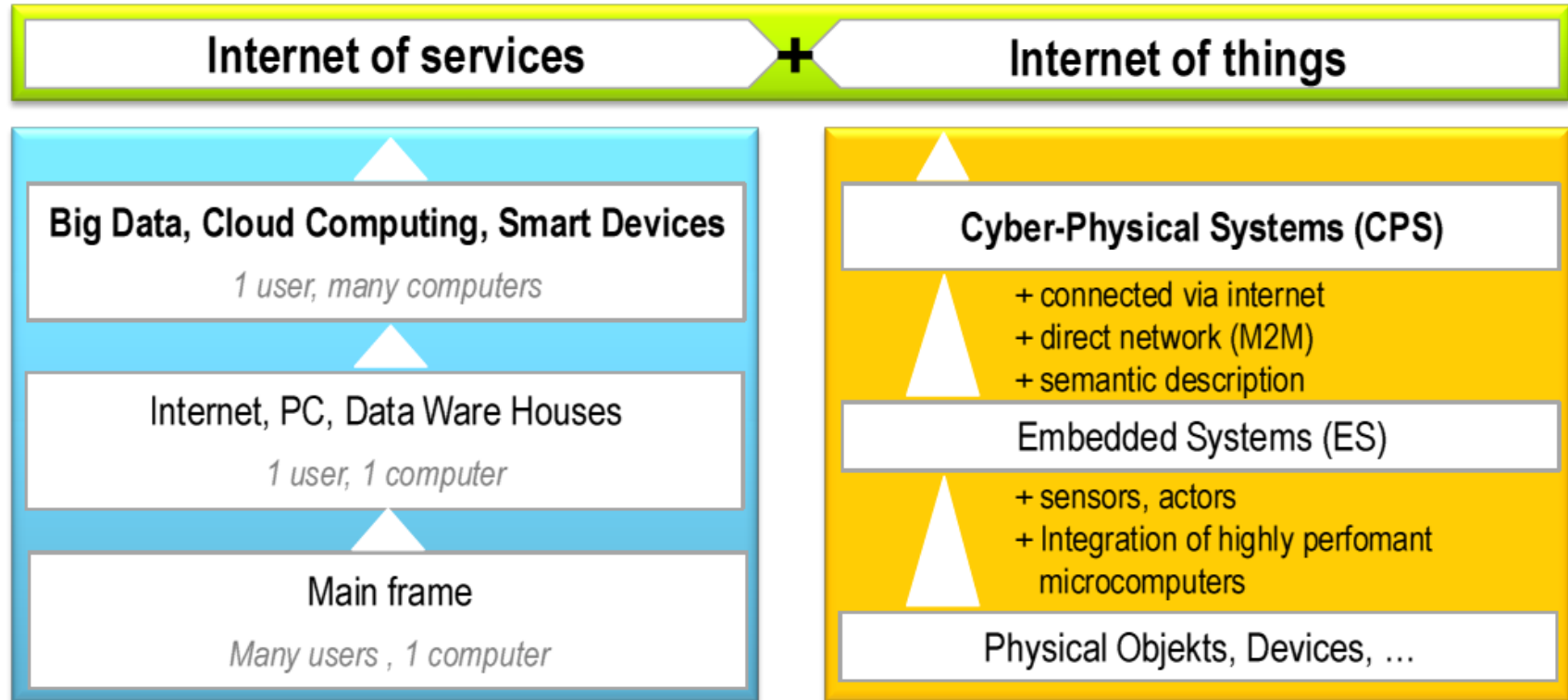
Accelerating Your Success™

.... And the growth of the IoT is....

..... From the Internet of Devices to the Internet of Everyday Things

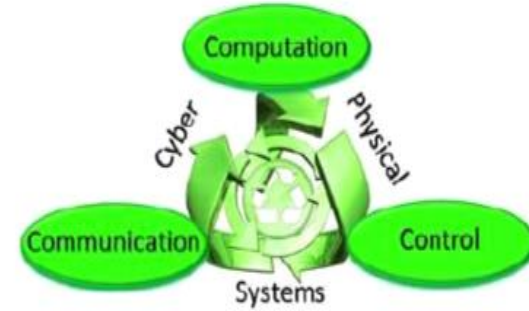


The innovation is driven by two converging technologies

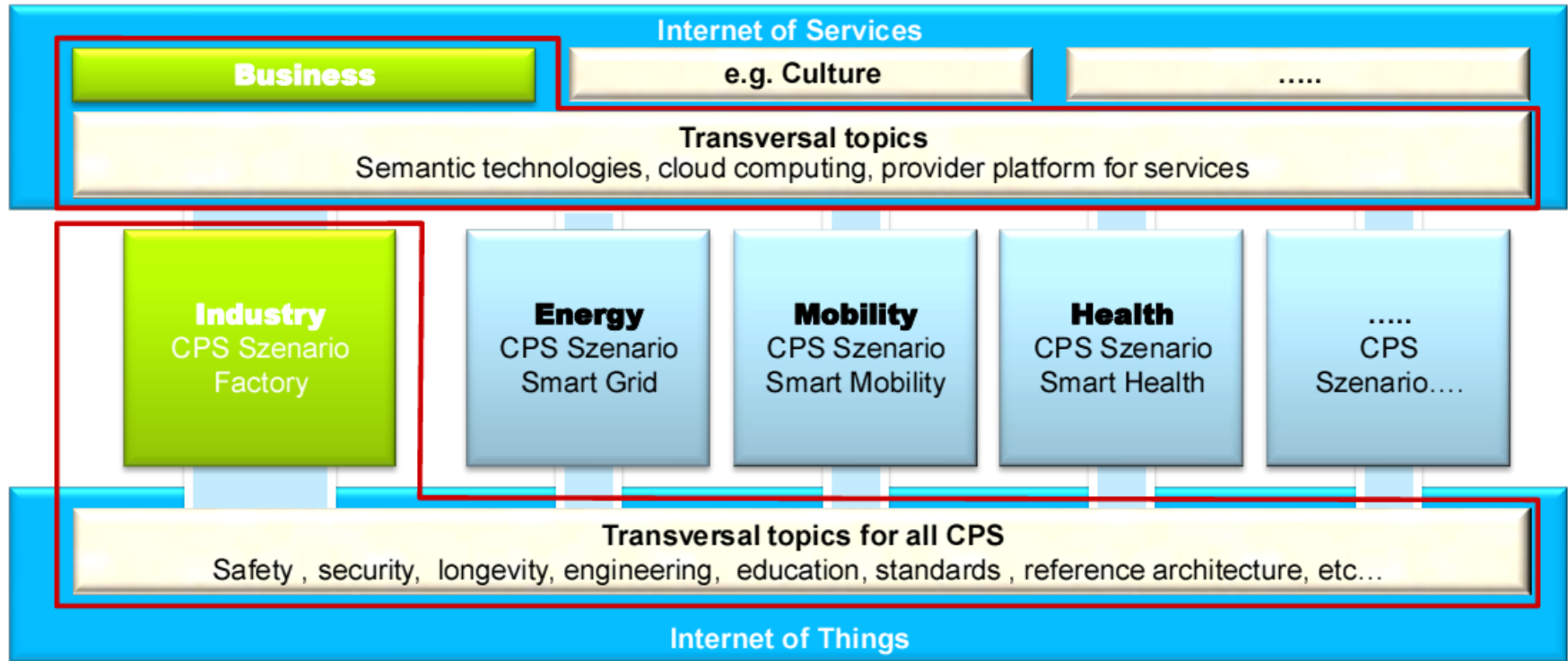


CPS = Cyber Physical System

- ❑ Autonomous embedded systems as well as process modules for production, logistic, engineering, coordination and management and even as internet services
- ❑ With sensors and actuators to collect physical data and influence physical processes (preferably) wirelessly connected to each other and the internet, using w.w. data and Services
- ❑ Providing multimodal (man-machine) interfaces
- ❑ In a smart factory environment these CPS become CPPS (Cyber physical production systems) -> connected to machines, storage systems and production facilities



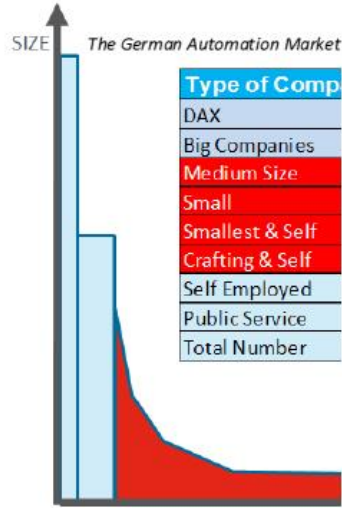
ICT* is the innovation driver for all areas of demand



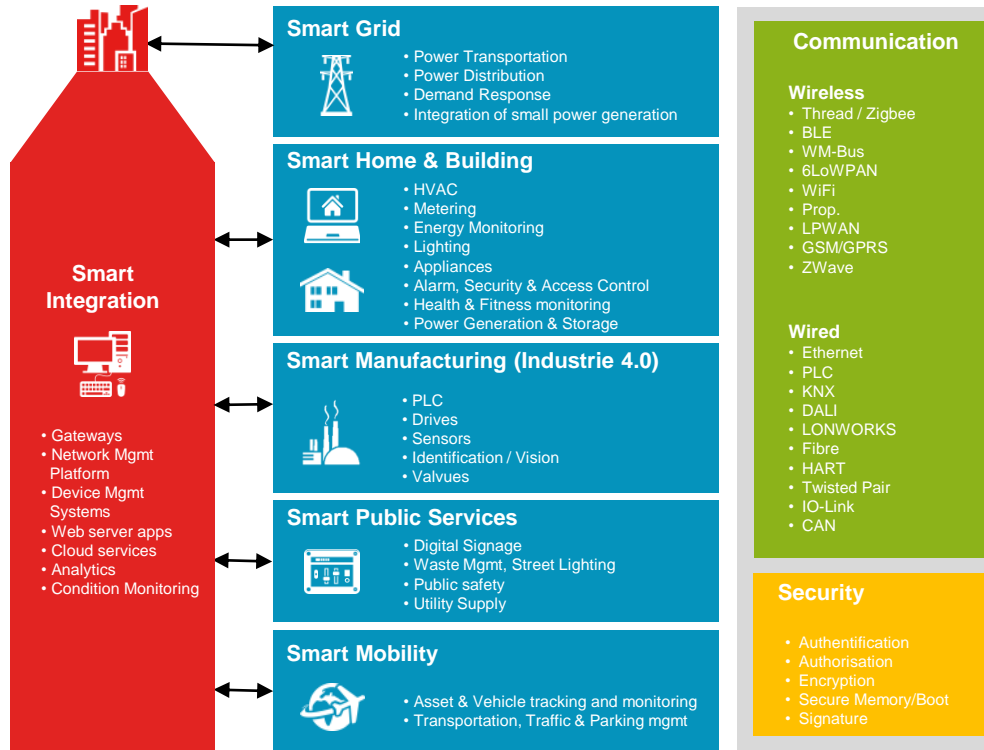
* ICT = Information and Communication Technology

... what next ? Industry 4.0 !

Industry 4.0 is the technical integration of CPS into production and logistic and the utilization of the IoT within industrial processes – this will also have consequences as well on value chains, business models and downstream services as well as on the organisation of workforce.

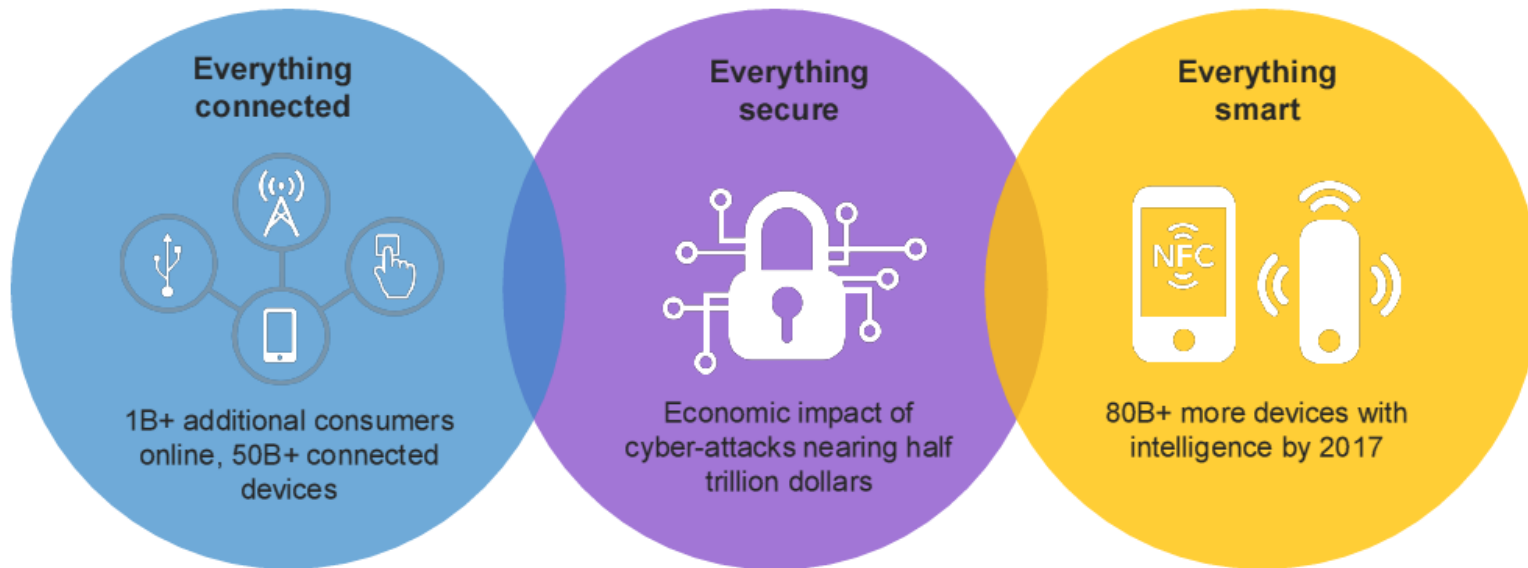


... some markets



Hyper-connectivity has changed our world forever

80% of the World's Economic Value will come from Improvements to existing products

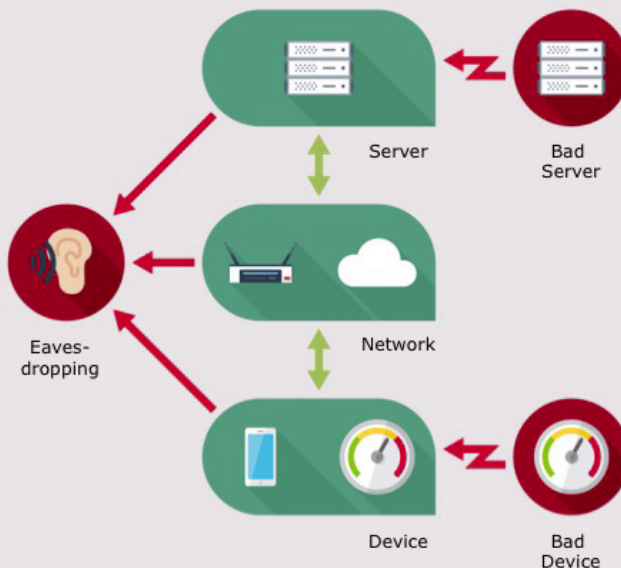


Source: Euromonitor, Gartner, ARM Holdings, UBS, Center for Strategic and International Studies, McAfee, NXP analysis, International Telecommunications Union

Security threats at all levels of IoT architectures

Security threats for IoT

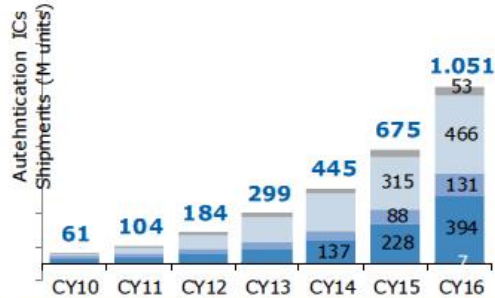
An **Eavesdropper** listening in on data or commands can reveal confidential information and active attacks can cause serious damage.



A **Bad Server** sending incorrect commands can be used to trigger unplanned events, to send some physical resource (water, oil, electricity, etc.) to an unplanned destination, and so forth.

A **Bad Device** injecting fake measurements can disrupt the control processes and cause them to react inappropriately or dangerously, or can be used to mask physical attacks.

Why do we need HW security Counterfeiting



IACC (int'l anti-counterfeiting coalition)

- It is estimated that counterfeiting is a **\$600 billion a year** problem
- It's a problem that has grown over **10,000 percent** in the past two decades
- **~5% to 7%** of the world trade is in counterfeit goods

Daily more news

7 NEWS WISYR.COM
WISYR.COM
HOME NEWS WEATHER VIDEO SPECIAL REPORTS SPORTS NEWS TEAM
Local • National • World • Business • Politics • Entertainment • Odd • Tracking the Tropics

LOCAL NEWS

Officials confiscate counterfeit toys, may pose threats

UNODC
United Nations Office on Drugs and Crime

'Counterfeit: Don't buy into organized crime' - UNODC launches new outreach campaign on \$250 billion a year counterfeit business

14 January 2014 - A new global campaign has been launched by UNODC to raise awareness among consumers of the \$250 billion a year illicit trafficking of counterfeit goods. The campaign - 'Counterfeit: Don't buy into organized crime' - informs consumers that buying counterfeit goods could be funding organized criminal groups, puts consumer health and safety at risk and contributes to other ethical and environmental concerns.

Del.icio.us Digg It Facebook reddit Stumble It Twitter



Fake Medications Are a Growing Threat
There's lots of profit in counterfeit drugs, so consumers should be on guard
By Nancy Shute, Posted 8/21/07

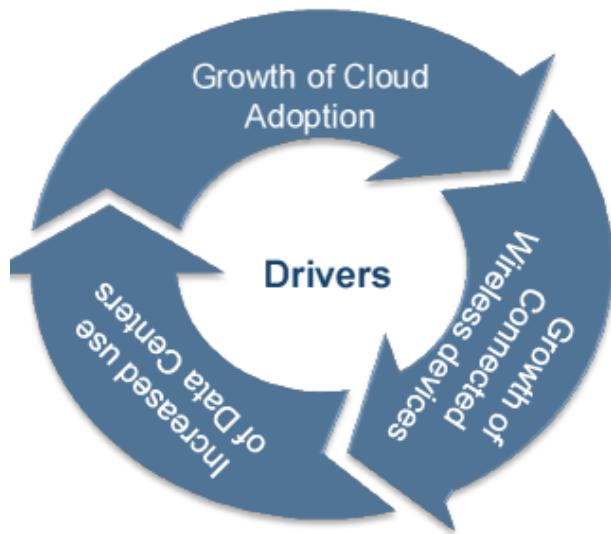
The Washington Times

Indian firm probed over counterfeit medicine
Ranbaxy supplies drugs to U.S., Bush's AIDS initiative
Amy Fagan, Friday, August 1, 2008

Why is CYBERSECURITY essential?

Cybersecurity Overview

The growing number of cyber-attacks across sectors has resulted in compromised confidential information, network outages, and loss of control over essential computing resources. With the increase in digital applications, mobile users, process automation and wireless network usage, the attack surfaces for cyber threats are increasing. The Cybersecurity concept helps secure computing resources, information, networks and applications from cyber attackers and prevents unauthorized access, control, abuse or destruction of the same.



Importance of Cybersecurity

Access Security is an essential aspect of cybersecurity to prevent unauthorized access to significant computing systems. Such unauthorized access leads to abuse of data and applications.

Network Security ensures the reliability and availability of the network by preventing intrusions and malicious traffic.

Data Security is a key deliverable of cybersecurity as compromise of confidential data may lead to disclosure of private strategies and facts leading to huge losses.

Application Security eradicates the vulnerabilities of the application, closing down the attack surfaces, thereby preventing abuse of resources handled by the applications.

Security of Autonomous Systems is a key area of focus due to the convergence of operational technologies with information and communication technology. With Industry 4.0 and Internet-of-Things (IoT) concept setting in, securing autonomous systems has become a major priority.

National Security is of importance to safeguard critical national infrastructure.

Why do we need HW security Hack Attacks

BBC News Sport Weather Earth Future Shop

NEWS TECHNOLOGY

Home UK Africa Asia Australia Europe Latin America Mid-East US & Canada Business Health Sci

finca llorca

Finca Can Moragues
8 - 9 Personen
Typisch mallorquinisches
Flair, Herrliche ...

8 July 2014 Last updated at 12:52 GMT

Smart LED light bulbs leak wi-fi

By Jane Wakefield
Technology reporter

Security experts have demonstrated how easy it is to hack network-enabled LED light bulbs.







Context Security released details about how it was able to hack into the wi-fi network of one brand of network-enabled bulb, and control the lights remotely.



Software Cannot Protect Software: An Argument for Dedicated Hardware in Security and a Categorization of the Trustworthiness of Information

Matthew Judge, Paul Williams, Yong Kim, and Barry Mullins

Air Force Institute of Technology
2950 Hobson Way
Wright Patterson AFB OH 45433, USA
{matthew.judge,paul.williams,yong.kim,barry.mullins}@afit.edu

NETWORKWORLD Most read:      

Protecting Against Online Banking Fraud [More +](#)

Home > Security

Basic hacks can compromise industrial systems

attacks is up, but defenses lag

[RELATED](#)

BBC Sign in News Sport Weather Shop Earth

NEWS

Home Video World US & Canada UK Business Tech Science Magazine

Technology

Hack attack causes 'massive damage' at steel works

22 December 2014 | Technology

U.S. government probes medical devices for possible cyber flaws

BY JIM FINKLE
BOSTON | Wed Oct 22, 2014 7:11am EDT

[Tweet](#) 452 [Share](#) 368 [Share this](#) 841/39 [Email](#) [Print](#)



The Economist World politics Business & finance Economics Science & technology Culture

Special report: Cyber-security

The internet of things

Home, hacked home

The perils of connected devices

Jul 12th 2014 | From the print edition

[Timekeeper](#) [Like](#) 228 [Tweet](#) 125



.... Public Safety & Cyber Security for Government

Why Device ID for every SmartGrid node:

- › Attacker can shut down meters or feed incorrect values to the SmartGrid to **de-stabilize the load and collapse the power generation plants** or transformers.
- › Non Authentic car batteries could explode while in a charging station and pose a safety hazard.
- › 100M's of un-attended entry points that could act as a Trojan horse. No need for physical presence to attack a network.
- › State of the art of security technology is necessary to future proof the long life cycle of SmartGrid equipment.
- › Low cost compared to potential damage.

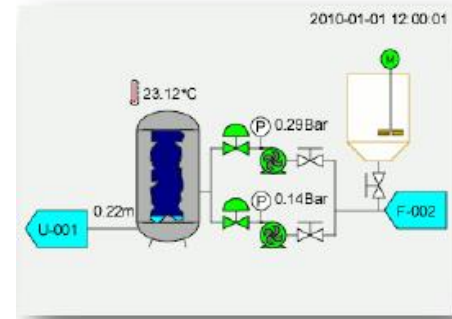
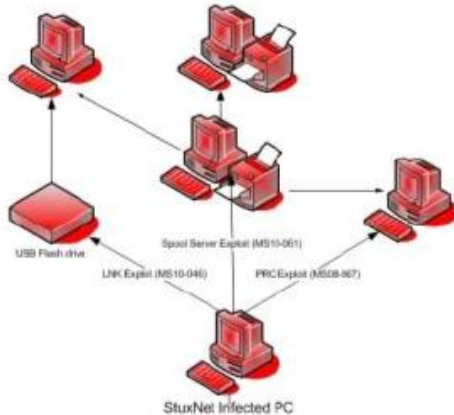


The **2003 Blackout** affected 55 million people between Ontario and eight U.S. states. Lightning caused cascading failure of power transmission grid.



..... Industrial Automation Systems....

- ❑ More than 100000 systems affected by — “Stuxnet worm”
- ❑ Industrial Computers even in Nuclear Facilities
- ❑ A tamper resistant secure element validating that only signed software is executed



HW vs SW for key protection Key Benefits

	SW running on main µController	HW Security IC attached to main µController
Benefits	<ul style="list-style-type: none"> ✓ Flexible, easy to upgrade / update ✓ Easy distribution ✓ Perceived lower cost 	<ul style="list-style-type: none"> ✓ HW isolation of crypto operations and isolation of keys ✓ Best in class Tamper Resistance, including against non invasive attacks (box closed) ✓ TRNG, essential for crypto & protocol operations ✓ Secure transport of keys thru pre-inject at IC manufacturing, solving key management across untrusted supply chain and untrusted networks ✓ Proven/certified product, reduced attack perimeter on simple interface ✓ Crypto co-processing (energy budget)
Drawbacks	<ul style="list-style-type: none"> ✗ Currently no SW-only solution has been proven secure! Protection of keys is a real issue with SW. ✗ Often very difficult to control where keys are stored (typical with open source SW, e.g. "Heartbleed" attack) ✗ Hacked SW easy to distribute (leading to massive attacks) ✗ Code size and runtime 	<ul style="list-style-type: none"> ✗ Additional IC cost

New Business Cases are



How to achieve “Security by Design”

Security toolbox for connected objects = cryptography



Access control

Authentication

Anti-cloning

Signature / Certificate

Non-repudiation

Signature / Certificate

Encryption & Signature

Data integrity

Secure memory

- Anti-tampering
- Authentication

IP protection

Attack detect - Anti-tampering
- Authentication

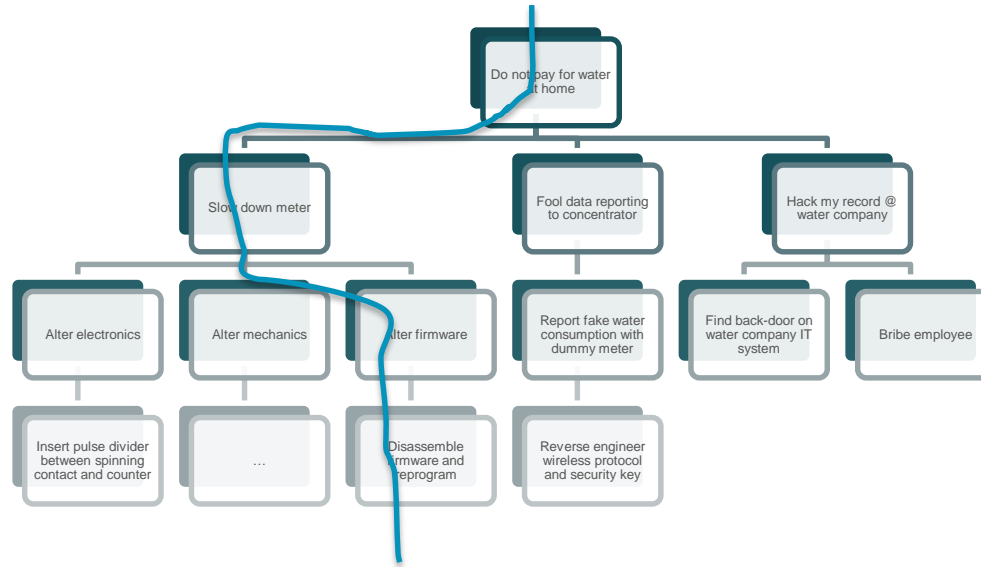
Resilience

Encryption (Pk,Pr)

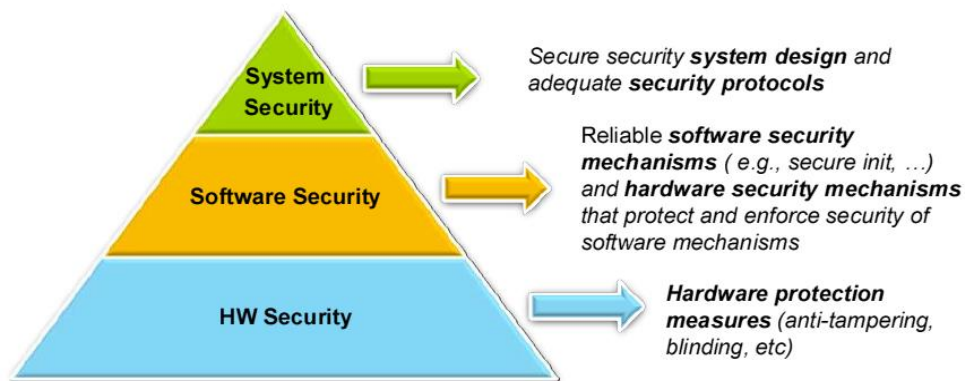
Confidentiality



Attack tree – Tool for evaluating the cost of attacks



A trustworthy HW security Anchor



The trend against hacking is better authentication



Key integrity is essential for system security

- 1 Compromised keys = no Security
- 2 Cloning of key leaves no traces
- 3 Key handling must be secured through the whole lifecycle including manufacturing

Trust Anchors

- Key store
- Crypto operation
- Key management



...major challenges for HW security solution... to meet



- ☐ **TRNG**
- ☐ **Secrets (keys) never leave the Valut**
- ☐ Secure MCU / Secrets (keys) stored in **Tamper Resistant Valut**
- ☐ **Secure Trust Provisioning & Key Generation / Management**

Certification Standards & Organizations

... by applications ...

eGov:

- Smartcard hardware & software
- Digital Tachograph components
- Operating systems, firewalls, signature applications
- Biometric verification systems
- eID and electronic passport
- Smart Meter Gateway



eBanking:

- POS
- ATM
- Credit Cards
- Payments

EMV ICC Specification for
Payment Systems
Common Criteria Version
3.1 level EAL5+ in
conformance to
BSI-PP-0035-2007
EMVCo approval

Some of the Computer based application systems require TCG certification of components based on TPM1.2 or 2.0

*TCG = Trusted Computer Group

*TPM = Trusted Platform Module

Trusted Platform Module (TPM)

Standards comparison

TPM 1.2 supports

RSA encryption

RSA signature

RSA-DAA

SHA-1

HMAC

One-time-pad with XOR

AES (optional)

TPM 2.0 supports

RSA encryption and signature

ECC encryption and signature

ECC-DAA

ECDH

SHA-1, SHA-256

HMAC

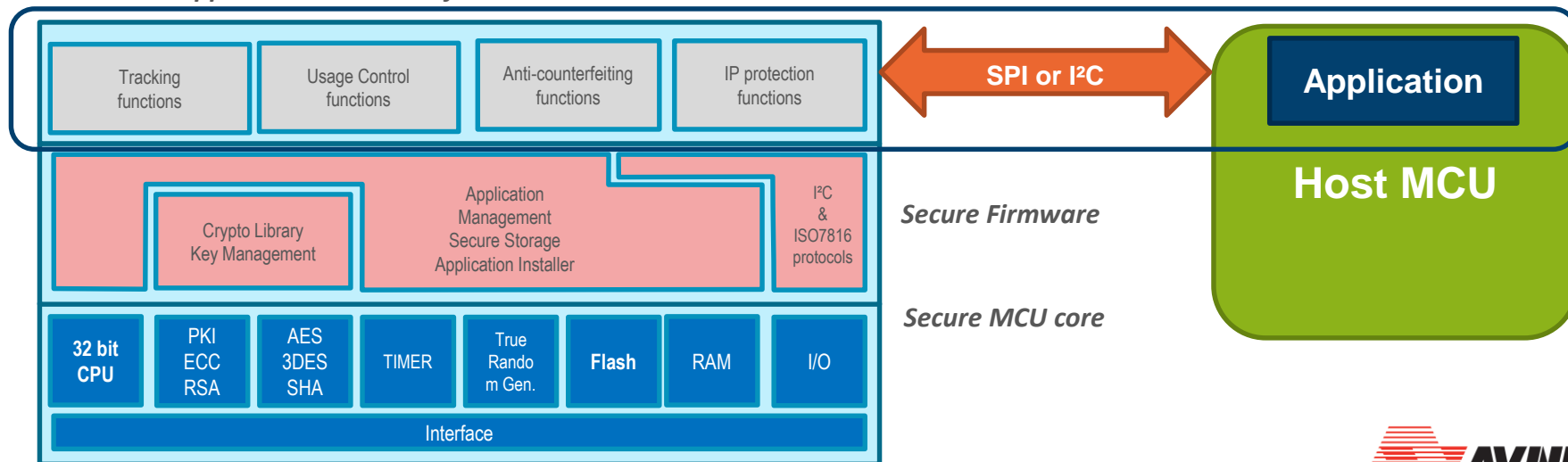
AES and one-time-pad with XOR

More flexibility and enhanced security

This is what a Secure Element is

- A **Secure Element** is basically a micro-controller with added co-processors for the cryptographic protocols plus integrated tamper resistant techniques to protect against all sort of attacks.
 - Typical MCU functions: CPU, memory (ROM, E2PROM, RAM), Interface (I2C, SPI, UART), Clock/timers; reset function, I/Os, voltage regulators, etc.
 - Coprocessor for cryptographic algorithms: symmetric and/or asymmetric
 - Tamper-resistant techniques, i.e. glue logic, security routing, shielding, sensors, etc.

Application-dedicated functions



.... Secure communications

Problem


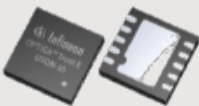


- Protect data exchanges from potential eavesdroppers
- Secure systems against hackers from sensor to server



Solution

- A secure element capable of:
 - Strong authentication
 - Root key storage
 - Session key generation and storage
 - Encryption / decryption

INF OPTIGA™- Hardware-based security solutions

	OPTIGA™ Trust	OPTIGA™ Trust E	OPTIGA™ Trust P	OPTIGA™ TPM
				
Security Level	+	+++	CC certified	CC certified
Design in complexity	low	low	medium	medium
Feature set	One function	Enhanced	Programmable	TPM standard
Personalization (loading of keys and certificates)	✓	✓	✓	✓

System complexity

NXP A-Series Turnkey Solution: Overview



	A710x	A700x	A800x
CPU	SMX1, 31 MHz	SMX1, 62 MHz	SMX2
RAM / ROM	6.14 KB / 196 KB	7.68 KB / 264 KB	8.125 KB / 384 KB
Co-processor	AES, (T)DES Fame (PKI)	AES, (T)DES Fame (PKI)	AES, (T)DES Fame2 (PKI)
TRNG	■	■	■
Interface	I2C 400 kbps SPI 2 Mbps	I2C 100 kbps, ISO7816 Optional contactless (NFC)	I2C 400 kbps
GPIO	2	1	-
SW Options	Embedded Firmware Secure OS + applet	Secure OS + applet	Embedded Firmware
EEPROM	20 KB	80 KB	80 KB/144 KB
Sleep Mode / Deep Sleep	■ / ■	■ / -	- / -
Package	HVQFN32, WLCSP, SO-8 HVSON-8, HVQFN20	HVQFN32	HVQFN32
Max Temperature Range	-40...+90° C	-40...+90° C	-25...+85° C

Note: All Security ICs are **pin compatible** with HVQFN32 package and in I²C mode.

AIS-31 compliant True Random Number Generator



Maxim Security ICs

Analog Micros

Integrated Analog and Security Support for private and public key cryptography

e.g. **MAX66300**, **MAX71637**



DeepCover Secure Microcontrollers

Generic cryptographic support enabling trusted boot and trusted communications

- **MAXQ1050**
- **Future micros**

DeepCover Authentication ICs

Enables hardware authentication as well as simple Public Key Infrastructure

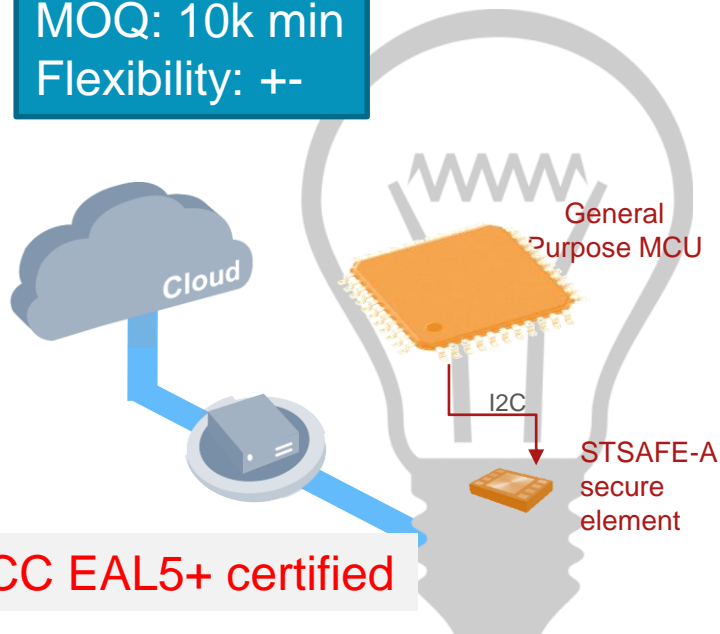
- **DS28XXXX**

STM STSAFE-A – STSAFE-J (Java) & TPM



Easy to use security services for IoT developers

MOQ: 10k min
Flexibility: +-



CC EAL5+ certified

Authentication

Secure communication

Secure storage

Secure Firmware upgrade

USB Type-C



30

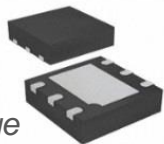


20 January 2017

AVS-exclusive TO136 – Safran-StarChip/Trusted Objects

Volumes: <1k-100M!

Flexibility: ++

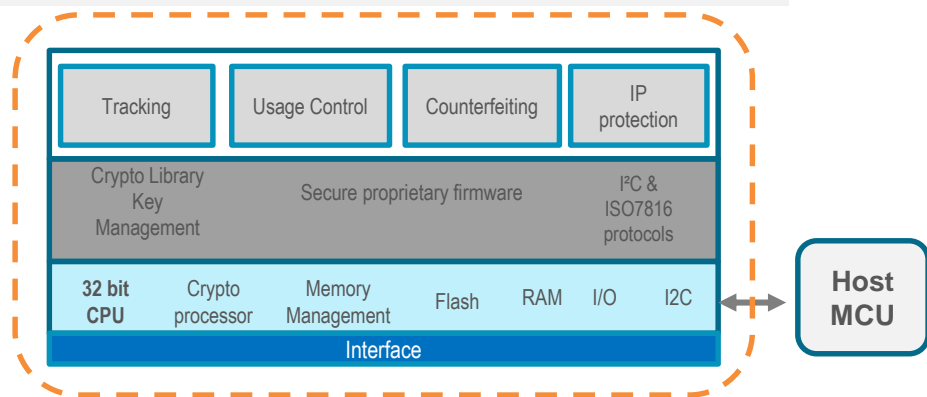


DFN6 package

TO 136 is a fully integrated solution:

- 32 bit Secure CPU hardware, compliant with EMV Co standard
- Customizable on-demand software, optimized for the IoT
- Host code to interface with secure hardware through I2C
- Product personalization with AVS-exclusive secure logistics

HW EMVco and CC EAL4+ certified



- Authenticate Device and/or Server
- Secure communication
- Session key establishment
- Broadcast key management
- Secure data storage
- Setup a TLS connection
- Implement USB Type C authentication



Thank you.



32



20 January 2017