

NREL Smart Grid Educational Series webinar

Hardware Security for Smart Grid End Point Devices

Shrinath Eswarhally (EV)

Senior Staff Engineer -Security

Shrinath.Eswarhally@infineon.com

640 McCarthy Blvd. Milpitas CA 95035

4083167853

Infineon Technologies America

May 11th , 2016



Agenda

1 End points: Security Needs & Priorities

2 End point Security threats

3 Hardware Root of Trust (HROt) security: A comprehensive Solution

4 Hardware Security Use cases

Agenda

1

Security Needs & Priorities

2

Security threats & Risks

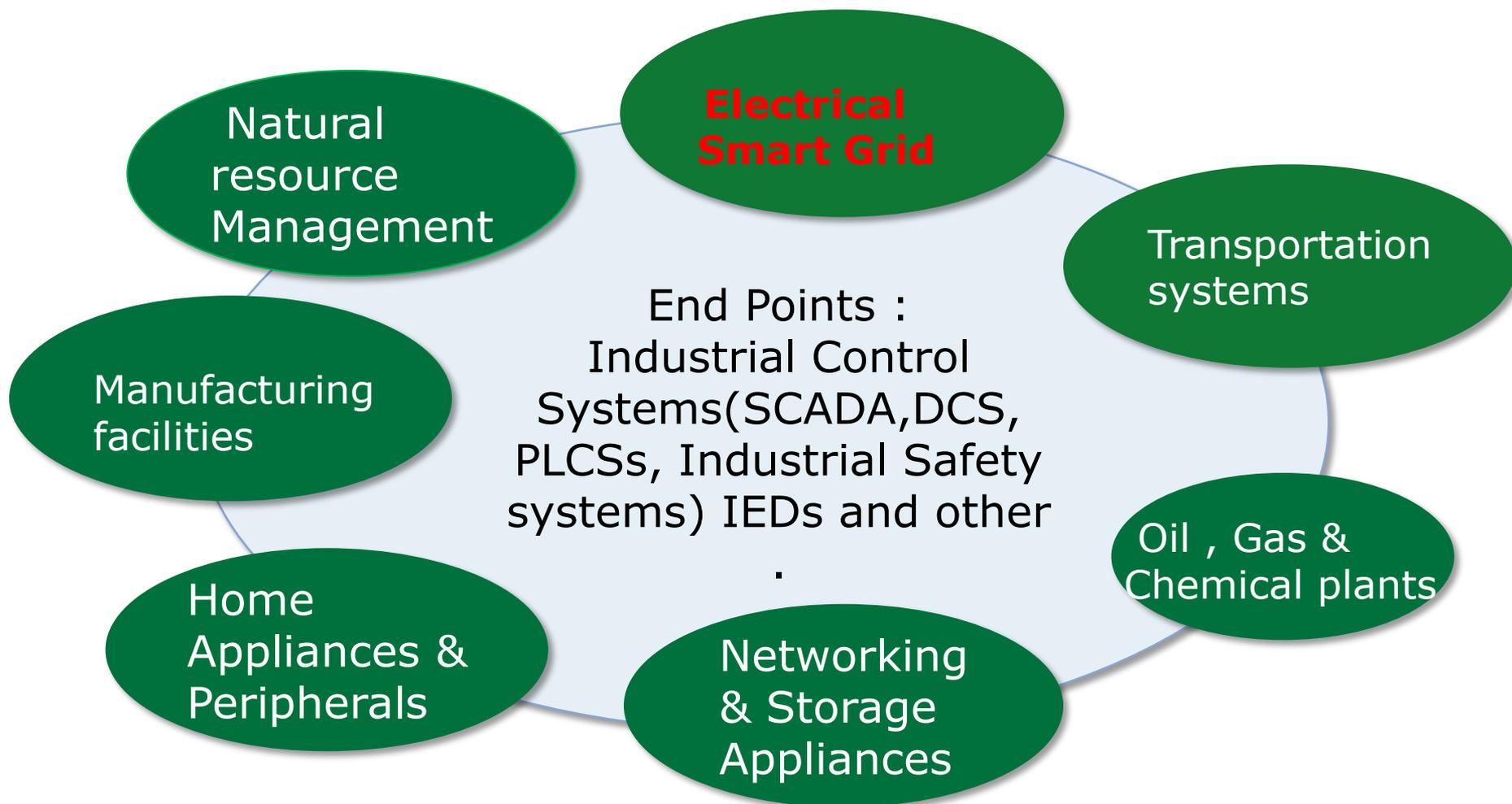
3

Hardware Root of Trust (HROT) security: A comprehensive solution

4

Hardware Security Use cases

Segments of the Critical Infrastructure

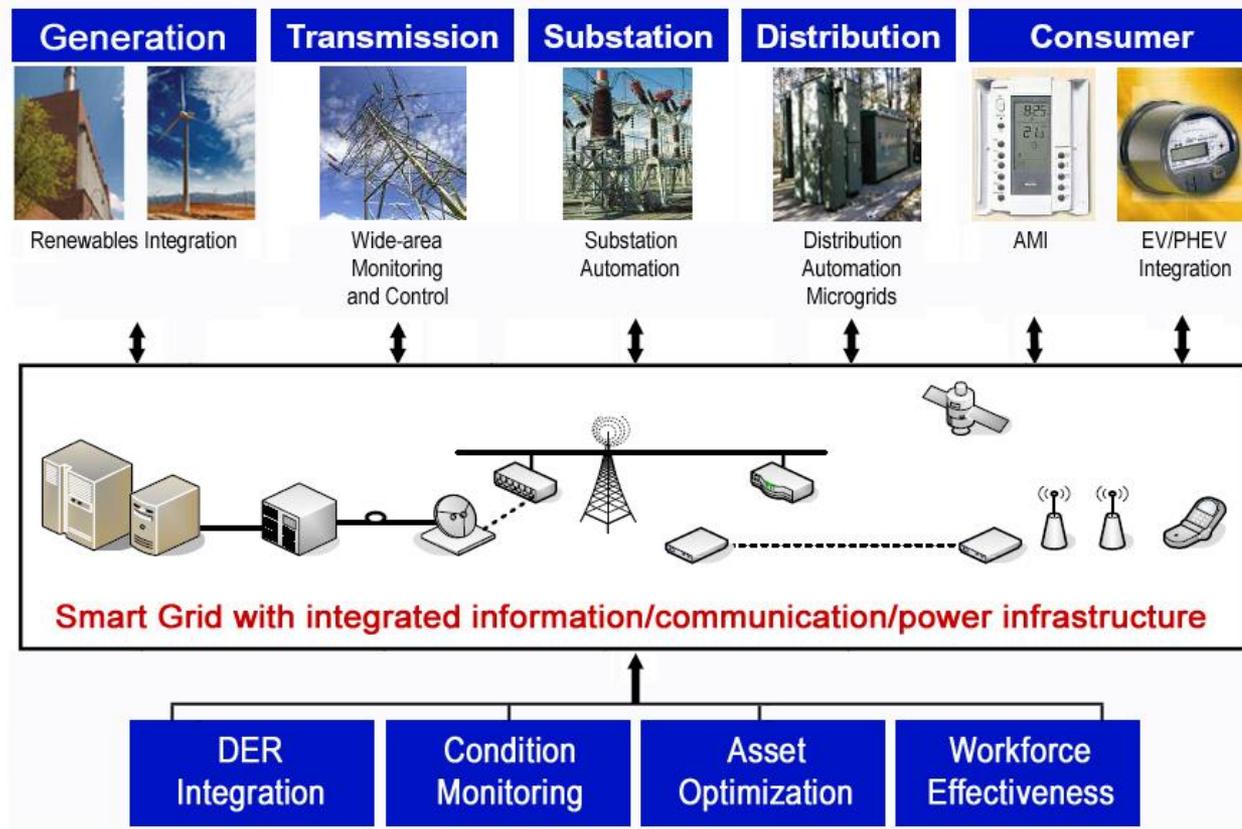


A View on Security

*Sandia Labs 06/2010



Sandia view: Smart Grid Enables Dynamic Optimization of Grid Resources and Operations



Smart Grid NOW requires **bidirectional secure** communication with end points. So **Secure 2 way** Communication = Strong **Authentication for** Messages & Commands

Trends Impacting End-Point Security

- › **Common Operating Systems:** Standardized computer platforms increasingly used to support control system applications: **Knowledge**
- › **Open Protocols:** Open industry standard protocols are replacing vendor-specific proprietary communication protocols: **Knowledge**
- › **High computing/low power** microcontrollers with easy access to **free development tools** .
- › **Interconnects to other systems:** Connections with enterprise networks to obtain productivity improvements and information sharing: **Trust boundary spread**
- › **Reliance on external networks:** Use of public telecommunication systems, the internet, and wireless for control system communications: **Trusted channels**
- › **Increased capability of field equipment:** “Smart” sensors and controls with enhanced capability and functionality: **Functional boundary spread**
- › **Limited security management policies and procedures** for ICS and other automation systems compared to IT: **Security policy enforcement**
- › Problematic **co-ordination of existing standards: Regulation?**

Key statements on current state from Experts

- › Currently if you walk into power station in **China or in California**, You will find that deployed SCADA systems are manufactured by same company and running the same software and when they are connected over internet, they will be **universally accessible**–
Richard Clarke Advisor on cybersecurity.
- › Larger RTOs (Regional Transmission organization) use 10's of thousands of devices, many of them are **insecure and all need to be interconnected**. So they will wait for till the device vendor builds cryptography into them –**George Cotter Former Chief scientist for NSA**
- › SCADA systems controlling **nuclear centrifuges** (Stuxnet attack) manufactured by Major SCADA vendor is also used by **electric power industry** in USA. The software of this system has a **built-in access point** accessible only to system maintenance engineer just with a password. With this access system software can be modified and system can be compromised. **Ted Koppel (Author: Lights Out)**
- › In terms of power grid, no. of **attack surfaces increased exponentially** with the integration of end point devices on internet. Hacker need not have to go for finding server to get access to corporate network and he can do any smart devices (Ex: Thermostat) connected , which enables consumer to program the lighting or heating(Ex:) remotely/automatically. **Ted Koppel (Author: Lights Out)**
- › Although notion of **Administrative network** is “**air-gapped**” from **operational side** and two networks absolutely separate is not correct. “*Worker bringing a thumb drive/laptop and hooking into an isolated system, can infect secure system*” it will **bridge** the “air-gap”.
Ted Koppel (Author: Lights Out)

Industry Pattern of Undervaluing Security

- › Cost impacts of increasing end point assurance often misunderstood
 - B.O.M. vs. System cost: e.g. key diversification cost leads to global keys
 - End point cryptography processing cost modeling
 - Cybersecurity threat risk modeling maturity
- › Early end points did not use encryption or require authentication
 - This left early networks extremely vulnerable to attacks
- › In some cases SCADA systems have been directly connected to the internet
- › End point security too often discussed & addressed after installation
 - “The remote disconnect function was disabled in one of the largest smart meter deployments in the US after security concerns emerged”

Agenda

1

Security Needs & Priorities

2

Security threats & Risks

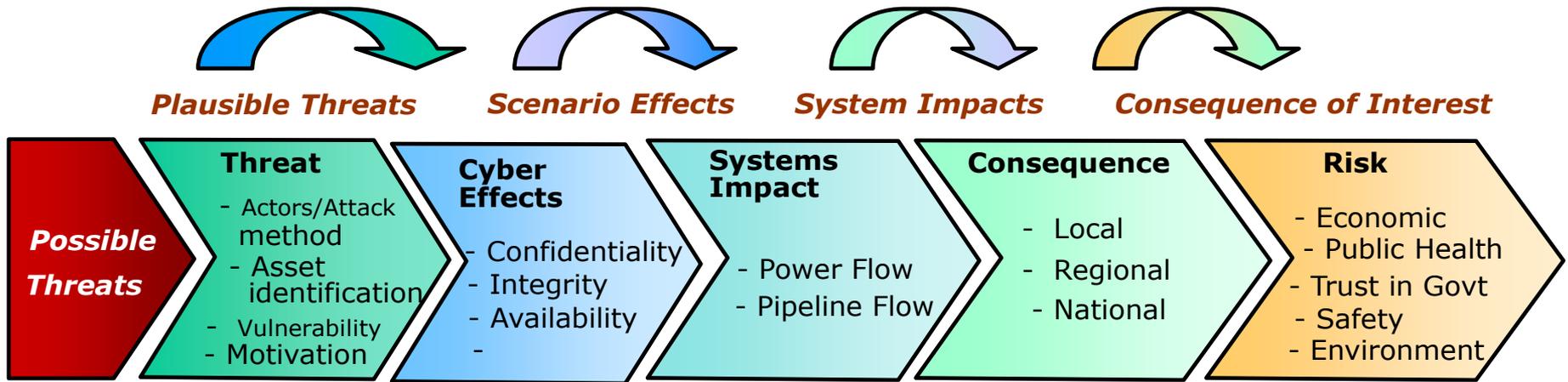
3

Hardware Root of Trust (HROt) security: A comprehensive solution

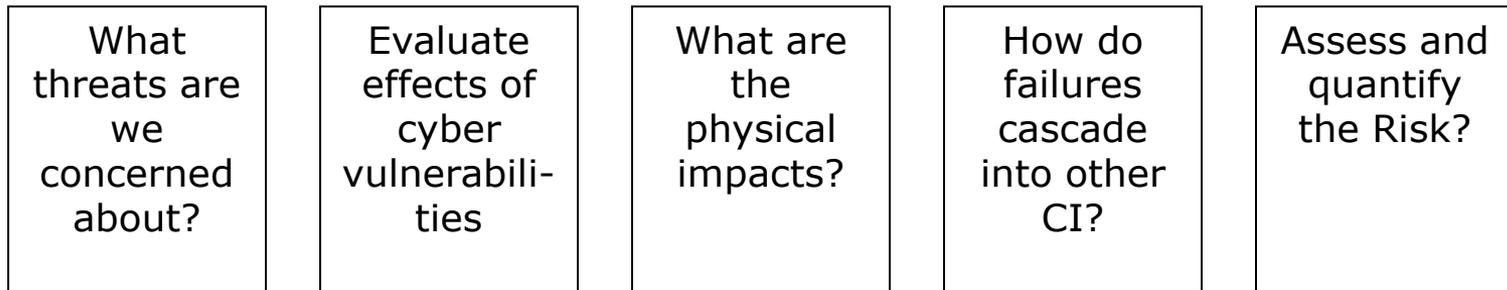
Hardware Security Use cases

Integrated Risk Analysis

Sandia Labs



Threat-to-Consequence Risk Model

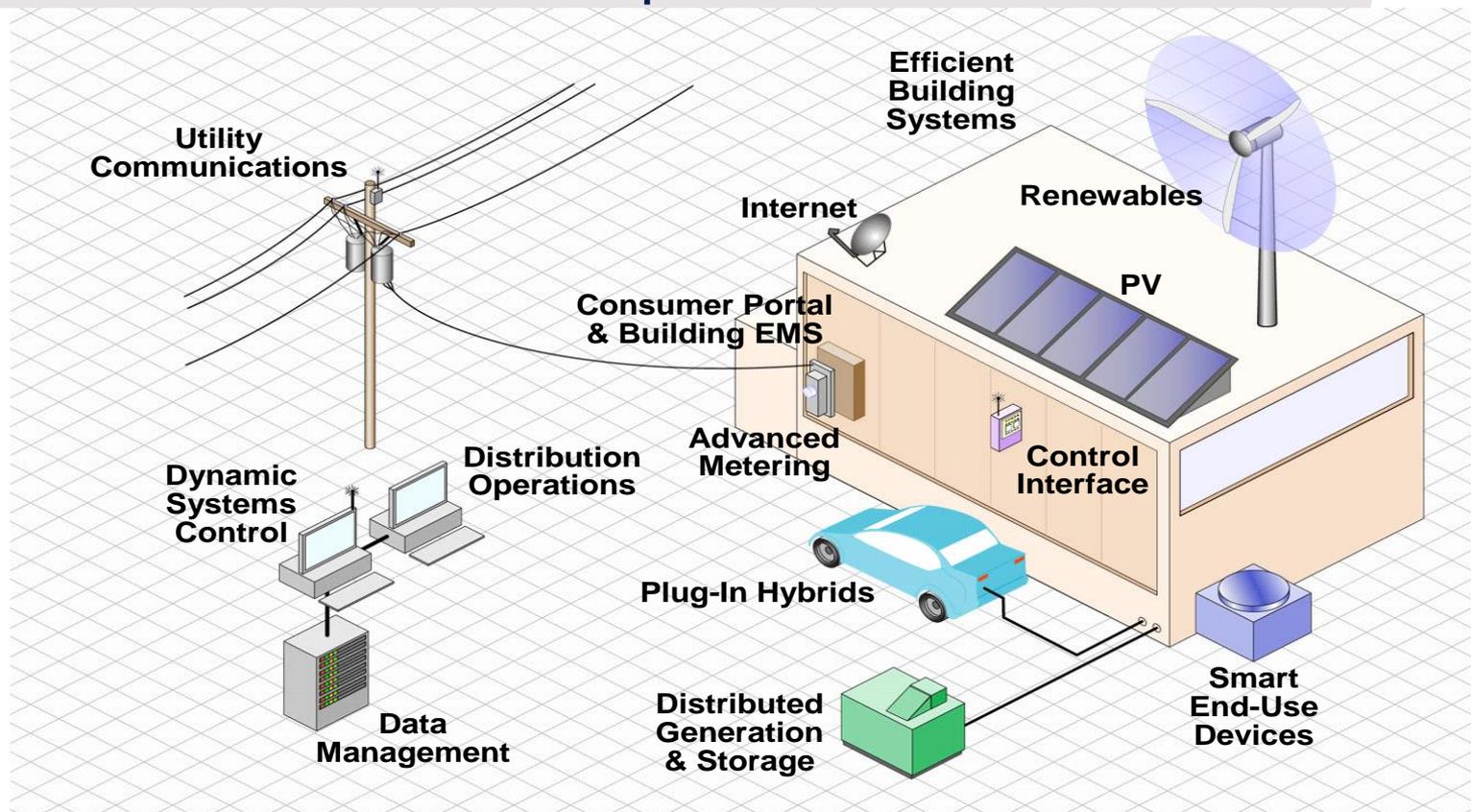


Provides a Framework for Conducting Control Systems Risk Analysis

End Point Threats

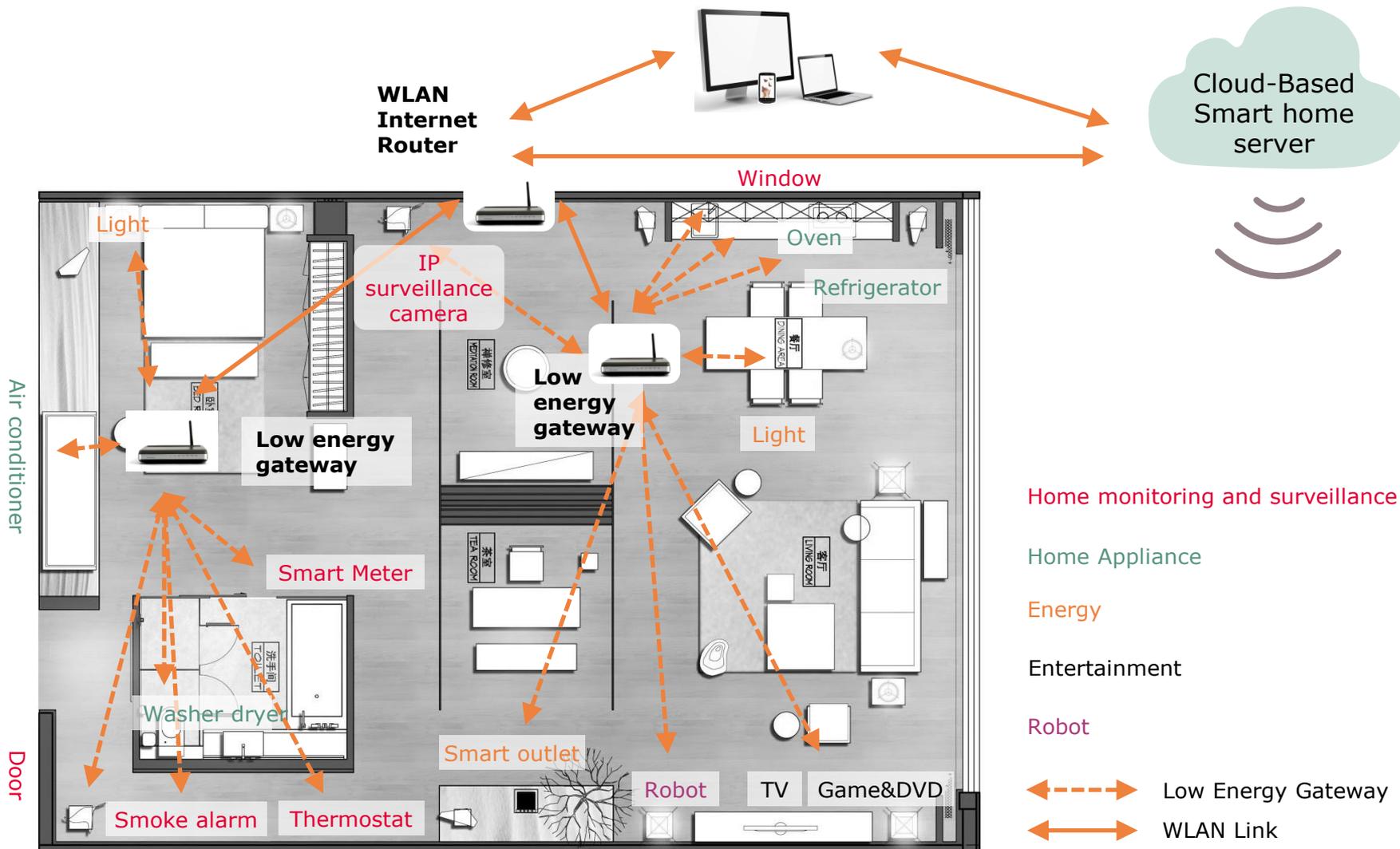
- › “It's possible to sniff and read the data (remotely), replace the data with erroneous data, and we've been able to cause the smart meters themselves to fail by sending it different types of traffic that cause it to reboot or crash” - **Jonathan Pollet, founder of Red Tiger Security** ([CNET](#))
- › “People could exploit security holes in smart meters to not only find out when a consumer is away from home to rob the house, but eventually also to shut off power to elevators and air conditioning units, disrupt city lights, and interfere with other critical systems” - **Fred Cohen, Chief executive of Fred Cohen & Associates, Principal Member of Technical Staff at Sandia National Laboratories**
- › “Networks of smart meters which allow two-way communications and controls between customers and utilities could be hacked to boost or cut power to millions of homes at once. That could crash the grid, all with as little as \$500 worth of equipment and the proper training” - **Security firm IOActive presentation**
- › If an attacker were to install a malicious program on one smart meter, the internal firmware could be made to issue commands that would flash adjacent smart meters until all devices within an area were infected with the malicious firmware. - [IOActive researchers](#) were able to simulate and produce a proof-of-concept worm
- › “Vulnerabilities could arise in the encryption schemes used in smart-grid systems, given that the systems are expected to have a lifespan of 15 to 20 years. Advances in encryption cracking that are likely to occur over that time period would make the encryption obsolete” - [Matthew Carpenter, InGuardian](#)
- › As per **Maxim Rupp, Independent researcher**, Recently it was found that an authentication bypass vulnerabilities in the Eaton Lighting Systems EG2 Web Control application. The attackers could remotely exploit these vulnerabilities “**to perform operations allowing the EG2 connection to configure the system via the Internet rather than by connecting directly into the network.**” - In response, Eaton has produced a **firmware patch** to fix the flaw, but it will also be **removing the EG2 web control functionality** from future devices

End Point Threat: Example AMI

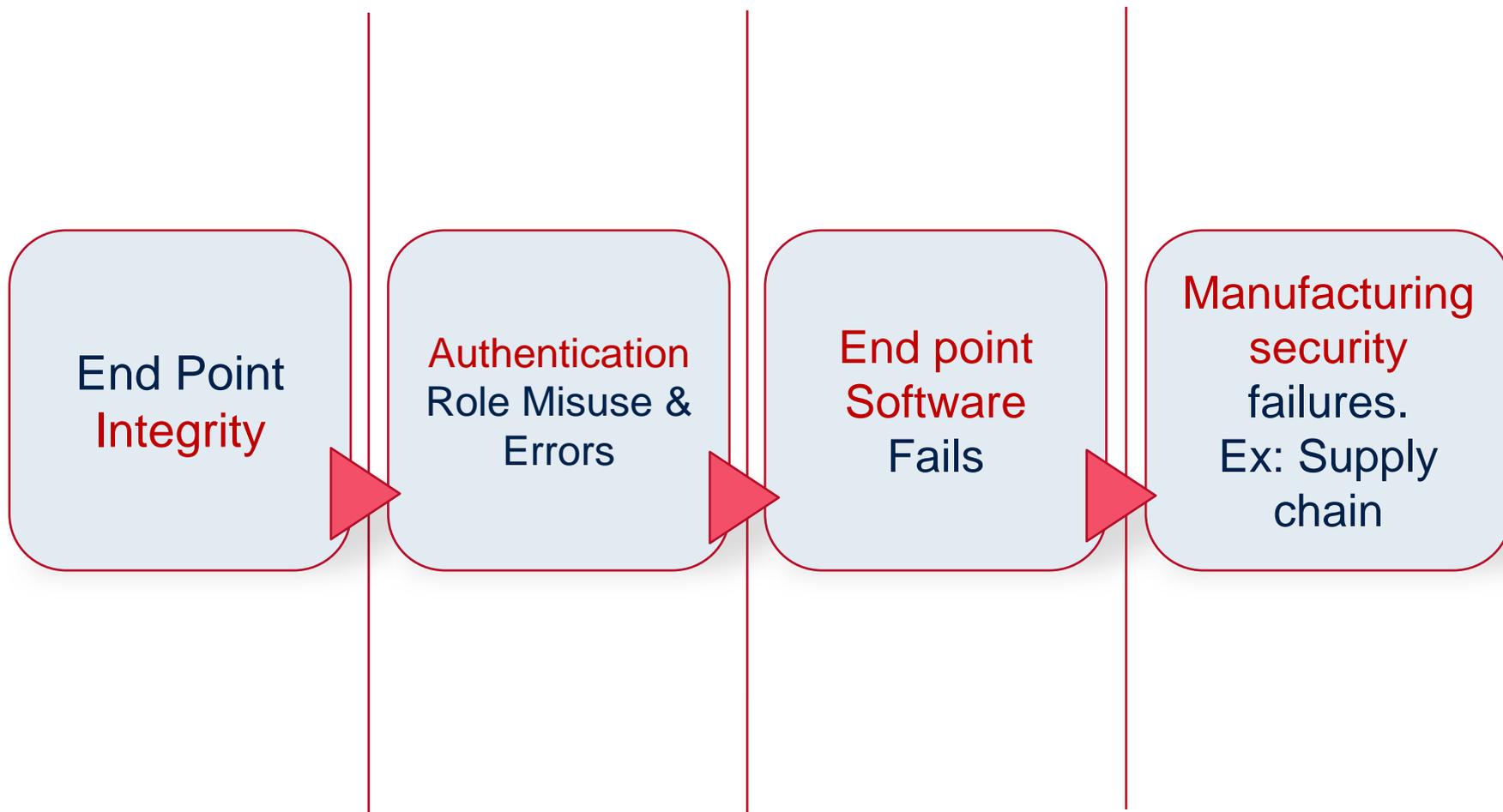


- Hybrid environments (DGS, variety of smart Appliances, IT systems)
- Multiple configurations (not unique) and channels are possible.
- So, One size security policy is problematic
- Results in Widely available attack vectors

Smart Home/Smart Buildings



End Point Security Threats



Compromised End Point Integrity

An attack alters end point operations

Physical and/or remote attacks to hack or clone **unsecure ROM / MCU**

Remote attack that alters functionality and/or communications



Data integrity lost

Malware in the firmware leads to unknown state and privacy invasion

Denial of service attacks threatens grid instability or collapse



Crippling financial losses

Consumer backlash leads to costly **litigation**

Contracts are lost due to corporate image and product reliability

New security regulations force **end points to be manually reset or reinstalled**

Cascading Effect of Compromised Authentication

Certificates Compromised

- Via Authentication escalation (Pkey)

Malware Installation

- Firmware Replaced
- Worm able to spread malware across network
- Software published to remotely install firmware (rootkits)
- Knowledge spreads

End Point Network Compromised

- Denial of Service
- **Data Manipulation**
- User privacy
- Grid Instability

Contingency Plan for Mitigation

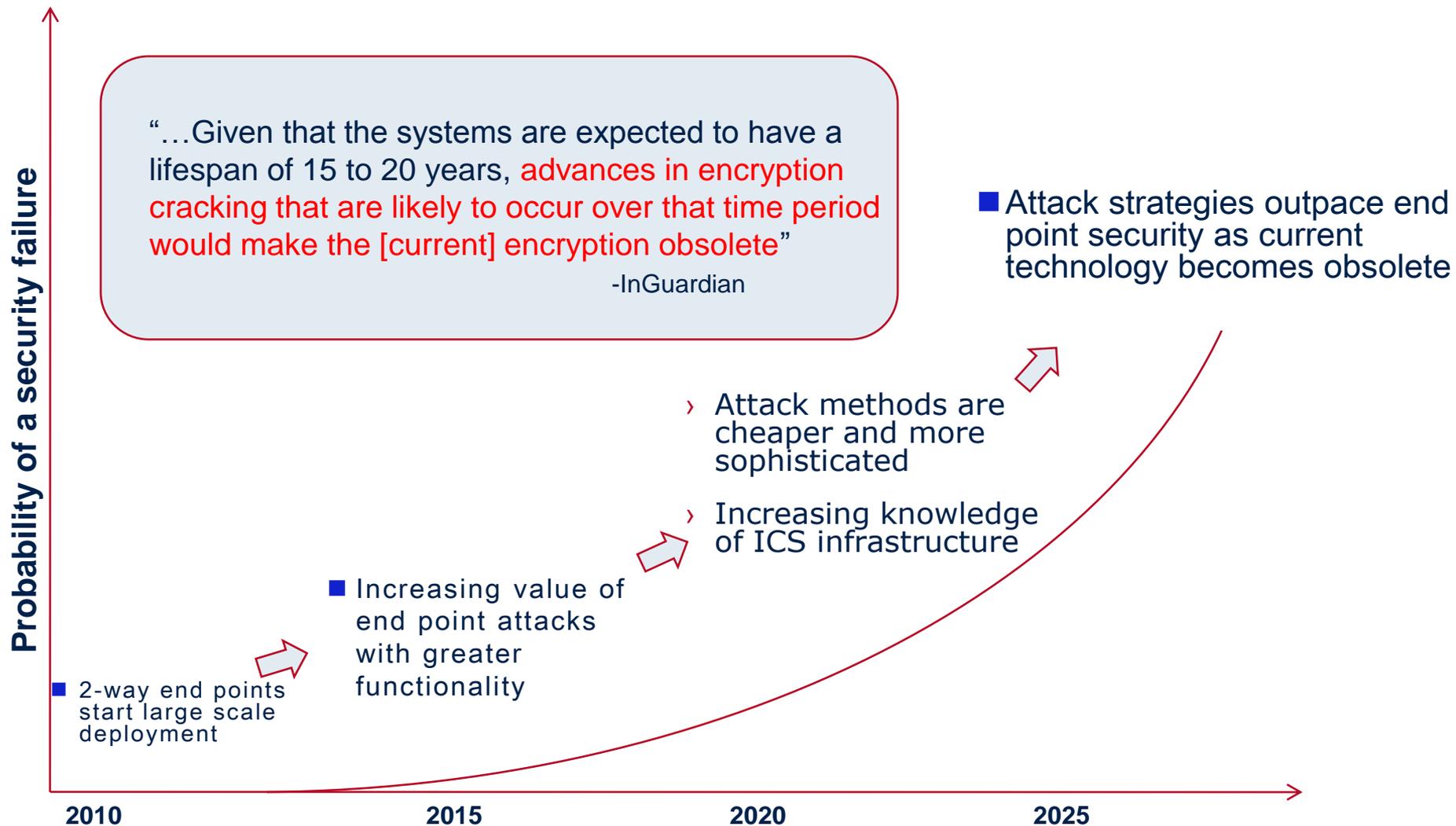
- **Physical** reinstallation of end point equipment and/or firmware
- Customer Reimbursements
- Litigation

Supply Chain Security Considerations

- › “Encryption is **only as robust** as the ability for any encryption based system to keep the **encryption key hidden**”
 - [IEEE Whitepaper: Hardware Security Physical Layer Security in Standard CMOS](#)

- › “...There have been real instances in the broader market with devices that had unauthentic parts or were themselves totally unauthentic (**Counterfeit**)...This situation brings a strong possibility of reliability issues to the Smart Grid... it will take things to a new level of possible impact”
 - NISTIR 7628: Guidelines for Smart Grid Cyber Security, July 2010

Evolving Threats Over Lifetime



Security Threat Summaries

Use Case	end point Integrity	Authentication Escalation	end point Malfunction	Supply Chain Compromise
Threat	OTP ROM spoofed or remote attack compromise communication & functionality	Lost, stolen, or misused authentication credentials used for system attacks	Part malfunctions, reliability concerns over lifetime, parts unable to meet evolving needs	Compromise of Keys and trade secrets during manufacturing
Result	Data integrity lost, malware attack, corporate image damage, loss of end point control	Integrity loss, system failure, corporate image damage, loss of end point control	Loss of functionality & reliability, inability to fulfill market demands	Trade secrets disclosed to public, Malware installed in during manufacturing
Contingency Mitigation Plan	Dispatch of maintenance to each effected compensate for billing or service failures	Dispatch of maintenance to each effected, compensate for billing or service failures	Redesign & reinstallation, Loss of contracts	Supply chain redefinition, redesign, lawsuits against suppliers

Typical End Point Security (Current state)

- › Now the need for a stronger end point security is perceived
 - **Authentication** to ensure remote platforms cannot be controlled by unauthorized entities
 - **Secure storage** to protect critical keys, tariff data, configuration, and audit logging.
 - **Data encryption** to make sure data can be transmitted over untrusted communication channels
 - **Digital signing of messages/commands** to authenticate source and ensure message integrity (man in the middle attacks)
 - **One secret key per end point** is inserted at production stage by the device manufacturer (provisioning). **Sometimes global keys are used!!!**
- › Typically managed through standard IT software tools.
 - Assumes that each node in the chain has not been compromised

However Expert Opinion of Current End Point Security

- › “From a hardware perspective, **cell phones today are more secure than many of the smart meters in deployment...** They deserve nothing less than the best hardware protection available”
 - Karsten Nohl, security researcher

- › “Data encryption and IP security schemes are necessary but, by themselves, **nowhere near sufficient.**”
 - [Andres Carvallo](#), CIO Austin Energy, 2010

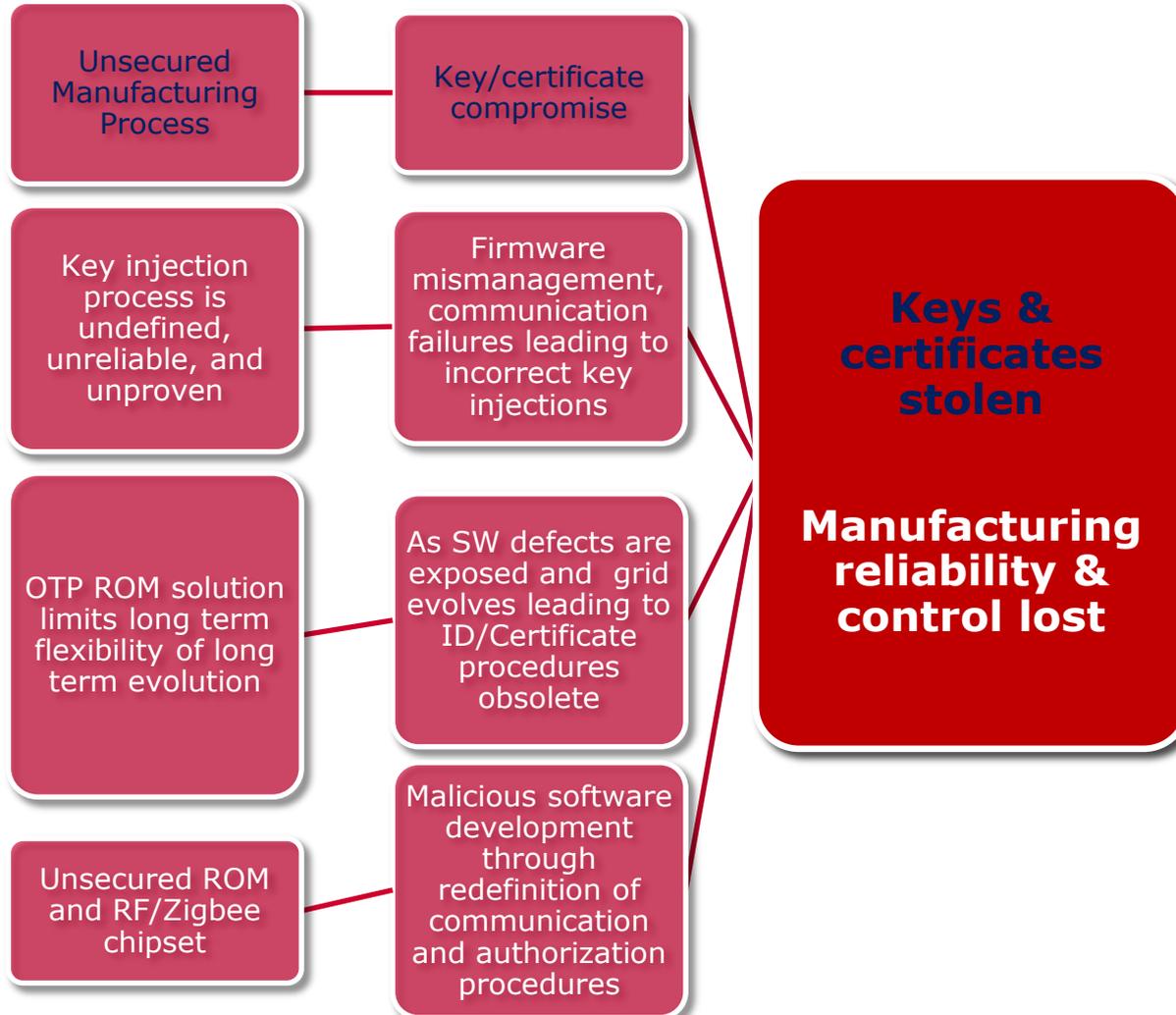
- › “Because the cost of smart meter is low, **there is no significant barrier to entry for hackers interested in attacking AMI.** AMI security, as it currently stands, is insufficient to protect the national power grid from attack by malicious and knowledgeable groups.”
 - INL – April 2009 – Study of Security Attributes of Grid Systems – Current Cyber Security Issues

- › “...Outside the United States **criminals have offered firmware update services** to homeowners, manipulating the software that runs the meter. ”
 - [Jason Larson](#), Security Researcher, Idaho National Laboratory

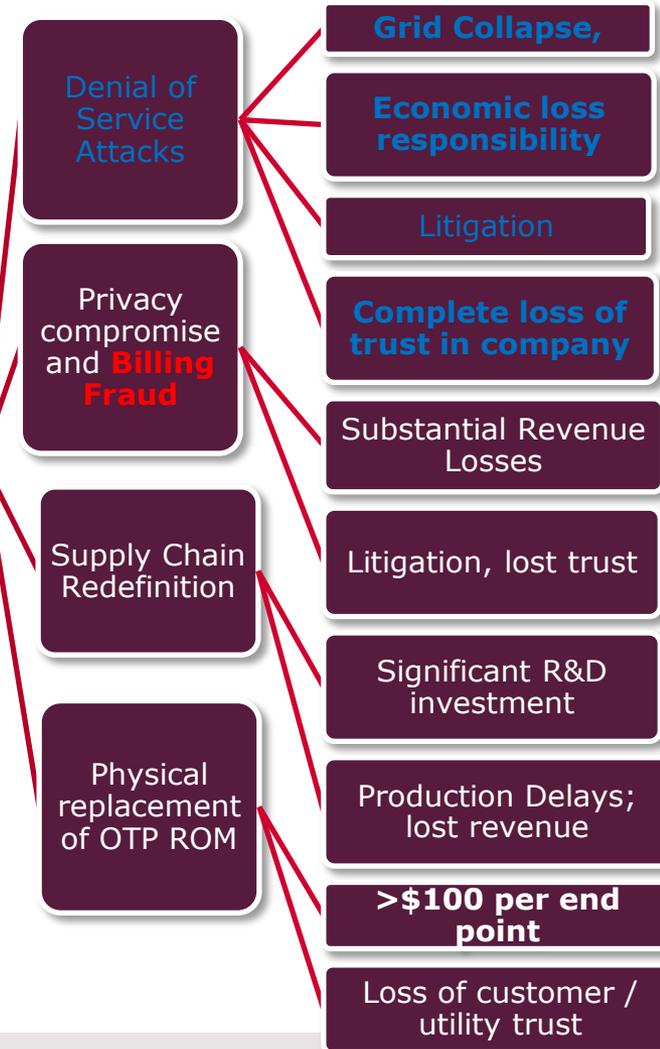
Supply Chain & Key Storage Security Vulnerabilities – One Example



Security Failure Causes



Security Failure Effects



Agenda

1

Security Needs & Priorities

2

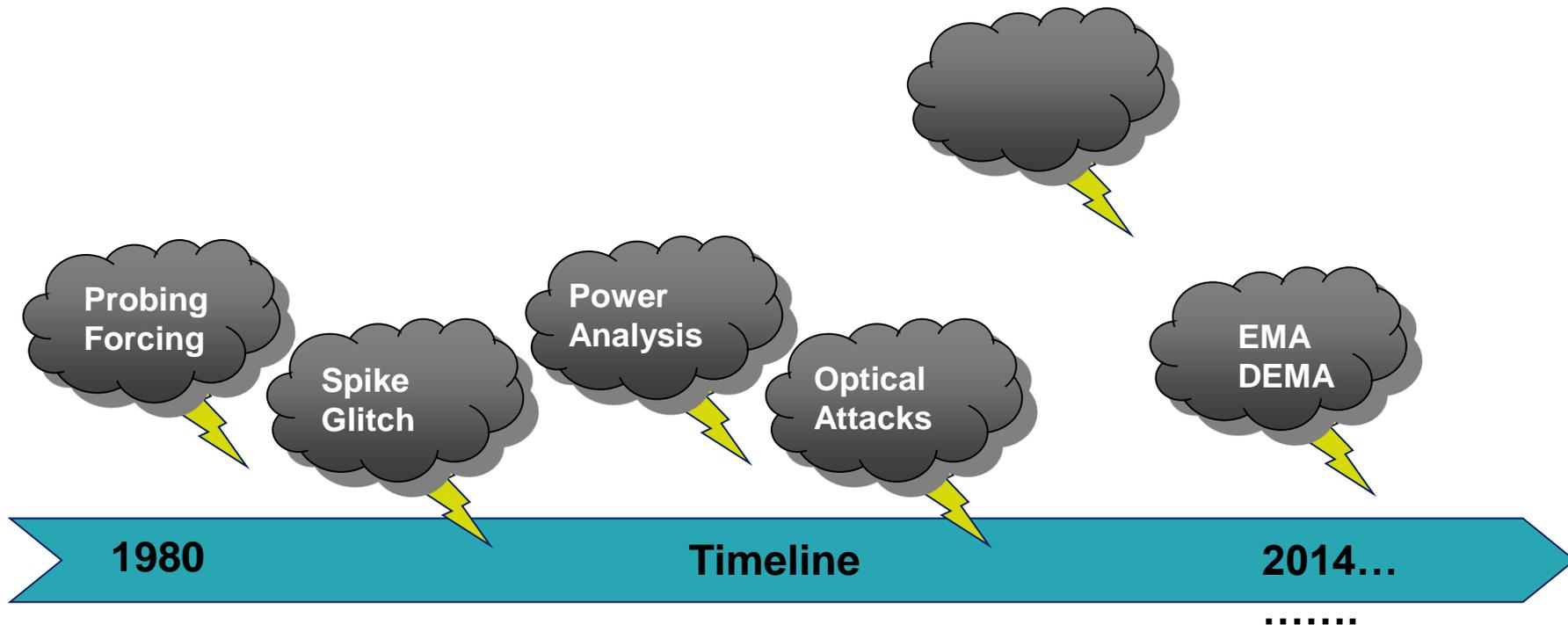
Security threats

3

Hardware Root of Trust (HROt) security: A comprehensive solution

Hardware Security Use cases

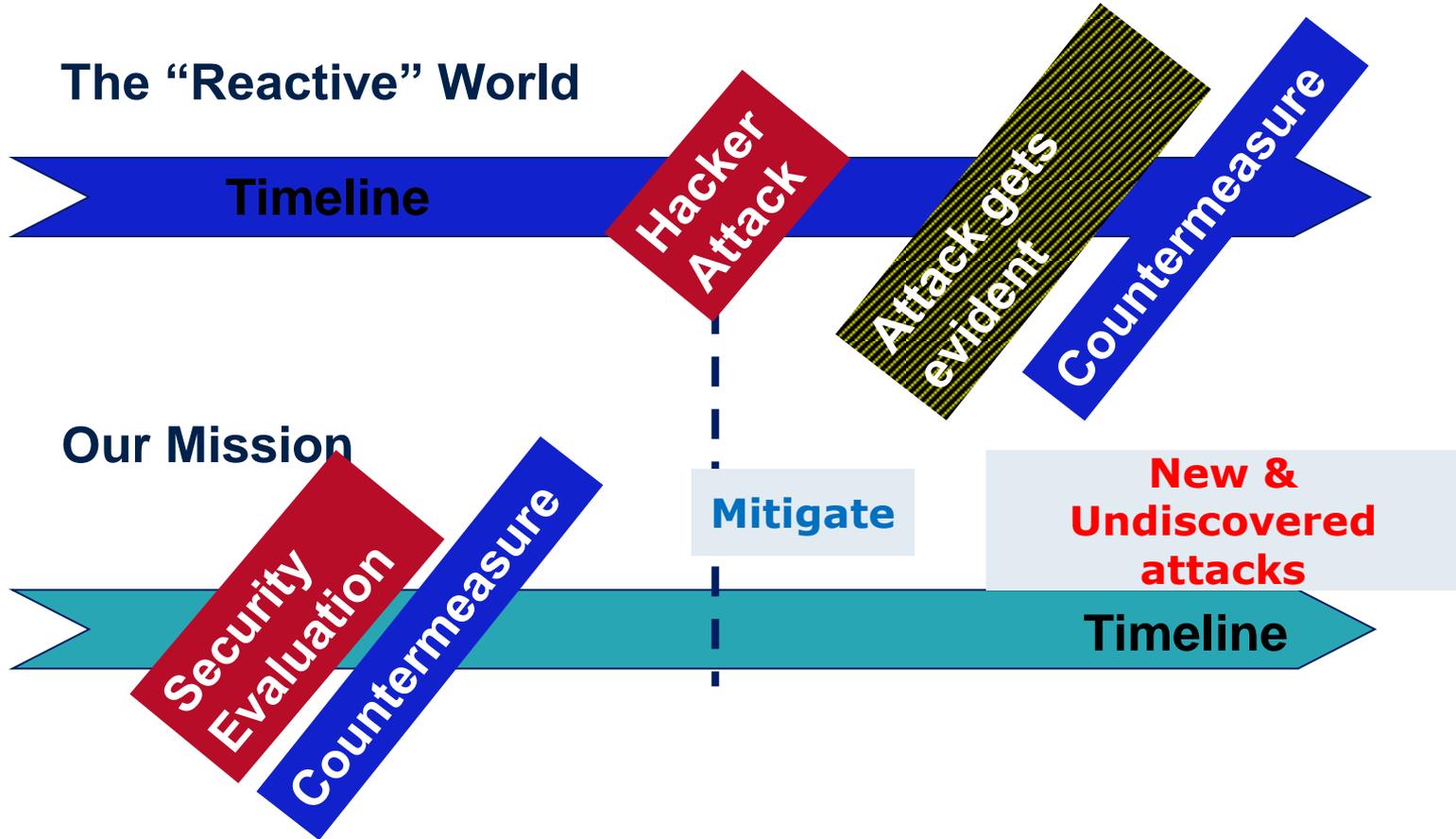
Attacks And Countermeasures An Ongoing Technology Race?



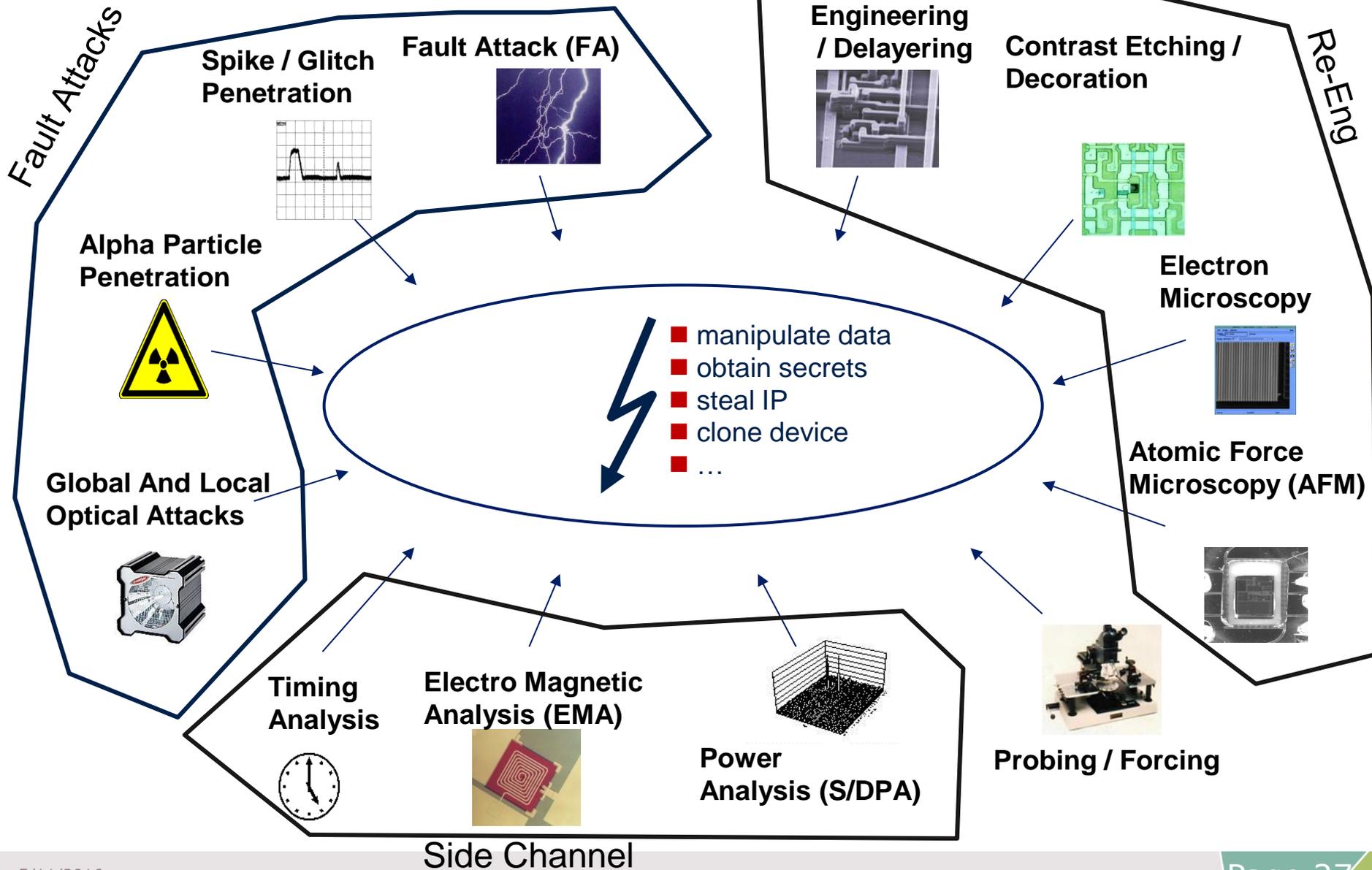
Is "protection against known attacks" enough for you ?

Product Security *Mission*

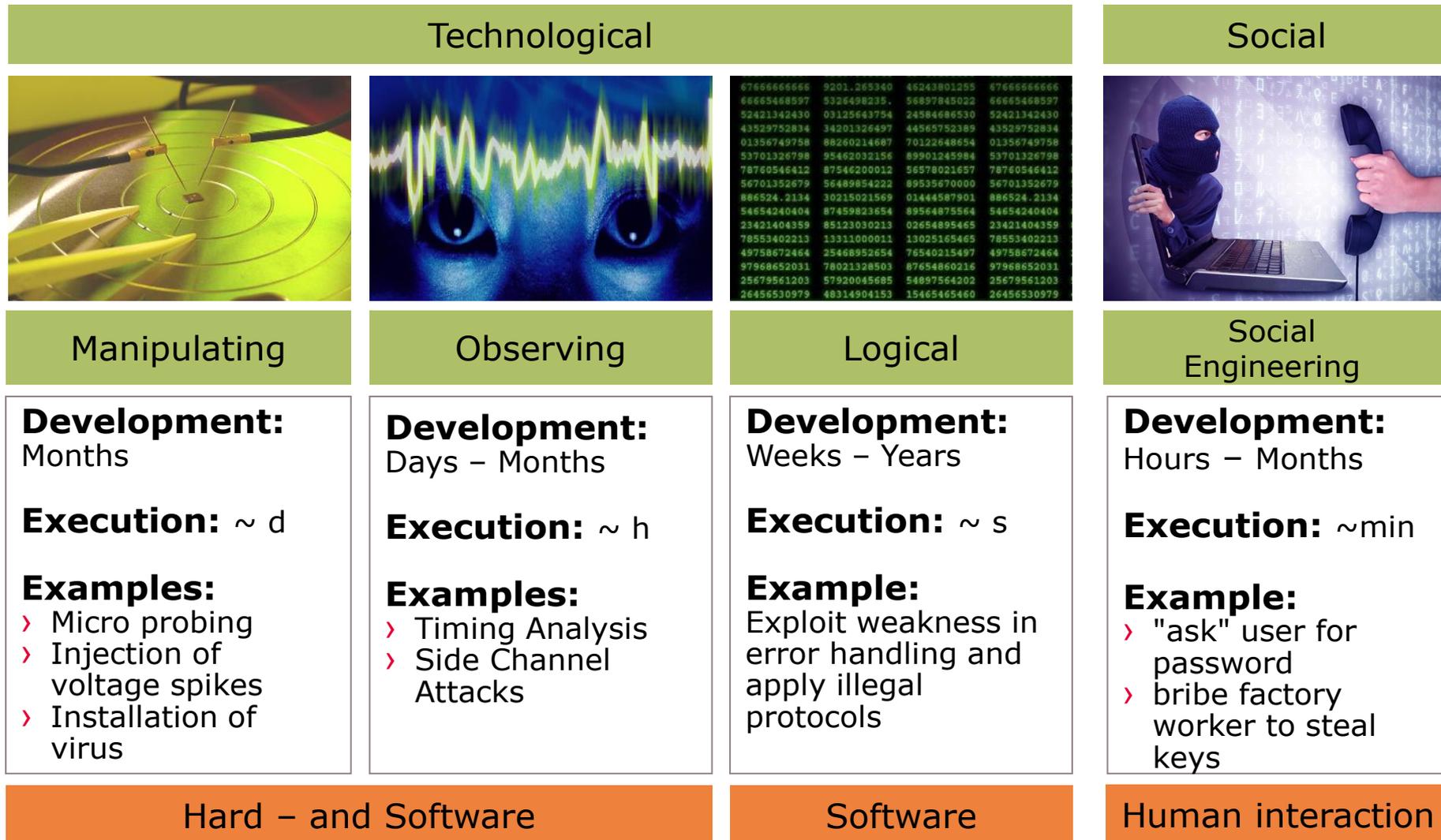
Smart Heads keep the Circle of Knowledge alive



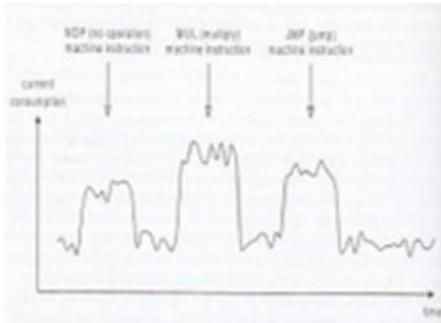
Today's attack methods



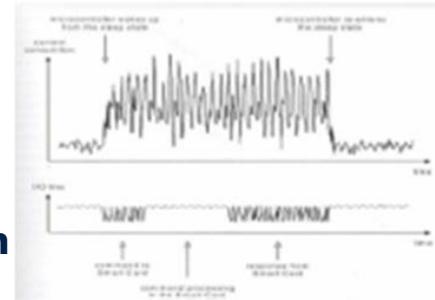
Attacks can occur at various levels



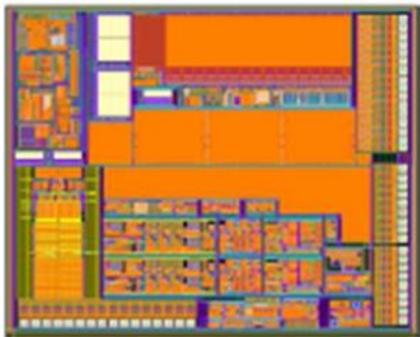
What Makes Secure uC Different From Conventional General Purpose uC



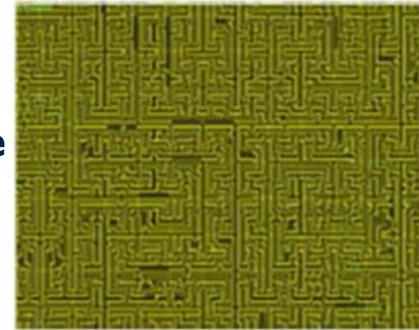
Attacker can read data by monitoring current consumption



- **Current consumption is scrambled by dynamically generated noise so that Data cannot be extracted by current monitoring.**

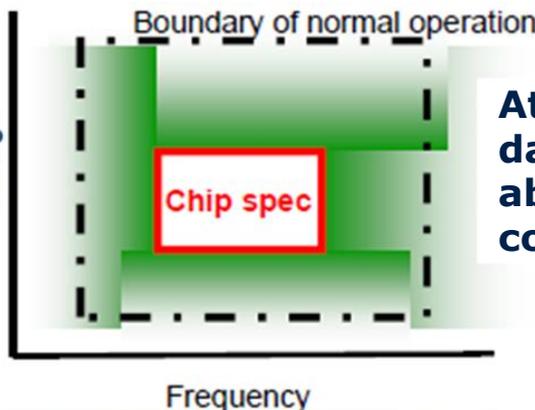


Attacker can capture data by probing metal patterns

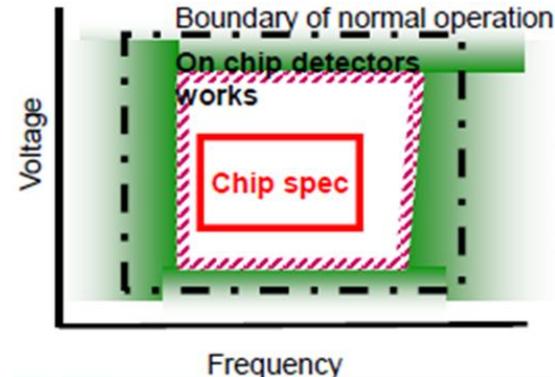


Chip is protected with:

- "Active" metal shield to prevent data capture
- Randomized layout



Attacker can read data under abnormal conditions

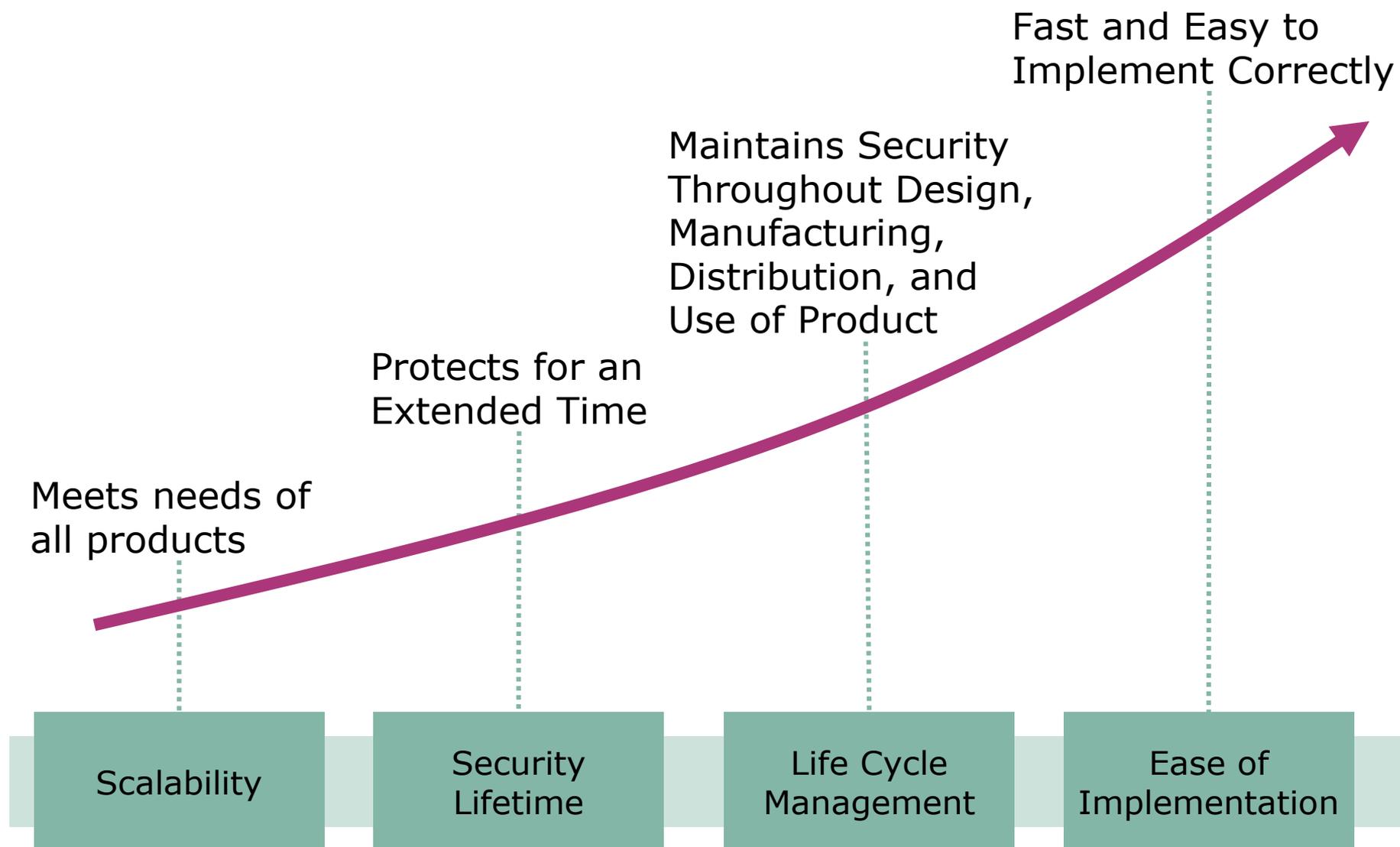


On chip sensors force to stop Operation under Abnormal conditions

Why Secure Micro

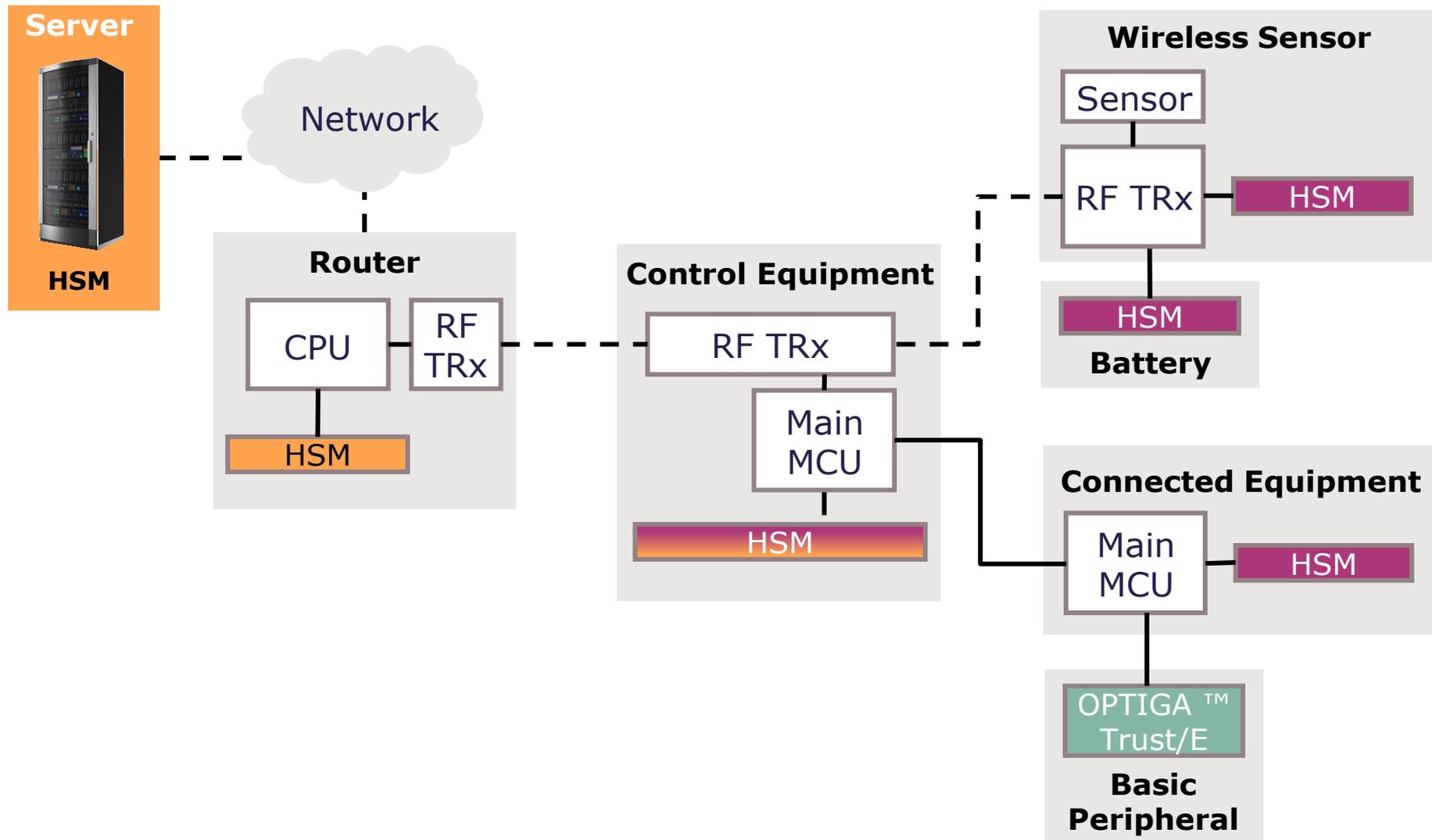
- › **Protected memory** (NVM/RAM/Cache) to avoid snooping and reverse engineering
- › **Secure Code fetching** & Execution (Integrity checks)
- › Use of Code and data **signatures**, built during compilation and stored and then **verified** during execution.
- › **Dynamically encrypted** calculation in the CPU.
- › **Limited** interface lines
- › **No JTAG** debugging
- ›

Key Considerations for a Security Solution

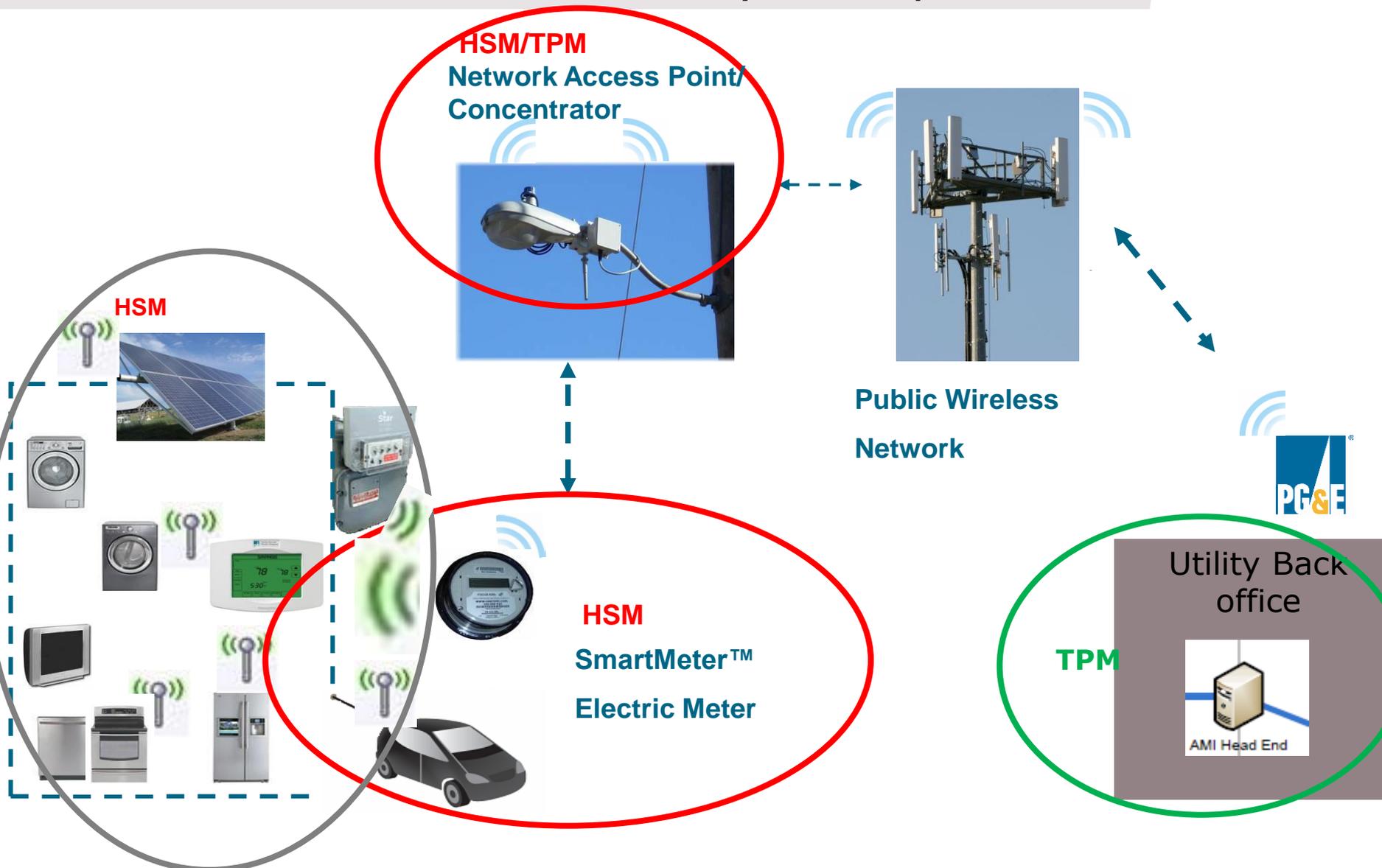


Key Considerations for a Security Solution

Scalability : Infrastructure Control Systems



SmartGrid : Scalable Security example



Key Considerations for a Security Solution-Lifetime



- › **Attack cost, time, and difficulty constantly reducing**
- › Need to Protect against **tomorrow's attacks**, not just against what happened yesterday
- › Instead of **Attack** → **Analyze** → **build counter measure** → **Mitigate** approach. Need to design and build robust secure devices & system which addresses the **effect of attack and resilient to vulnerabilities for an extended period**
- › **Hardware-based security in complement with software security with** multiple layers of protection **extends security lifetime**
- › **For Example, TPM deployed in field for last 10-15 years are still working with out any need for updates**
- › So, need to use **trusted source** for security solutions. What is Trusted Source?

Scalability

Security
Lifetime

Life Cycle
Management

Ease of
Implementation

Key Considerations for a Security Solution: Life Cycle Management & Secure Supply chain

Corporate security rules (e.g. communication encryption, IT Security, Data Protection)

State-of-the-art security control center (e.g. about 8000 sensors in development center)

Design & Development

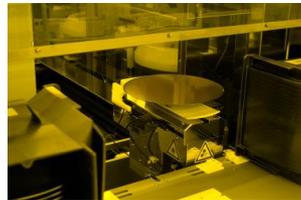
- > Security **certified design environment**
- > **Internal Blue and Red Team**
- > Security **infrastructure** (biometric gate access, monitoring system)
- > Need-to-know principle, strict IT security **regulations**



Scalability

Production

- > High security **production environment**
- > Processes fully automated
- > Production facilities under strict review by **security audits**



Security Lifetime

Evaluation & Certification

- > **Evaluation** by 3rd party **Security test labs**
- > All major certification schemes: **Common Criteria, EMVCo, ZKA, FIPS, VISA, Amex, MasterCard, ITSEC**
- > More than 230 product security certifications



Life Cycle Management

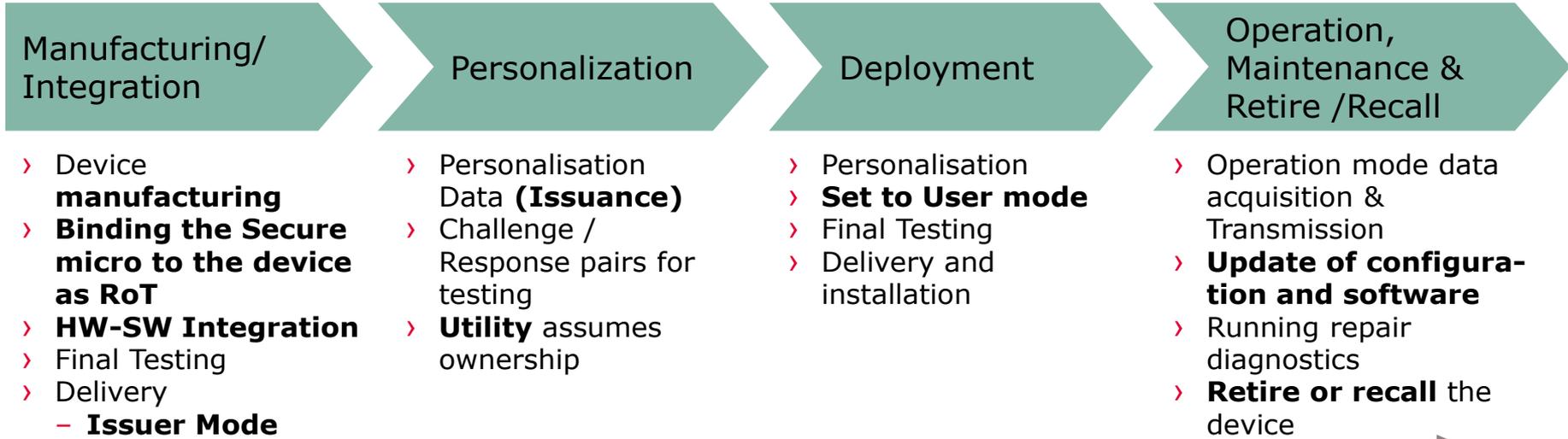
Logistics

- > Protected safety areas for CCS products in DCUs
- > **Secured logistics**
- > **Protected with Transport keys**
- > **Transport partners audited by Infineon**



Ease of Implementation

Extend LCM to Trusted Device Manufacturing by Crypto Methods



Locked and protected with Transport Keys



Scalability

Security Lifetime

Life Cycle Management

Ease of Implementation

1) Life Cycle Management

- Secure key management to introduce a **root of trust very early into the product lifecycle**. This has the advantage of protecting system components during manufacturing and programming. Secure key management also enables lifecycle management such as subsequent initialization, integrity checking, upgrading, and disablement of any System Client or end point.
- Throughout the entire life cycle of all system components.

2) PKI – key management

- HROt improves, enforces and simplifies existing solutions for controlled distribution of chips/devices/systems and IP using **asymmetrical PKI infrastructures while enabling symmetrical cryptography on the end point platform**.

3) Operational Mode functionality

- HROt enables custom use cases in Operational (deployed) mode adding high level security functionality to customer's applications. (Ex: **Sign/Verify blob of data or on the fly Generate Key pair/certs**)

4) Anti-Tampering

- The HROt improves and expands Anti-Tampering features of existing infrastructure, and increases **trustworthiness** of the entire system

Common Defenses to protect the Grid End Points

Common Defenses



Authentication



Key Generation and Management



Lifecycle Management



Boot Protection Platform Integrity



Audit



Stored Data Protection



Secure Communications



Secure Updates

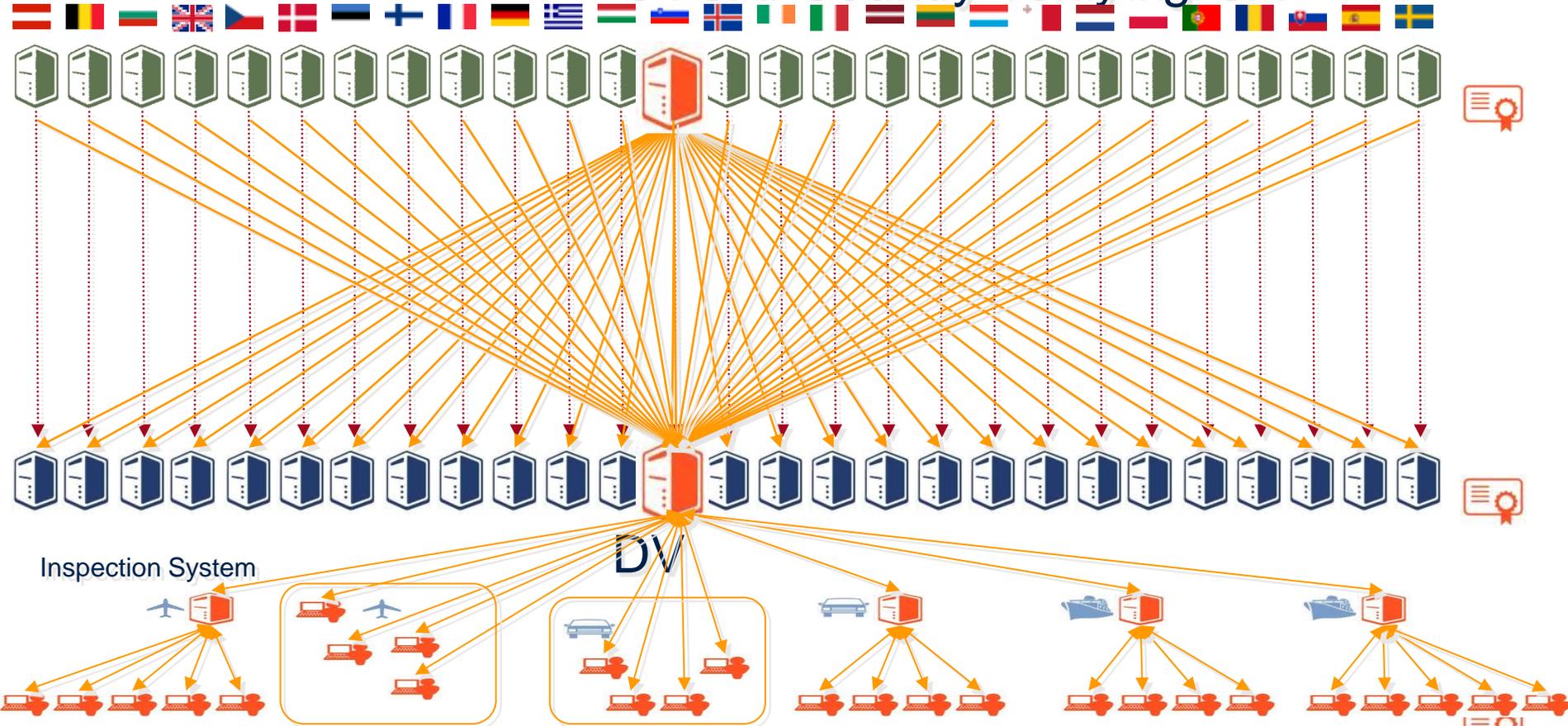
Options for Grid Security solutions



	Software		Hardware		
	Main CPU	Software	Main CPU	Software	Hardware
Crypto functionality	✓		✓		
Strong isolation	STOP		✓		
Security certified	STOP		✓		
Tamper resistant	STOP		✓		
Manufactured by security certified processes	STOP		✓		
Resistant against reverse engineering	STOP		✓		

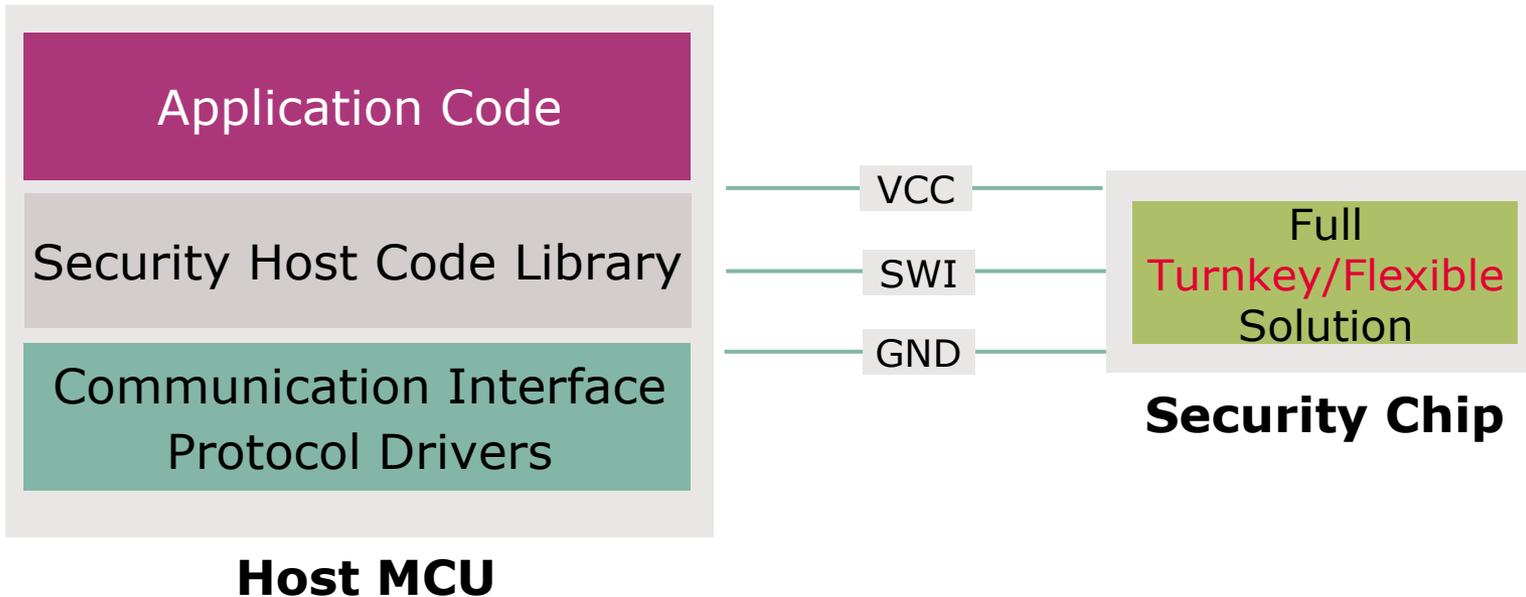
Reuse Example of interoperability of deployed ePassport read/write EAC Protocol- EU 27 Countries

CVCA: Country verifying CA



- Operational in 27 countries, 210 millions issued in circulation embedded with HRoT secure micro controller
- 10s of thousands of authorized inspection systems (IS) with access rights given from issuing country
- Mechanism of revocation
- Multiple vendors
- All interoperable
- Security certified.

Key Considerations for a Security Solution- Ease of implementation



- › Need to provide Security IC Code **Pre-loaded with Secure OS & Apps**
- › Need to provide Host crypto **Library and protocol drivers in C for customers to port to any Host MCU without any security expertise and minimum testing and delta qualification**



Scalable Hardware Security Solutions

Low level end point Peripherals



- > **Secure Memory** with **ECC State machine**
- > One-Way **ECC 163** Authentication and MAC
- > Single Wire Interface **448 B** Memory
- > Full Turnkey **fixed** Solution
- > Host Code Provided

Mid level End point Peripherals & Consumables



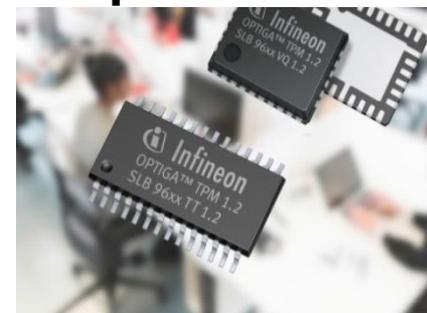
- > Secure Micro HW with **Crypto engine**
- > One-Way **ECC 256** Authentication
- > SHA256 support for MAC
- > **I2C Interface (400KB) & 10KB Memory**
- > Extended Temp Range -40 to +85C
- > **Certificate Exchange/ PKI support for customer domain**
- > Full Turnkey **fixed** Solution
- > Host Code Provided

High level end Flexible for Embedded systems



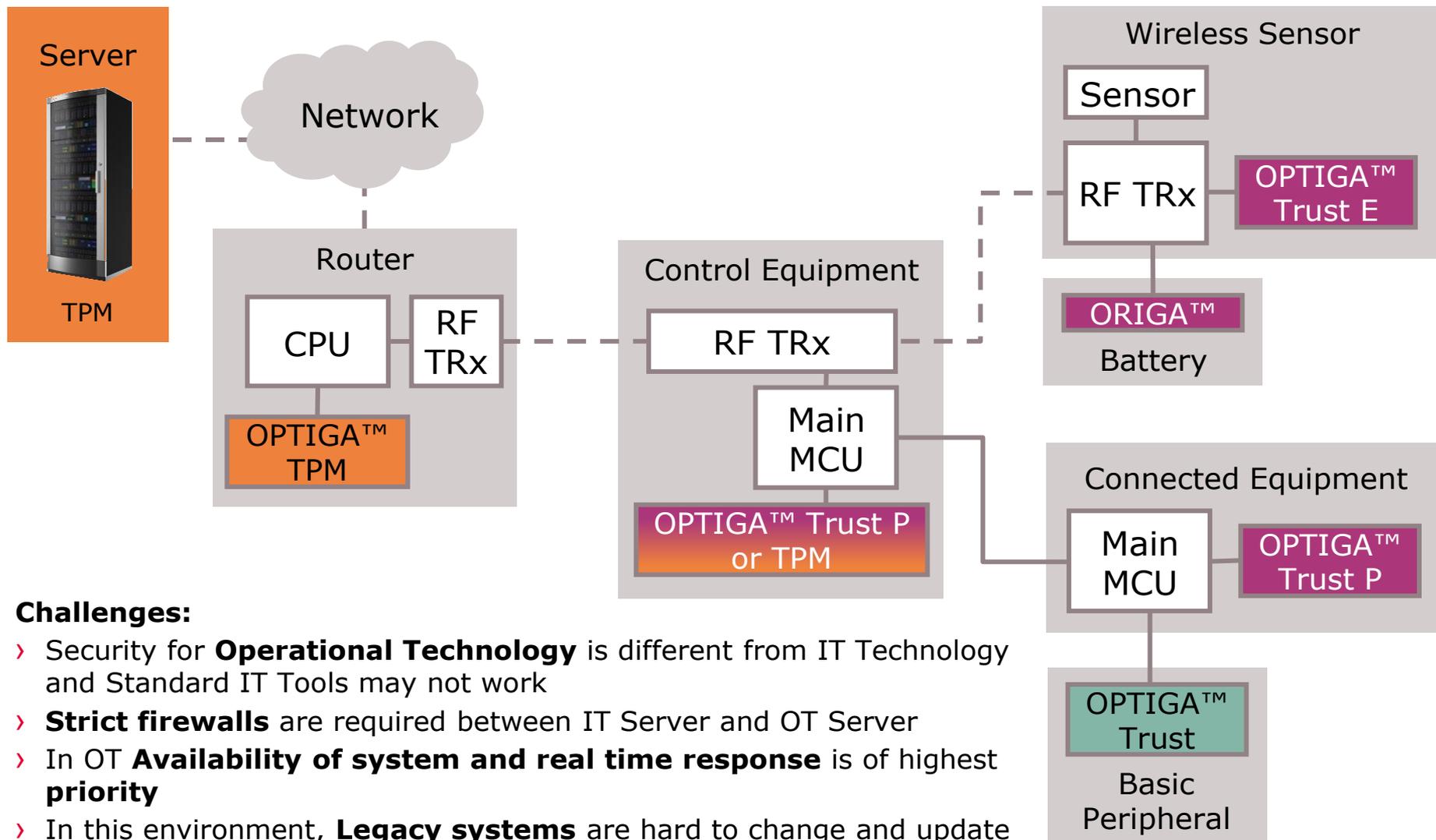
- > CC **EAL5+** Certified
- > Symmetric/Asymmetric Crypto Engine (AES/ RSA,ECC) & True RNG
- > Flexible solution(JAVA CARD OS with Exposed API)
- > **ISO Serial interface (512KB) & 150kB User Memory**
- > **Reference Crypto Applets and Host crypto Library (C code)** to support Functions for: Mutual authentication, secure updates, key generation, key exchange, Secure messaging, ...

High level computing platforms



- > CC **EAL4+** Certified
- > Symmetric/Asymmetric crypto and SHA Engine
- > **TCG v1.2 compliant** Full Turnkey fixed Solution on Chip
- > **I2C, SPI (Nonx86) & LPC (x86) interface.** 6K memory
- > Extended Temp. Range **-40 to 85C**
- > **Industry-standard Host Code Available for high end host micro with Std. OS (Linux, Windows)**
- > Functions for: measured boot, system integrity, key storage, key Gen., ...

Solution: Critical Infrastructure Systems



Challenges:

- › Security for **Operational Technology** is different from IT Technology and Standard IT Tools may not work
- › **Strict firewalls** are required between IT Server and OT Server
- › In OT **Availability of system and real time response** is of highest **priority**
- › In this environment, **Legacy systems** are hard to change and update

Agenda

1

Security Needs & Priorities

2

Security threats

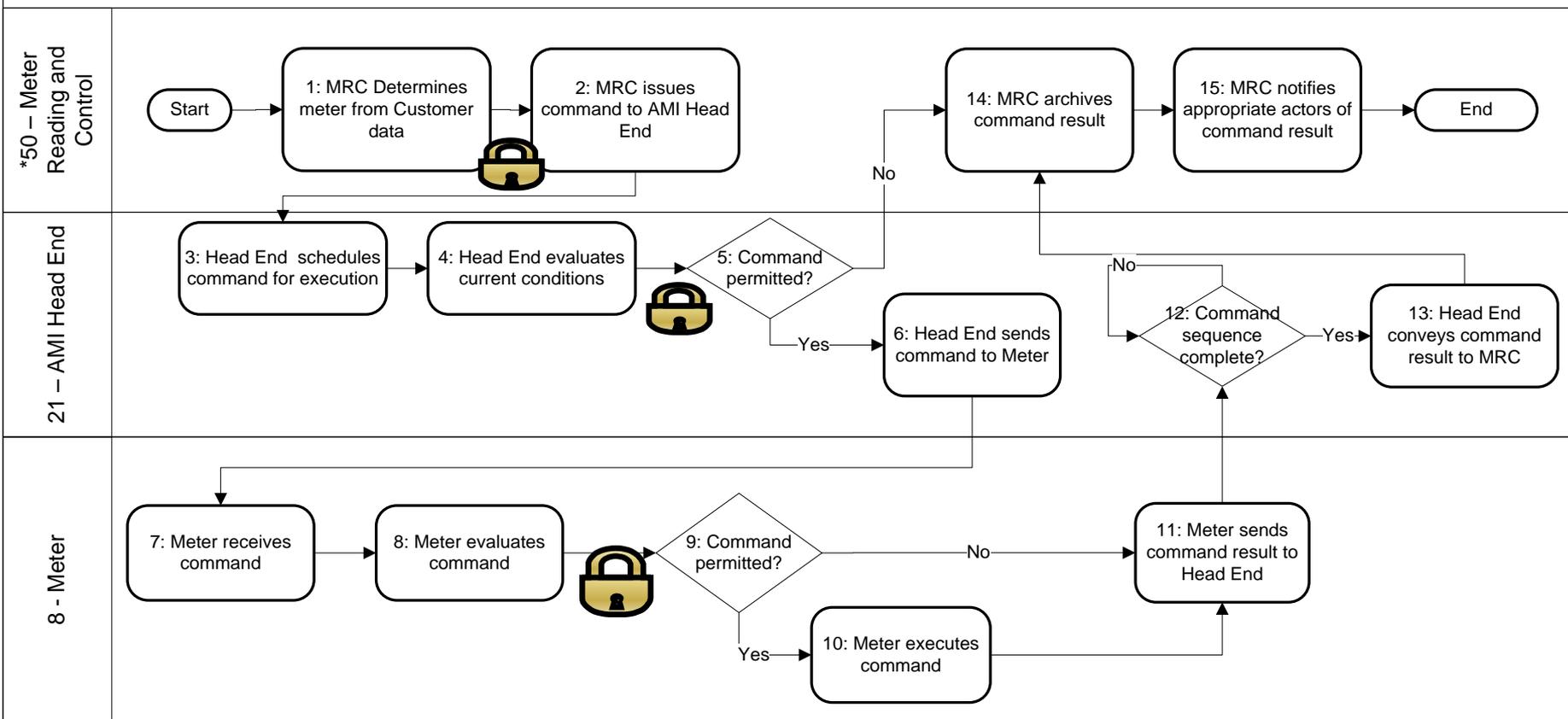
3

Hardware Root of Trust (HROt) security: A comprehensive solution

Hardware Security Use cases

Use Case :Remote Secure Operational command to End devices in field

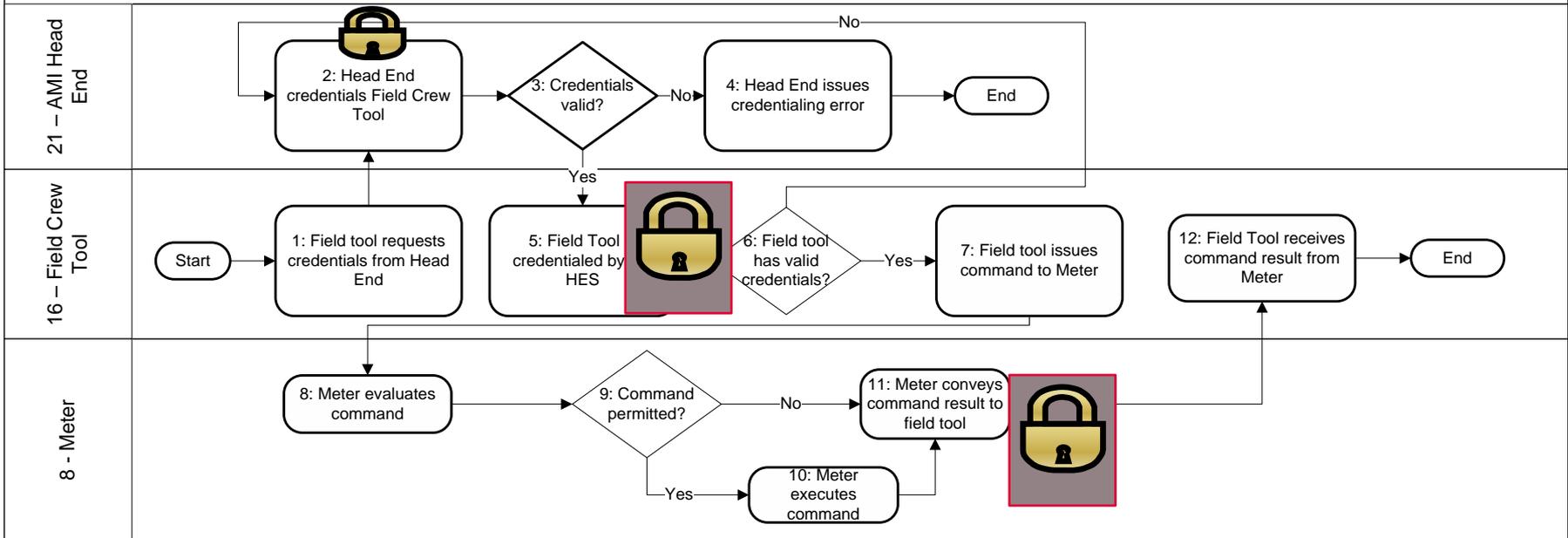
1: Utility Sends Operational Command to the Meter



HSM

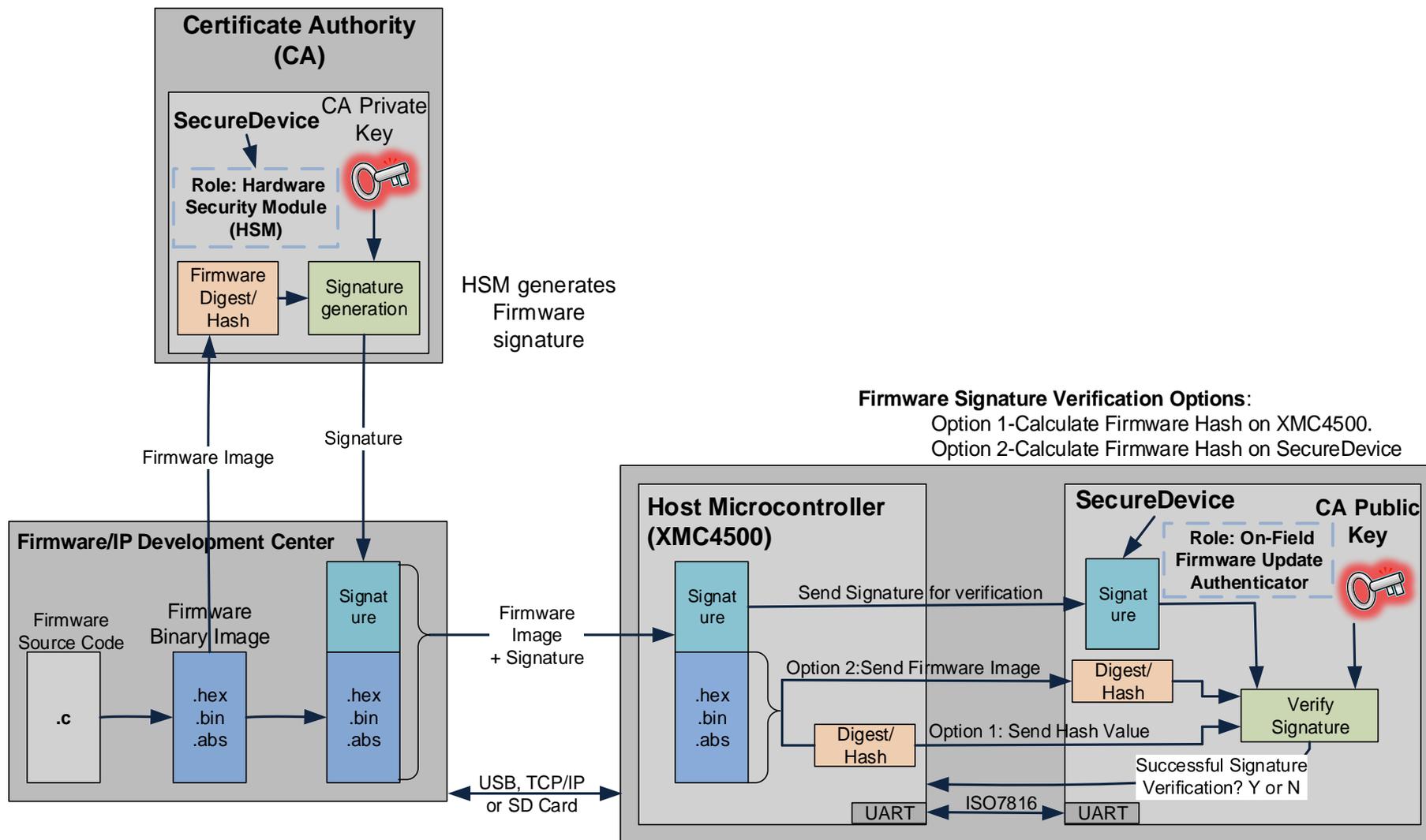
Use Case Example – Field Tool Sends Instruction to the end device

6: Field Tool Sends Instruction to the Meter



HSM

Firmware Signature Verification





Part of your life. Part of tomorrow.



Hardware Security Module as a Trust Anchor for Smart Grid devices

This document is to provide detailed Information on how Hardware Cryptographic modules can protect the various devices connected to the Smart Grid Network and increase the level of security of the grid and protect from Cyber attacks. This covers the following:

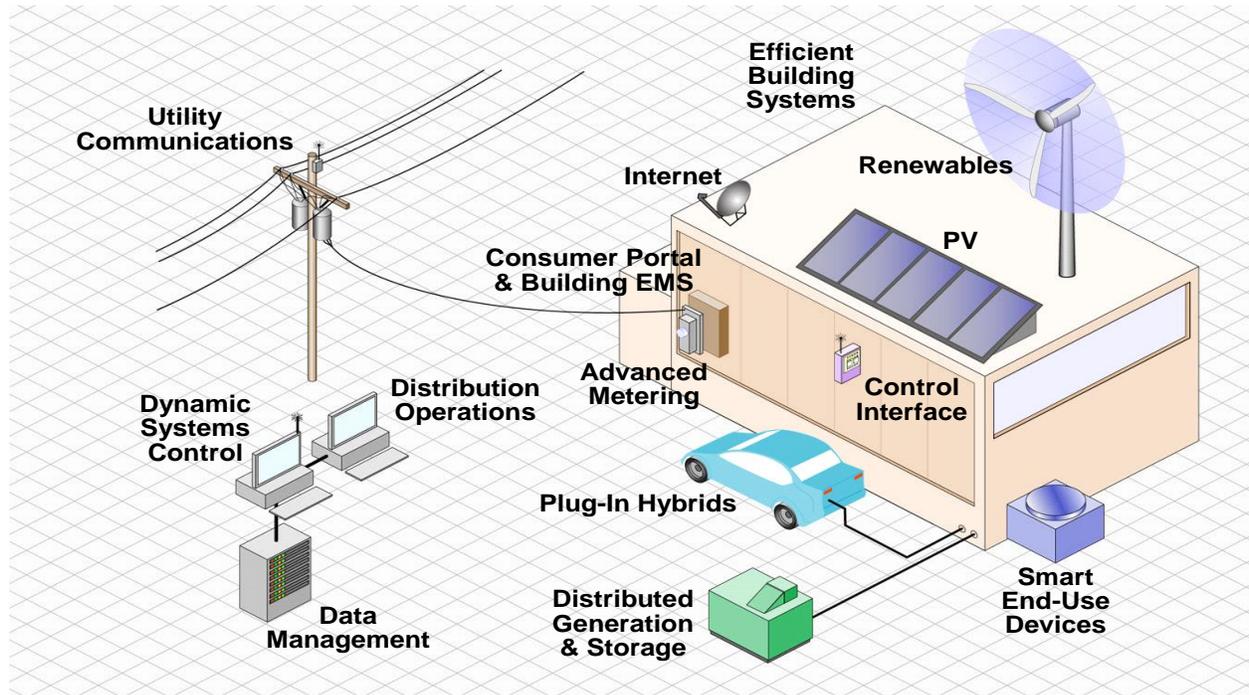
- Cryptographic Hardware
- Various Attacks
- Secure Microcontroller Use cases for Smart Grid devices
- Security coprocessor : Required Features

CRYPTOGRAPHIC HARDWARE

Security processors are vastly utilized for protected processing and storage of data in many of today's applications. Security devices that are situated in the field are facing more and more threats, which in turn grow more dangerous from day to day. Meanwhile, new applications like two way secure communicable smart meter and other end devices, electronic passports and national identification cards, demand increased security lifetimes. In a recent study conducted by one of the national lab has identified various threats to the smart Grid Control and IT network. Trends impacting security are:

- Open Protocols: Open industry standard protocols are replacing vendor-specific proprietary communication protocols
- Common Operating Systems : Standardized computer platforms increasingly used to support control system applications
- Interconnected to Other Systems: Connections with enterprise networks to obtain productivity improvements and information sharing
- Reliance on External Communications: Increasing use of public telecommunication systems, the Internet, and wireless for control system communications
- Increased Capability of Field Equipment: "Smart" sensors and controls with enhanced capability and functionality.
- Pressure against recognizing security as critical for automation system development, deployment, and management
- Limited security management policies and procedures for PCS and automation systems
- Wide availability of conventional information technology (IT) hardware and software/operating systems
- Desire for improved operational and process efficiency
- Lack of business case for PCS security investment
 - Little concrete data on automation system attacks
 - Legal precedent not well-established
 - Automation products that have limited intrinsic security capabilities
 - No contractual requirements for security
- Security is 5-10 years behind typical IT systems

Client side threats:



- Increasing interconnectedness at all levels
- Adoption of standardized technologies with known vulnerabilities
- Connectivity of control systems to other networks
- Insecure connections
- Widespread availability of technical information about control systems Increasing reliance on automation

Considering the above threat to the end devices at client side we need to Change some of the Availability, Confidentiality and Integrity for Logical interface categories in NISTIR. The end device such as Main meter @ home is not just electricity measuring meter. As smart grid will involve distributed Energy resources (Solar, PHEV wind energy), Energy will be fed back to the grid. In this scenario, Meter needs to address reverse energy flow control and data. This increases the end devices and its interfaces availability, Integrity and confidentiality levels. Hardware security Module (HSM) are high end security micro controllers acts as a root of trust for End-to-End authentication with secure Storage capability. For our Smart Grid environment, We can call this as “**Secure Meter Element (SME)**”.

Four Pillars of Security Meter Element at End point are:

1) Life Cycle Management

- Secure key management to introduce a root of trust very early into the product lifecycle. This has the advantage of protecting Grid system components during manufacturing and programming. Secure key management also enables lifecycle management such as subsequent initialization, integrity checking, upgrading, and disablement of any System Client.
- Throughout the entire life cycle of all system components.

2) PKI – key management

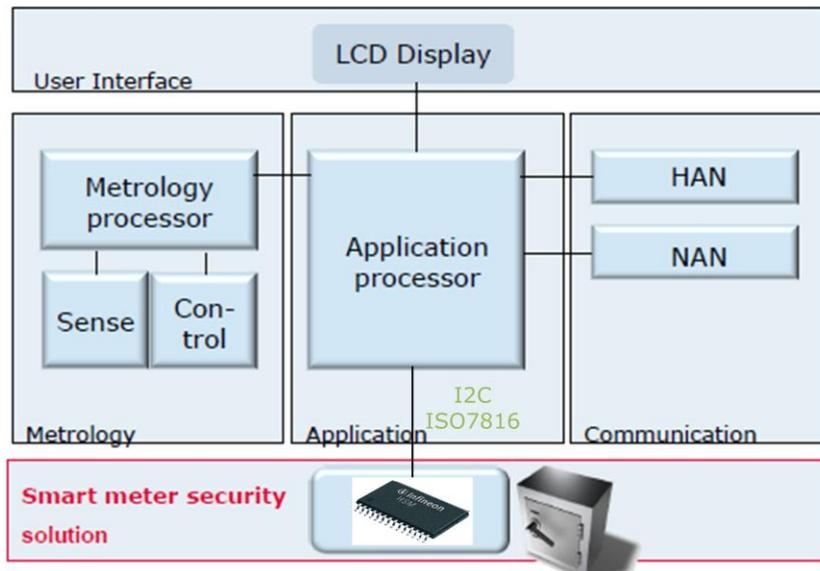
- Secure Meter Element improves, enforces and simplifies existing solutions for controlled distribution of chips/devices/systems and IP using asymmetrical PKI infrastructures.

3) Operational Mode

- Secure Meter Element enables custom use cases in Operational (deployed) mode adding high level security to customer's applications.

4) Anti-Tampering (Trustworthiness)

- The Secure Meter Element improves and expands Anti-Tampering features of existing infrastructure, and increases trustworthiness of entire system

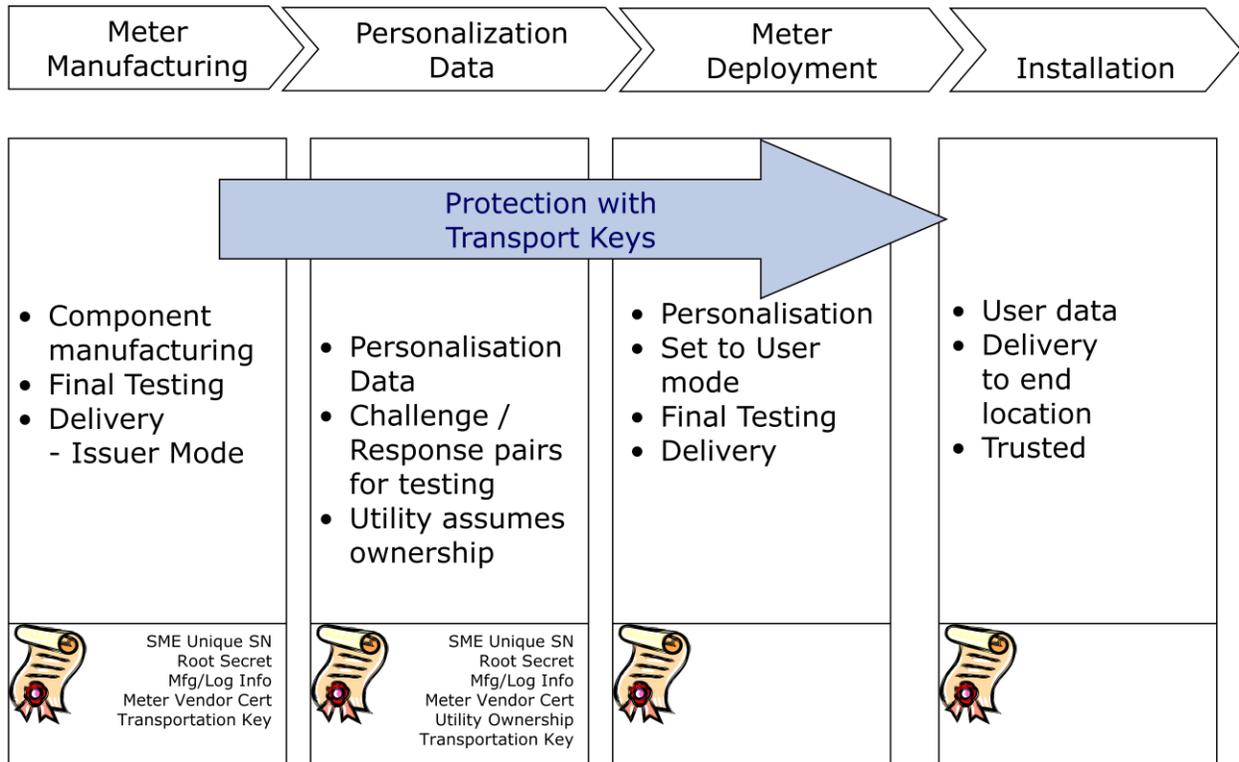


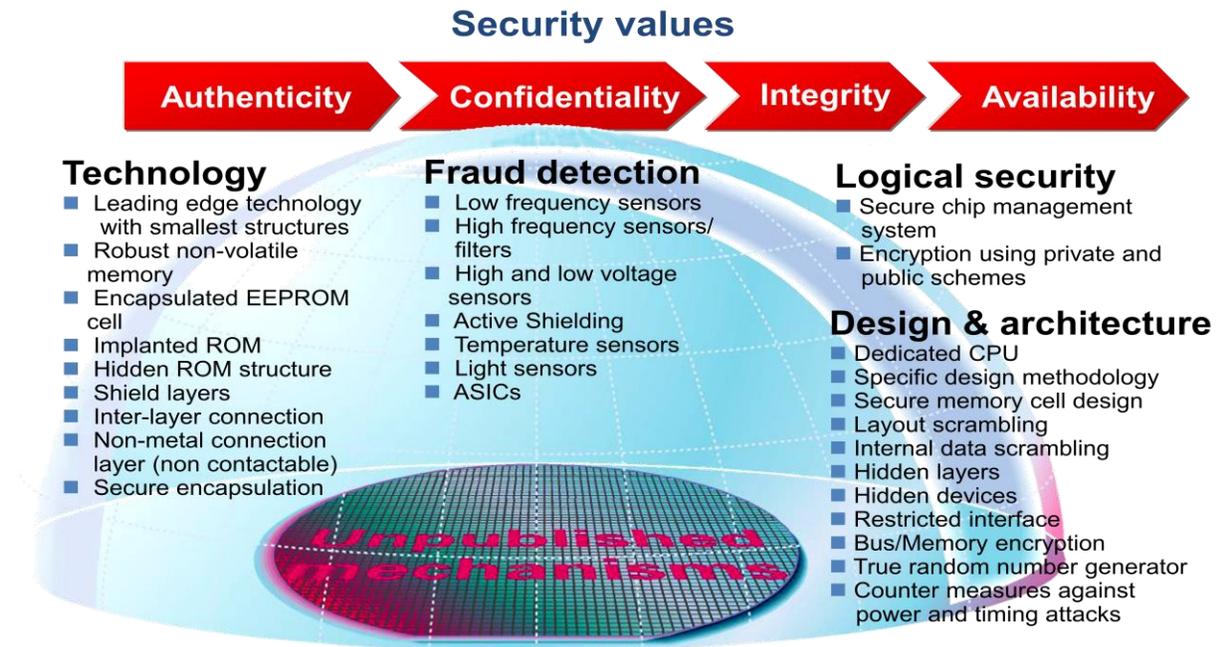
SMEs have following features:

- Certified by independent third party.
- Tamper proof storage and execution environment of security functions
- Personalized; secrets and algorithms incorporated in security certified manufacturing
- Mutual authentication between smart meter and back office server

- Verification of updates of the smart meter
- Assurance of command and data integrity
- Support of rights management
- Recording of error conditions
- Protected Storage of meter data/control parameters and price signal info.
- Unique identification for Each device...injected into the SME during Manufacturing.
- Mutual authentication between smart meter and back office server.
- Smart Meter data and communication integrity

SME Life cycle:





“Known” and “unknown” attacks

The target of every attack is mainly determined by the specific application that is used. Even until today, it was often common sense to primarily survey the protection against so called “known attacks”, which were transferred into test scenarios for dedicated products. But taking into account that several hundred new attack scenarios are evolved every year, it is obvious that many questions are left open. First, one should ask who would know a specific attack? It is not surprising that proficient attackers often keep their findings secret.

Manufacturers of security Crypto controllers also have to care about the question “What can be done to protect a device in a better way against unknown attacks?”.

Three attack classes, which are used against hardware, have been known since the beginnings. They remained constant for decades, and are also expected to remain constant over many coming years:

Semi-Invasive attacks

Utilizing “Semi-Invasive” attacks, an adversary tries to induce faulty behavior in a security controller. Then, he can try to circumvent security decisions in the software, or manipulate data for his own purpose. A faulty cryptographic calculation may even lead to the extraction of a secret key. In principle, attackers can utilize everything which affects the behavior of silicon chips: Electrical transients, called “Spikes” or

“Glitches”, but also electromagnetic pulses, light or lasers, ionizing radiation from radioactive sources, or temperature changes can be applied. For example, protection measures against “laser attacks”, an attack test often used in evaluation, would not automatically give indications about protection against neighbored Semi-Invasive attack scenarios.

Manipulative attacks

If the attacker performs manipulations of the hardware itself, such attacks are called “manipulative attacks”. This could include the use of microscopic needles which are set on the signal lines, over which secret information from the heart of the chip would be extracted. Other manipulative attacks imply the modification of a chip’s structure and circuit by utilizing micro-surgery on the silicon, typically by the use of a Focused-Ion-Beam (FIB) workstation. More recent manipulative attacks include the use of atomic force microscopy needles, which are only a few atoms wide and therefore

are compatible with even the latest, smallest technology sizes.

Observing attacks

Observing attacks have existed for many decades now. For example, the observation of the power consumption of a security

device could yield information concerning the secret data processed therein or even the secret key that is used to process this information. In principle, every side-effect of semiconductor operation, the timing behavior, or even smallest traces of light emission or heat generation can be utilized to extract secret data. For example, protection measures against the “Differential Power Attacks” (DPA), would not automatically give indications about protection against neighbored attack scenarios like the successor “Electromagnetic Analysis” (EMA).

Many of today’s products are equipped with security features that are focused on very special attack scenarios or subgroups, like laser attacks or DPA. The situation gets worse if the countermeasures are tailored to only meet the attack equipment or parameters that are used in common tests: Would such a chip be designed only for the purpose of surviving evaluation and certification? Would this be the intention or only the fault of a semiconductor manufacturer? The industry had to find a way out of this situation. The more the countermeasures were scenario-oriented, the more available space they would leave open for an adversary. This is the reason why the overall philosophy of countermeasures had to be dramatically changed.

New, comprehensive security concepts

Most typical security features cannot be used any more for building the main security layer, as they are always bound to the specific parameters of the attack. A new comprehensive security concept utilizes mechanisms that work independently of the specific detailed characteristics of a single attack scenario. Main requirements for designing future-orientated security

concepts:

- Hardware security should be strong
- Security technology should be easy to use
- Security systems should work autonomously

- Hardware should be able to check itself
- Designs should be robust
- Security mechanisms should be mathematically modeled.

Technical realization

In the history of security controllers, one most important aspect was typically neglected – the CPU itself, the heart of the microcontroller. Indeed, a real protection of the CPU itself, at first sight, seems to be a hard problem: Simple protection concepts like adding parity bits in the registers or other parts of the CPU, under attack conditions, turned out not to be sufficient. Utilizing a dual-CPU with very close denticulation allows for very comprehensive protection against semi-invasive attacks. It should be fully transparent for the software developer, and should not have a negative impact on performance. Interestingly, in reality it turned out that such a system could often be even much more energy efficient than a conventional chip, as other security measures, usually decreasing performance, would not be needed anymore.

For protection against observing and manipulative attacks, encryption is very important. Even older products usually employed encryption in the chip's memory blocks, but conventional concepts still show a major weakness: Typically, the CPU, if it wants to process the information stored in the memories, had to utilize clear text. But today, with New CPU design techniques, it is even possible to process data in encrypted form in the CPU itself making end to end encryption of data processing upto last mile. . Two CPUs can employ even different key sets in both parts. In unpowered chips, such keys should of course not be "present", so they have to be volatile.

Outlook

The future of security controllers is being built by comprehensive digital security mechanisms. Mathematical modeling and simulation greatly simplifies pre-evaluation. Uncertainties concerning upcoming attacks can be greatly reduced, a need for long-living applications. Software developers regain freedom in operating system design and application coding.

Although absolute security will never be possible, the paradigm shift towards the encrypted processing of data in the CPU itself in combination with efficient error detection will be a major step in security technology.

Passive and Semi-Invasive Attacks on Cryptographic Primitives

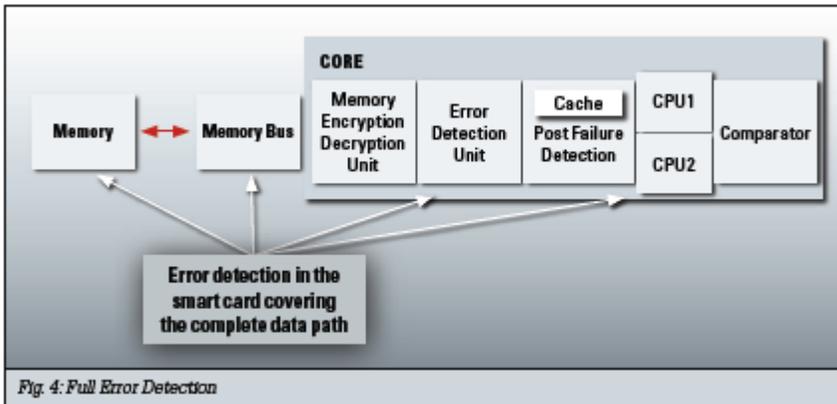
State of the Art Security microcontrollers designed today , plan and anticipate for long lifetime , as the devices uses these controllers must be in field typically for around 15-20 years as in the case of smart grid devices , The security level achievable by a specific design, can be derived from its resistance against attack scenarios both known and unknown. The resistance against known attacks will provide the security level today, while the resistance against future attacks may provide information about the security level of the same product in the future. Therefore, in order to gain a comprehensive overview, attacks from the past, present and even the future should be given the utmost consideration.

As we discussed earlier Attacks against the hardware used in Secure microcontrollers smart card and security controllers can be assigned to three main classes: Fault Induction (Semi-Invasive) Attacks, Side Channel (Observing) Attacks, and Physical (Manipulating) Attacks.

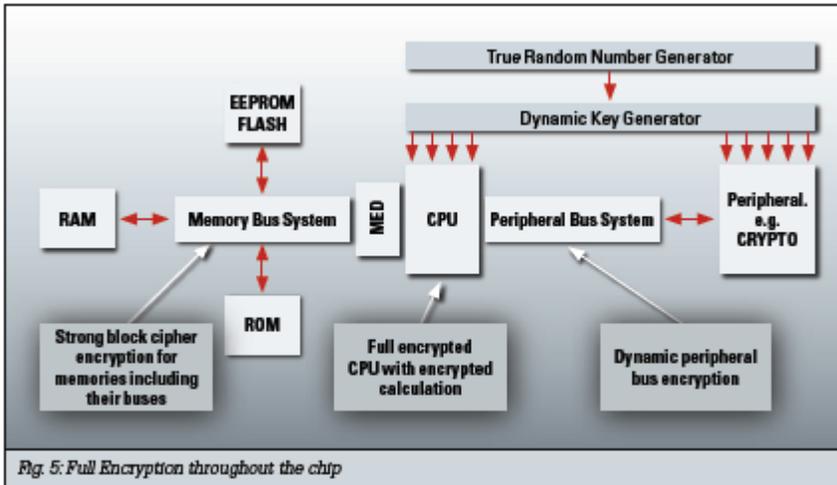
These three attack classes are populated with many thousands of different types of specific attacks, and even with combinations of these.

Fault Induction Attacks, for example, being the most popular attack form in the last years, have diversified into methods using electrical impulses (“Spike Attacks”), frequency variations (“Glitch Attacks”), laser radiation (“Optical Attacks”), thermal transients (“Temperature Attacks”) and even radioactive sources (“Alpha Radiation Attacks”). Each method, in turn, can be used in a large variety of scenarios. Nevertheless, every year a multitude of new methods are researched and applied against security devices. Interestingly, till recently, many of the countermeasures that are available in some products was not covering the attack class itself, but instead only focus on specific varieties. In reality, this means that for counteracting Fault Induction Attacks, some of these controllers comprise specific detectors for each known particular scenario – for example voltage detectors against spike attacks, temperature detectors against temperature variation attacks and light detectors against optical attacks this may lead to the remaining risk of attacks that are not foreseen, even by top experts. Therefore, all future orientated concepts that are targeting the next decade of security controllers, must be based on comprehensive approaches and research.

The actual and future attacks applied by internal evaluation, external test laboratories and, of course, by attackers, are mainly characterized by their local application, which means that the complete chip is not targeted, but only small areas or even single transistors. Now, as attacks become locally focused, the complete chip can no longer be protected by global sensors. In the conventional approach, area-localized countermeasures (sensors) would have to be applied, which further drives up the costs. In the future, applying conventional concepts could not only endanger the security products that rely mainly on sensor security, but could also endanger the cost element of such products, as immense amounts of sensor elements would have to be introduced. Furthermore, if a security system was to be only sensor-based, irrespective of which attack medium a hacker would choose, the right sensor must be present in nearly every part of the chip. Even for amateurs, it quickly becomes clear that a comprehensive security system cannot be purely sensor-based. With this in mind now, security controllers are designed for a security lifetime of many years. For this, approach of moving in the direction of error-detecting circuits and their utilization in security controllers, Instead of setting up legions of sensors against every possible threat, a new and innovative barrier was set up – the identification of errors before they could cause harm to the chip security. Now these secure controllers are equipped with error detection codes (EDC) for all the memories (RAM,NVM,ROM), Hardware checks for the chip’s internal states, e.g. bus systems and CPU functionalities along with Trap system which enables the operating system to identify errors that could have been introduced to try an attack. The “trap system” distinguishes between approximately 50 different error scenarios, such as bus access errors, illegal CPU states, illegal address or code configurations, memory access violations and many more. These support Multi level concept which enforces strict true Firewall between Multi Applications running on the chip. The new security concept of Guarding the integrity of the chip with a full error detection capability for the complete data path as shown in the diagram.



These new security controllers will comprise of two CPUs in every chip. The dual-CPU approach allows error detection in real time, even while processing. Both CPUs deliver their calculation results independently from each other. A comparator detects whether a calculation was performed without errors, or if an erroneous calculation was made, e.g. under attack conditions. In the case of an error, an alarm is instantly issued. This concept enables relevant attack scenarios to be detected, whereas other conditions that would not lead to an error, would mainly be ignored. All memories are included in a comprehensive Error Detection System, which protects the complete data path from CPUs through the buses to the memories and also back to the CPUs. Needless to say, standard CPU cores must NOT be used in advanced security controllers. Therefore, both CPU implementations were designed in such a way to allow full control over all internal functions. Even the cache is an active part of Error Detection – which is essential, as cache based attacks will become a major threat for security in the near future. The error detection system is mathematically modeled and therefore its protection functionalities can be simulated. This simulation and mathematical modeling of security systems will be of much higher importance in the future security evaluations. The prediction of security behavior by mathematical means allows truly scalable security, making security evaluation and certification more efficient and reliable. For example, fault attack simulations and their effects on the complete system can now be modeled and evaluated before the silicon prototypes are even available. Tests using real attack conditions have already shown that the mathematical models are correct. Digital security features, in contrast to analog technologies, do not require calibration or adjustment. They are not process dependent and their efficiency can be simulated before integration and also easily tested. The robustness against environmental parameters is very high. As mentioned earlier both CPUs are now able to perform encrypted calculations, enabled by a feature called Full Encryption. These controllers will be equipped with full encryption over the complete core and memories, leaving no plain data on the chip.



The two CPUs utilize full hardware encrypted calculation, with different secret keys used in both of the CPUs. All memories are completely encrypted. For the memory blocks RAM, ROM, EEPROM and FLASH, a strong block cipher hardware encryption engine is utilized, which also protects the memory bus systems. Mathematical methods enable re-ciphering from the memory encryption system to the encrypted CPU itself to be done without exposing clear text. Peripheral buses are protected using dynamically changing keys. Symmetric coprocessor Engine used for AES and DES utilizes internal dynamic encryption – just like the encrypted CPUs. This prevents the presence of secret plaintext inside important parts of the chip. Indeed, significant mathematical efforts were required to develop this non-plaintext, full-encryption concept. This will enable unchallenged protection potential in the light of upcoming advanced attacks, such as micro coil based localized DEMA (Differential Electromagnetic Analysis). These microcontrollers also provide signal protection. The most important part about signal protection, is to reduce the attractiveness of signals for an attacker. This is done by full encryption – encrypted signals are of no use to the attacker; neither for manipulating them, nor for eavesdropping. Nevertheless, for every design there are some signals that are of more importance than others, so a new protective shielding concept, combined with intelligent secure wiring, is introduced. An intelligent shielding algorithm finishes the chip's layers.

Secure Microcontroller Use cases for Smart Grid devices

This section covers use cases on how secure microcontroller enhances the security of smartgrid devices. As an Example, we can take AMI. AMI components and their functions are as follows:

Environment description (Context of use cases):

As an Example we have listed some of the AMI Components and their functions. We can add additional devices from Other segments of power sector (Bulk Generation, Transmission, Distributed Generation..) :

1. Smart Meter: AMI Meter is an advanced electric revenue meter capable of two-way communications with the utility. It serves as a gateway between the utility, customer site, and customer's HAN devices and/or load controllers. It measures, records, displays, and transmits data such as energy usage, generation, text messages, and event logs to authorized systems. It may optionally include a disconnect switch that can be used to remotely provide or disconnect service.

Commands from AMI Head end to Meter

- Meter read requests,
- Turn on/off commands
- Pricing Tariff information tables (Pricing Signals) ,
- Provisioning requests,
- Firmware updates,
- Prepayment information

Response from Meter to AMI Head end

- Meter read data,
- Various meter events (e.g., tampering, outage, and restoration),
- Various confirmations (e.g., meter turn on/off, load shed start/end, and meter provisioning),
- HAN communication, error logs
-

2. Non-electric Meters are components used for metering non-electric services (e.g., gas and water meters). Non-electric Meters sometimes use AMI networking infrastructure to provide information back to non-electric utilities. Like AMI Meters, Non-electric Meters are deployed in the field, and as such have limited physical protection. They are battery operated and have limited computing resources.

3. A Third Party Meter/Sub meter is a metrology device that allows for the monitoring of usage on a portion of a distribution network past (at a finer granularity) a main meter. A sub meter may not be owned by the utility. Third Party Meters/Sub meters are deployed in the field, and as such have limited physical protection.

4. Concentrators: These are like a Hub between Smart meter (end device) and head end. These devices periodically collect info from all the meters and relay that back to

head end and additionally gets commands from Head end and appropriately routes to individual smart meters. These are very scalable hub units serving from 5-10 (small group of homes) meters to 100's of meters (big Apartment complex)

5. Field Tool/device: Field tools and devices are portable computing systems used by field personnel to connect to components in the field to perform maintenance, upgrades, diagnostics, and similar activities. It has a wireless connection to utility systems, which communicates information utility field personnel may need to perform installations or other service

- Stored meter data (including meter read data and ID) and logs,
- Turn on/off confirmation,
- AMI system registration success, meter test results
- Request for all meter data and logs,
- Credentials for field person using Field Tool/Device,
- Turn on/off commands,
- Meter configuration data,
- Request communication test and self-test results

These are small set of example devices in AMI. We can add more devices later. Considering level of functionality and security requirements, a scalable security approach can be adapted to these devices. The 3 main points needs to be considered are Integrity(I), Confidentiality (C) and Availability (A).

Use cases

Let us list some of the use cases for Security IC requirement for the devices described in previous section

Use case 1: Life Cycle management: All the above listed devices will have various phases in their life cycle. They are

- Device (Ex: Meter) module Manufacturing/Production (Hardware/Software)
- Device module System Integration (Meter + Communication module)
- Device Initialization/configuration setting by Owner (Utility)
- Deployment by utility/3rd Party in field.
- Periodic field Updates of price and service info
- Firmware upgrade and maintenance.

- Remote Deactivation/Reactivation (temporary)
 - Termination (End of life)
1. Secure micro can act as a root of trust and extend the chain of trust as the devices moves from one phase to another in Life cycle of each device. Unique chip ID, individual PKI certificate and corresponding private key of the secure micro and also the public key of the Root Certificate Authority are injected during the chip manufacturing in a secure environment. They can be used as a unique identifier for the mutual authentication and secure communication between devices and external components. Additionally various components of the devices can be bind together with Unique ID of the device and integrity metric of the whole system can be established. This integrity metric info will be stored in protected storage of the secure IC and at any phase of the life cycle, Integrity metric is recalculated and compared to see, no hardware change is done. If there is a mismatch, then Secure Micro can conclude that device is compromised and appropriate action can be taken as per the set policy. This integrity metrics can also be extended to Software. All the secrets (symmetric and asymmetric private keys) are stored in Secure Micro and are never exposed outside of the Secure Micro. Device's life cycle state is protected by Transport keys (symmetric or asymmetric) and PKI certificates. Authentication enabled and assisted by Secure Micro is required before changing the device's life cycle state.
 2. During the integration phase, when new modules are added, Integrity metrics are updated in a Cryptographically Authorized/Authenticated way. Secure Micro enables the establishment of trust for secure integration.
 3. All the configuration setting (default configuration), initialization parameters and utility/3rd party profile/customer profile are injected in a secure way with secure micro as a trust entity. These configuration setting/ profile info will be stored encrypted with unique key of the device in protected storage of the secure micro which has built in countermeasures to prevent from various attacks to access the info. So, here secure micro Act as a secure vault.
 4. Secure micro acting as a trust establisher provides Protection from malicious intent inserts of hardware or software into infrastructure. Also it will identify untrustworthy components in its supply chain.
 5. In AMI currently the perception is Meters and poll-top and other systems *without* significant controls and external monitoring cannot be amply secured and should always be considered relatively untrusted. Secure Micro provides trustworthiness to devices with trust extension.

Use case 2: Integrity (Anti-Tampering)

Requirements

1. Software Integrity Check: The system shall maintain a complete image of all currently deployed component software. All components shall maintain a hash and a signature of all installed software components, including patches. All hashes and signatures shall be generated by trusted software provider(s). Signature shall include signer's certificate signed by a trusted CA (Secure Micro shall have one or more trusted CA certificates installed to enable certificates verification). Any update to component software shall require an update of hashes / signatures repository. A periodic integrity check of all software components shall be performed by comparing the hash on the component to the hash in the repository. Acceptable technologies are specified by FIPS PUB 186 (signature) and FIPS PUB 180 (Hash/SHA).
2. Software and Firmware Authenticity:
 - a. Shall not accept software or firmware updates that are not cryptographically signed.,
 - b. Shall not execute any software or firmware before validating its hash or cryptographic signature.
3. Configuration File and Sensitive Data Integrity Check: Configuration files and other sensitive data (Configuration info: manufacturer, type, serial number, version number, and location (logical and physical). Enabling and disabling functionalities/Communication services should include cryptographic integrity checks (e.g., cryptographic hashes) and the integrity of the file should be checked whenever it is read by an application.
4. Configuration File Authenticity: shall not accept any message payload containing configuration files that is not cryptographically signed. Acceptable technologies shall be specified by FIPS 186
5. Storage Integrity Check: shall perform automated checks (e.g., file system checks, database integrity checks, and checksum comparisons)
6. Health Monitoring: The system periodically interrogates and validates current connectivity by observing communication from <role> on at least a daily basis.
7. Shall time stamp and cryptographically sign (symmetric MAC or asymmetric signature) all configuration and management messages that it sends.

How secure micro can help in meeting this requirements:

1. Firmware image hash value will be cryptographically signed by the firmware developer and verified by the secure micro and will be stored in protected memory of the secure micro.
2. When a request for software/firmware is received, secure micro checks the Authenticity of the request using cryptographic methods, validates the request, identifies and validates the source of the request. Cryptographic credentials required for this shall be

well protected in a secure vault. Cryptographic credentials comprise a public key certificate of a Trusted Certificate Authority (CA), a device specific public key certificate issued by the Trusted CA and accompanying chip private key.

3. As mentioned earlier Configuration data and other sensitive information are stored encrypted with device unique key and stored in secure micro protected vault. If needed Application processor will establish a secure session with secure micro and get these configuration parameter and critical data to do some processing or Application processor can allocate this task to secure micro and get only the end result. In that way these critical info will not leave the secure micro boundary.
4. If there is a need to modify the Configuration data or critical parameters, Secure micro will cryptographically check the authenticity, accepts only cryptographically signed requests and cryptographically verifies the signed messages. Again for this it uses crypto credential stored in secure vault.
5. Base time info can be logged during boot and stored in Secure vault and used as a reference time for all time stamp.
6. If there is a need for re calibration of the device, calibration test programs can be stored in secure vault.
7. As a value added service, if 3rd parties would like to add some Application software to the devices (Java Applets), secure micro enables the new IP provider to securely load the applets to the devices.

Use Case 3: Operational mode usage:

Requirements:

- Code Locking and Encryption
 - Command Validation (Integrity check, Sign/verify by secure micro)
 - Periodic Checking of code integrity and critical parameters
 - Trusted Execution environment
 - Audit Logging of critical events, failure modes for forensics
 - Cryptographic Services
1. Once the Application processor code is securely loaded to flash of the system, the code area can be locked with cryptographic key and access right is restricted only for Execution and preventing read or write by any external sources (debug port JTAG). This access rights info is stored in Secure micro protected memory and will not be accessible for hacker to modify.
 2. Secure micro will enable the device to receive only cryptographically signed commands along with integrity check and process only authentic commands. Every command received by the device will be checked and validated by secure micro and if it is genuine one, then this will be routed to Application processor to process this command.
 3. Application processor operating system can have a feature to ask secure micro to periodically (Programmable) validate the integrity of the code stored in the flash.

4. Enabling/disabling of some of the Application processor/Metrology processor resources (Ports, dynamic memory allocation, ADC parameters..) can be securely managed by Secure micro.
5. All commands are logged, stored, and periodically transferred securely and once the transfer is successful, they can be deleted.
6. When security event is seen, Application processor can use the secure vault to store that event info as forensic evidence, so that this info will not be deleted.
7. In Operation mode, if Application processor requires carrying out any cryptographic services, it can use the secure micro hardware crypto modules for that (Random number Generator, SHA, AES...)
8. Secure micro enables the Main electric meter to communicate securely and gather data from sub meters and 3rd party devices (Gas, water, PHEV...), do appropriate calculation and communicate to back end. In this way Secure Micro enables the main devices to act as a cash register.

Use case 4: Audit and accountability:

All AMI components shall generate audit records, at a minimum, for the following events whether or not the attempts were successful:

- Security Events
- Control Events
- System/Device Configuration Changes

AMI systems and components shall transmit all audit records and logs to a dedicated log management system. Audit record generation and processing shall not degrade the operational performance of the AMI components or system

- Startup and shutdown of the audit functions;
- Successful and failed logins
- Failed authentications of signed or encrypted requests
- Change in access control or privilege
- Changes to security settings
- Creation, deletion, or modifications of users, password, tokens, and security keys
- Triggering of tamper sensors

As mentioned earlier secure micro protected memory can be used for logging the security/control events to use at a later stage for forensic operation. All control requests are validated by secure micro using crypto methods and the operations are logged and stored in protected memory

Use case 5: Cryptographic Key Establishment and Management:

1. Key generation process is in accordance with a specified algorithm and key sizes are based on an assigned standard. Key generation needs to be performed using an effective random number generator (e.g., a NIST approved PRN/RNG that passes its test vectors, such as for auxiliary quantities used in generating digital signatures, or for generating challenges in authentication protocols).. The policies for key management need to address such items as periodic key changes, key destruction, and key distribution.
2. key management infrastructure shall be able to distinguish individual sending and receiving devices
3. The AMI components shall reliably associate security parameters (e.g., security labels and markings) with information exchanged between the enterprise information systems and the AMI system.
4. Public Key Infrastructure Certificates: The organization shall utilize public key certificates under an asset owner defined certificate policy. Registration to receive a public key certificate needs to include authorization by a supervisor or a responsible official and needs to be accomplished using a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party. Any latency induced from the use of public key certificates shall not degrade the operational performance of the AMI system.

How secure micro can help in meeting this requirements:

1. All the keys and certificates are securely stored in secure micro vault.
2. Secure micro with its built in hardware crypto modules can generate intermediate keys (session key, blob key.)
3. Secure Micro sign/verifies all the certificates internally without exposing the secret.
4. Secure micro can encrypt/decrypt a blob of data along with sign and verify.

Security coprocessor : Required Features :

Cryptographic Hardware IC **Functional Characteristics shall have:**

- Onboard Coprocessors
- Fully Encrypted CPU core ad cache.
- Onboard True Random Number generator: capable in accordance with FIPS 140-2
- Strong Block cipher Encrypted memories and their buses.
- Encrypted Bus and registers for peripherals access.
- Built in error detection capability

- Memory Bus and peripheral Bus are not exposed to outside the IC Package. A very limited 2-3 signals for communication.
- CRC generator
- Dynamic Power management modes.
- Open Standard Communication interface and protocol.
- Asymmetric crypto processor : To support key length for RSA upto 4096 and ECC 512; the crypto engine performance shall be in accordance with xxx for doing active authentication tasks.
- Symmetric crypto coprocessor for AES/3DES : High speed engine to run AES 256 Encryption/Decryption. Capable of running 3DES algorithm. The crypto engine shall perform Secure Messaging

Secure Micro Operating System (Firmware)

The Secure micro OS is a required component in the secure micro IC. It defines the characteristics and features of the IC in the AMI. Specifically, the operating system is a software layer that works in conjunction with the IC hardware, including the cryptographic operation, security, communication, data storage, and other functions. The design and implementation of an AMI operating system plays a critical role in determining the quality AMI security, flexibility, interoperability, and performance.

The IC operating system required for the device.

The OS shall support NIST Approved/Recommended Symmetric algorithms/modes, as described in NISTIR 7628. Some of them are:

- TDEA
- MAC
- MAC3
- IMAC
- IMAC3
- AES 256

The OS shall support NIST Approved/Recommended Asymmetric algorithms/modes as described in NISTIR 7628:

- RSA 1024
- RSA 2048

- DSA 1024
- ECC 224
- ECC 512

The OS shall supports NIST Approved HASH :

- *SHA-1*
- *SHA-2 (256, 512.)*

OS shall support Secure boot capability

OS shall support a Secure flash loader to Flash the updated software and data in field

Os shall support Secure Audit log for forensic purpose.

Micro-Controller/Processor

At a minimum, ICs shall have a 16-bit processor. Multiple processors are acceptable in a single IC. All IC functions shall be performed on a single IC package.

Accessible Memory

Utility accessible memory shall be secure (factory lockable and Utility lockable), programmable and non-volatile during the production processes. At the final personalization phase, the memory will be capable of write-locked (also referred to as permanently locked).

The IC shall have a minimum of XX KiloBytes (KB) of electrically erasable programmable read-only memory (EEPROM) space available for the Utility's discretionary use.

IC Security

Offerer shall provide evidence (i.e. documentation or certification) and explain to what level and how their solution will provide the following hardened security requirements:

- Hardware and software (logical) tamper-resistance.
- Security/exception sensors such as voltage, frequency, and temperature.
- A design to prevent unauthorized access via hardware and software security features.
- Auto detection if tamper attempt is made.

Attack Security

- DFA = Differential Fault Analysis
- SPA = Simple Power Analysis
- DPA = Differential Power Analysis
- DEMA = Differential Electro-Magnetic radiation Analysis
- Common Criteria, Protection Profiles, Vulnerability Assessment Activities, Side Channel Attacks
- Electro Static Discharge (ESD) protection
- Security policy complies with the Common Criteria EAL4+ (ISO/IEC objectives and requirements in a document specified by ISO/IEC 27002).

The IC Memory Management shall have:

- Secure EEPROM/Flash on the same IC
- Durability (data retention): At least 15-20 years
- Anti-tearing reading/writing mechanisms

The memory shall support a minimum of 500K read/write cycles without failure or performance degradation.

UNIQUE IC SERIAL NUMBER

Identification Method

- Unique IC shall be obtainable by reading the Chip UID
- Unique serial number shall be stored internally in the IC and not printed on the surface of the IC or IC package

Numbering Requirements

- The unique IC serial numbers shall be non-sequential numbers.
- The unique IC serial number shall not repeat for ten years from product delivery.

IC TRANSPORT KEY REQUIREMENTS

Transport Key(s) include: Transport, Format, Pre-personalization, and Personalization Keys for each life cycle phase (Manufacturing, Administration/Pre-Personalization, and Personalization).

Transport Key Characteristics

- The Transport Key length shall be a minimum of 24 bytes For signature the algorithm shall be MAC3/TDEA_MAC3, EDE, effective key length shall be respectively 112bits/168bits
- For encryption the algorithm shall be DES3/3TDEA, EDE, effective key length shall be respectively 112bits/168bits Initial Value (IV) shall support SSC (secure session counter) with random and IV=0
- Data Padding shall be ISO padding.