SNPTC

Sunport
Connecting Forward

阿海珐
集团

8th International Workshop on the Application of Field Programmable Gate Arrays in Nuclear Power Plants

Shanghai, 13–16 October 2015

Chipset Level Cybersecurity Issues

Dr. Karl Waedt, AREVA GmbH, Erlangen

Xin Xie, Siemens AG, Karlsruhe

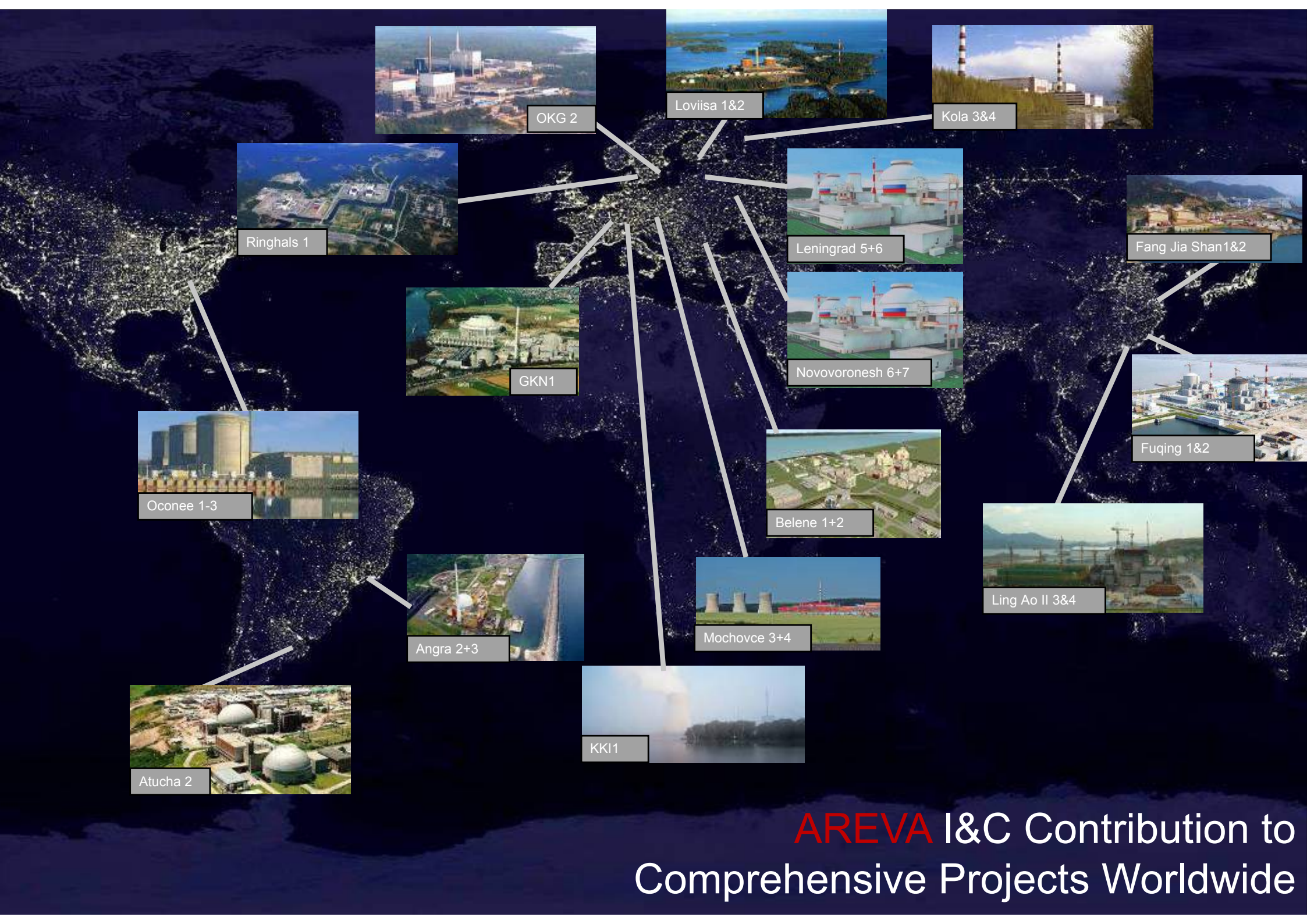
Yuan Gao, AREVA GmbH, Erlangen

Prof. Dr. Yongjian Ding, Univ. Magdeburg-Stendal

AREVA
forward-looking energy

Chipset Level Cybersecurity Issues Topics

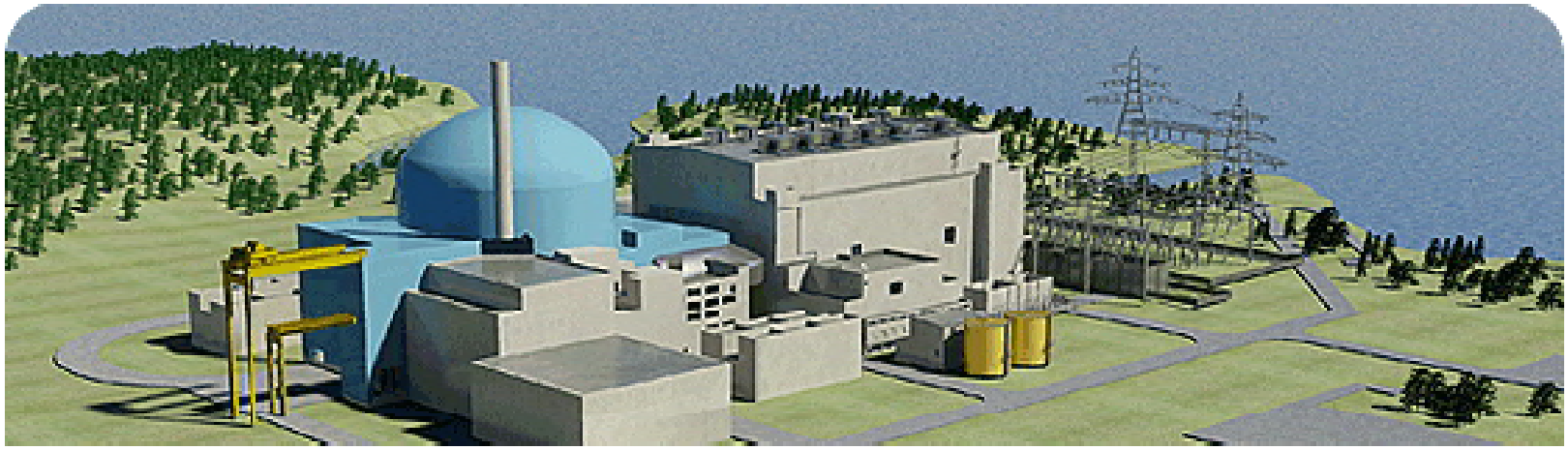
- COTS System HW Using Out-of-band Communication
- COTS HW Platform Management Interface
- The Unified Extensible Firmware Interface
- Preventive FPGA Based Security Controls
- Implications on Security Monitoring



AREVA I&C Contribution to Comprehensive Projects Worldwide

Domain Specific Cybersecurity for I&C New NPP Projects

AREVA EPR™



- Finland: Olkiluoto OL3
- France: Flamanville FA3
- China: Taishan TSN1, TSN2

TELEPERM XS Safety I&C

Chipset Level Cybersecurity Issues Topics

- COTS System HW Using Out-of-band Communication
  - Out-of-band communication
  - Example Scope of Applicability
  - DASH, SMASH, AMT
  - USB Redirection
- COTS HW Platform Management Interface
- The Unified Extensible Firmware Interface
- Preventive FPGA Based Security Controls
- Implications on Security Monitoring

Chipset Level Cybersecurity Issues
Commercial-off-the-Shelf System Hardware

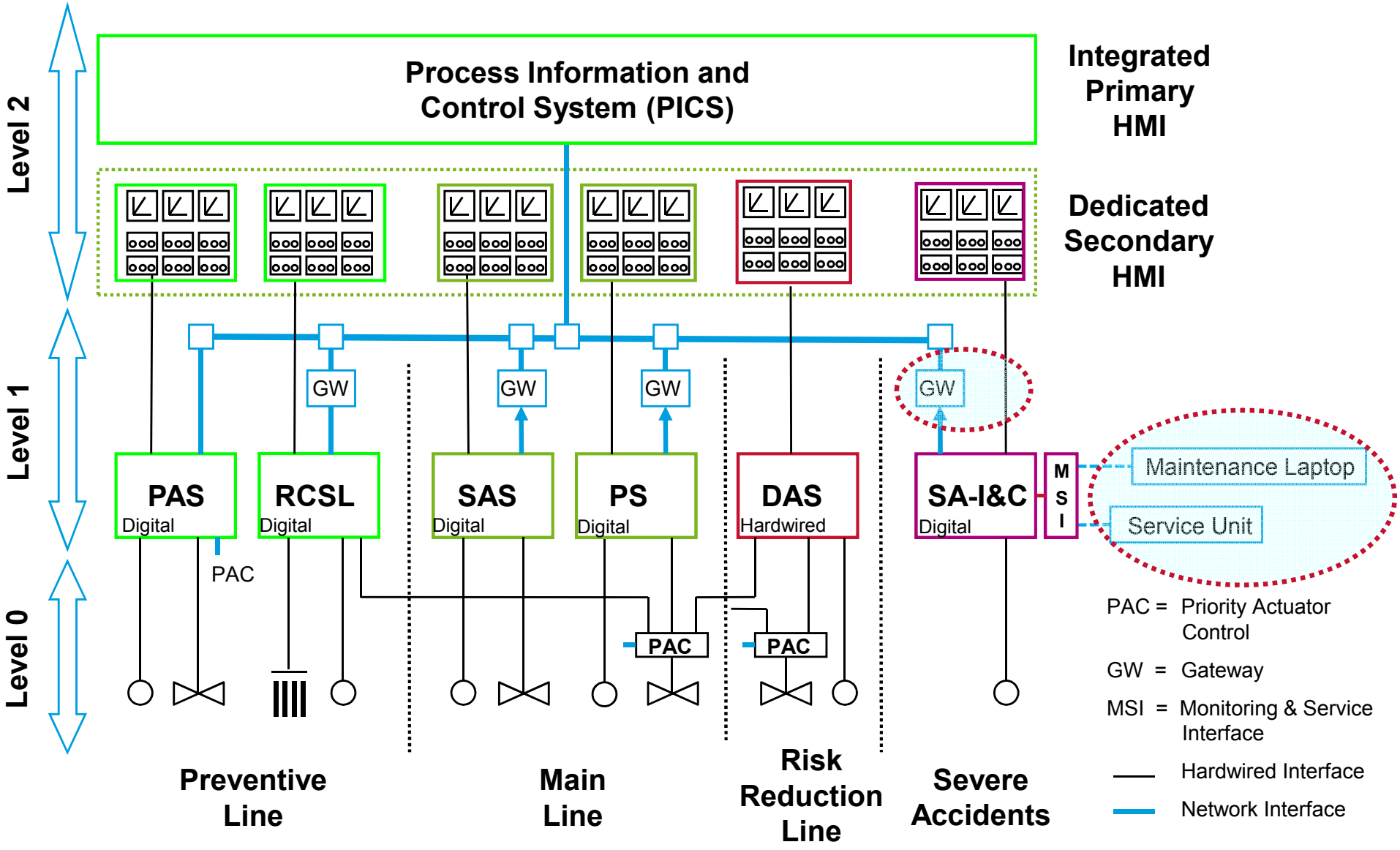
Era of mainboards with legacy single core processors

- **Functionality of chipsets and the Basic Input/Output Systems (BIOS)**
  - **rather limited**
  - **needing direct local access to the motherboard interfaces**
  - **often configurable via tiny Dual Inline Package Switches (DIP-Switches)**

Current Commercial-off-the-Shelf (COTS) office products

- **System Hardware level remote management technologies**
  - **Out-of-band communication at the mainboard level**
  - **System HW support for USB redirection via a Service Access Points (SAPs)**
  - **Optionally encrypted, remote power up/down/reset, like Wake-on-LAN** (remote wake-up, power on/up by LAN, resume by/on LAN, wake up on LAN)
  - **functionality resides in Flash memory** → [wrong settings / default passwords] **can be updated, e.g. via an infected USB key**

Chipset Level Cybersecurity Issues
Example Scope of Applicability



- **DASH (Desktop and mobile Architecture for System Hardware)**
  - **Uses out-of-band communication**
  - **Supports remote management of desktop and mobile systems**
  - **Support for the redirection of KVM (Keyboard, Video and Mouse)**
  - **Supports the management of**
    - software updates
    - BIOS (Basic I/O System)
    - Batteries
    - NIC (Network Interface Card)
    - MAC (Media Access Control)
    - IP (Internet Protocol) addresses
    - other configuration support

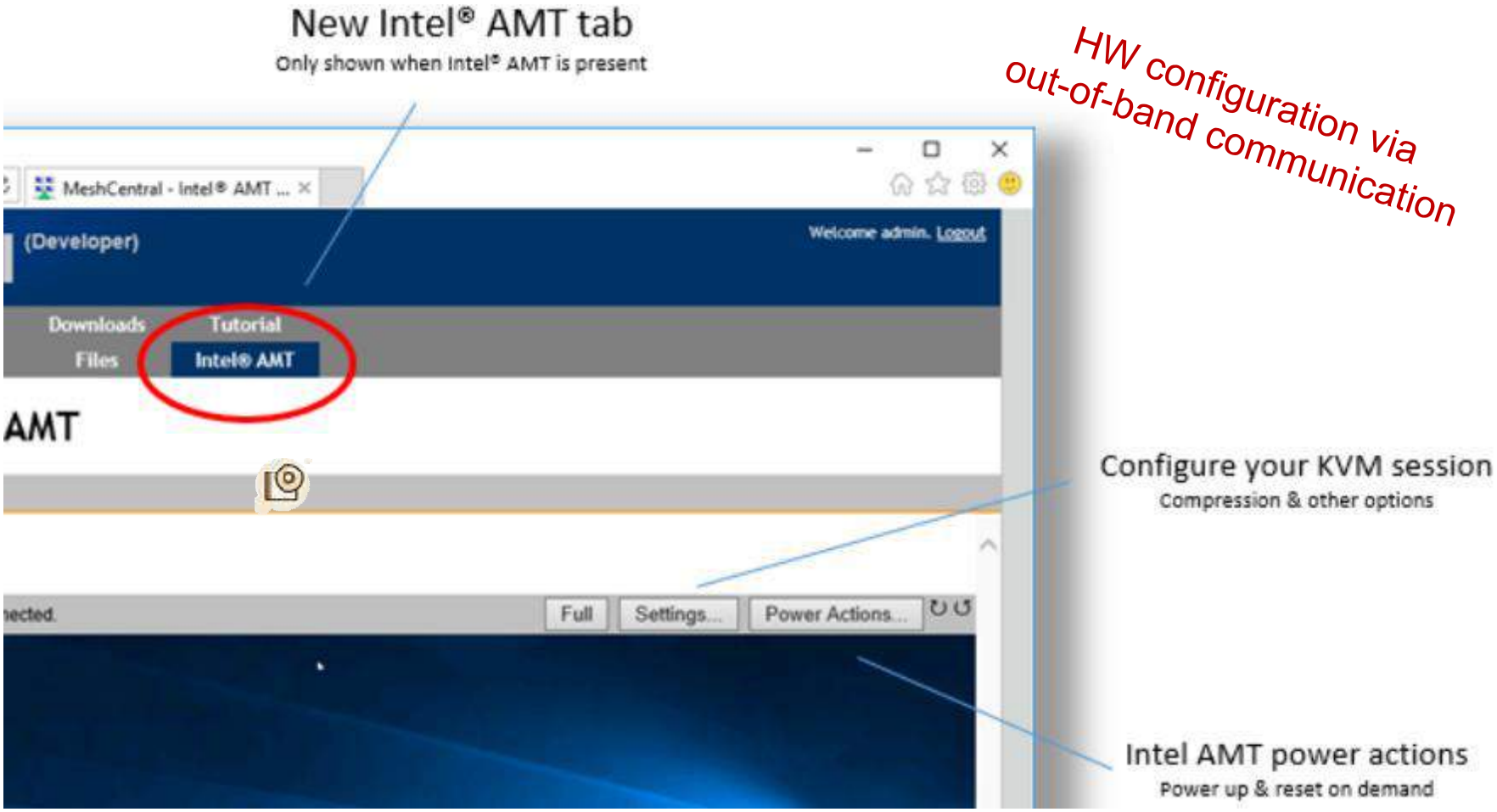
- **SMASH** (Systems Management Architecture for Server Hardware)
  - protocol specifications for increasing the productivity of the management of a data center
  - supports local and remote management of server hardware using out-of-band communication

- SMASH Command Line Protocol (SM CLP)
  - Provides an interface to heterogeneous servers
  - Independent of machine state or Operating System state
  - Independent of system topology or access method

Chipset Level Cybersecurity Issues
Active Management Technology (AMT)

- **AMT - Intel's Active Management Technology**
  - **currently a prevalent industrial mainboard level management solution**
  - **especially for remote desktop management**
  - Initially AMT was vendor proprietary. Since AMT 5.0 → DASH compliant
- **Other vendors, like AMD, also include DASH**
  - **as mainboard-level technology**
- Note:
  The frequently encountered Intel vPro logo advertises a set of mainboard level technologies that include AMT

Chipset Level Cybersecurity Issues
New: Web Based Hardware Configuration



- **Web based configuration (and possibly manipulation made easy)**
  - **MDTK Web Edition Commander 0.0.6**

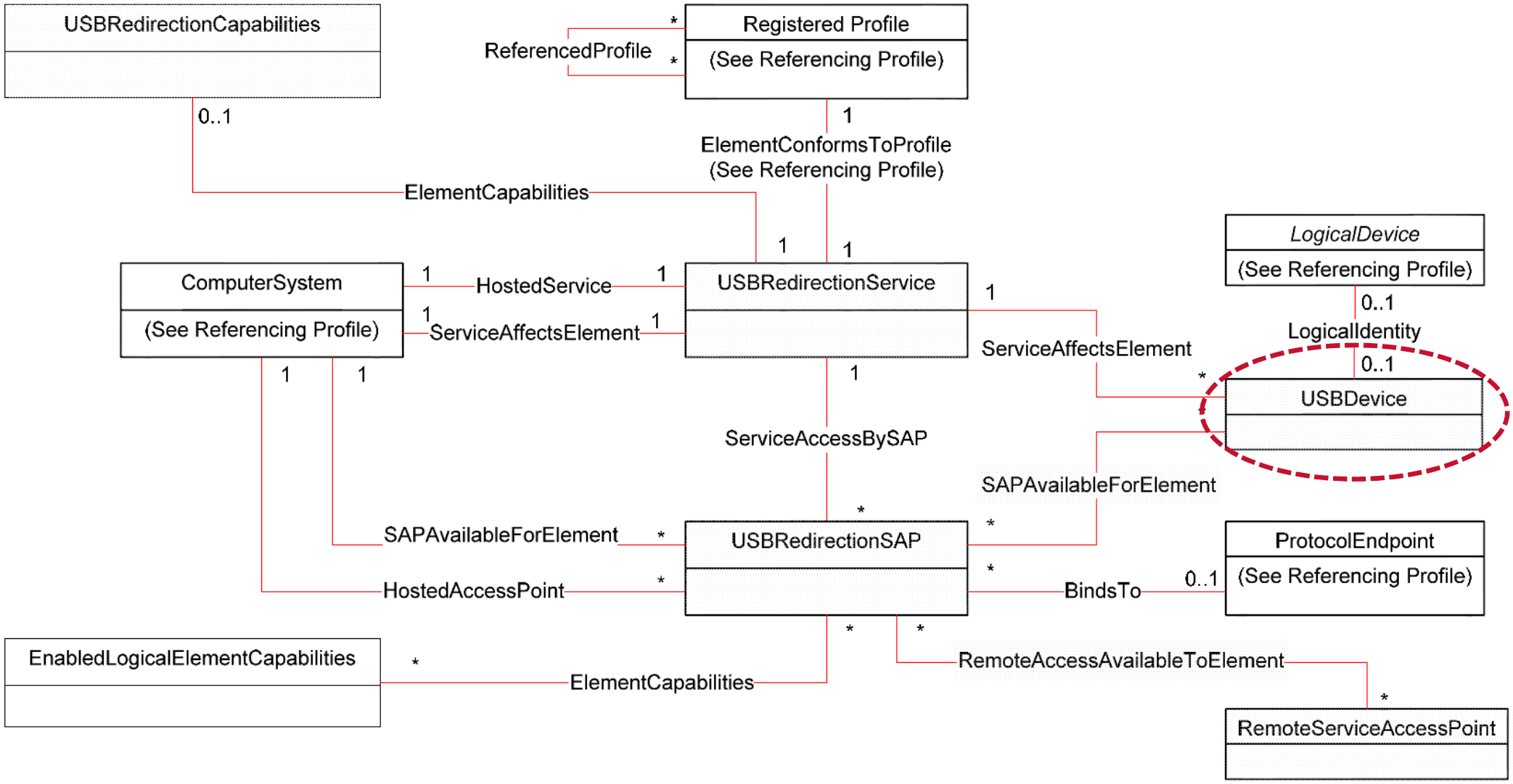
Chipset Level Cybersecurity Issues
Redirection Profiles

DASH Architecture for System Hardware specifies Implementation Requirements, including

- **Software Update Profile** (DMTF DSP1025 1.0)
- **Host LAN Network Port Profile** (DMTF DSP1035 1.0)
- **BIOS Management Profile** (DMTF DSP1061 1.0)
- **KVM Redirection** (DMTF DSP1076 1.0)
- **USB Redirection Profile** (DMTF DSP1077 1.0)
- **Media Redirection Profile** (DMTF DSP1086 1.0)
- **Role Based Authorization Profile** (DMTF DSP1039 1.0)
- **…**

DMTF = Distributed Management Task Force

Chipset Level Cybersecurity Issues
USB Redirection Profile

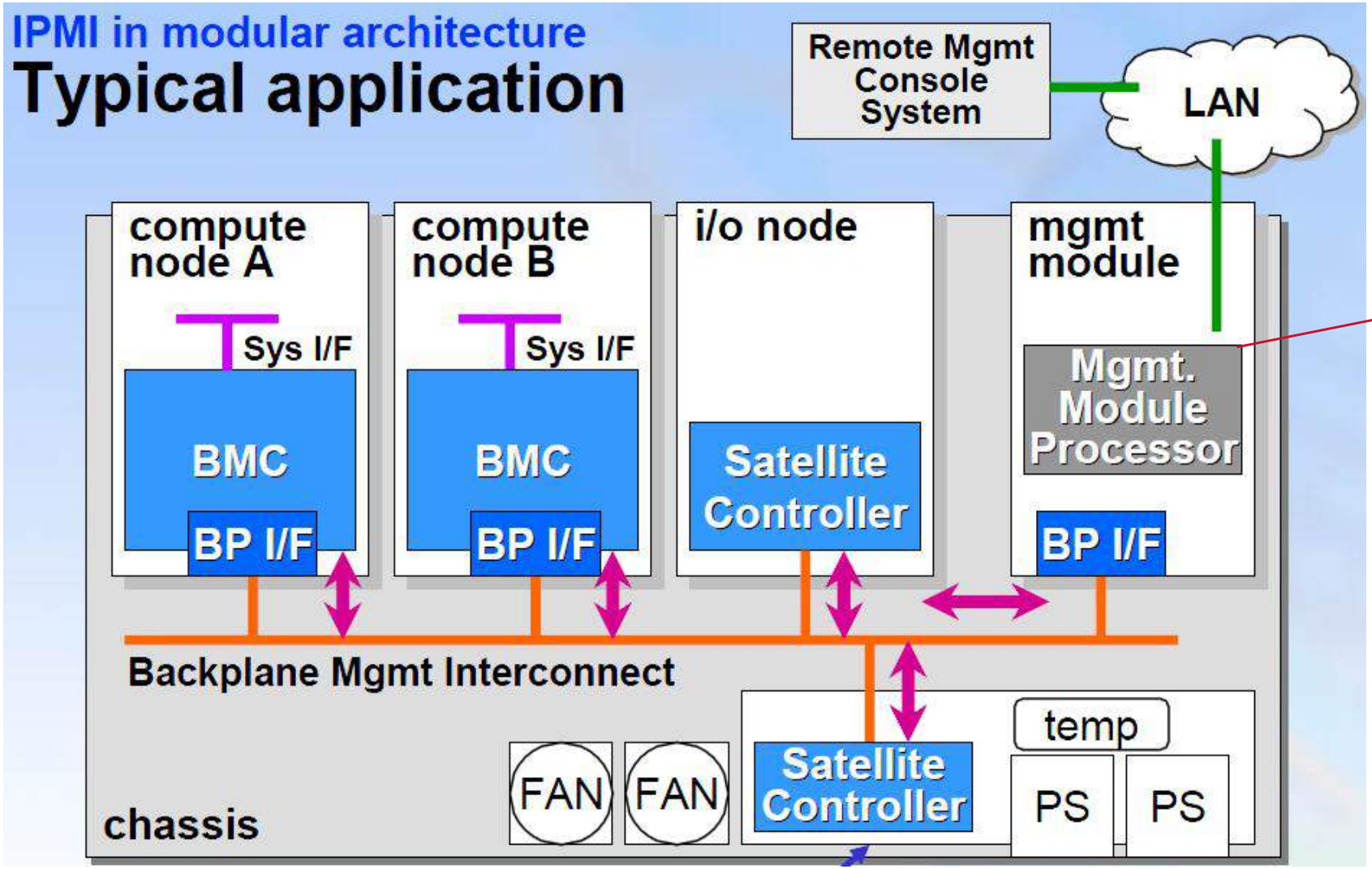


- **USBDevice → USBRedirectionSAP (Service Access Point)**

Chipset Level Cybersecurity Issues Topics

- COTS System HW Using Out-of-band Communication
- COTS HW Platform Management Interface
  - Intelligent Platform Management Interface (IPMI)
- The Unified Extensible Firmware Interface
- Preventive FPGA Based Security Controls
- Implications on Security Monitoring

Chipset Level Cybersecurity Issues
Intelligent Platform Management Interface



Dedicated Processor

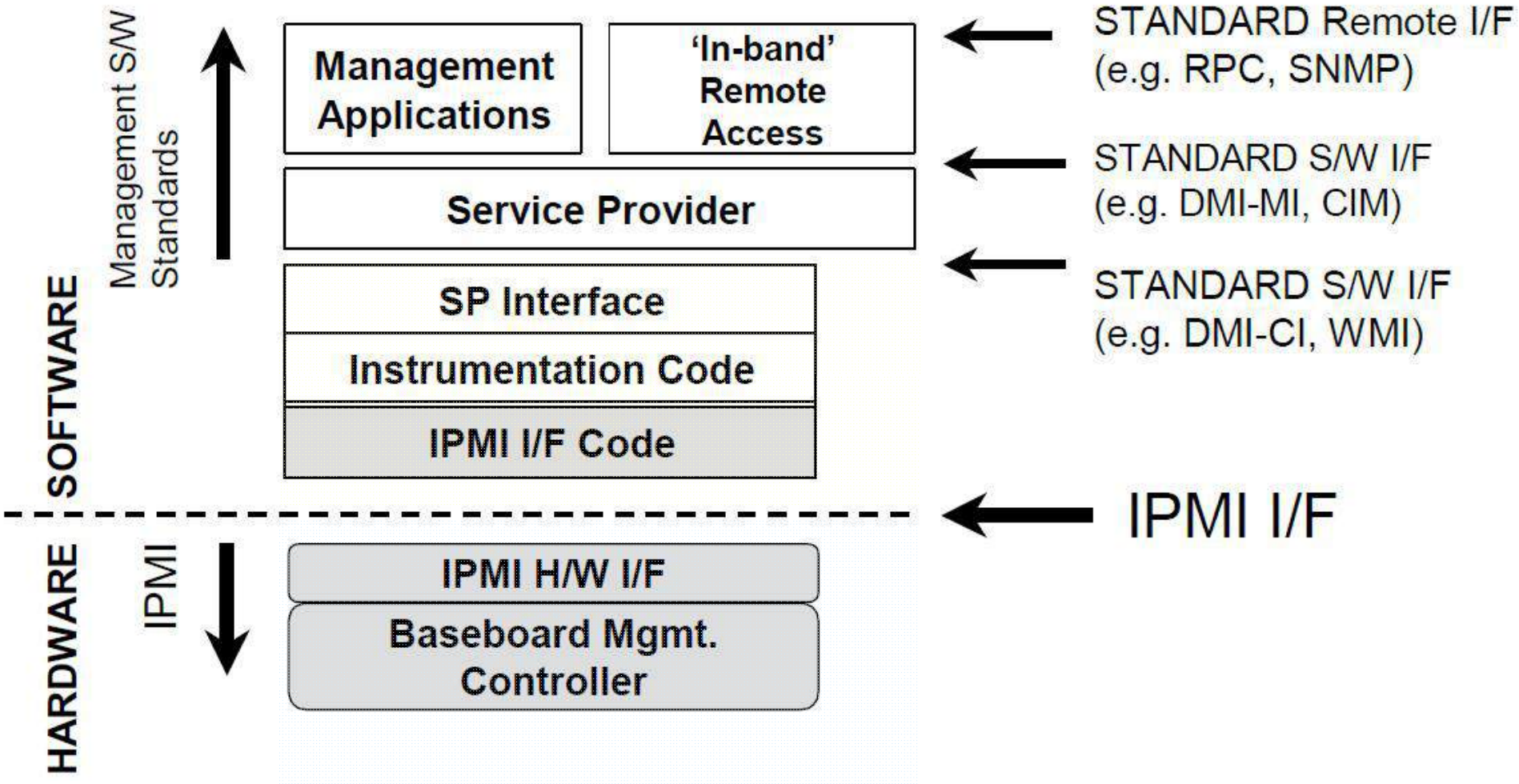
- **Initiation of actions without normal in-band mechanisms**

IPMI Platform Management Interface

IPMI (Intelligent Platform Management Interface)

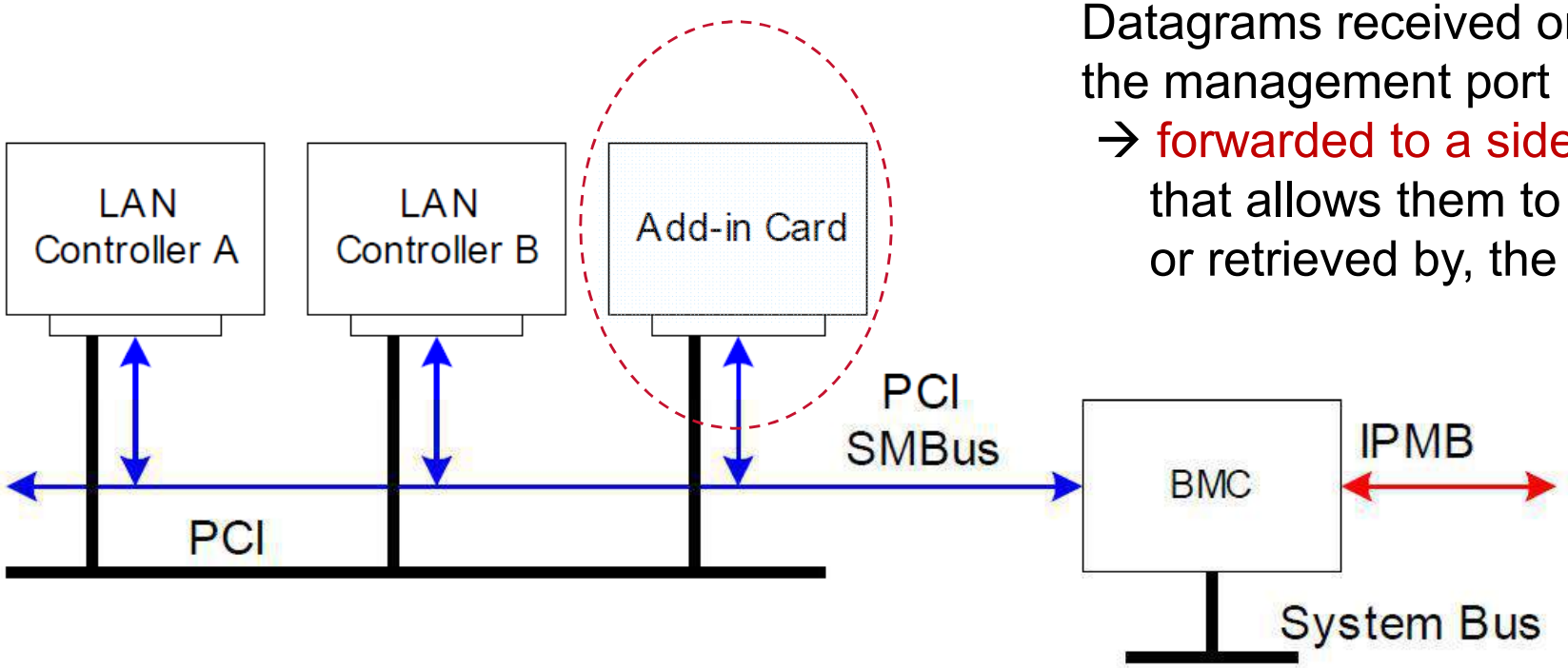
- Is a hardware level interface specification
- is management software neutral
- provides monitoring and control functions exposed through management software interfaces such as
  - DMI (Desktop Management Interface)
  - CIM (Common Information Model)
  - SNMP (Simple Network Management Protocol)
- The intelligence in the IPMI architecture is implemented by a Baseboard Management Controller (BMC)
  - a specialized microcontroller embedded on the motherboard of a computer

Chipset Level Cybersecurity Issues
HW and SW Part of IPMI



- Initiation of actions **without system management software**

Chipset Level Cybersecurity Issues
IPMI via LAN Controllers



Datagrams received on the management port
→ forwarded to a side-band interface that allows them to be delivered to, or retrieved by, the BMC

- **PCI** (Peripheral Component Interconnect)
- **BMC** (Baseboard Management Controller)
- **SMBus** (System Management Bus)
- **IPMB** (Intelligent Platform Management Bus)

Chipset Level Cybersecurity Issues Topics

- COTS System HW Using Out-of-band Communication
- COTS HW Platform Management Interface
- **The Unified Extensible Firmware Interface (UEFI)**
- **Preventive FPGA Based Security Controls**
- **Implications on Security Monitoring**

Unified Extensible Firmware Interface (UEFI)

UNIFIED EXTENSIBLE
FIRMWARE INTERFACE

- **UEFI gradually replaces the legacy Basic Input/Output System (BIOS) for COTS office IT hardware**
- **UEFI supports remote diagnostics and repair of computers**
  - **even with no operating system installed**
  - **includes remote attestation of a successful and secure boot**
  - **EFI UDPv4 Protocol can be used by network drivers, applications, or daemons**
    - to transmit or receive TCP/UDP (Transmission Control Protocol/User Datagram Protocol) packets
    - A protocol instance can either be bound to a specified port as a service or connected to some remote peer as an active client
  - **the EFI Debug Port Protocol provides services to communicate with a remote debug host**

Chipset Level Cybersecurity Issues Topics

- COTS System HW Using Out-of-band Communication
- COTS HW Platform Management Interface
- The Unified Extensible Firmware Interface (UEFI)
- **Preventive FPGA Based Security Controls**
- **Implications on Security Monitoring**

Chipset Level Cybersecurity Issues
System Hardware Impact on Security (1)

- **With Active Management Technology AMT version 7.0**
  → use of a 3G cellular signal to send a remote kill command
  - **Such a command can improve the chance of deactivating a stolen computer before it gives up any sensitive information**
    - and similarly to reactivate the computer by an administrator, once it is recovered
  - **Such a command may be misused either due to a vulnerability or by an insider threat agent**
    - e.g. as a special Denial of Service (DoS) attack towards multiple targets

Chipset Level Cybersecurity Issues
System Hardware Impact on Security (2)

- **More common scenario** (due to older AMT versions) **for current power plants and industrial automation systems**
  - **manipulations via USB keys, based on USB redirection via a SAPs**
- **Infected USB with SW for accessing COTS system HW management functionality**
  - **may obtain access to the management functionality either**
    - due to a vulnerability (of the complex implementation) or e.g.
    - due to an unchanged default password
  - **this exchange of messages goes unnoticed by the operating system**

Chipset Level Cybersecurity Issues
System Hardware Impact on Security (3)

- Deployment of these hardware level technologies may extend from the COTS office IT networking scenarios
  - to the industrial automation domain and
  - to power plants
- Initial purpose of the COTS system hardware level management functions
  - facilitate the day-to-day work of administrators and
  - reduce reconfiguration and maintenance costs
- Deployment of these new technologies has to be carefully evaluated
  - segregation of duties of the respective administrators and maintenance staff
  - (non-manipulated) firmware, coming from the same source and being deployed on (or infecting) different independent systems

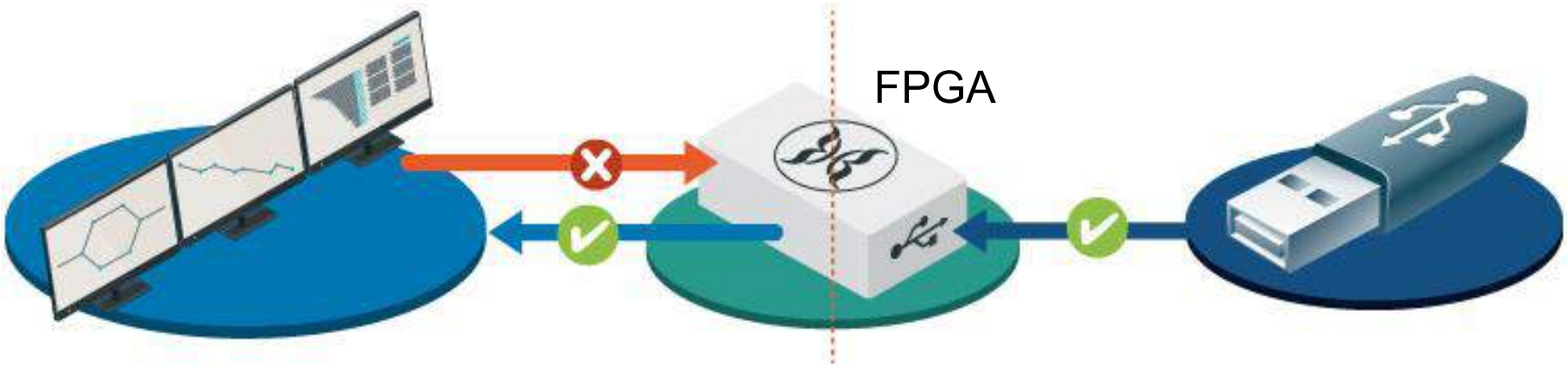
Chipset Level Cybersecurity Issues
System Hardware Impact on Security (4)

- **Cybersecurity threat due to unawareness**
  - **of new system level hardware functionality including**
  - **remote commands and remote debugging**
  - **USB redirection, out-of-band communication, …**

- **Staff technically knowledgeable and familiar with mainboard details deployed a decade ago**
  - **may not expect that switching to current COTS IT equipment will include**
    - new types of functionality that has not yet been addressed and thus
    - is not considered in locally maintained cybersecurity risk assessment procedures

- **Accordingly, I&C or industrial automation refurbishment projects**
  - **should be accompanied by appropriate security training and by**
  - **an update of the local security procedures**

Chipset Level Cybersecurity Issues
FPGA Based Security Controls

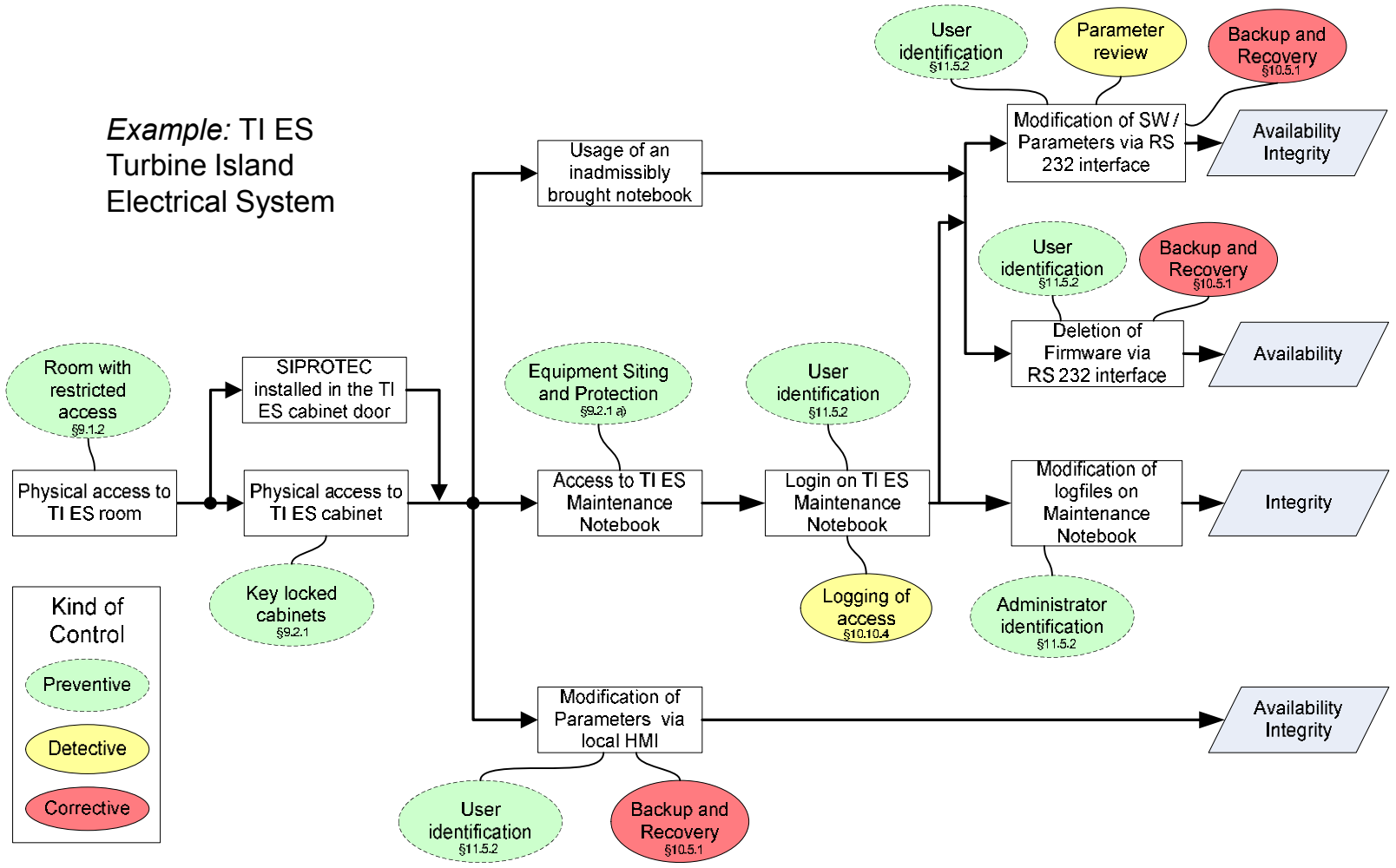


- **SECLAB SCOOP-MS**
  - **Selective COntrol Of Peripherals – Mass Storage**
  - **FPGA-based**
  - Note: Based on R&D results from SECLAB and EDF R&D
- **USB key (as Mass Storage example)**
  - **Read-write**
  - **Read-only → Reading logfiles without impact to the device**

Chipset Level Cybersecurity Issues
Topics

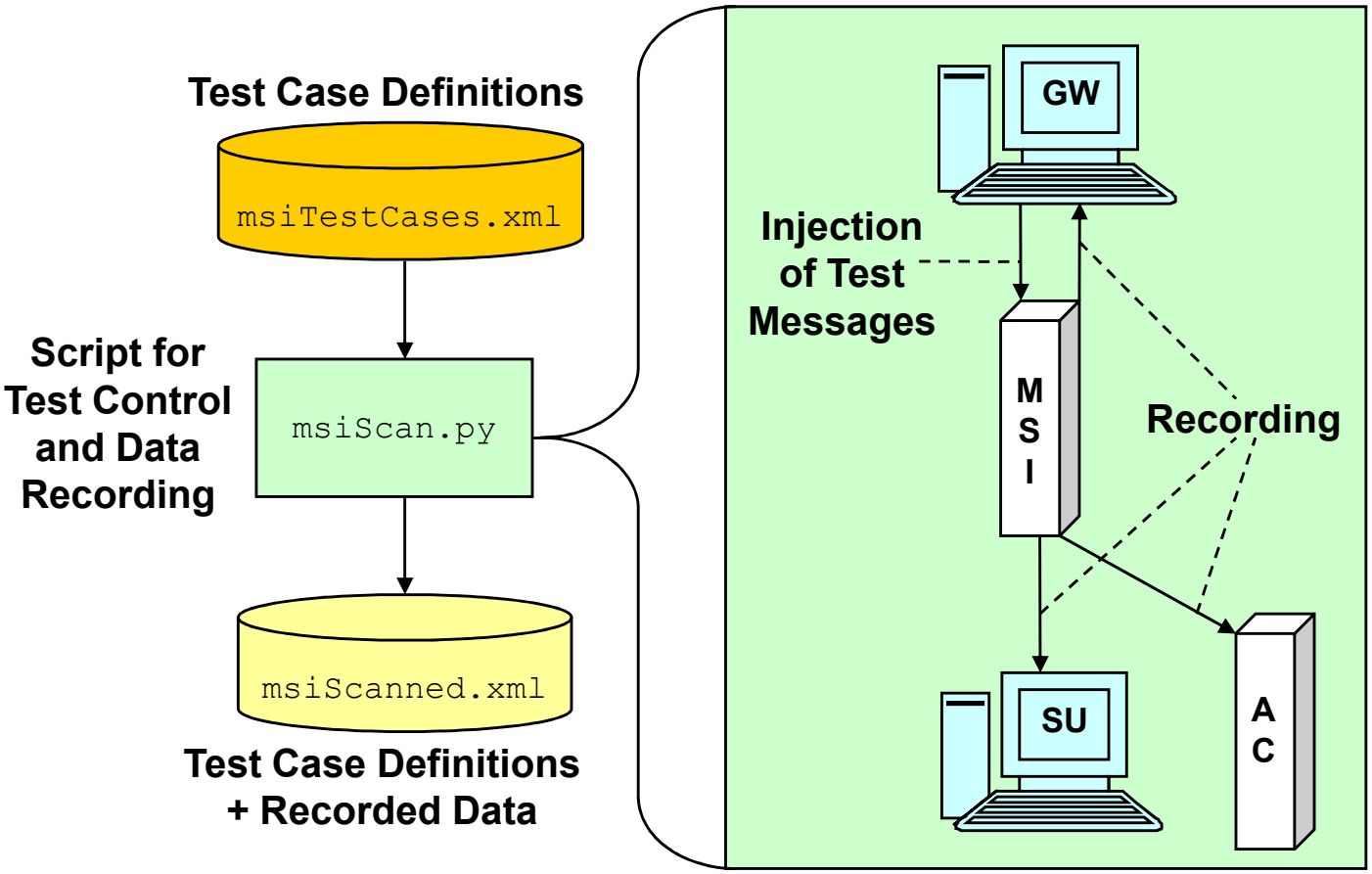
- COTS System HW Using Out-of-band Communication
- COTS HW Platform Management Interface
- The Unified Extensible Firmware Interface (UEFI)
- Preventive FPGA Based Security Controls
- **Implications on Security Monitoring**
- **Conclusion**

Preventive, Detective and Corrective Security Controls



- **SCOOP-MS can be deployed as a Preventive Security Control**
- **SIEM can be deployed as a Detective Security Control**

Chipset Level Cybersecurity Issues
Dedicated Network Security Tests



GW = Gateway
MSI = Monitoring and Service Interface
SU = Service Unit
AC = Automation Computer

- Dedicated network **security tests** can address the (absence of) **network traffic** initiated by system hardware management ports
  - Penetration and fuzz-testing suite with complete recording of network traffic

Chipset Level Cybersecurity Issues Conclusion

- DASH, SMASH, AMT, IPMI and UEFI show that
  - current COTS architectures of system hardware specifications support sophisticated functionality for remote administration
  - out-of-band communication at the mainboard level goes undetected by the deployed operating systems
- FPGA based Preventive Security Controls can be effectively deployed
- SIEM or network security tests can detect management messages on LANs
- Extended security awareness trainings needed
- Mandatory: update of local security risk management procedures

SNPTC

Sunport Connecting Forward

阿海珐集团

AREVA forward-looking energy

SNPTC

Sunport
Connecting Forward

阿海珐
集团

8th International Workshop on the Application of Field Programmable Gate Arrays in Nuclear Power Plants

Shanghai, 13–16 October 2015

Thanks to SNPAS for the org.!

Chipset Level Cybersecurity Issues

Thank you for your attention!

Dr. Karl Waedt, AREVA GmbH, Erlangen

Xin Xie, Siemens AG, Karlsruhe

Yuan Gao, AREVA GmbH, Erlangen

Prof. Dr. Yongjian Ding, Univ. Magdeburg-Stendal

AREVA
forward-looking energy