



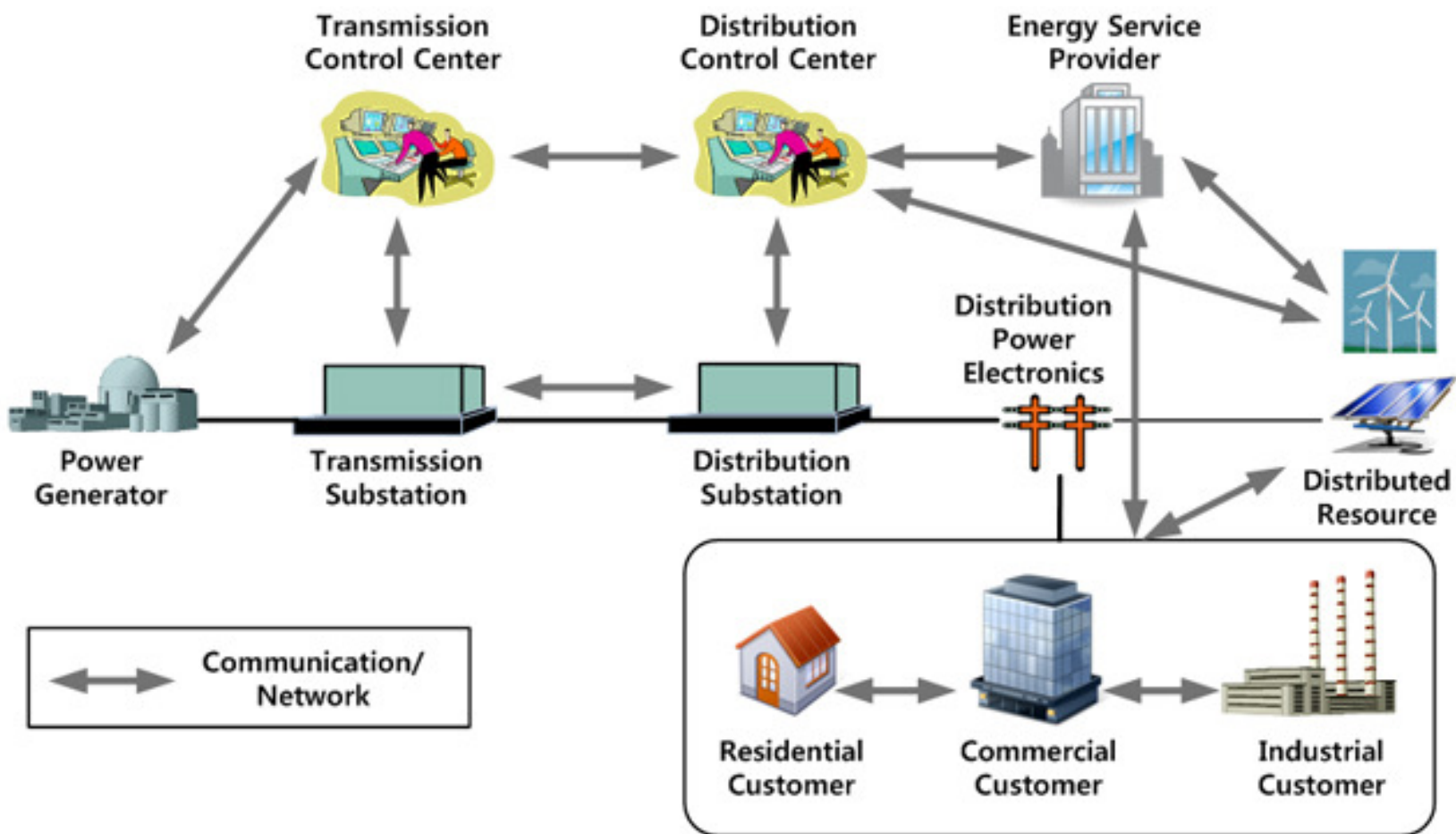
Smart Grid & Common Criteria

Eugene Polulyakh
President,
BKP Security, Inc.

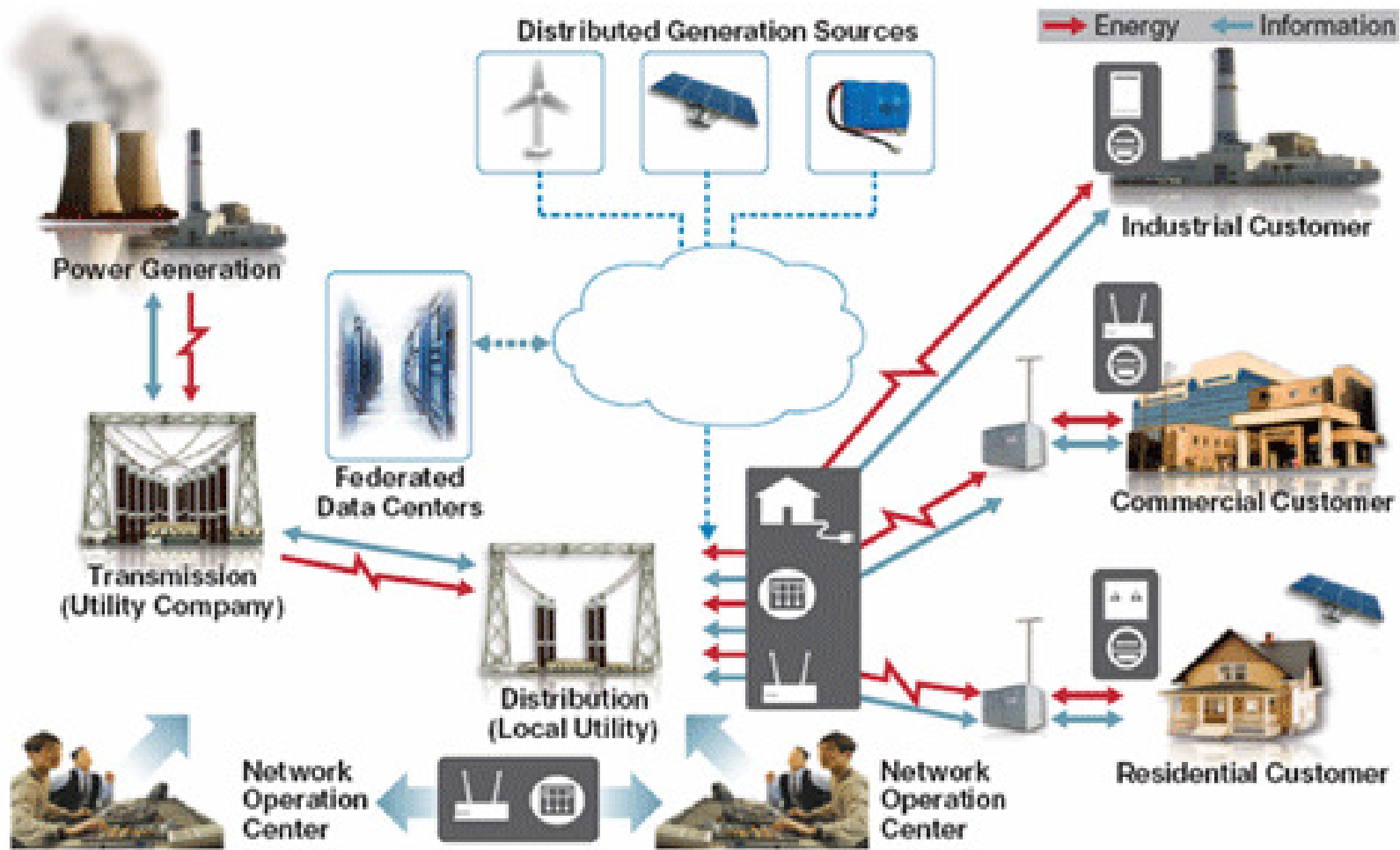
What is Smart Grid?

- Smart Grid is a collection of data communication networks that interface with the power grid to gather and analyze the data about power usage, transmission & distribution.
- The Smart Grid networks provide a wealth of information that can be used to optimize energy production by suppliers and its consumption by the customers.
- The additional connectivity layer increases the complexity of the system and creates a number of security issues.
- The Smart Grid is a part of the critical infrastructure and is therefore susceptible to cyber and physical attacks.
- New security approaches are required to secure the Smart Grid infrastructure as it evolves.





Source: <http://cnslab.snu.ac.kr/twiki/bin/view/Main/Research>



Source: <http://www.connectm.com/newsletter6.html>

NIST IR 7628, Guidelines for Smart Grid Cyber Security

- NIST Interagency Report 7628, *Guidelines for Smart Grid Cyber Security* was published in August 2010.
- It presents an analytical framework that organizations can use to develop effective cyber security strategies tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities.
- The guidelines include important elements, such as a high-level strategy that organizations can use to develop an approach to securing their Smart Grid systems, including identifying appropriate security requirements.
- In addition, the guidelines identified potential cryptography issues that entities may encounter and solutions for resolving these issues.



NIST IR 7628 (Cont.)

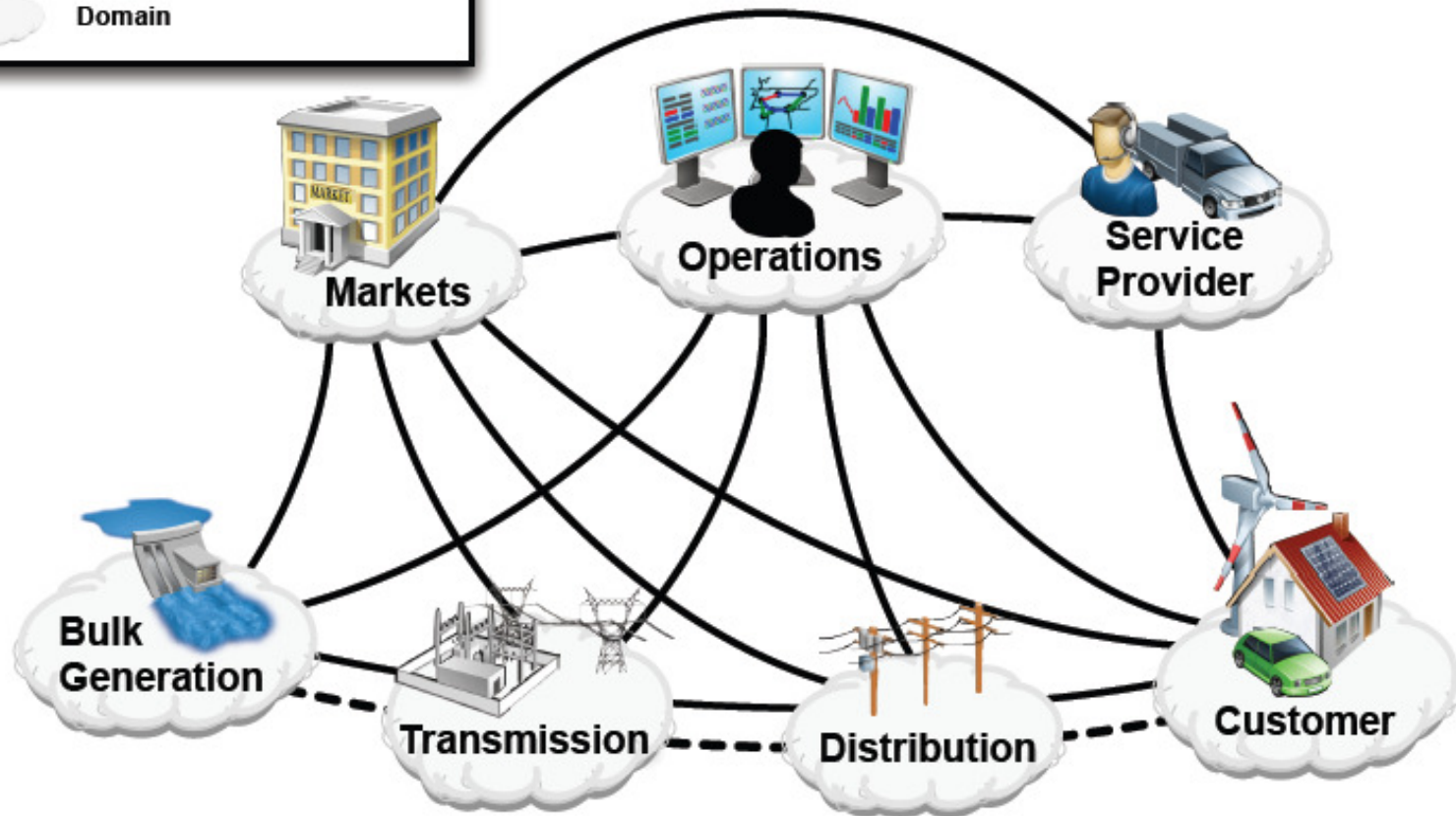
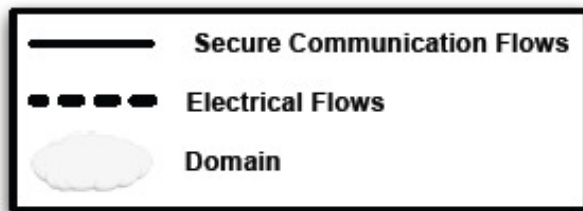
- Identified potential Smart Grid vulnerabilities, as well as the possible impacts to organizations should the vulnerabilities be exploited;
- Identified Smart Grid security problems, including how to ensure that access can be gained to critical devices and systems by personnel when ordinary authentication fails for any reason, and how to ensure that updates utilities send to smart meters are secure;
- Detailed cybersecurity design issues, such as for password complexity rules; and
- Identified Smart Grid cybersecurity areas requiring further research and development.
- Although NIST largely addressed the key elements in developing its guidelines, it did not address an important element essential to securing Smart Grid systems and networks, such as risk of combined cyber-physical attacks.



NIST IR 7628 (Cont.)

- Since 2009, NIST facilitated a process with stakeholders (e.g., utilities, Smart Grid technology vendors, standards development organizations, and others) to identify interoperability and cybersecurity standards related to smart grid.
- In January 2010, NIST reported that this process resulted in the identification of 75 standards that support Smart Grid interoperability. Of these, 11 involved cybersecurity.
- NIST is involved in developing a framework for identifying interoperability & cybersecurity standards, and has identified the need for developing cybersecurity guidelines for organizations such as electric companies, IT system vendors, and others involved in developing and implementing Smart Grid systems.





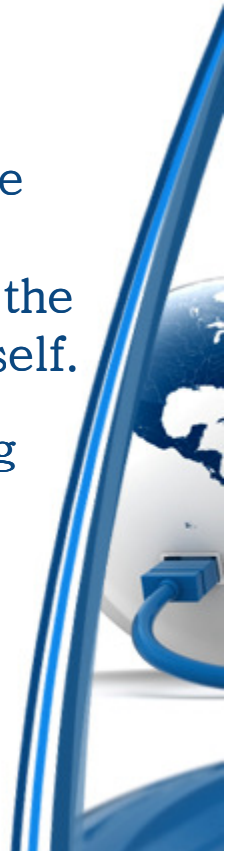
Interaction among actors in Smart Grid domains through secure communication flows and flows of electricity.

Source: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (NIST SP 1108)



NIST IR 7628 (Cont.) VULNERABILITY CLASSES

- People, Policy & Procedures. A failure in, lack of, or deficiency in policies & procedures can lead to security risks for the organization.
- Platform Software/Firmware. Errors or oversights in software and firmware design, development, and deployment may result in unintended functionality that lets attackers or other conditions to affect, via programmatic means, the confidentiality, integrity & availability of information.
- Platform Vulnerabilities. The platform comprises the software, the operating system used to support that software, and the physical hardware. Vulnerabilities arise in this part of the SG network due to the complexities of architecting, configuring & managing the platform itself.
- Network. Involves connections b/w multiple locations or units using many differing devices and similar protocols or procedures to facilitate a secure exchange of information. Risks occur within SG networks when policy management & procedures do not conform to required standards & compliance polices as they relate to the data exchanged.



NIST IR 7628 (Cont.)

- NIST IR 7628 describes the following approaches to securing the Smart Grid:
- Determine the logical interface categories. A thorough analysis of the actors, domains, information systems, and network and communications requirements is necessary to adequately determine the logical interface categories.
- Assess risk. Identify the threats, security constraints, and issues associated with each logical interface category along with the impact (low, moderate, or high) to the organization if there is a compromise of confidentiality, integrity, and/or availability.
- Select the initial set of baseline security requirements based on the logical interface categories. Tailor and supplement the security requirements as needed based on an organizational assessment of risk and local conditions.



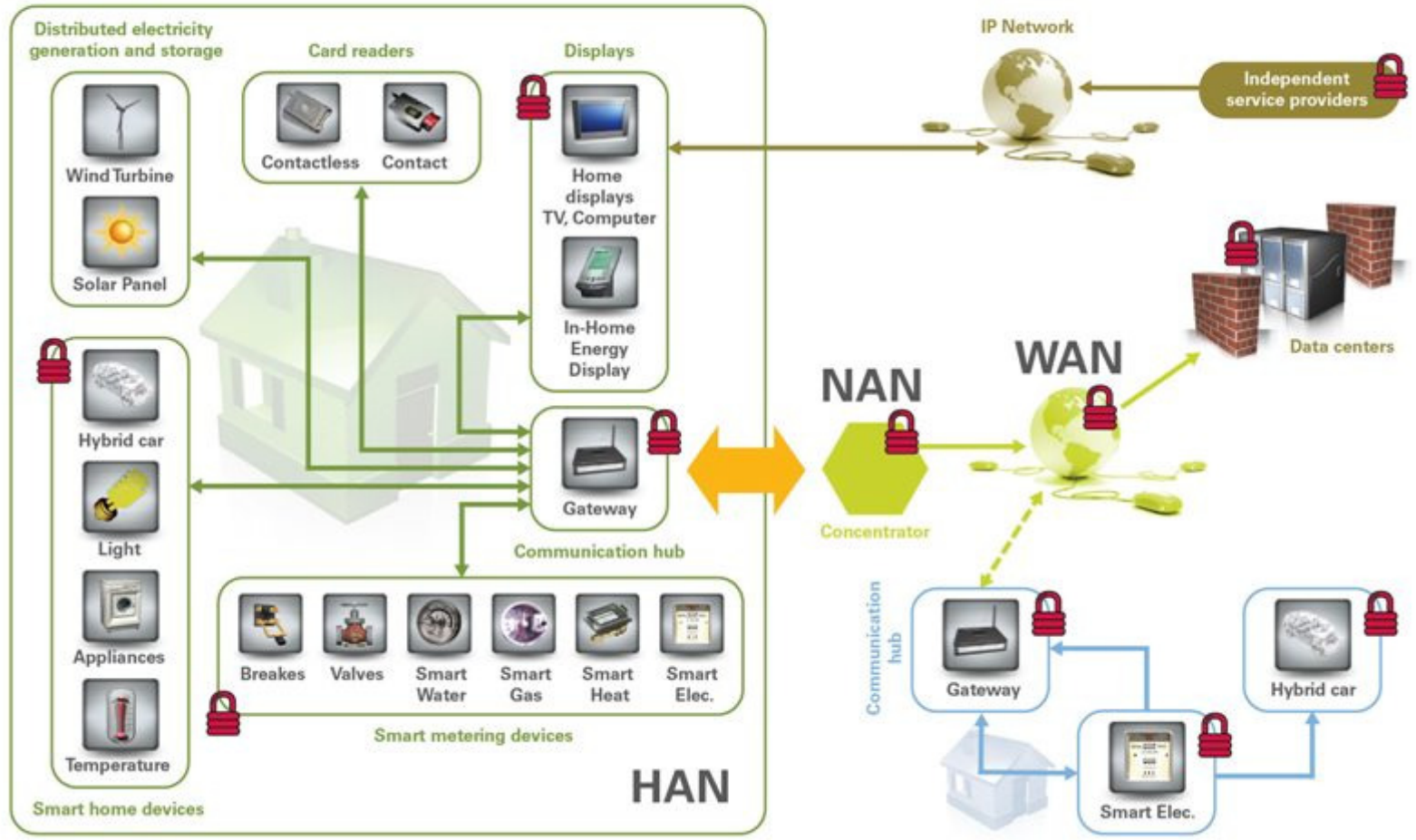
NIST IR 7628 (Cont.)

Critical SG R&D challenges fall into 4 categories:

- Device Level: research can guide efforts to devise cost-effective, tamper-resistant architectures for smart meters and other components, which are necessary for systems-level survivability and resiliency and for improving intrusion detection in embedded systems.
- Cryptography and Key Management: enables key management on a scale involving, potentially, tens of millions of credentials and keys as well as local cryptographic processing on the sensors such as encryption and digital signatures.
- Systems Level: research on a number of related topics is required to further approaches to building advanced protection architecture that can evolve and can tolerate failures, possibly of a significant subset of constituents.
- Networking Issues: research to investigate ways to ensure that commercially available components, public networks like the Internet, or available enterprise systems can be implemented without jeopardizing security or reliability.



Smart Grid Security



Source: http://www.nxp.com/news/content/file_1817.html

Challenges to SG Cybersecurity

- Unlike some legacy systems that rely on standalone devices, the Smart Grid system is a networked and integrated infrastructure.
- The Smart Grid's electricity transmission and distribution facilities also rely on data communications to optimize the transmission and distribution process.
- The Smart Grid vision and its increased reliance on IT systems and networks expose the electric grid to potential and known cybersecurity vulnerabilities associated with using such systems. These potential vulnerabilities include:

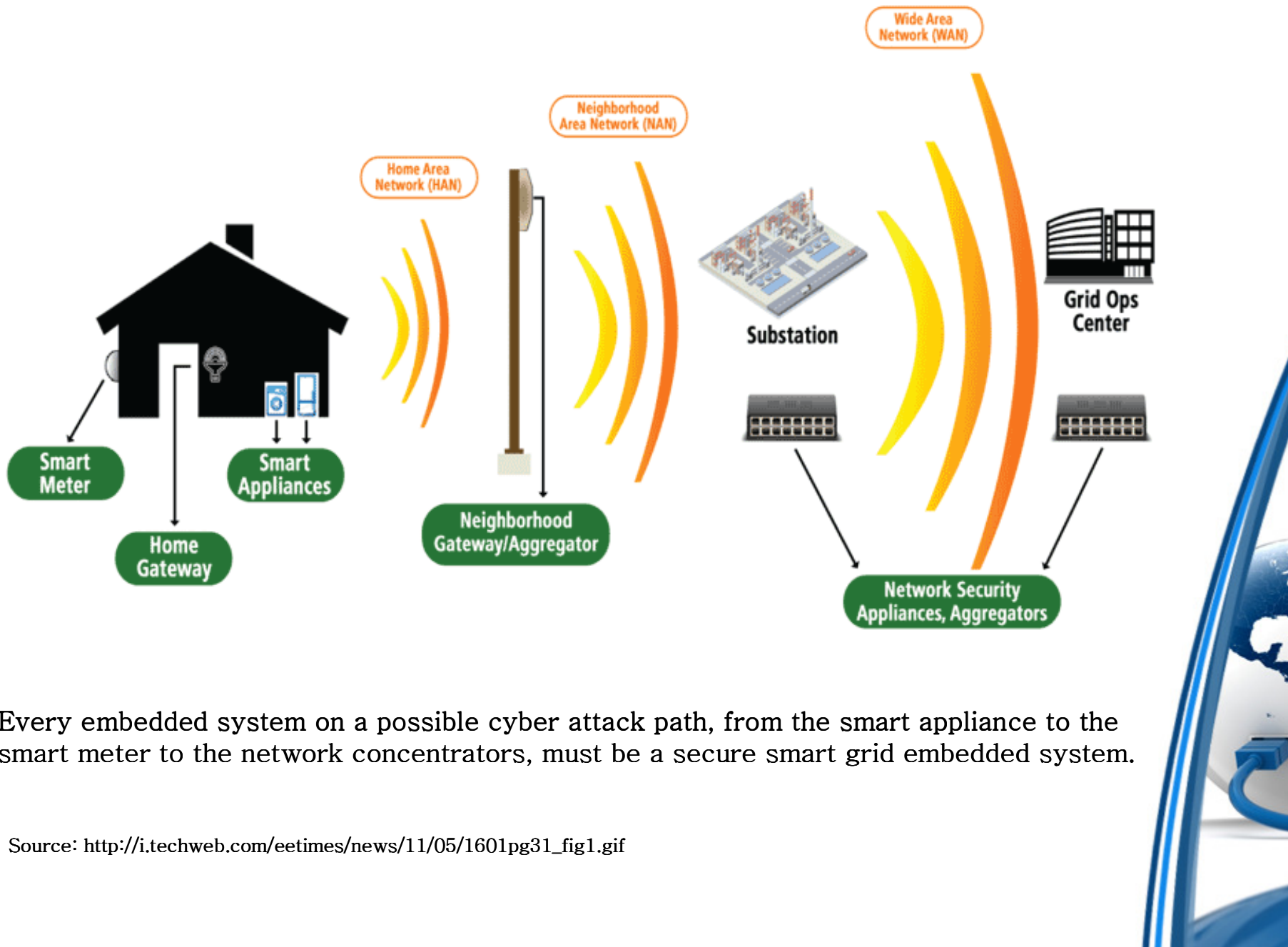


Challenges to SG Cybersecurity

(Cont.)

- Increasing the use of systems and networks increases the number of entry points and paths that can be exploited by potential adversaries and other unauthorized users;
- Increasing the use of new system and network technologies can introduce new, unknown vulnerabilities;
- Smart Grid and related systems have known cyber vulnerabilities. Cybersecurity experts have demonstrated that certain smart meters can be successfully attacked, and the impact of such attacks includes the ability to disrupt the electricity grid.





Every embedded system on a possible cyber attack path, from the smart appliance to the smart meter to the network concentrators, must be a secure smart grid embedded system.

Source: http://i.techweb.com/eetimes/news/11/05/1601pg31_fig1.gif

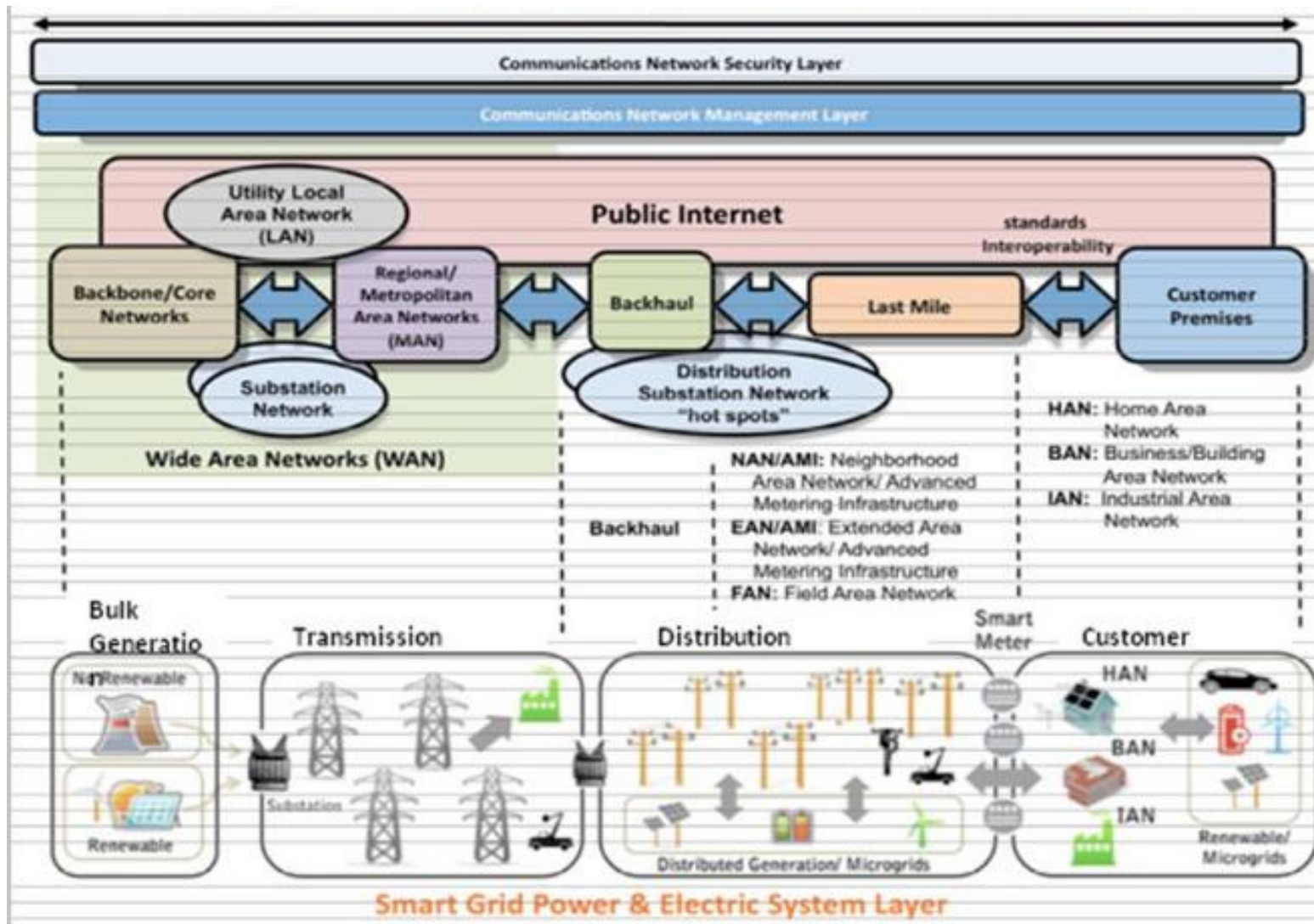
Challenges to SG Cybersecurity

(Cont.)

Network World identified the following cybersecurity issues:

- The utilities' focus is on regulatory compliance instead of comprehensive security.
- There is a lack of security features being built into Smart Grid systems.
- The electricity industry does not have an effective mechanism for sharing information on cybersecurity and other issues. The electricity industry lacks an effective mechanism to disclose information about Smart Grid cybersecurity vulnerabilities, incidents, threats, lessons learned, and best practices in the industry.
- The electricity industry does not have metrics for evaluating cybersecurity.





End-to-end Smart Grid communication model.

Source: <http://zeitgeistlab.ca/doc/Guide-for-Smart-Grid-interoperability.html>

Mapping of NIST IR 7628 Security Req's to Common Criteria Security Req's

- SG.AC-5 Information Flow Enforcement
 - The Smart Grid information system enforces assigned authorizations for controlling the flow of information
 - FDP_IFC.1 Subset information flow control
- SG.AC-8 Unsuccessful Login Attempts
 - The Smart Grid information system enforces a limit of organization-defined number of consecutive invalid login attempts by a user during an organization-defined time period
 - FIA_AFL.1 Authentication failure handling
- SG.AC-9 Smart Grid Information System Use Notification
 - The Smart Grid information system displays an approved system use notification message or banner before granting access to the Smart Grid information system
 - FTA_TAB.1 Default TOE access banners



Mapping of NIST IR 7628 to CC (Cont.)

- SG.AC-11 Concurrent Session Control
 - The organization limits the number of concurrent sessions for any user on the Smart Grid information system
 - FTA_MCS.1 Basic limitation on multiple concurrent sessions
- SG.AC-12 Session Lock
 - The Smart Grid information system prevents further access to the Smart Grid information system by initiating a session lock after a time period of inactivity or upon receiving a request from a user
 - FTA_SSL.1, FTA_SSL.2, TSF and User-initiated locking
- SG.AC-13 Remote Session Termination
 - The Smart Grid information system terminates a remote session at the end of the session or after a time period of inactivity
 - FTA_SSL.3, FTA_SSL.4 TSF and User-initiated termination



Mapping of NIST IR 7628 to CC (Cont.)

- SG.AC-14 Permitted Actions without Identification or Authentication
 - The organization identifies user actions that can be performed on the Smart Grid information system without identification or authentication
 - FIA_UAU.1 Timing of authentication and FIA_UID.1 Timing of identification
- SG.AU-2 Auditable Events
 - The organization develops the Smart Grid information system list of auditable events and includes execution of privileged functions in the list of the events
 - FAU_GEN.1 Audit Data generation
- SG.AU-3 Content of Audit Records
 - The Smart Grid information system produces audit records for each event
 - FAU_GEN.1 Audit Data generation



Mapping of NIST IR 7628 to CC (Cont.)

- SG.AU-5 Response to Audit Processing Failures
 - The Smart Grid information system alerts designated organizational officials in the event of an audit processing failure; and executes an organization-defined set of actions
 - FAU_STG.2 Guarantees of audit data availability
- SG.AU-7 Audit Reduction and Report Generation
 - The Smart Grid information system provides an audit reduction and report generation capability
 - FAU_SAR.1 Audit review and FAU_SAR.3 Selectable audit review
- SG.AU-8 Time Stamps
 - The Smart Grid information system uses internal system clocks to generate time stamps for audit records
 - FPT_STM.1 Reliable time stamps



Mapping of NIST IR 7628 to CC (Cont.)

- SG.AU-9 Protection of Audit Information
 - The Smart Grid information system protects audit information and audit tools from unauthorized access, modification, and deletion
 - FAU_STG.1 Protected audit trail storage
- SG.AU-15 Audit Generation
 - The Smart Grid information system provides audit record generation capability and generates audit records for the selected list of auditable events and allows authorized users to select auditable events
 - FAU_SEL.1 Selective audit and FAU_GEN.1 Audit data generation
- SG.AU-16 Non-Repudiation
 - The Smart Grid information system protects against an individual falsely denying having performed a particular action.
 - FCO_NRO.2 Enforced proof of origin



Mapping of NIST IR 7628 to CC (Cont.)

- SG.CM-11 Configuration Management Plan
 - The organization develops and implements a configuration management plan for the Smart Grid information system
 - ALC_CMC CM capabilities
- SG.IA-4 User Identification and Authentication
 - The Smart Grid information system uniquely identifies and authenticates users (or processes acting on behalf of users).
 - FIA_UAU.1 Timing of authentication and FIA_UID.1 Timing of identification
- SG.SA-3 Life-Cycle Support
 - The organization manages the Smart Grid information system using a system development lifecycle methodology that includes security
 - ALC Life-Cycle Support



Mapping of NIST IR 7628 to CC (Cont.)

- SG.SA-10 Developer Security Testing
 - The Smart Grid information system developer creates a security test and evaluation plan. The developer documents the results of the testing and evaluation and submits them to the organization for approval
 - ATE_FUN Functional Tests
- SG.SC-8 Communication Integrity
 - The Smart Grid information system protects the integrity of electronically communicated information
 - FDP_UIT.1 Data exchange integrity
- SG.SC-9 Communication Confidentiality
 - The Smart Grid information system protects the confidentiality of communicated information
 - FDP_UCT.1 Basic data exchange confidentiality
- SG.SI-2 Flaw Remediation
 - ALC_FLR.2 Flaw reporting procedures



Mapping of NIST IR 7628 to CC (Cont.)

- SG.SC-10 Trusted Path
 - The Smart Grid information system establishes a trusted communications path between the user and the Smart Grid information system
 - FTP_TRP.1 Trusted path
- SG.SC-11 Cryptographic Key Establishment and Management
 - The organization establishes and manages cryptographic keys for required cryptography employed within the information system
 - Cryptographic key management (FCS_CKM)
- SG.SC-19 Security Roles
 - The Smart Grid information system design & implementation specifies the security roles & responsibilities for the users of the Smart Grid information system
 - FMT_SMR.1 Security Roles



Protection Profile for the Gateway of a Smart Metering System

- The Gateway serves as the communication component between the components in the LAN of the consumer and the outside world. It can be seen as a special kind of firewall dedicated to the smart metering functionality. It also collects, processes and stores the records from the Meter(s) and ensures that only authorized parties have access to them or derivatives thereof. Before sending relevant information the information will be signed and encrypted using the services of a Security Module. The Gateway features a mandatory user interface, enabling authorized consumers to access the data relevant to them.
- The Meter itself records the consumption or production of one or more commodities (e.g. electricity, gas, water, heat) in defined intervals and submits those records to the Gateway. The Meter Data has to be signed before transfer in order to ensure its authenticity and integrity unless the transmission is physically protected due to the Meter & the Gateway being implemented within one device and utilizing a wired or optical connection. The Meter further supports the encryption of its connection to the Gateway.

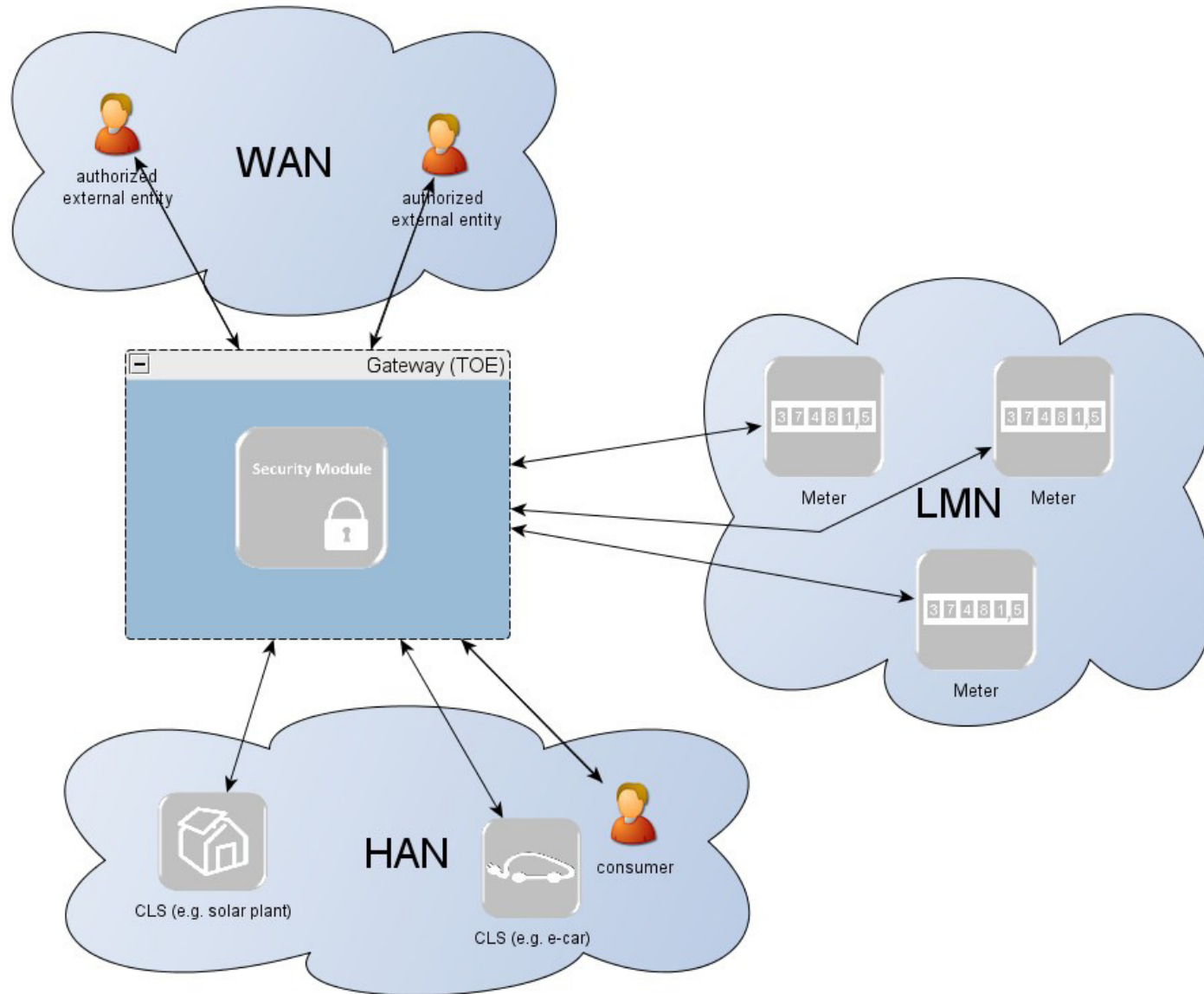


Protection Profile for the Gateway of a Smart Metering System (Cont.)

- The Gateway utilizes the services of a Security Module (e.g. a smart card) as a cryptographic service provider and as a secure storage for confidential assets. The Security Module will be evaluated separately according to the requirements in the corresponding Protection Profile.
- Controllable Local Systems may range from local power generation plants, controllable loads such as air condition and intelligent household appliances to applications in home automation. CLS may utilize the services of the Gateway for communication services. However, CLS are not part of the Smart Metering System.
- EAL 4 augmented by AVA_VAN.5 and ALC_FLR.2 is used



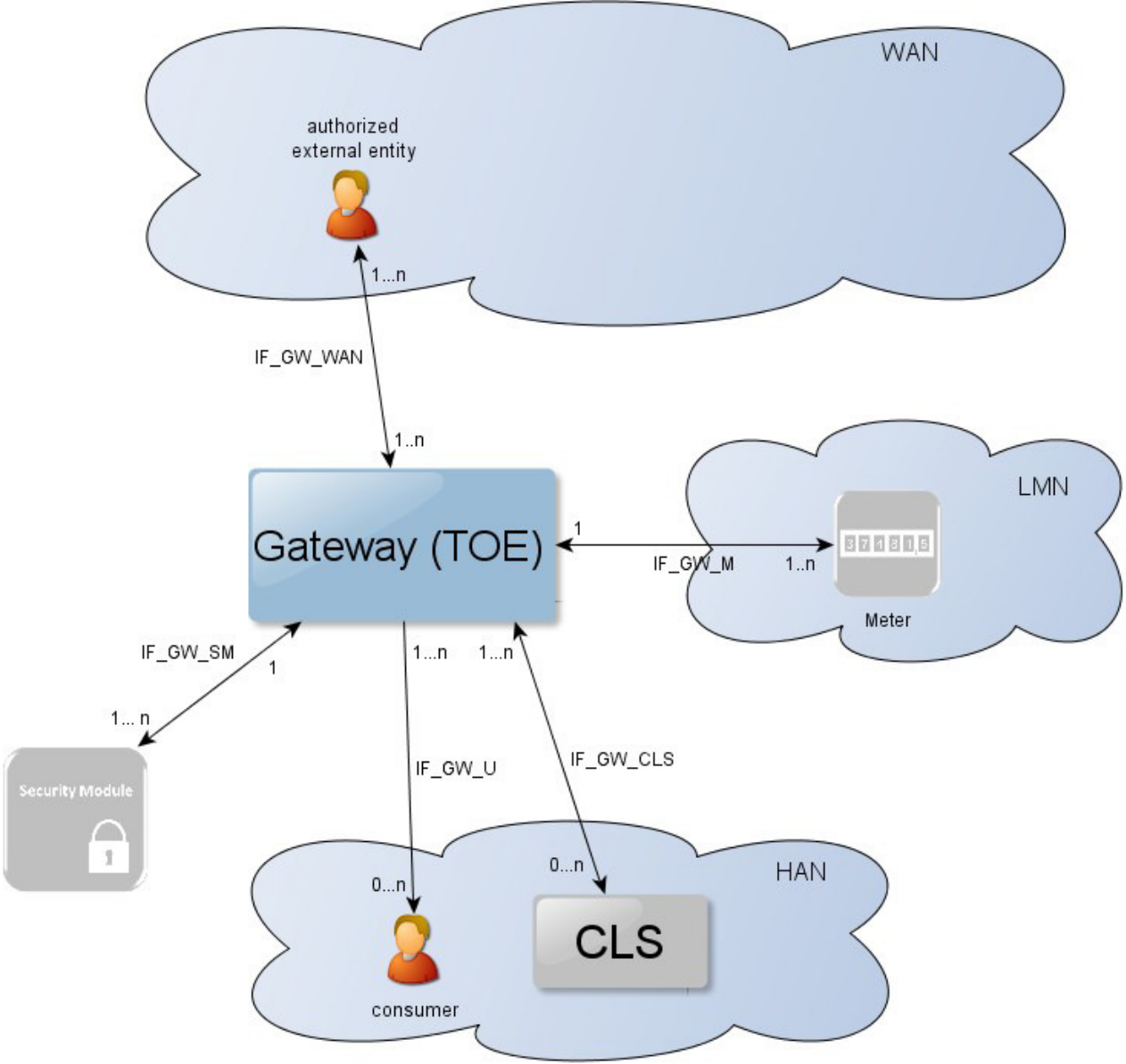
TOE and its environment



Source: Protection Profile for the Gateway of a Smart Metering System, German Federal Office for Information Security



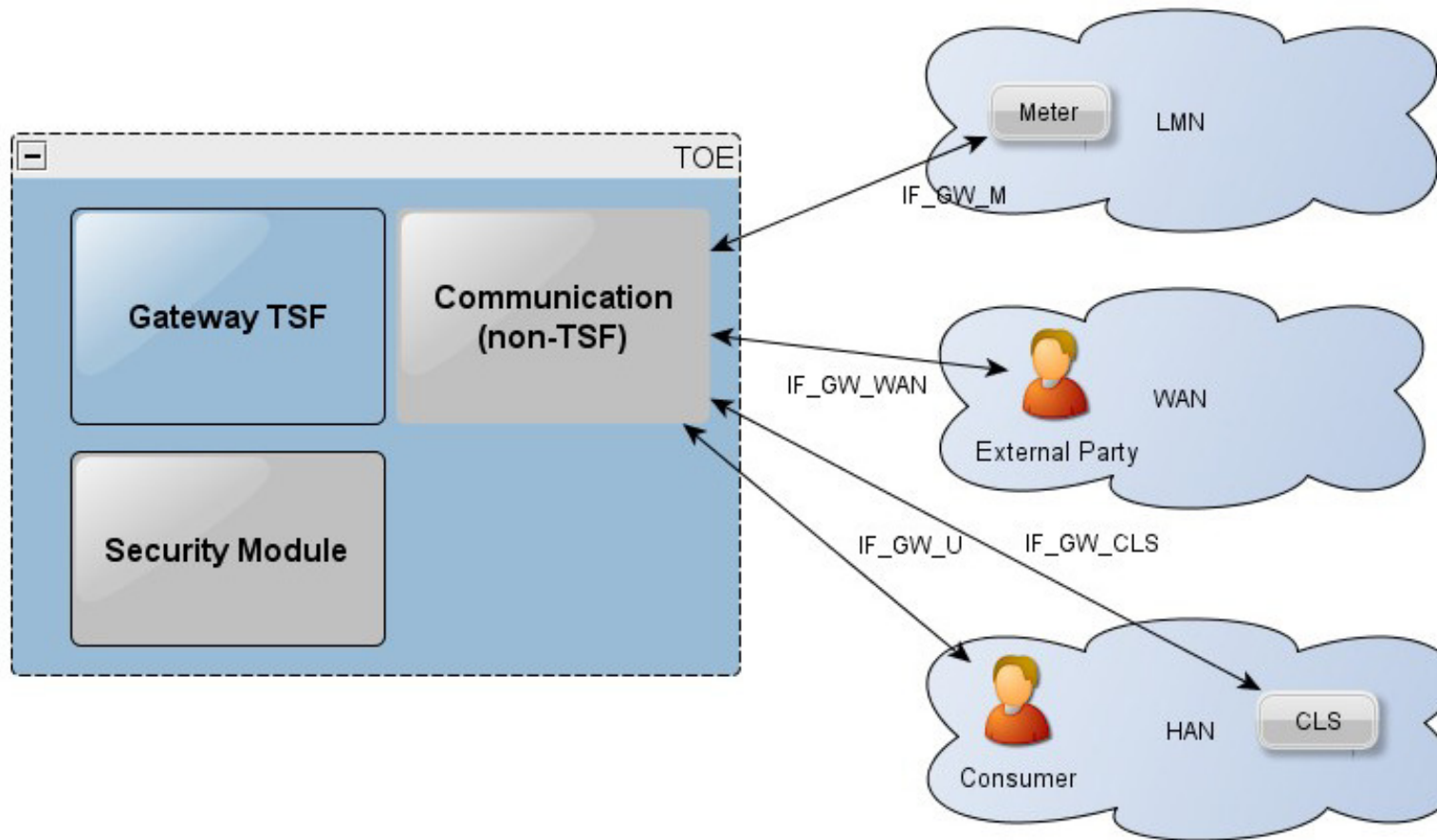
Logical Interfaces of the TOE



Source: Protection Profile for the Gateway of a Smart Metering System, German Federal Office for Information Security

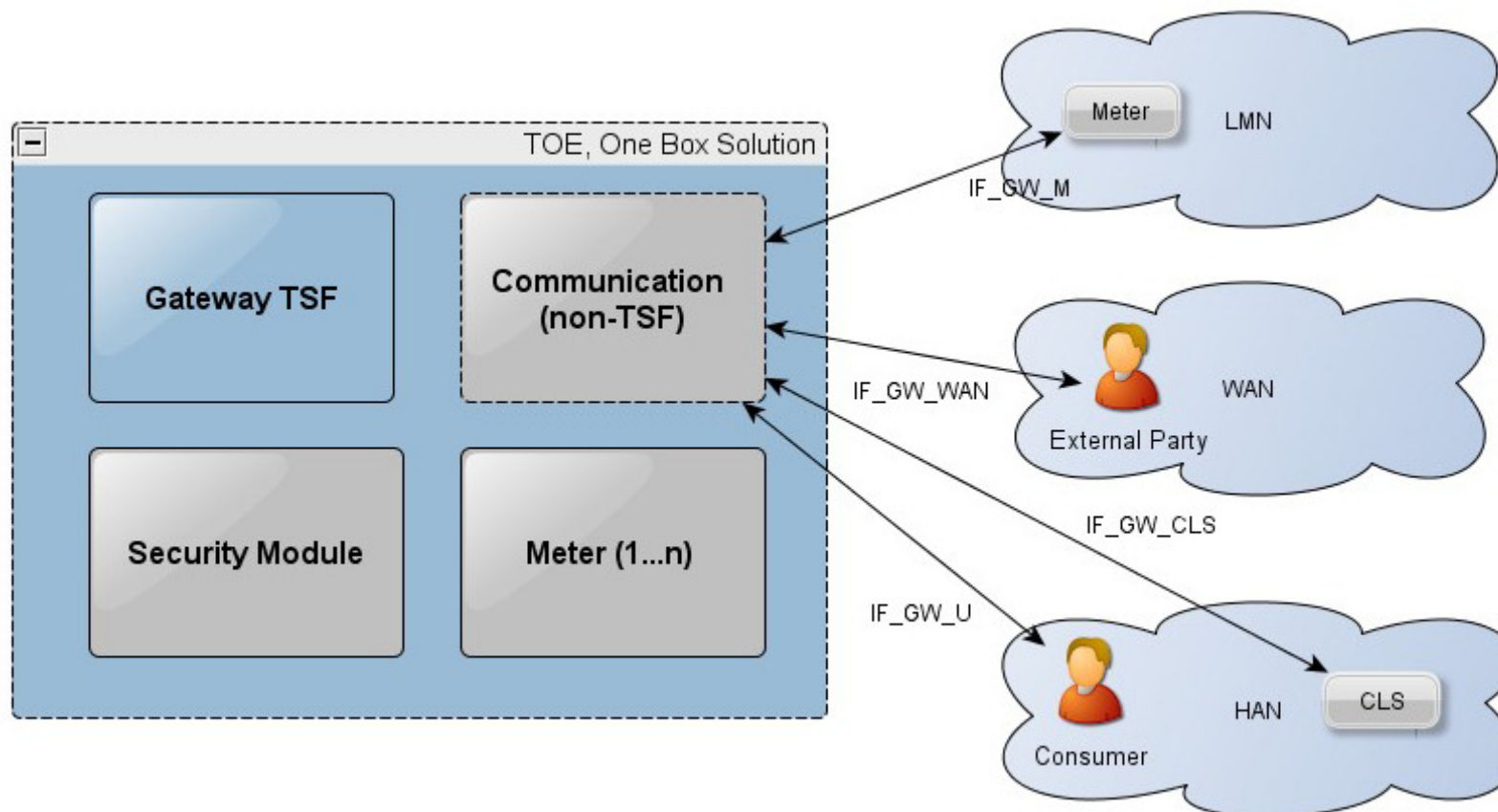


A Gateway and multiple Meters



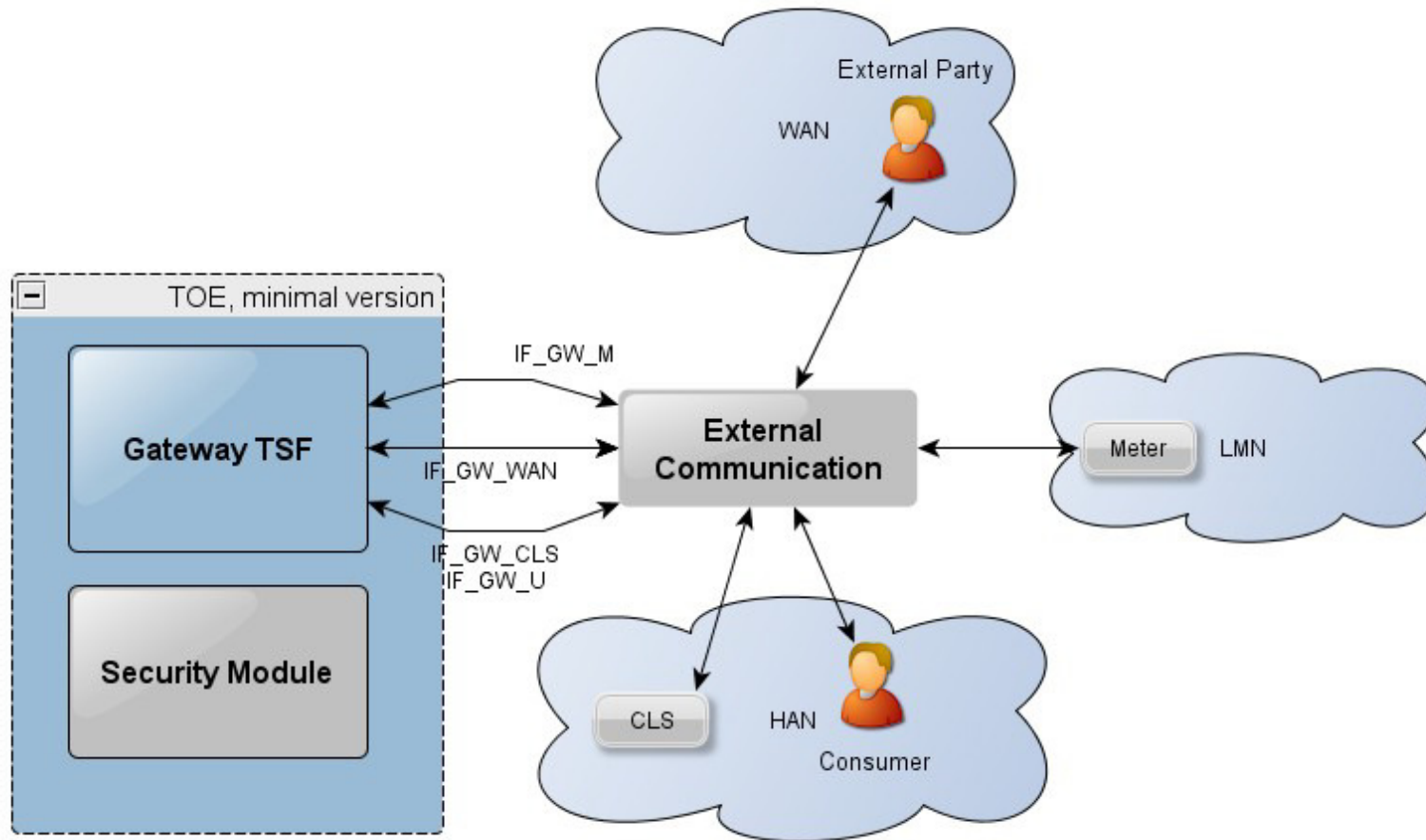
Source: Protection Profile for the Gateway of a Smart Metering System, German Federal Office for Information Security

One Box Solution



Source: Protection Profile for the Gateway of a Smart Metering System, German Federal Office for Information Security

Minimal implementation



Source: Protection Profile for the Gateway of a Smart Metering System, German Federal Office for Information Security



Class FAU: Security Audit

- FAU_ARP/SYS.1 Security alarms for system log
- FAU_GEN/SYS.1 Audit data generation for system log
- FAU_SAA/SYS.1 Potential violation analysis for system log
- FAU_SAR/SYS.1 Audit review for system log
- FAU_STG/SYS.4 Prevention of audit data loss for the system log
- FAU_GEN/CON.1 Audit data generation for consumer log
- FAU_SAR/CON.1 Audit review for consumer log
- FAU_STG/CON.2 Guarantees of audit data availability for consumer log
- FAU_GEN/CAL.1 Audit data generation for calibration log
- FAU_SAR/CAL.1 Audit review for calibration log
- FAU_STG/CAL.4 Prevention of audit data loss for the calibration log
- FAU_GEN.2 User identity association
- FAU_STG.1 Protected audit trail storage for all logs
- FCO_NRO.2 Enforced proof of origin



Class FCS: Cryptographic Support

- FCS_CKM/TLS.1 Cryptographic key generation for TLS
- FCS_COP/TLS.1 Cryptographic operation for TLS
- FCS_CKM/PKCS.1 Cryptographic key generation for PKCS
- FCS_COP/PKCS.1 Cryptographic operation for PKCS#7
- FCS_COP/MTR.1 Cryptographic operation for Meter communication encryption
- FCS_CKM.4 Cryptographic key destruction
- FCS_COP/HASH.1 Cryptographic operation for Signatures
- FCS_COP/MEM.1 Cryptographic operation for TSF and user data encryption

Class FDP: User Data Protection

- FDP_ACC.2 Complete Access Control
- FDP_ACF.1 Security attribute based access control
- FDP_IFC/FW.2 Complete information flow control for firewall
- FDP_IFF/FW.1 Simple security attributes for Firewall
- FDP_IFC/MTR.2 Complete information flow control for Meter information flow
- FDP_IFF/MTR.1 Simple security attributes for Meter information
- FDP_RIP.2 Full residual information protection
- FDP_SDI.2 Stored data integrity monitoring and action



Class FIA: Identification and Authentication

- FIA_ATD.1 User attribute definition
- FIA_AFL.1 Authentication failure handling
- FIA_UAU.2 User authentication before any action
- FIA_UAU.6 Re-Authenticating
- FIA_UID.2 User identification before any action
- FIA_USB.1 User-subject binding

Class FMT: Security Management

- FMT_MOF.1 Management of security functions behavior
- FMT_SMF.1 Specification of Management Functions
- FMT_SMR.1 Security roles
- FMT_MSA/AC.1 Management of security attributes for gateway access policy
- FMT_MSA/AC.3 Static attribute initialization for gateway access policy
- FMT_MSA/FW.1 Management of security attributes for firewall policy
- FMT_MSA/FW.3 Static attribute initialization for Firewall policy
- FMT_MSA/MTR.1 Management of security attributes for Meter policy
- FMT_MSA/MTR.3 Static attribute initialization for Meter policy



Class FPR: Privacy

- FPR_CON.1 Communication Concealing
- FPR_PSE.1 Pseudonymity

Class FPT: Protection of the TSF

- FPT_FLS.1 Failure with preservation of secure state
- FPT_RPL.1 Replay Detection
- FPT_STM.1 Reliable time stamps
- FPT_TST.1 TSF testing
- FPT_PHP.1 Passive detection of physical attack

Class FTP: Trusted Path/Channels

- FTP_ITC/WAN.1 Inter-TSF trusted channel for WAN
- FTP_ITC/MTR.1 Inter-TSF trusted channel for Meter
- FTP_ITC/USR.1 Inter-TSF trusted channel for User





Suddenly, knowing a lot about the U.S. power grid became sexy at cocktail parties.

Source: http://files.eesi.org/hoecker_011509.pdf



Questions?

Eugene Polulyakh

BKP Security. Inc., Aspect Labs FIPS & Common
Criteria Lab

3080 Olcott Street
Santa Clara, California 95054

Phone: + 1-408-876-7470
E-mail: ep@aspectlabs.com

