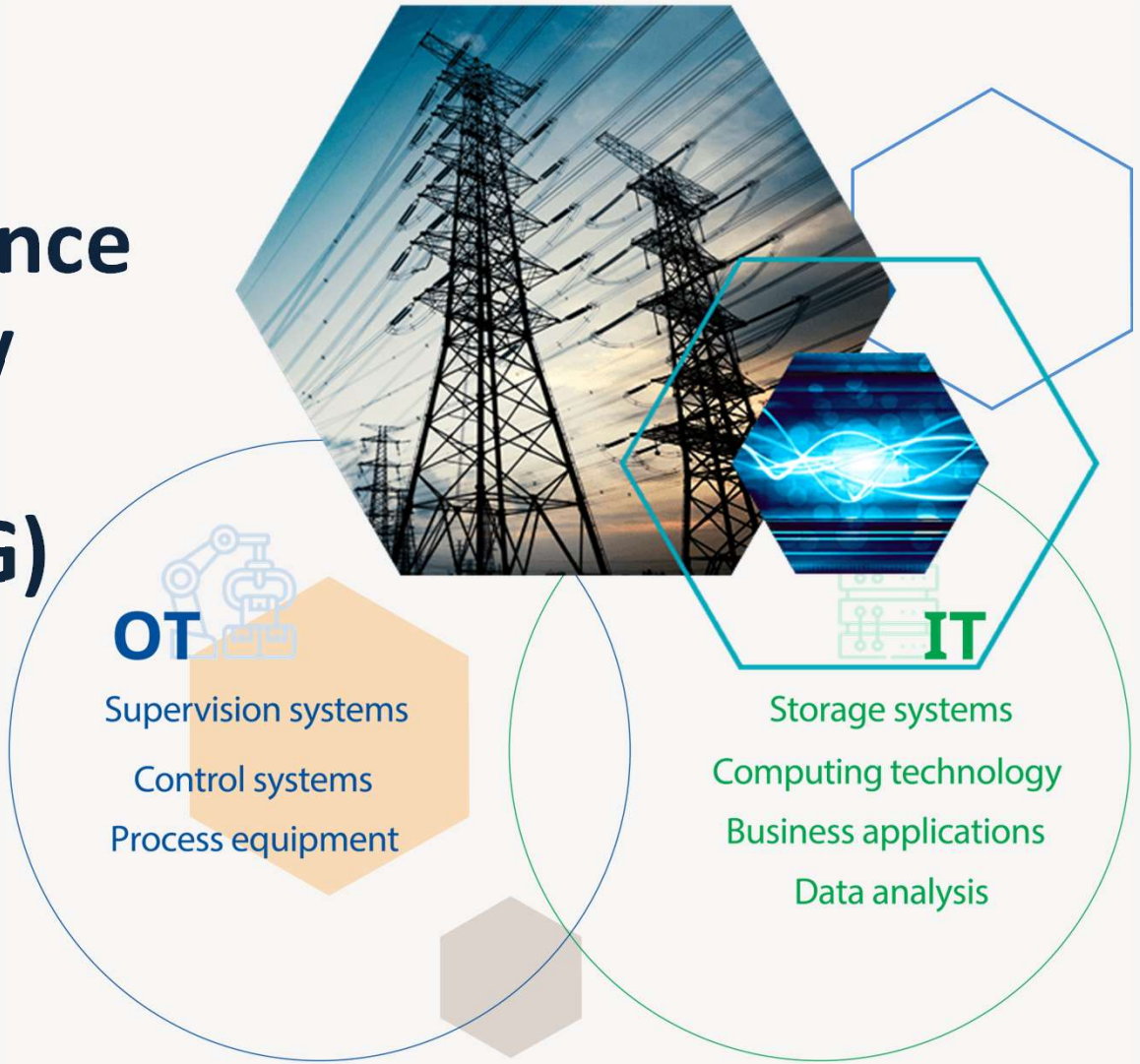
IT/OT Convergence & Cybersecurity Challenges in Electric Grid (EG)

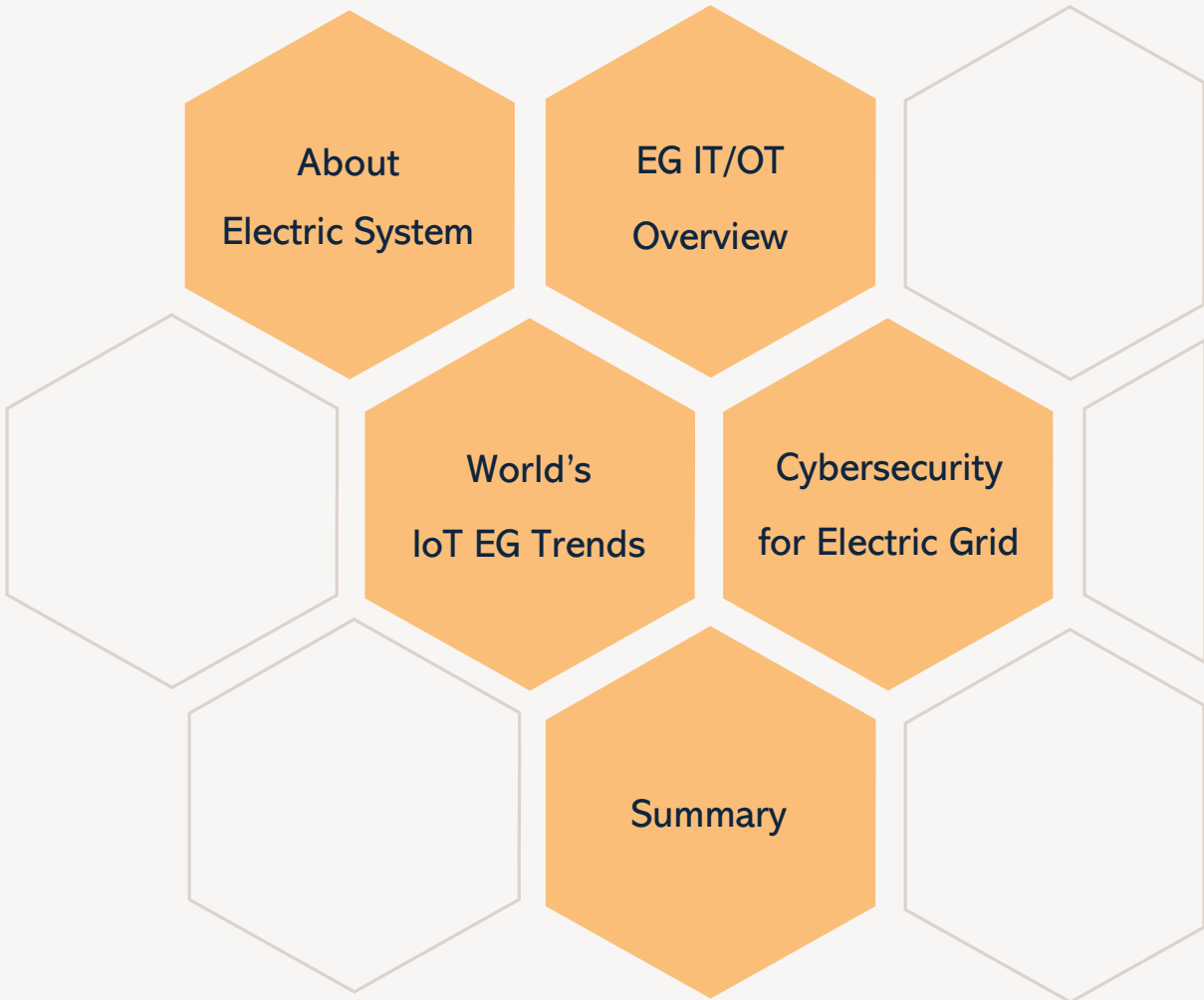
Presenter

Trung Kien DONG

SAS/SCADA/PROTEC



Plan

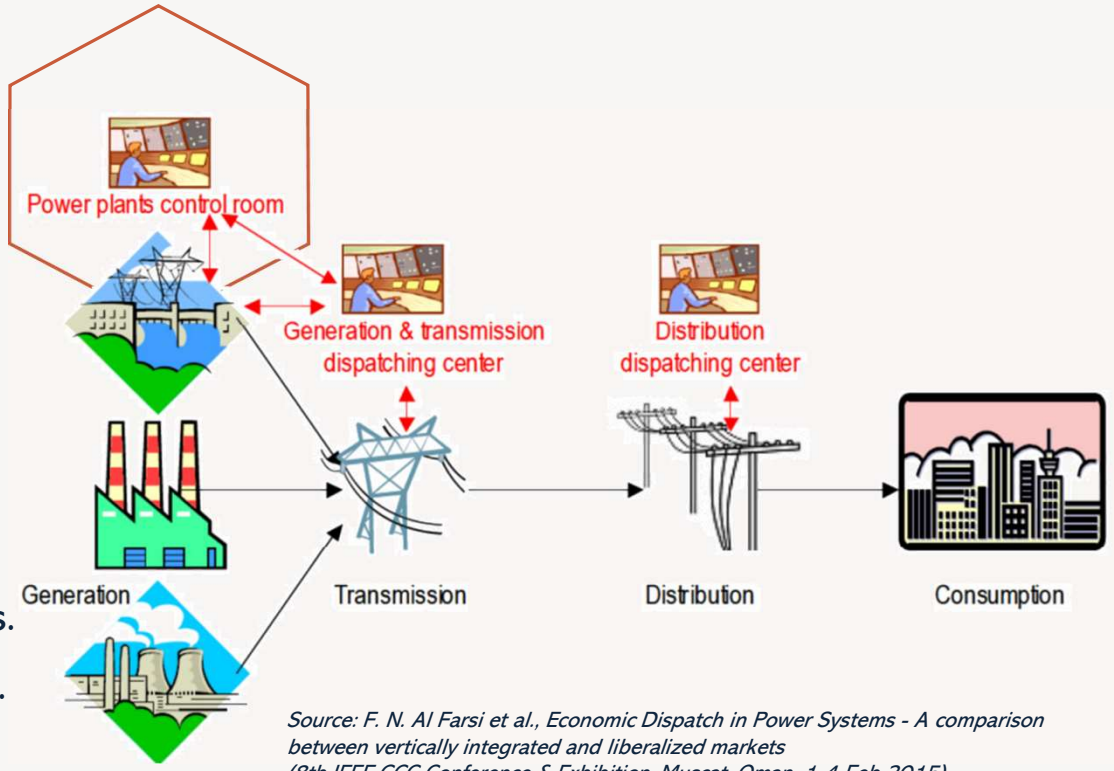

About
Electric System
EG IT/OT
Overview
World's
IoT EG Trends
Cybersecurity
for Electric Grid
Summary

About Electric System

- Generation & Transmission dispatching centers
- Generation units.
- Transmission grids.
- Distribution networks & Dispatching centers.

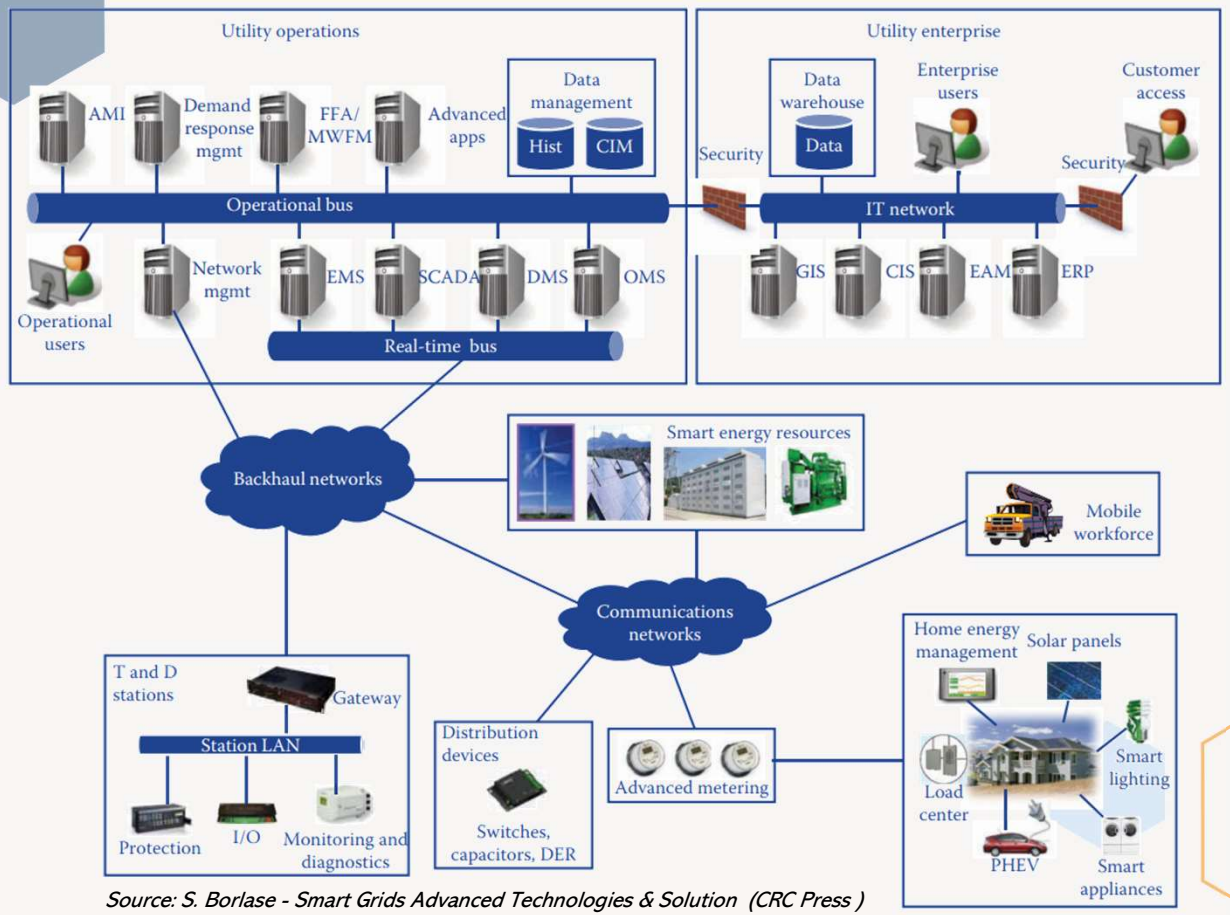
Dispatching Centers are:

- Remote Control Center of unmanned subsations.
- “Heart” of smart grid with “core” IT/OT systems.



Source: F. N. Al Farsi et al., Economic Dispatch in Power Systems - A comparison between vertically integrated and liberalized markets (8th IEEE GCC Conference & Exhibition, Muscat, Oman, 1-4 Feb 2015)

Overview EG IT/OT



Source: S. Borlase - Smart Grids Advanced Technologies & Solution (CRC Press)

- SCADA: Supervisory Ctrl & Data Acquisition
- AMI: Advanced Metering Infrastructure
- MWFM: Mobile Workforce Management
- EMS: Energy Management System
- DMS: Distribution Management System
- OMS: Outage Management System
- GIS: Geospatial Information System
- CIS: Customer Information System
- DER: Distributed Energy Resources
- CIM: Common Information Model
- EAM: Enterprise Asset Management
- ERP: Enterprise Resource Planning

Overview EG IT/OT (2)

IT/OT Dichotomy

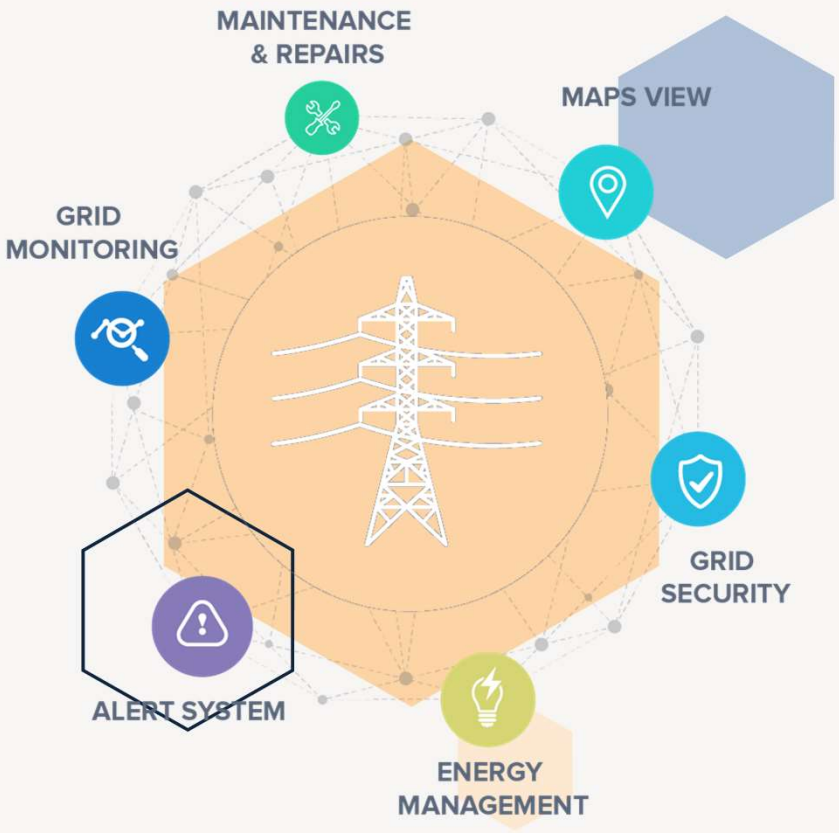
- IT and OT systems reside in different parts of the organization and are implemented on separate data and communications infrastructures with limited connectivity and data exchange between the two ones.

Current evolution

- Convergence of OT applications & processes
- Integration of the OT applications with “enterprise” or “back-office” IT applications.
- Integration through various interfaces such as file transfers, application programming interfaces (APIs), middleware, and, most recently, Web services.

Major challenges

- Adoption and integration of new technologies, many of which are unproven.
- Complexity of applying evolving standards, protocols, and operational guidelines that has high requirements for reliability, security, and control.
- Gap between technical operations and business decision-making.



OT/IT Convergence is Inevitable, and

Critical to the success of the Smart Grid (SG)

World's IoT SG Trends

The intense pressure to improve reliability, operational efficiencies;

The increase in automation and the amount of data collection points;

The ability of network operators to proactively manage large and complex networks;

... will require:

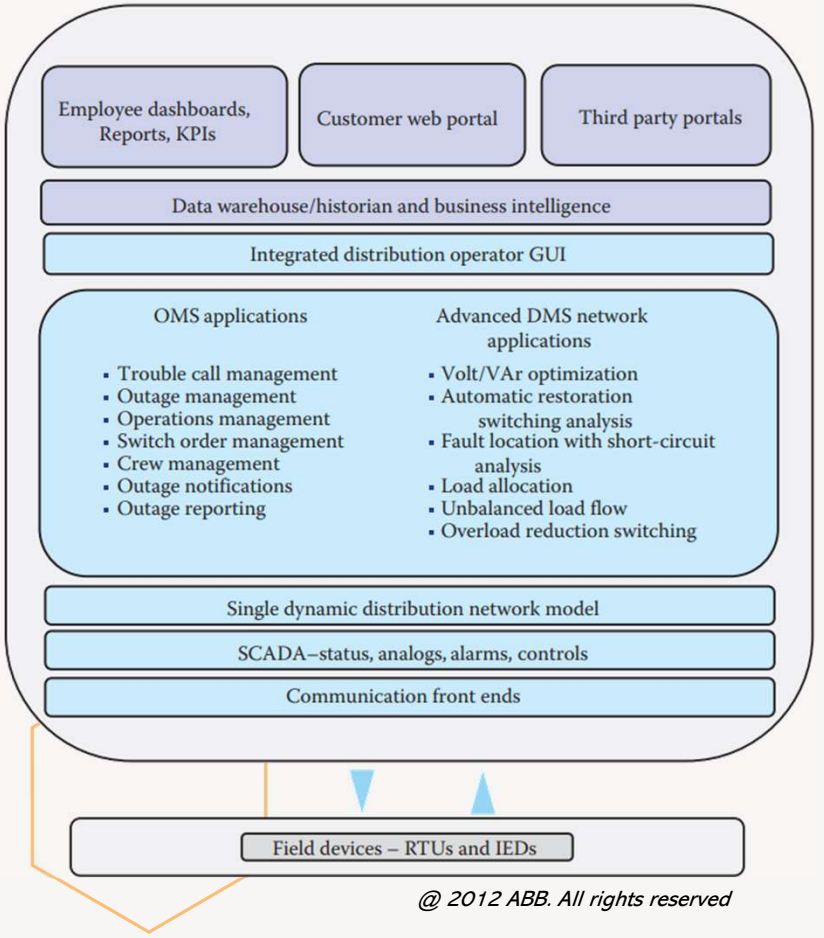
Advancements in real-time grid management systems.

New advanced tools that can turn grid data into useful information for safe, timely, and effective operational decisions to be made.

World's IoT SG Trends (2)

Case No.1: Intergrating SCADA with DMS/OMS

- Improved operations by close integration of DMS with SCADA
- Increased operator efficiency, eliminating the need for multiple systems with potentially different data
- Integrated security analysis for substation and feeder operations to check for tags in one area affecting operations in the other
- Streamlined login and authority management within one system
- One network model for OMS and DMS analysis
- Consolidated system support for DMS/OMS and SCADA



World's IoT SG Trends (3)

Case No.2: Mobile Workforce Management (MWFM/GIS)

Plan

Plan/predict future demand for long-term budget plans and short-term operational plans

Schedule

Plan, optimize, schedule, and auto-assign all work across all field technicians

Dispatch

Monitor field progress in real time; manage exceptions and emergencies

Excute

Industry leading field mobility for all work – from short-cycle to long-cycle and complex work

Analyze

Turn operational data into actionable insights to drive industry best practices/processes

World's IoT SG Trends (4)

Case No. 2: Intergrating OMS with MWFM/GIS

- Transmittal of outage assignments directly to the mobile data terminal (MDT) from the OMS
- Receiving of crew assignment status updates from the MDT (en route, arrived)
- Updating of assignments automatically to MDT as the OMS outage engine predicts outages
- Verification and completion of outages in the OMS from the MDT
- Display of crew login status in the OMS, as entered from MDT

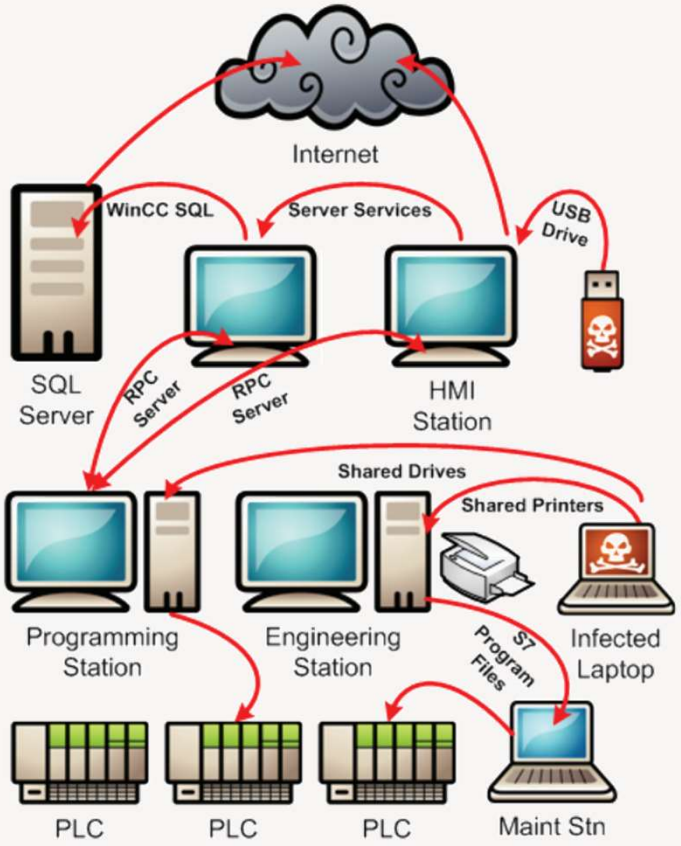
Cyberscurity for EG

Cybersecurity probleme

Cybersecurity for the utility's electrical grid monitoring and control systems (SCADA) provides the actions required to preclude the unauthorized use of, denial of service to, modification to, disclosure of, loss of revenue from, or destruction of, critical system or informational assets (IEC/TC 62443-1-1, 2009-07).

In this modern world, where remote operations are common, where physical changes can occur through the click of a button or because of the logic programmed into a device, the questions that need to be asked are:

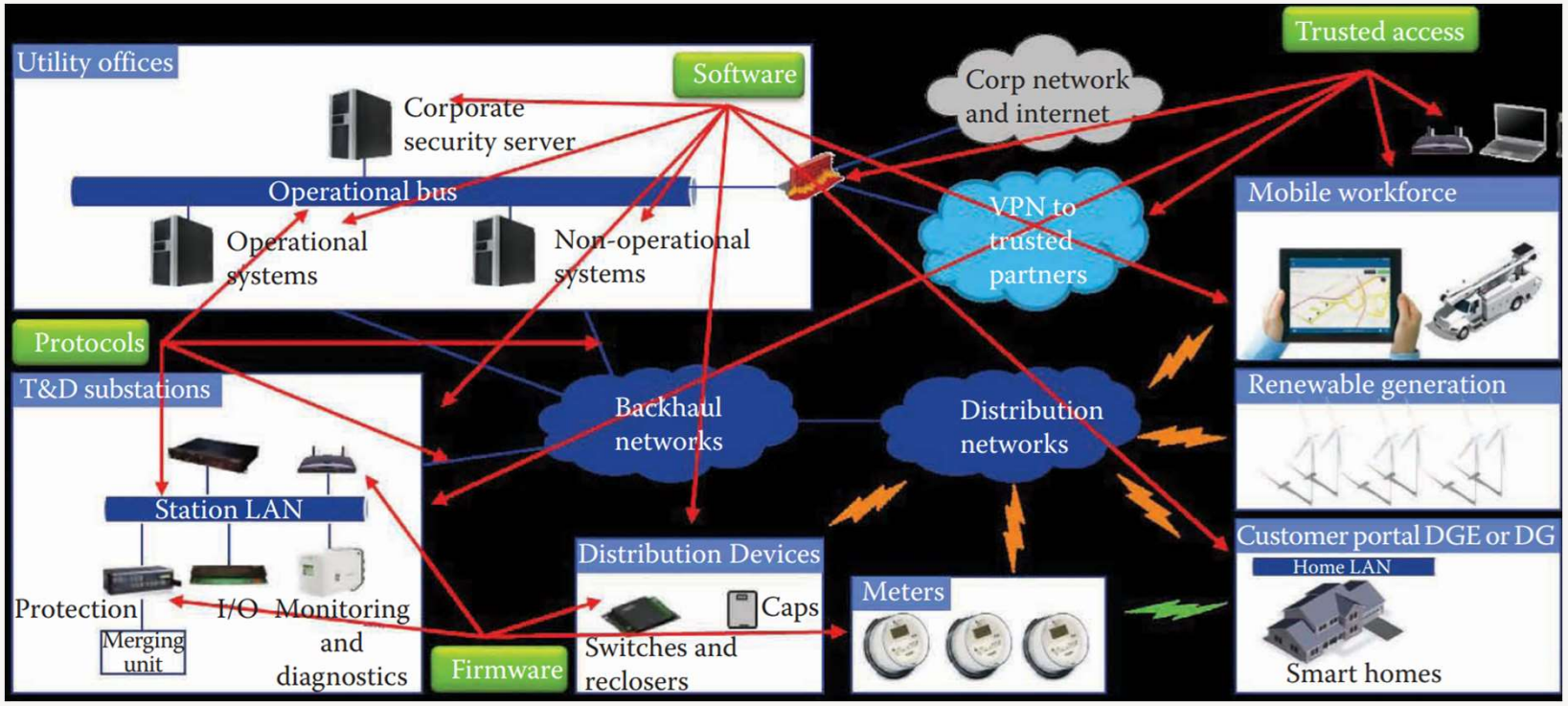
- If the utility operator can control the grid remotely, who else can?
- What happens when the information that the operator receives is not correct?
- What happens when equipment starts to act and react differently than expected?
- Is it possible for cyber attackers to navigate their way into a utility's control network (isolated) , and take control of the system?



Stuxnet's attack, Juin 2010 (Iran)

Cybersecurity for EG (2)

Common Vulnerabilites



Cyberscurity for EG (3)

Protocol Vulnerabilites

Communication protocols commonly used in utility OT applications do not have built-in security features, such as authentication, authorization, or tamper-checking capabilities. Utility protocols, such as Modbus, DNP3, IEC 60870-5-101 and IEC 60870-5-103 were first developed as proprietary serial protocols. With the addition of TCP/IP functionality and commercial off-the-shelf IT components, these protocols were given a TCP/IP wrapper, but the basic functionality of the protocol, including the lack of security features, were not changed:

- The software or hardware device must assume that the command is coming from a trusted source, and it will execute the command.
- The attacker needs to do is gain access to the network, and then send his/her own commands to the controller.
- The attacker could intercept the information, modify it, and send it on, providing false information.

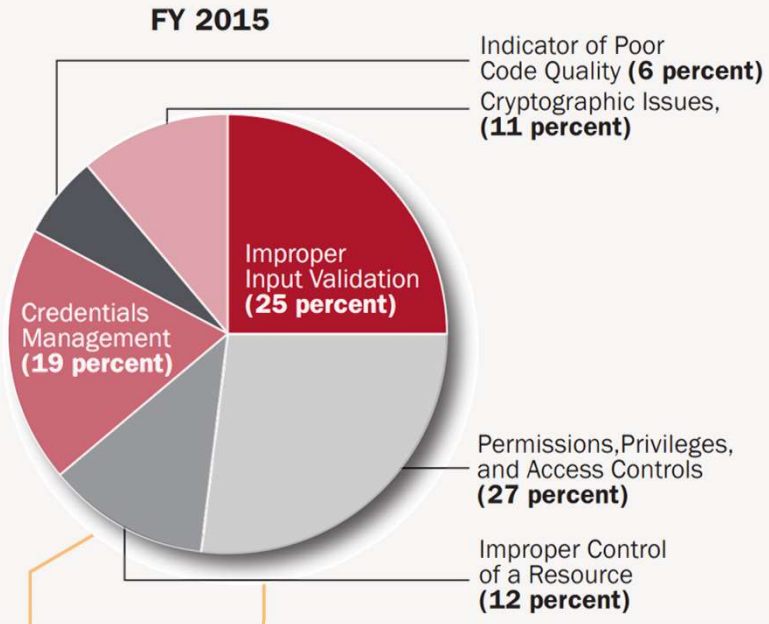
Cyberscurity for EG (4)

Firmware Vulnerabilites

Modern OT devices are much more complex:

- Some IEDs include web server for configuration and status.
- More lines of code lead to more bugs
- Modern IEDs require patching just like servers.

The two types of vulnerabilities that have consistently been more that 50% of the issues discovered are improper input validation, and permissions, privileges, and access control. Improper input validation vulnerability occurs when the software does not properly validate the data being input by the user. Permissions, privileges, and access control vulnerabilities occur when an attacker is able to bypass a defined authorization policy.



NCCIC/ICS-CERT FY 2015 Annual

Cyberscurity for EG (5)

Software Vulnerabilites

The products used in the OT world have a long-life span. That means utilities are working with OT & OS products that were potentially designed before the need for cybersecurity was generally accepted in the control system world. What used to be considered good coding practices are now potentially insecure coding practices.

- Many SCADA systems are not patched current.
- No patches available for older versions of windows.
- OS and application patches can break SCADA systems.

Existing OT products are being modified, replacing vulnerable code with secure code, and updating the products to include security features. However, this is a process and not a one-time event. They are continually finding vulnerabilities, fixing them, and providing patches to us, their customers.

- Patching often requires all system update & re-testing.

Unauthorized applications installed on SCADA systems can interfere with SCADA operation. For example:

- Web browsing from HMI can infect OT systems by: browser vulnerabilities, downloads, cross-site scripting, spyware.

Cyberscurity for EG (6)

Trusted Access Vulnerabilites

Firmware updates and PLC, IED programming are sometimes done by vendor:

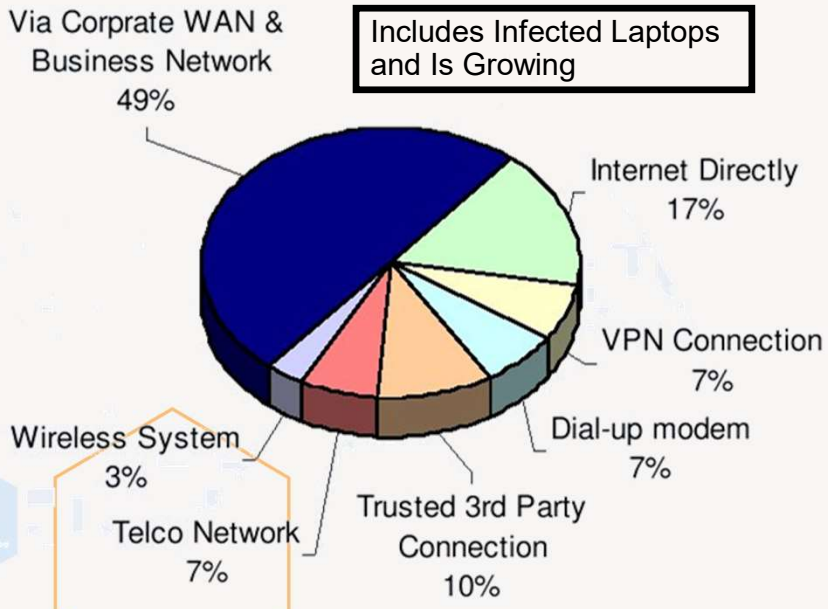
- Many PLC, IED have open maintenance ports.
- Infected vendor laptops can bring down PLC, IED via LAN.

Partners may require continuous status information for maintenance and monitoring via trusted accesses (e.g VPN):

- Partner access is often poorly secured.
- Partner channels can serve as backdoors.

3rd parties may include:

- OPC, historian storage (SQL), monitoring service or agency...



A. Wright ACM CCS Conf.erence Tutorial Nov. 2019

Summary

OT/IT convergence is inevitable, and critical to the success of the Smart Grid and of the digital transformation in the Electric Grid.

IT security solutions (e.g firewall) are insufficient and the isolated silos are insecure under cyber attack.

Convergencing OT and IT systems into a networked environment to monitoring and control cyber risque is nowaday world's trend (M. Kranz – Building the Internet of Things @Wiley 2017)

Thank you