IEEE Power System Communication & Cybersecurity Committee

IEEE PES - Chicago Chapter
Grid Automation Communication Protocols

January 12, 2022
Benton Vandiver III
Chair - PSCCC P0 Subcommittee
(Protocols & Architecture)

NIST 2010 Milestones for Smart Grid Requirements

Smart meter upgradeability standard (completed)

- Common specification for price and product definition (early 2010)
- Common scheduling mechanism for energy transactions (early 2010)
- Common information model for distribution grid management (EoY 2010)
- Standard demand response signals (early 2010)
- Standards for energy use information (mid 2010)
- DNP3 Mapping to IEC 61850 Objects (2010)
- Harmonization of IEEE C37.118 with IEC 61850 and PTP precision time Sync (mid 2010)
- Transmission and distribution power systems models mapping (EoY 2010)
- Guidelines for use of IP protocol suite in the Smart Grid (mid 2010)
- Guidelines for use of wireless communications in the Smart Grid (mid 2010)
- Energy storage interconnection guidelines (mid 2010)
- Interoperability standards to support plug-in electric vehicles (EoY 2010)
- Standard meter data profiles (EoY 2010)
- Harmonize power line carrier standards for appliance communications in the home (EoY 2010)

The industry changed much quicker than expected…

Power Grid ICS Disruptive Events

2005-2010: Stuxnet
2014: German Steel Mill Attack
2015: Ukraine BLACKENERGY 2/3 (Sandworm)
2016: Ukraine Kiev Substation (Crashoverride)
2017: Saudi Arabia TRISIS

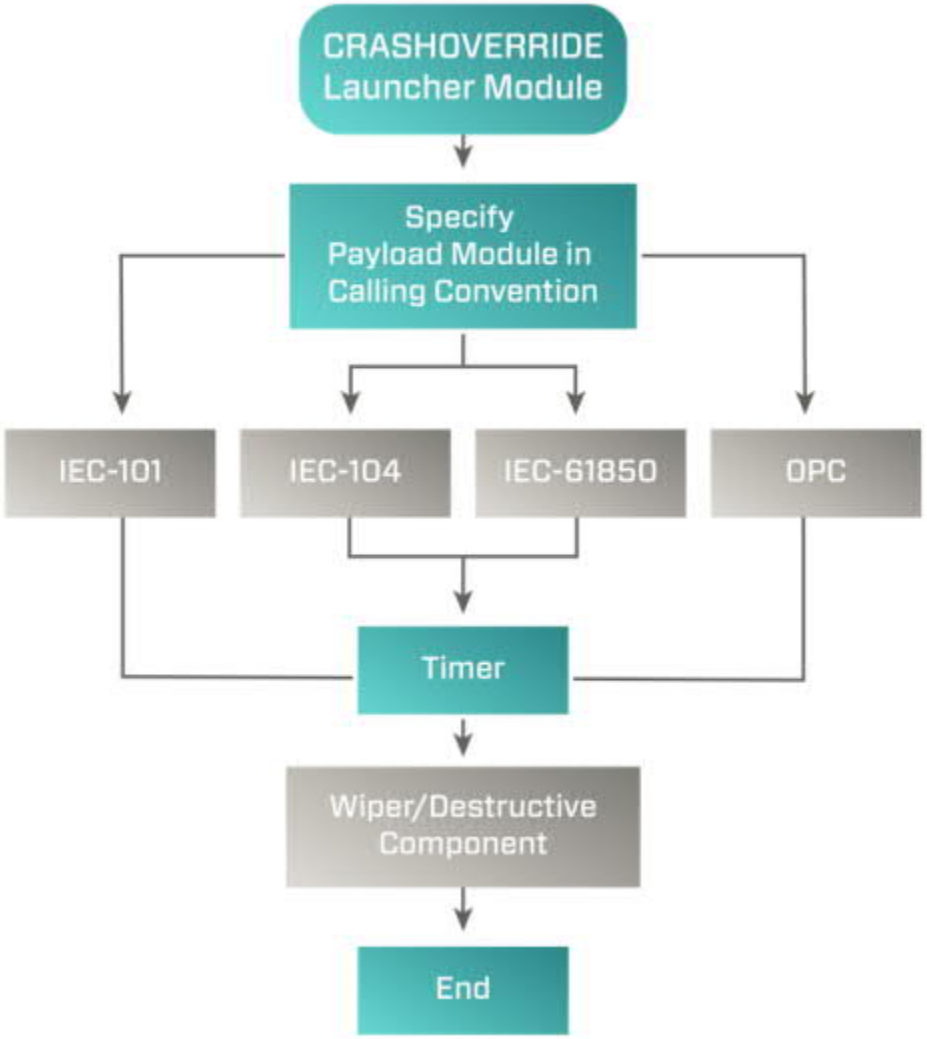
Source: Dragos_Crashoverride2018 report.

Note: Crashoverride was the first ICS-targeting malware against the electric grid. Of concern is the protocol specific packaging targeting grid operations devices.

Power Grid ICS Disruptive Events

Note: Crashoverride was the first ICS-targeting malware against the electric grid. Of concern is the protocol specific packaging targeting grid operations devices.

Once delivered in the network any device using the protocol was infected. Mitigation requires early detection of a network breach.



Source: Dragos_Crashoverride2018 report.

Introduction to PES-PSCCC:

The Power System Communications committee was recently rebooted (2012-2015) to dedicate resources to the standards evolving from cybersecurity issues in power networks and refocus on communications.

The new Power System Communications and Cybersecurity Technical Committee (PSCCC) is a standards developing committee of the IEEE Power & Energy Society. Our members are industry leaders, practitioners, researchers, and students with a common professional interest in addressing the challenges of enabling the transfer of information and in securing all aspects of the power system domain.

The PSCCC is made up of seven (7) subcommittees; they are:

[C] Power Line Carrier, [D] Wireless, [E] Wire Line, [F] Optical Fiber, [P] Protocols and Architecture, [S] Cybersecurity, and [T] Broadband PLC

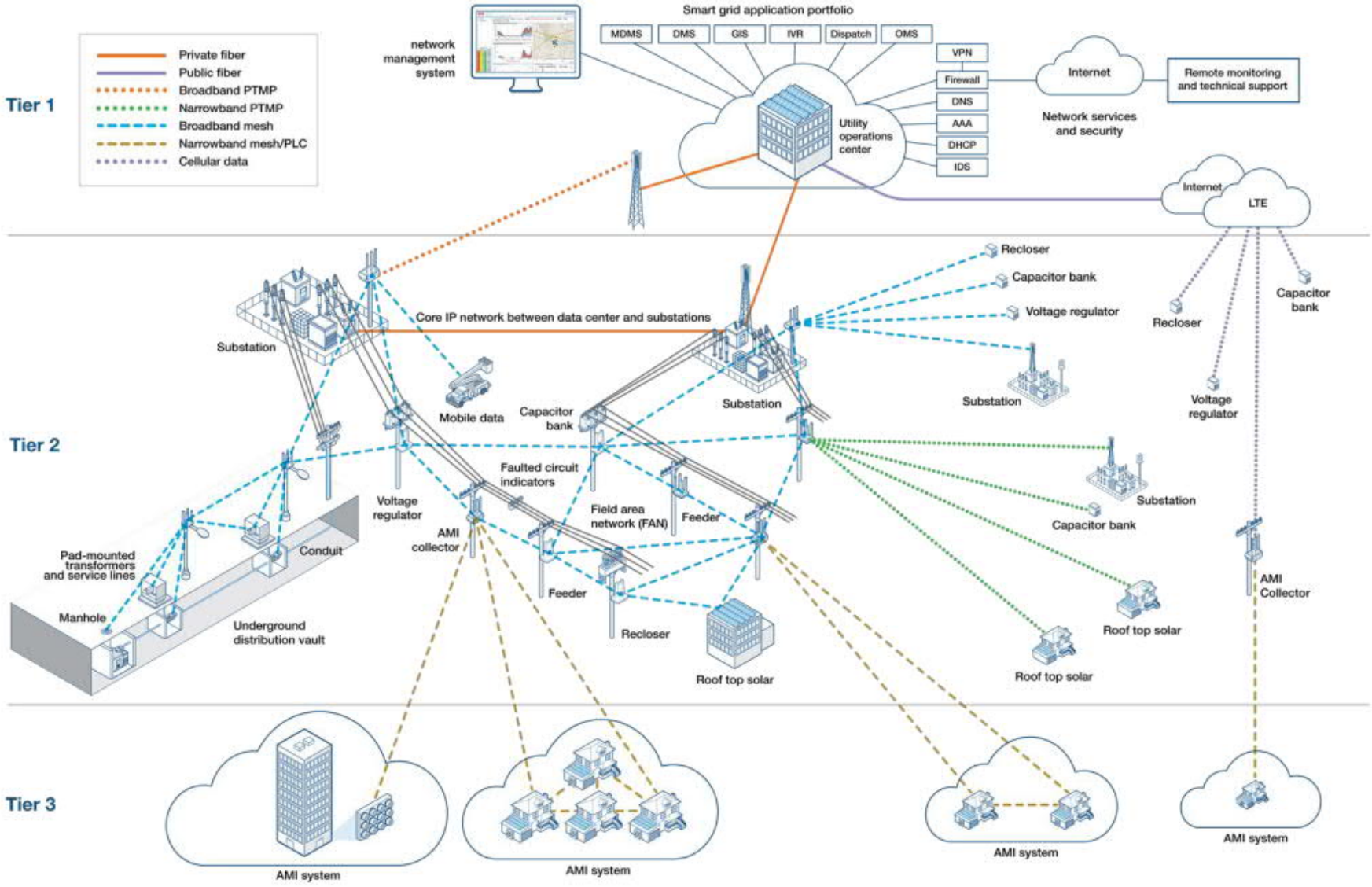
Standards that are Current:

[C] Power Line Carrier,	P643; PC57.13.9; PC93.5
[D] Wireless,	(802.x when grid specific)
[E] Wire Line,	P487a; P820; 367-1996/2012; 487-2000/2007/2015; 487.1-2014; 776-1992/2018; 820-2006; 1137-1991/2018
[F] Optical Fiber,	1590-2003/2009; P1591.1 /.3 /.4; P1594; P1595; PC37.94
[P] Protocols and Architecture,	P1815; P1815.2; P2030; P2664; PC37.118.2; PC37.236; PC37.238;
[S] Cybersecurity,	711-200; P1547.3; P1686; P1711; P1711.1; P2030.102.1; P2658; P2808; PC37.240
[T] Broadband PLC,	(pending)

P0 Standards Work:

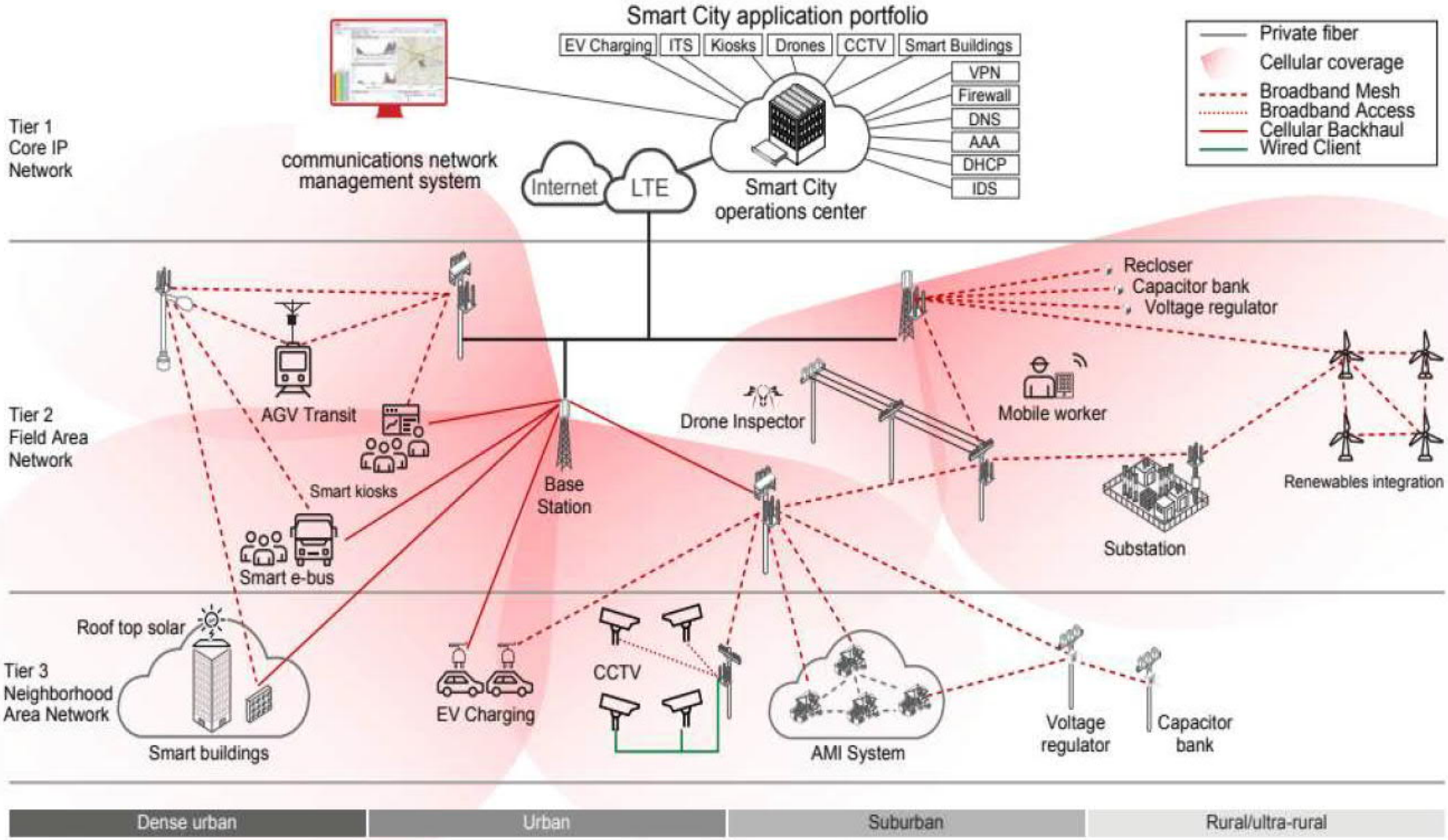
[P] Protocols and Architecture,
P1547; (DER Interface - Joint WG)
P1815; (DNP 3.0)
P1815.2; (DNP 3.0 for DERs)
P1854; (Smart Distribution Applications - Joint WG)
P2030; (Smart Grid Interoperability - Joint WG)
P2664; (Streaming Telemetery Transport Protocol)
PC37.118.2; (SynchroPhasors)
PC37.236; (Protection Applications over Digital Comm Channels)
PC37.238; (PTP Power Profile)
IEEE/IEC 61850-9-3 (PTP-PUP - Joint WG)
New PAR - Universal Utility Data Exchange (UUDEX)
New PAR - Architectures Supporting Virtualization of P&C Applications
Reports - Beginner's Guide to IEC61850; Analog Leased Line EoL Migration; Cloud Computing Requirements for EP Utilities; Recommended mappings between C37.118.2 and IEC61850; Application of Ethernet Networking Devices Used in P&C Applications in EP Substations.

Utility architecture diagram



MDMS = meter data management system DMS = distribution management system GIS = geographic information system IVR = interactive voice response OMS = outage management system
VPN = virtual private network DNS = domain name system AAA = authentication, authorization and accounting DHCP = dynamic host control protocol IDS = intrusion detection system PTMP = point-to-multipoint PLC = power line carrier

Smart City Application



AGV Automated Guided Vehicle; **EV** Electric Vehicle; **ITS** Intelligent Transportation System; **LTE** Long Term Evolution; **VPN** Virtual Private Network; **AAA** Authentication Authorization and Accounting; **DHCP** Dynamic Host Control Protocol; **IDS** Intrusion Detection System; **PTMP** Point To Multi Point; **FCI** Faulted Circuit Indicator; **DNS** = Domain Name System

Approved & Proposed IEEE Smart Grid Standards

See:
12.2.Approved and Proposed IEEE Smart Grid Standards.pdf

Present key protocol standards are:
IEC 61850 - all parts and reports
Timing Profiles using 1588 (PTP) - **IEC 61850-9-3/C37.238**
P1815 - DNP3.0
P2030.100 - (series)
C37.118.1&2 (PMUs)
P1547.x (series)

Questions?

Please join us if interested, https://site.ieee.org/pes-pscc/