Dissecting Smart Meters

Justin Searle
Managing Partner – UtiliSec

Who is UtiliSec

- A security services company specializing in helping electric utilities
- Managing Partners
  - Darren Highfill (darren@utilisec.com)
  - Joe Bucciero (joe@utilisec.com)
  - Justin Searle (justin@utilisec.com)
- List of services
  - Critical Functionality in Industry Collaboration
  - Security Architecture Guidance and Review
  - Penetration Testing and Security Assessments
  - On the Job and Classroom Training
  - Policy Composition

Who are we to give this Talk?

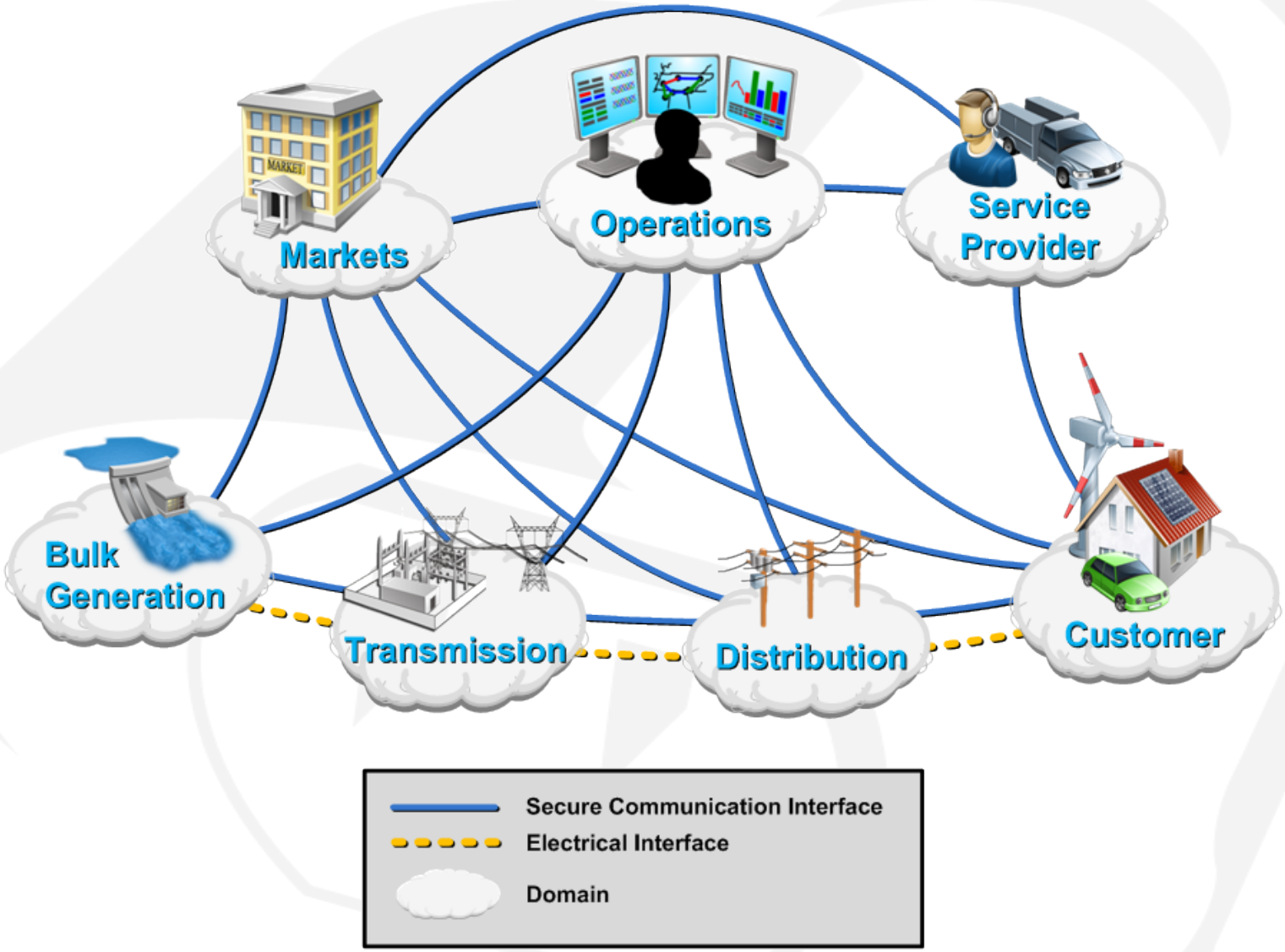
- UtiliSec team has been working with electric utilities, vendors, and Smart Grid community for years
- UtiliSec team has lead and participated in numerous "Smart Grid" security efforts:
  - Facilitates the NERC CIP standards drafting team
  - Served in leadership positions some of the electric utilities largest community groups, including UCAIUG's AMI Sec, Smart Grid Security Working Group, Advancing Security for the Smart Grid (ASAP-SG)
  - Actively contributed to and lead several teams in the creation of NIST Inter-Agency Report 7628: "Guidelines for Smart Grid Cyber Security" (available at: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf, also see vol2 and vol3)
  - Continued participation in DOE's Smart Grid Interoperability Project (SGIP) and new National Electric Sector Cybersecurity Organization (NESCO).

Purpose of this Talk

- Many talks have been given on the "Smart Grid"
  - Some accurately and articulately represent the security issues we are dealing with
  - Others over-hype vulnerabilities using outdated, first generation hardware, use fringe vendor products, or simply disable security modes all together
  - Most mistakenly imply that Smart Meters and SCADA are the whole picture
- The media "coverage" always runs with the worst case scenarios, regardless of the messages their interviewees are trying to present
- Lack of clarity in "Smart Grid" security benefits no one
- We need to generate more interest in the security industry to help us secure these systems
  - There is more than enough work to go around

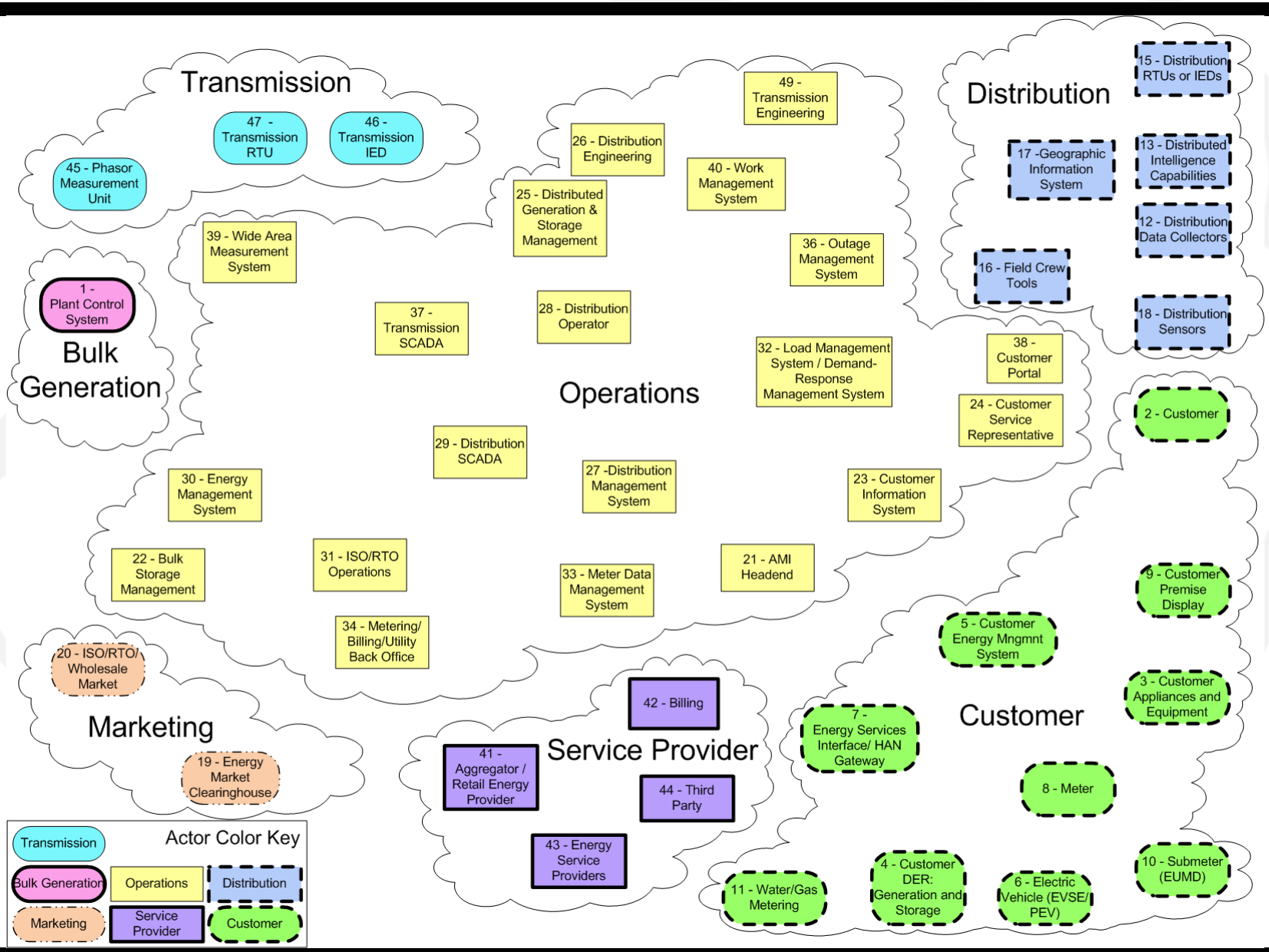
Architectural Overview of the Smart Grid

What is the "Smart Grid"?

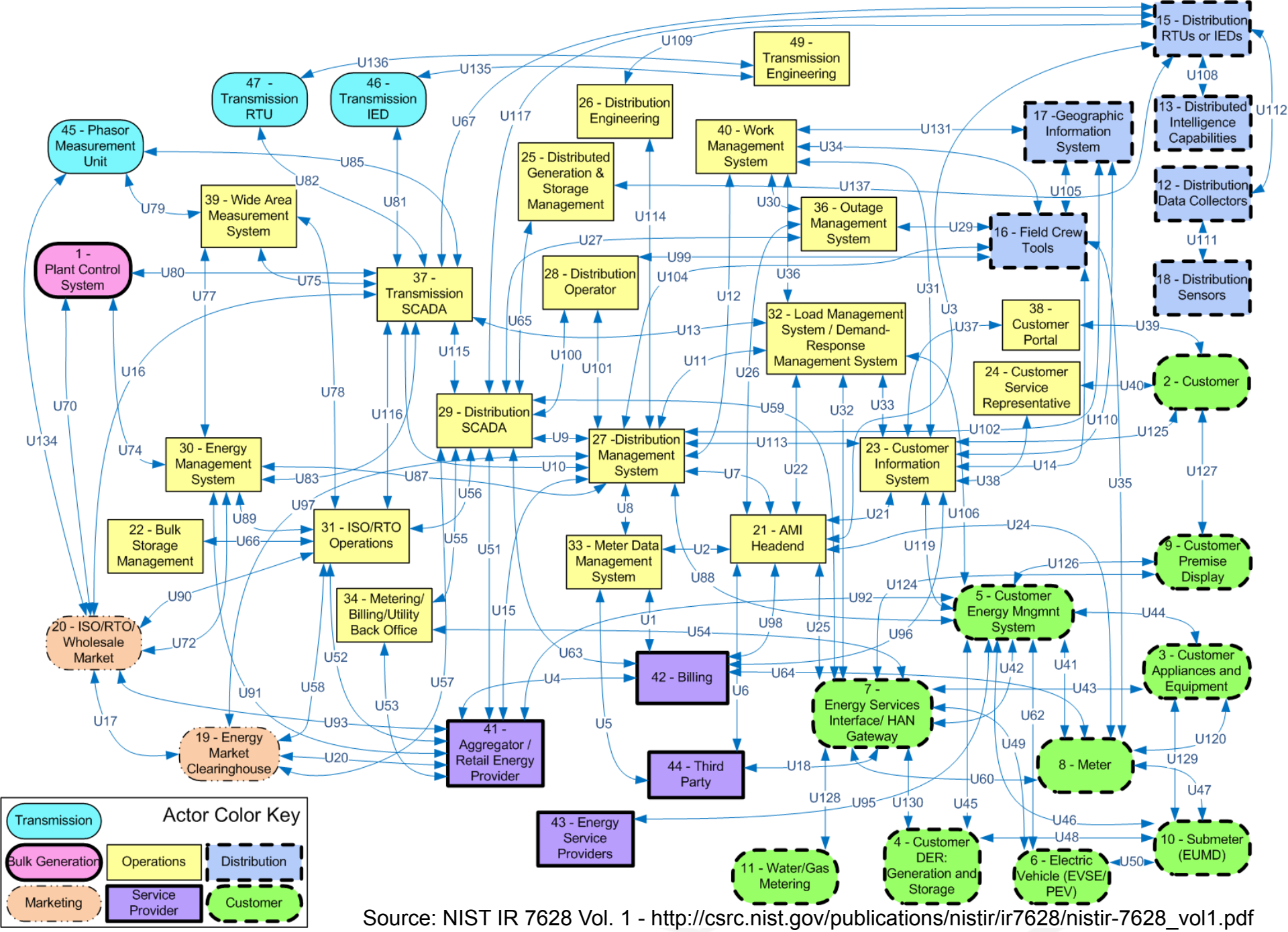


Source: http://www.sgiclearinghouse.org/ConceptualModel

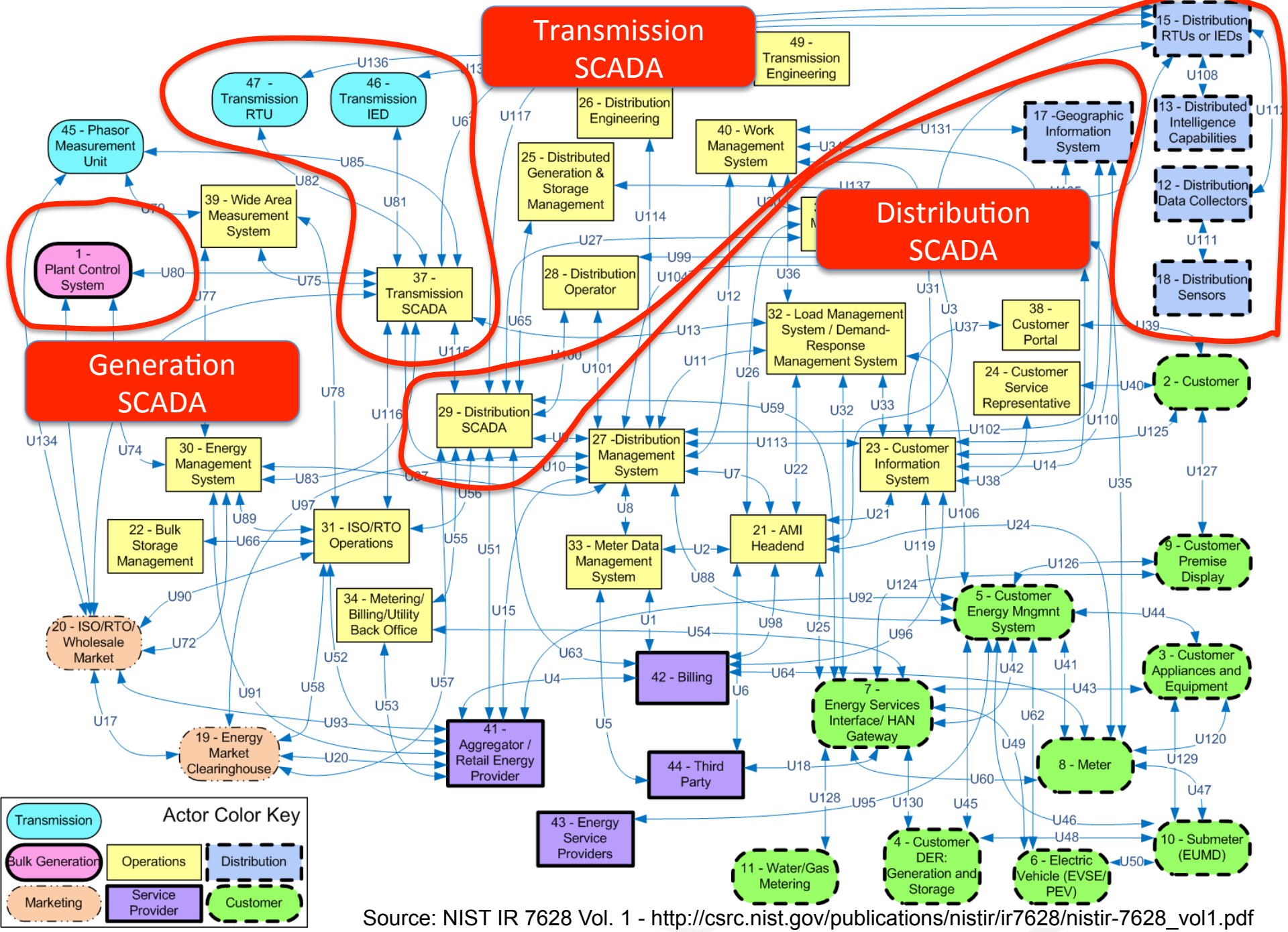
NIST Smart Grid Reference Model



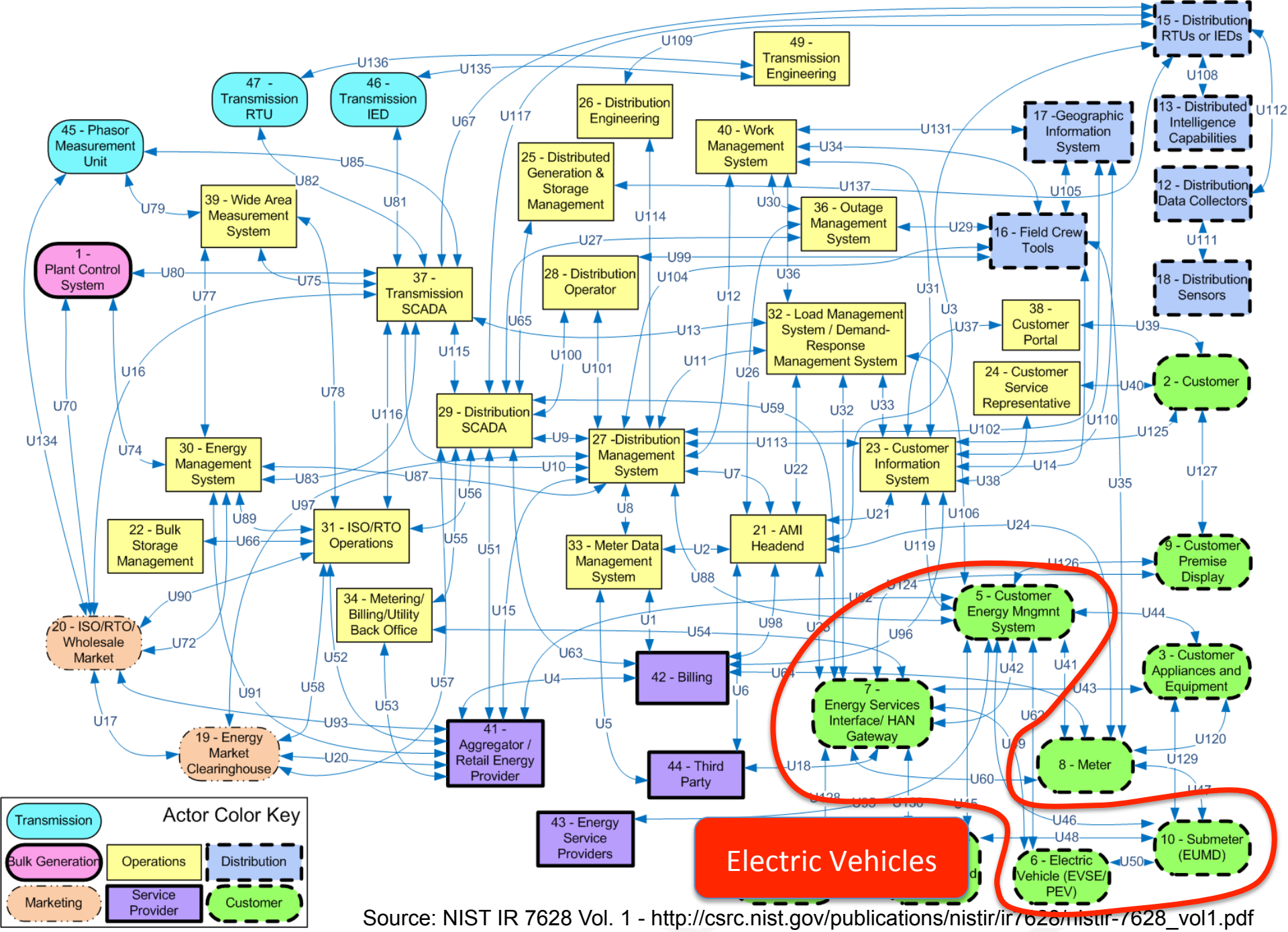
Source: NIST IR 7628 Vol. 1
http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf



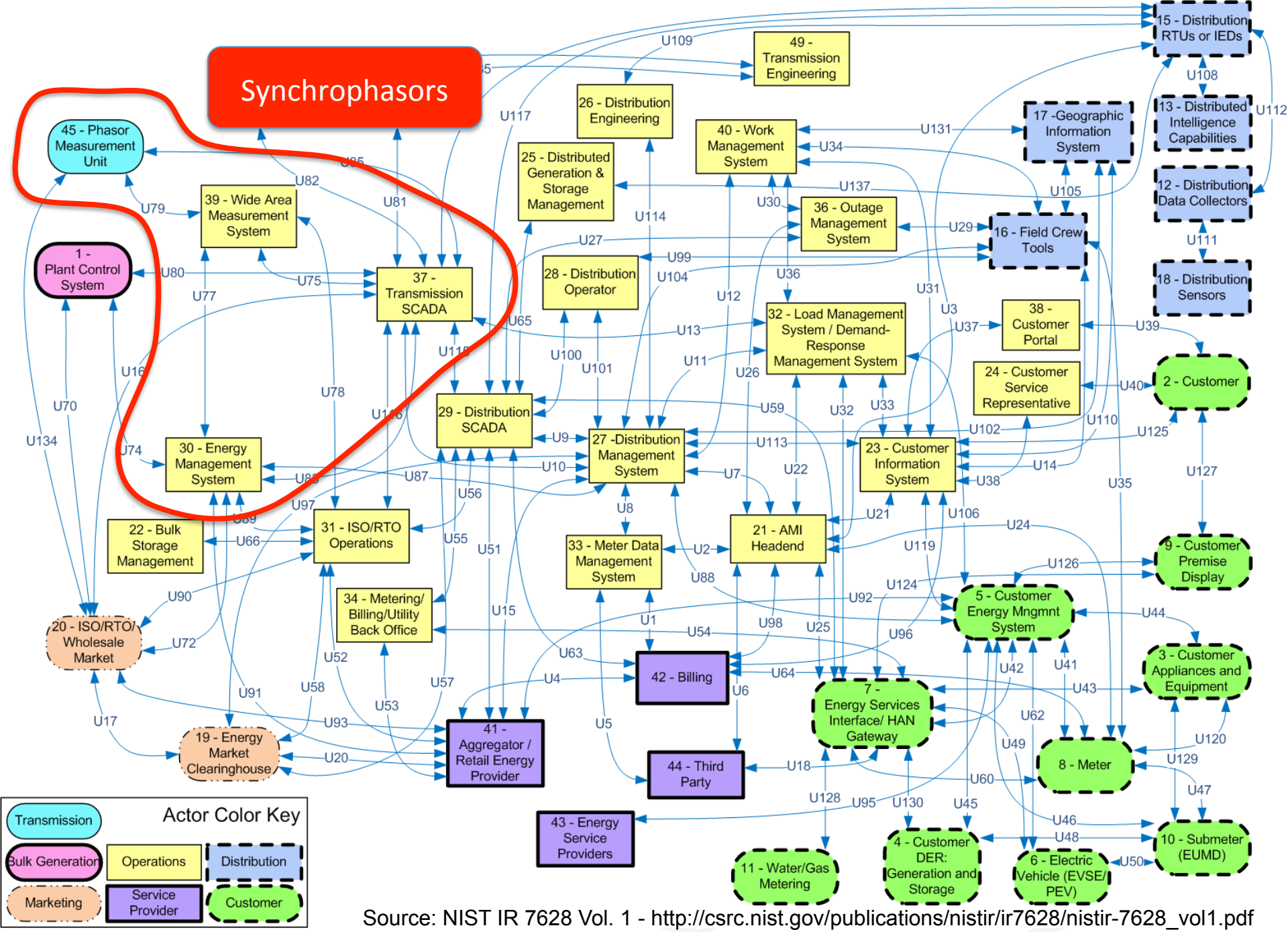
Source: NIST IR 7628 Vol. 1 - http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf



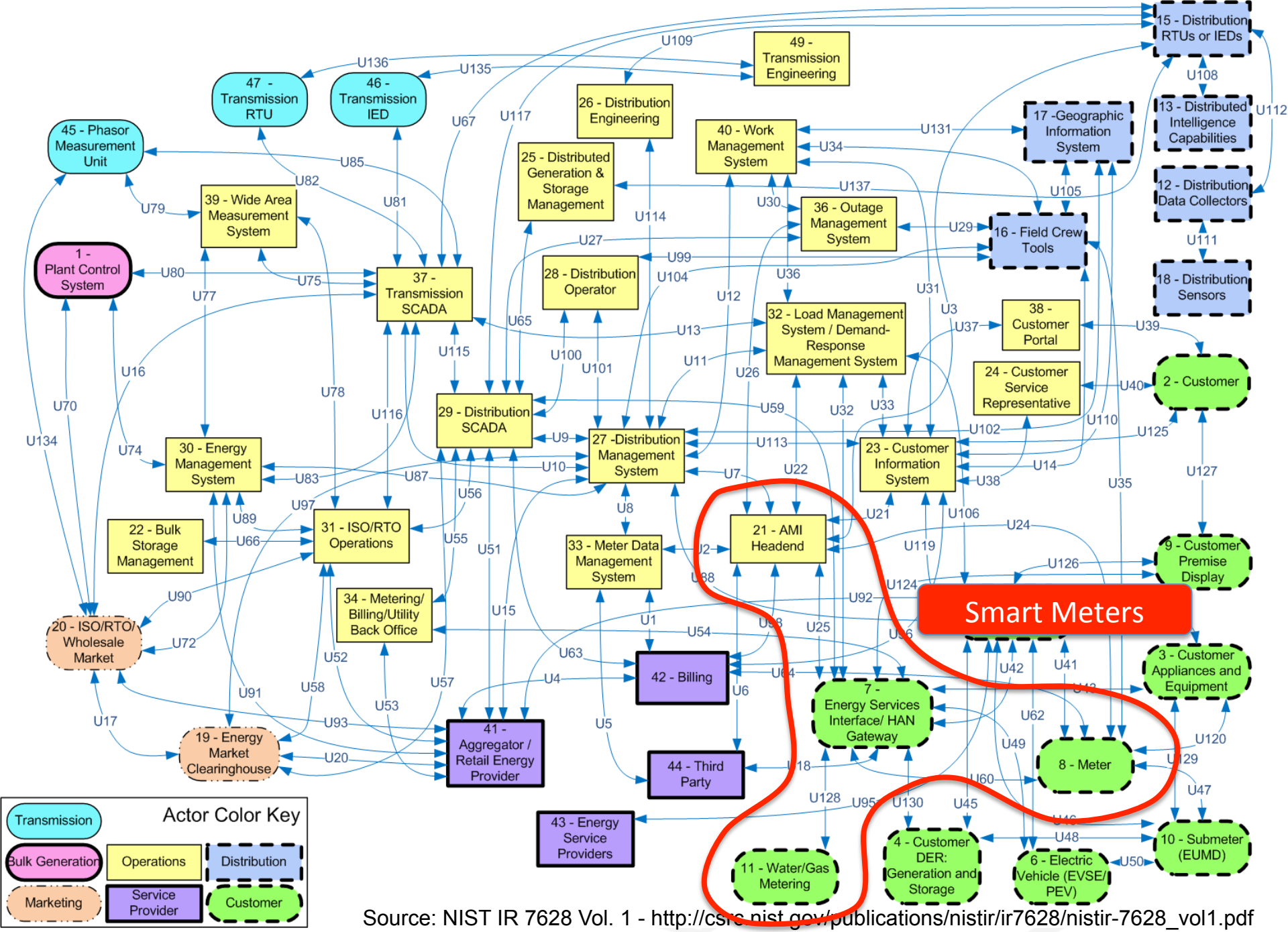
Source: NIST IR 7628 Vol. 1 - http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf



Source: NIST IR 7628 Vol. 1 - http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

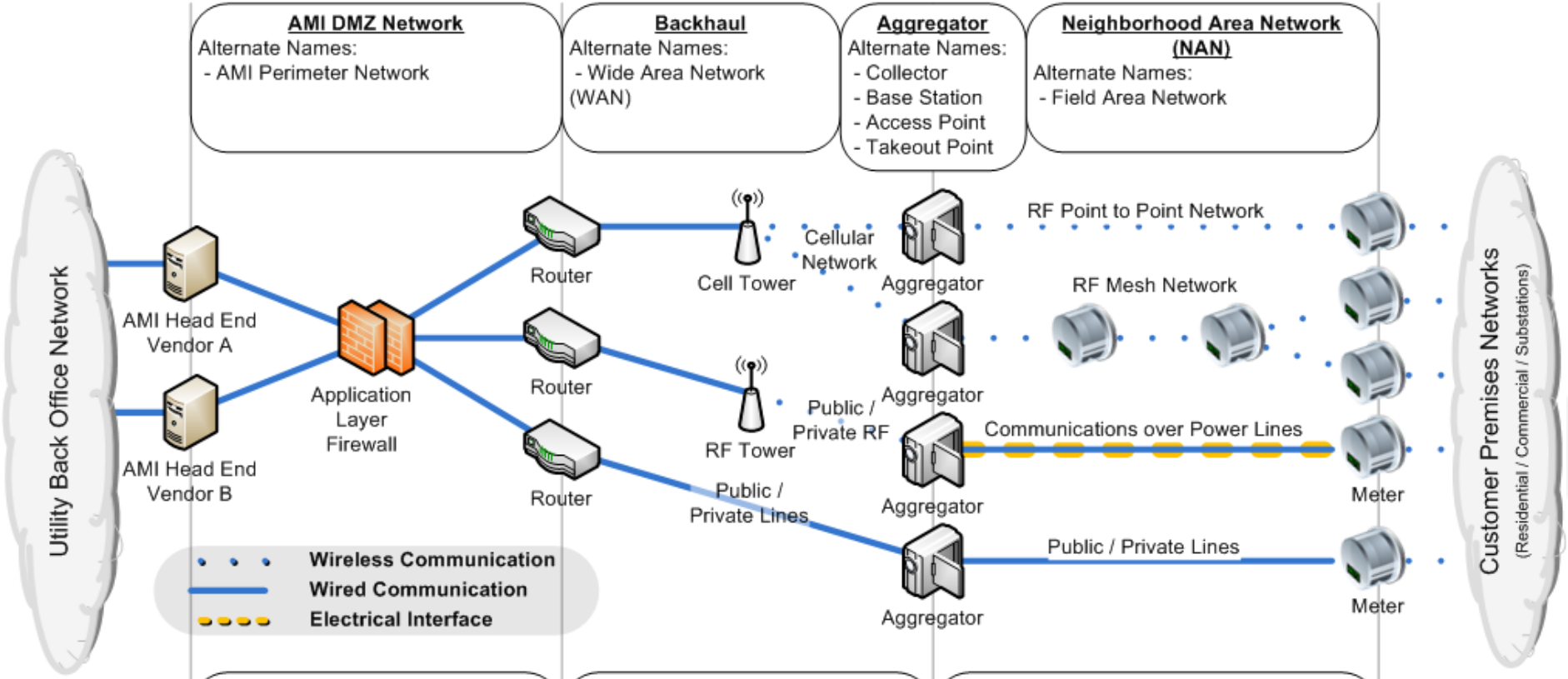


Source: NIST IR 7628 Vol. 1 - http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf



Source: NIST IR 7628 Vol. 1 - http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

AMI Network Diagram



AMI DMZ Protocols

Application Layer (OSI 5-7):
- ANSI C12.22
- ANSI C12.18 / C12.19 / C12.21

Transport Layer (OSI 4):
- TCP / UDP

Network Layer (OSI 3):
- IP4 / IP6

PHY / MAC Layter (OSI 1-2):
- Ethernet

Backhaul Protocols

Application Layer (OSI 5-7):
- ANSI C12.22
- ANSI C12.18 / C12.19 / C12.21

Transport Layer (OSI 4):
- TCP / UDP

Network Layer (OSI 3):
- IP4 / IP6

PHY / MAC Layter (OSI 1-2):
- Radio (WiMax 802.16d/e)
- Cellular (EVDO / GPRS / …)
- Power Line Carrier (BPL / P1901)
- Fiber (RFoG / FTTP / Ethernet)

NAN Protocols

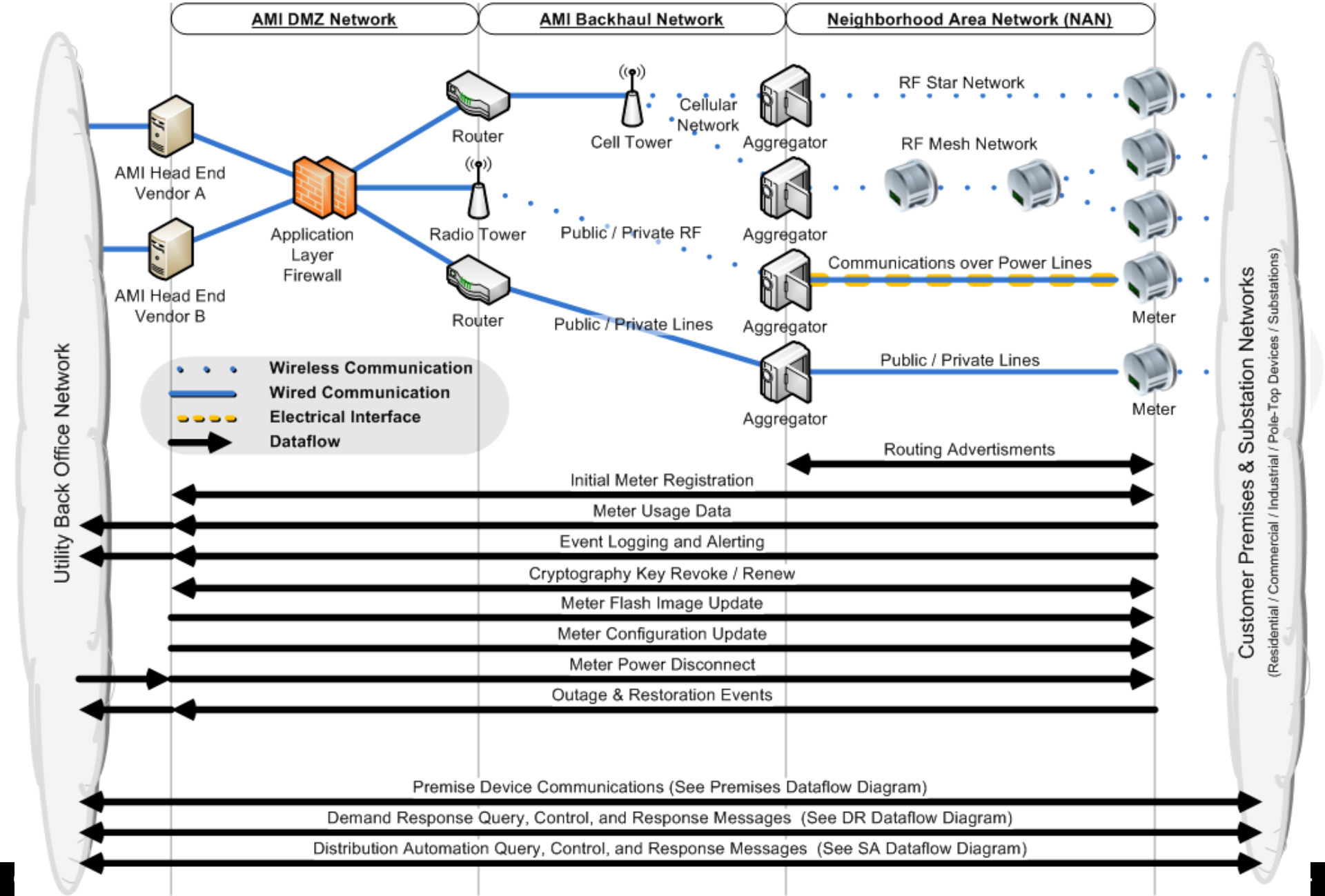
Application Layer (OSI 5-7):
- ANSI C12.22
- ANSI C12.18 / C12.19 / C12.21

Transport Layer (OSI 4):
- TCP / UDP
- ANSI C12.22

Network Layer (OSI 3):
- IP4 / IP6
- ANSI c12.22

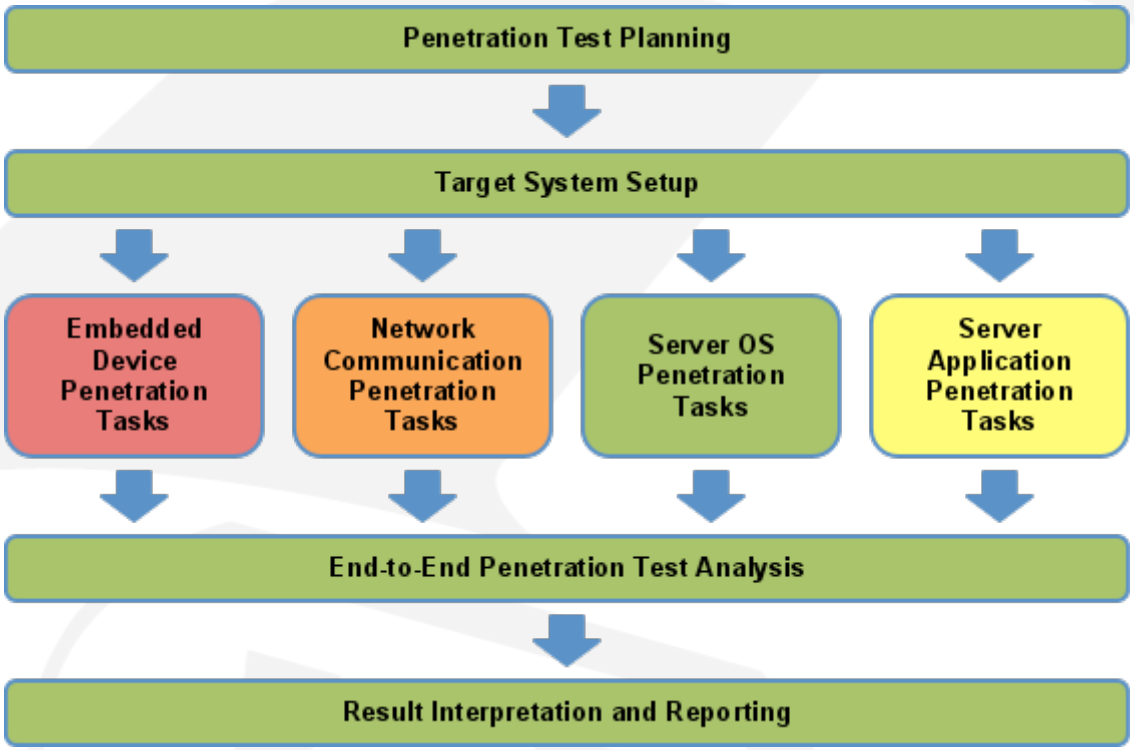
PHY / MAC Layter (OSI 1-2):
- Radio (WiMax 802.16d/e)
- Proprietary Radio (900 MHz)
- Cellular (EVDO / GPRS / …)
- Power Line Carrier (BPL / P1901)
- Fiber (RFoG / FTTP / Ethernet)

AMI Dataflow Diagram



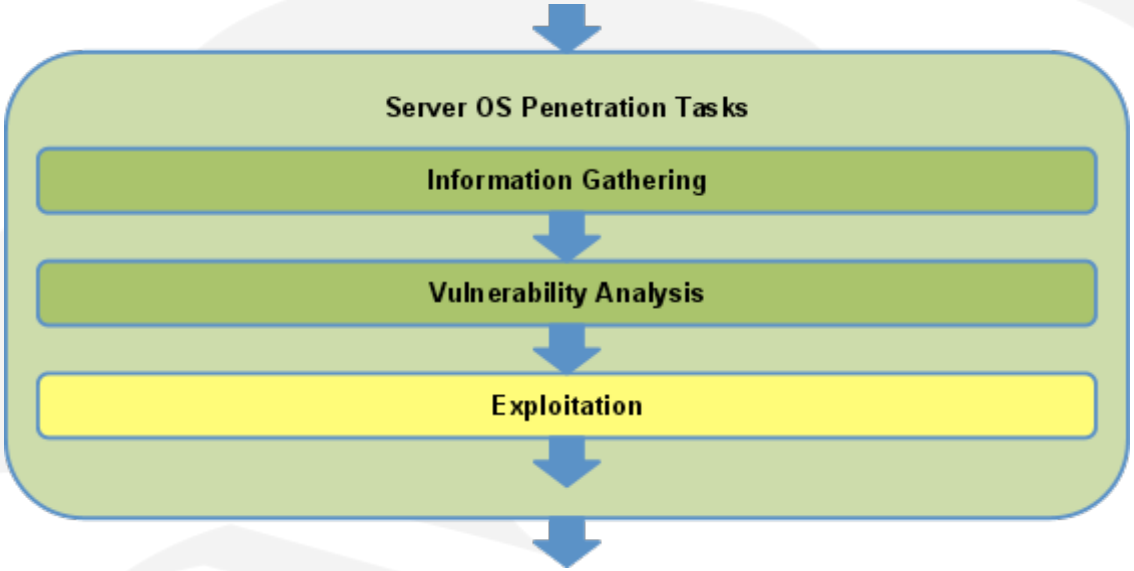
Penetration Testing Methodology

Smart Grid Penetration Test Plan



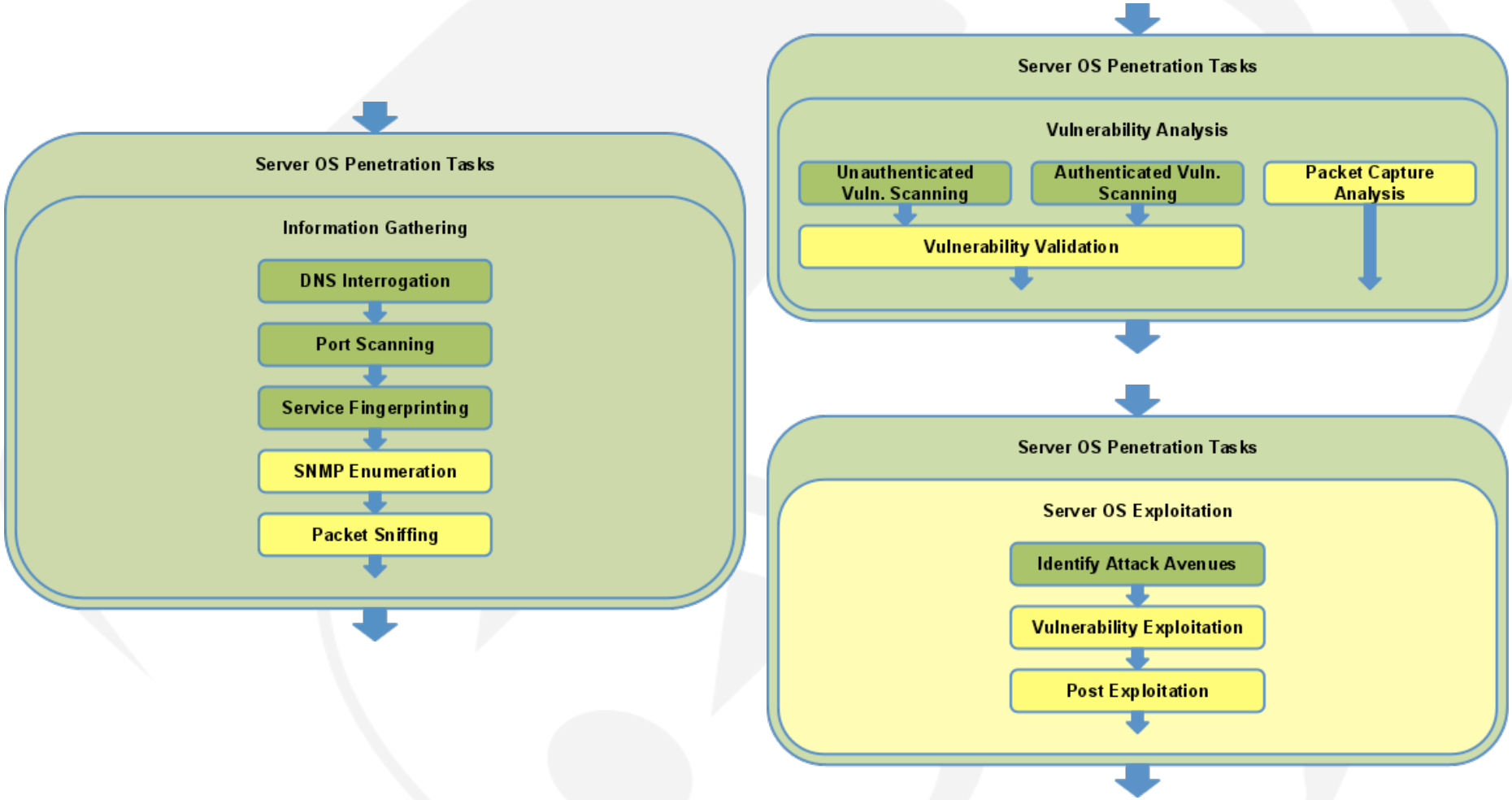
- Green: Tasks most frequently and require the most basic of penetration testing skill
- Yellow: Tasks commonly performed and require moderate penetration testing skill
- Orange: Tasks that are occasionally performed but require higher levels of expertise
- Red: Tasks performed infrequently and require highly specialized skills

Server OS Task Sub-Categories

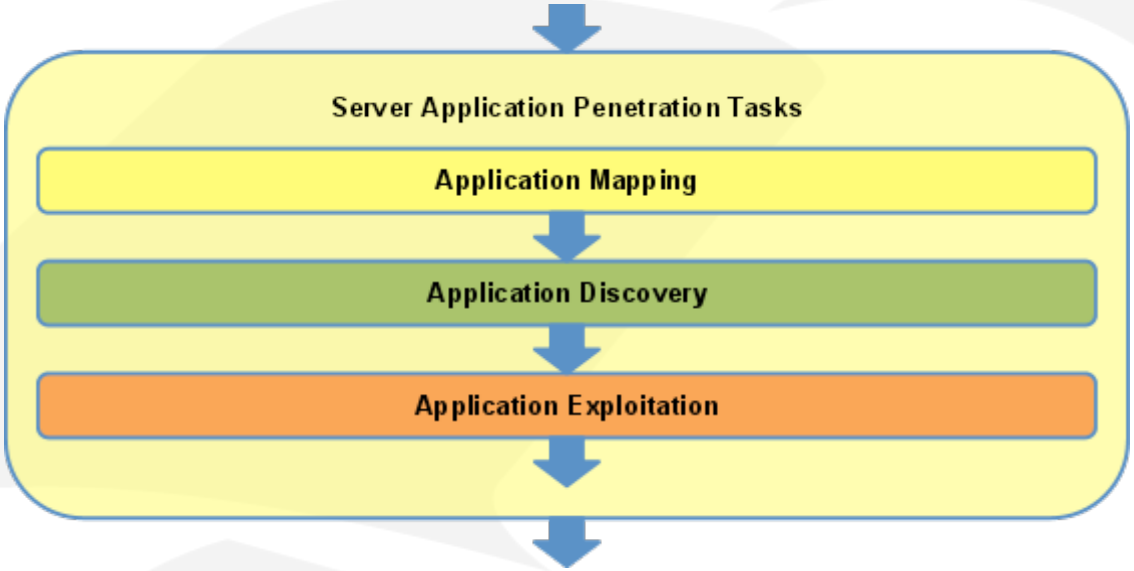


- Most servers in the datacenter controlling Smart Grid systems are running commodity OSes like Windows and Linux
- Skills needed to pentest these systems are no different than non-smart grid pentests
- Level of care when testing production systems is greatly increased
- Mastery and understanding of automated tools used is critical

Server OS Pentest Tasks

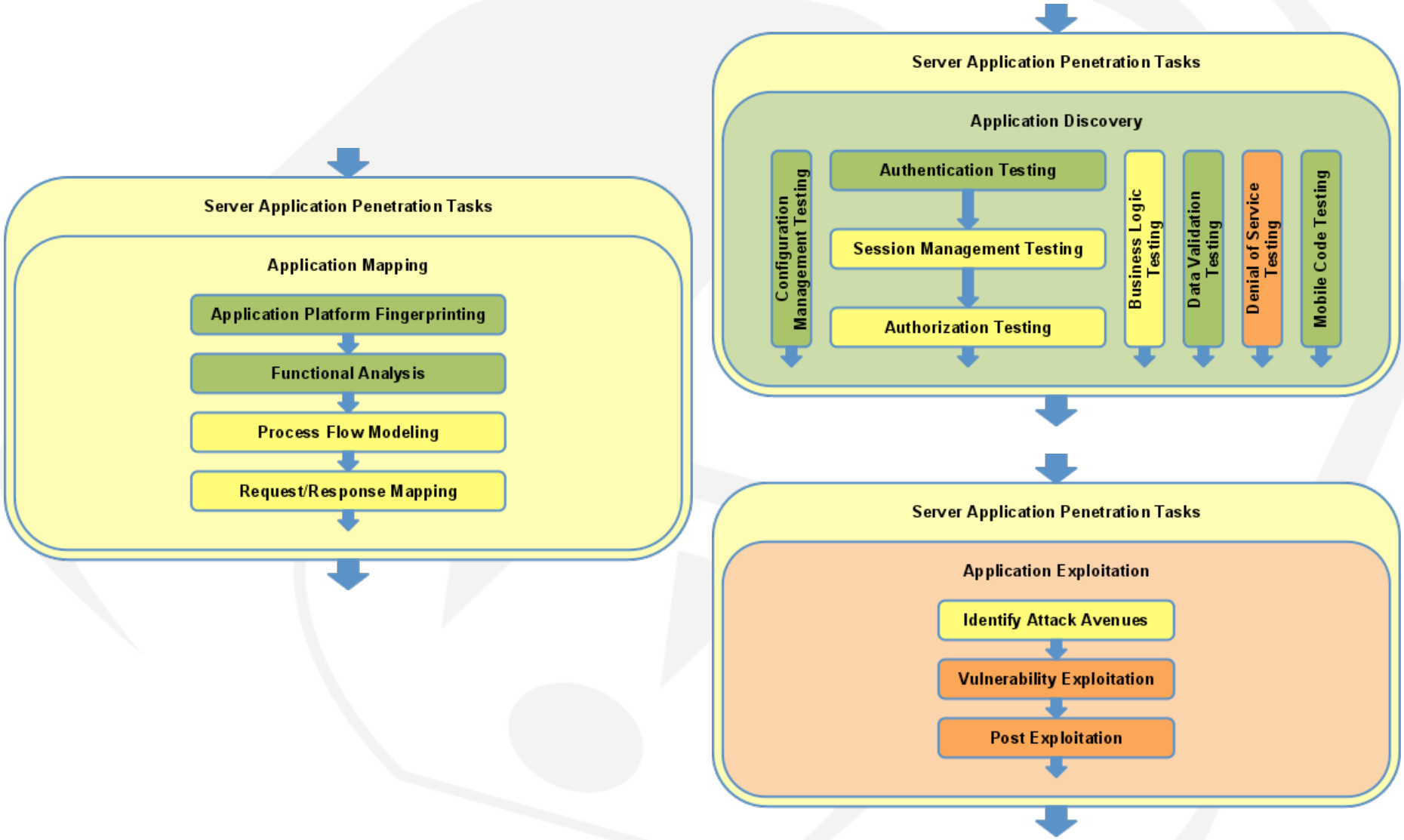


Server App Task Sub-Categories

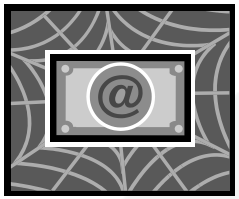


- Includes all user interfaces and smart grid services
- Most modern user interfaces are web applications or fat applications speaking to a web service
- Most server-to-server communications use SOAP or REST web services, but other interfaces like RPC are occasionally seen
- Automated tools can be VERY dangerous in these applications as POST reqests can shut down power or brick field devices

Server App Pentest Tasks



Task: Session Management (CSRF)



Attacker Controlled Site

Attack Prerequisites

- Attacker must have knowledge of the application he is attacking (can be obtained at conferences)
- Attacker must know the hostname or IP address of the CIS system (can be obtained by browser based attacks)

Employee opens a second tab and surfs to the Attacker website (or MySpace page…)

2

3

Hidden in the page, the Attacker's website tells the employee's web browser to disconnect a customer's power

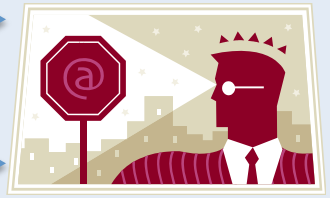
Utility Network

1

Employee using CIS system throughout the day

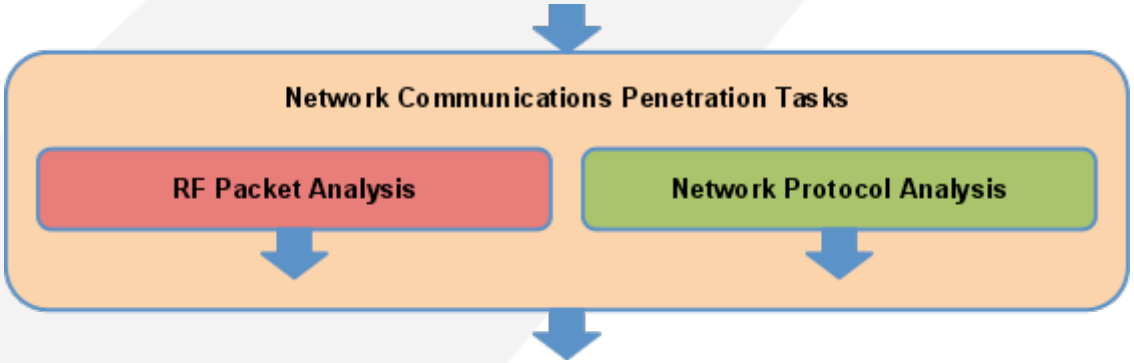
4

Web browser sends disconnect request to CIS



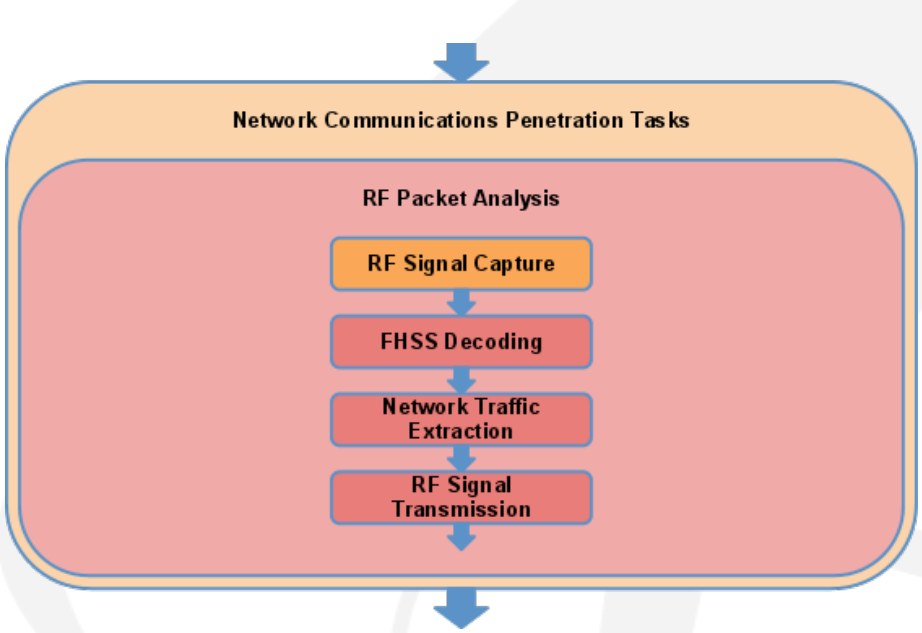
Customer Information System with Power Disconnect Capabilities

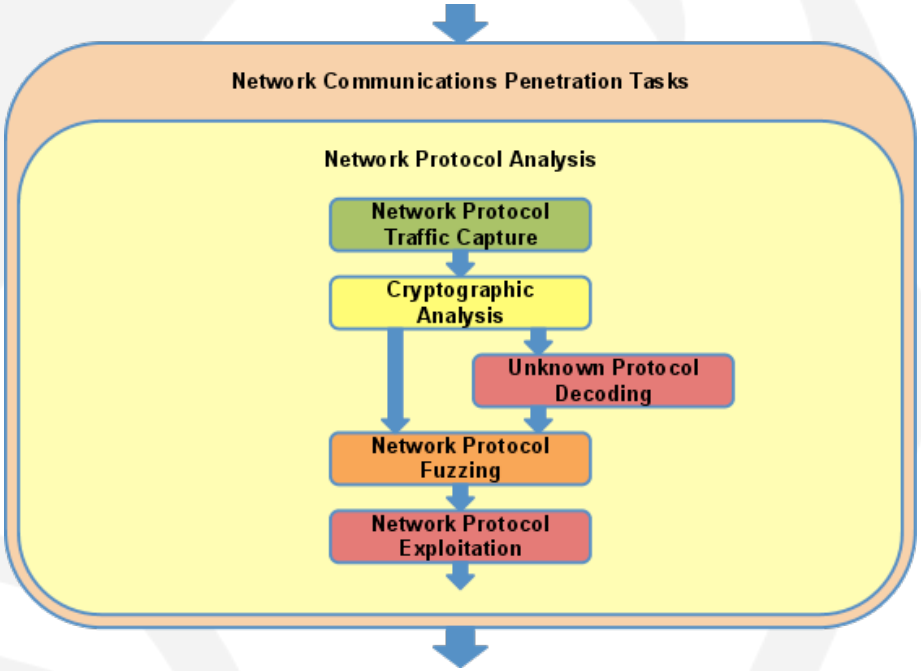
Network Coms Task Sub-Categories



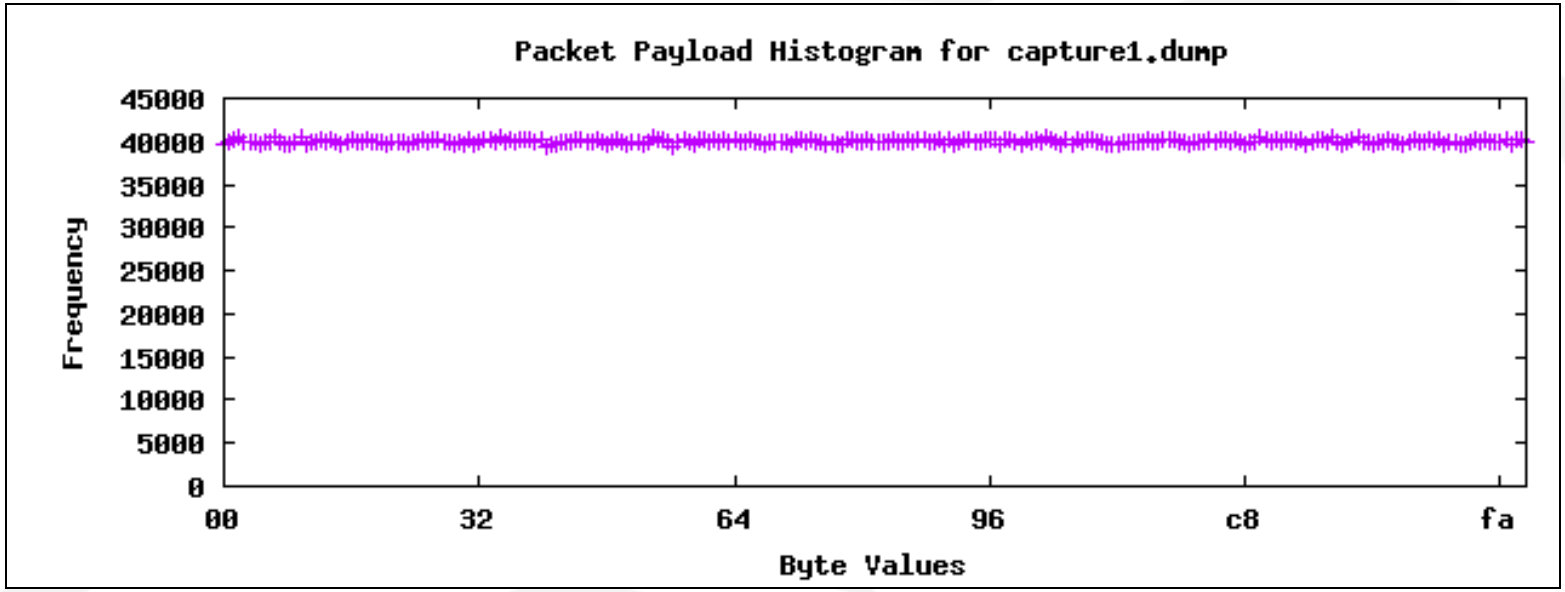
- These tasks include all network traffic between any of the devices regardless of its location such as sever-to-server, server-to-device, device-to-device
- RF Packet Analysis is not commonly performed because we assume all security is handled in the network protocols
  - Frequency hopping isn't a security control

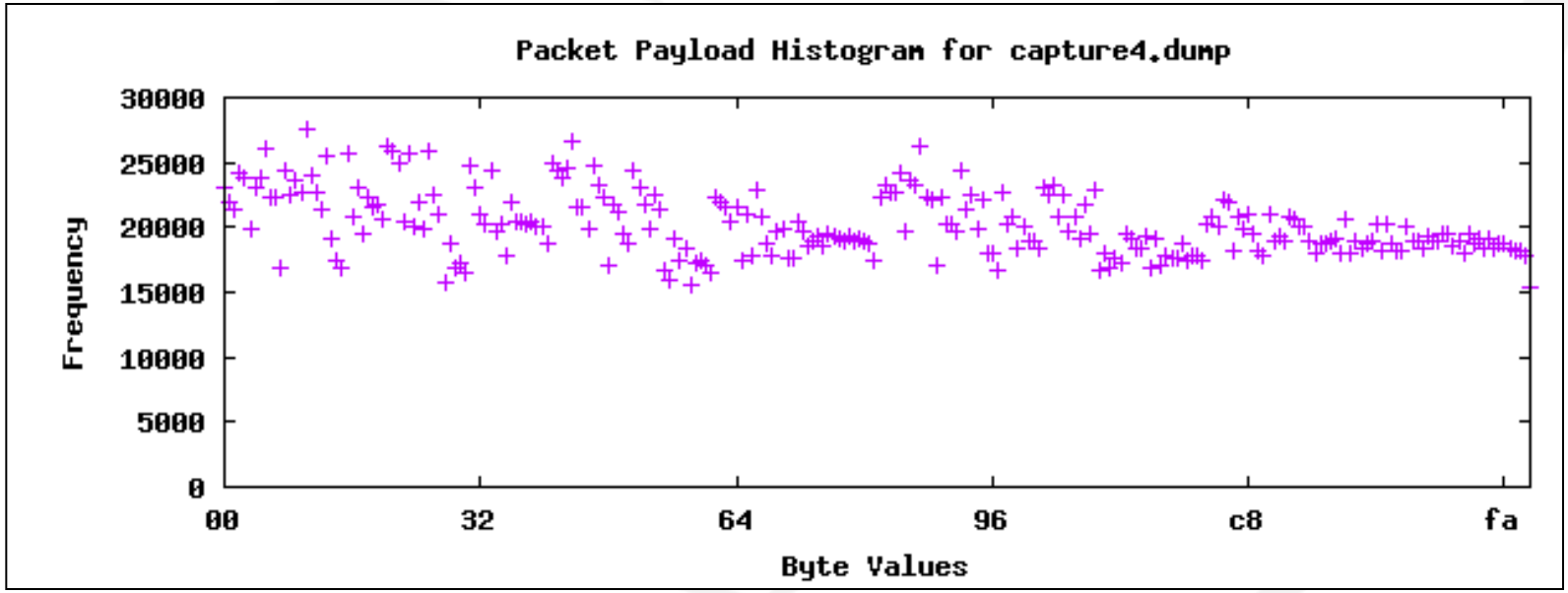
Network Coms Pentest Tasks





Task: Cryptographic Analysis



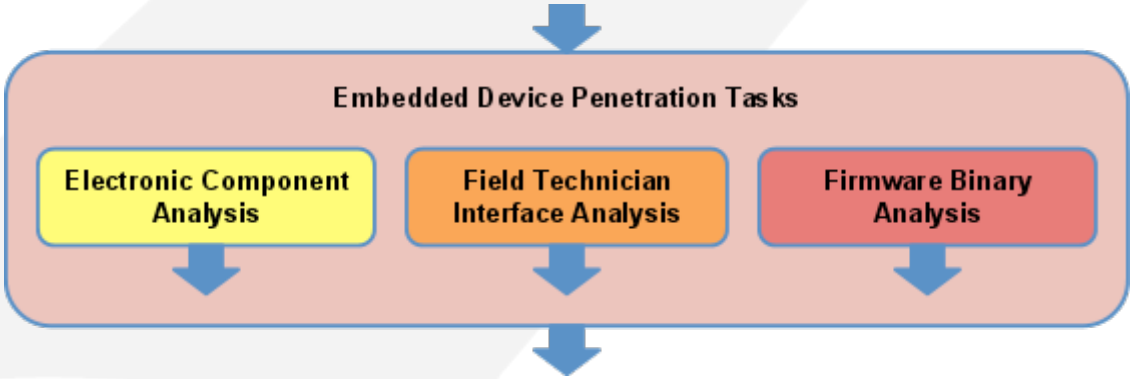


Insecure Block Cipher Modes

- AES ciphers using CTR mode effectively become a stream cipher
- Without key derivation and rotation, IV collisions compromise integrity of cipher

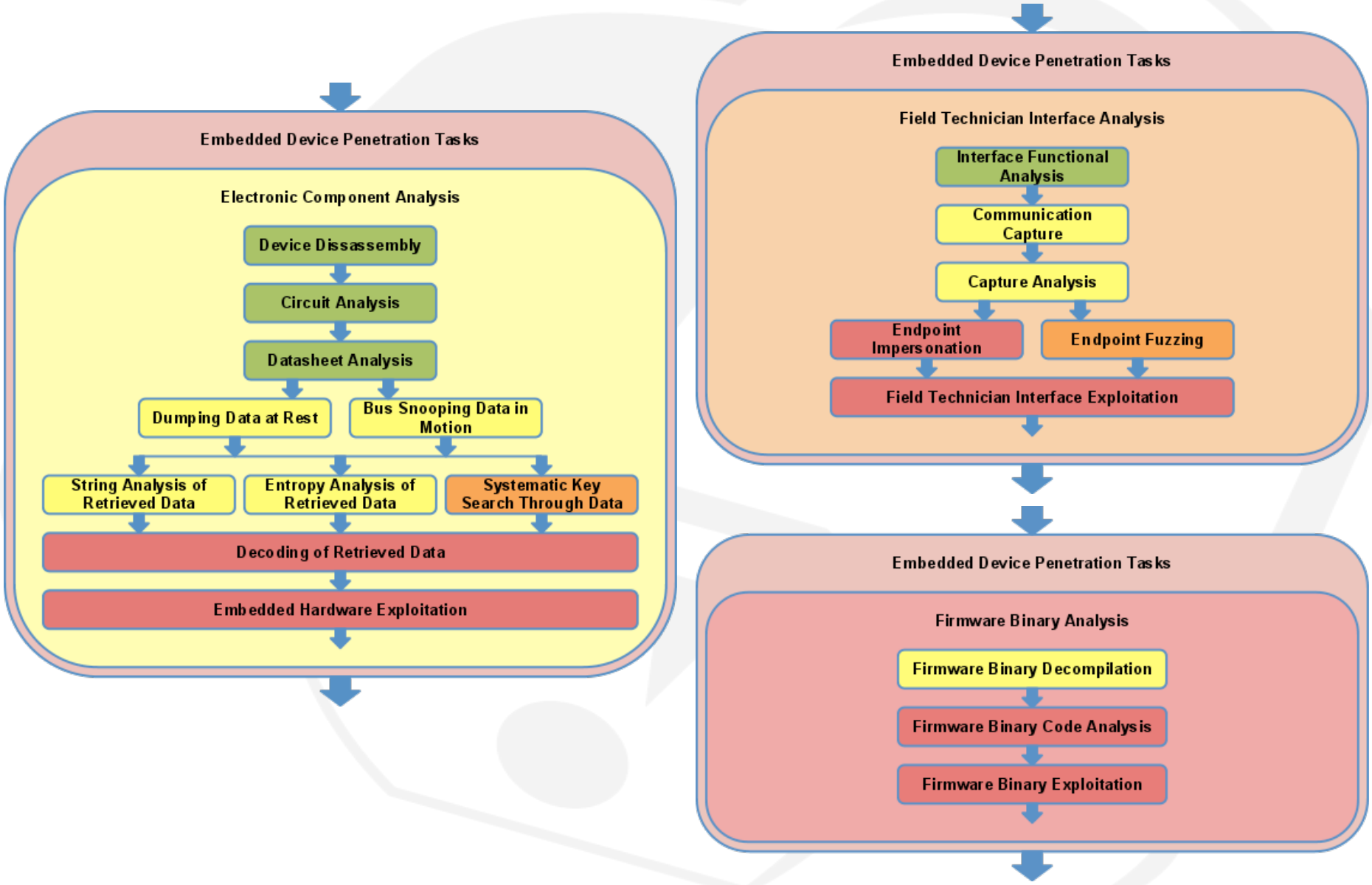
```
C:\>type ivcoltest.py
#!/usr/bin/env python
knownplain = "\xaa\xaa\x03\x00\x00\x00\x08\x00\x45\x00\x01\x48\x00\x01\x00\x00"
knowncip = "\x31\xb9\x84\x81\xe1\x96\x6e\x71\xd8\xa3\x39\x0c\xfb\x48\xaa\x61"
unknowncip = "\x31\xb9\x84\x81\xe1\x96\x6e\x71\xd8\xa3\x3d\x0c\xfb\xb5\xaa\x61"
print "Decrypted packet: "
for i in range(0,len(knownplain)):
    print "%02x"%( (ord(knownplain[i]) ^ ord(knowncip[i])) ^ ord(unknowncip[i]) ),
print("\n")

C:\>python ivcoltest.py
Decrypted packet:
aa aa 03 00 00 00 08 00 45 00 05 48 00 fc 00 00
```

Embedded Task Sub-Categories



- These tasks target physical attacks on embedded field devices:
  - electronic components that store data (EEPROM, Flash, RAM, MCu storage)
  - buses that pass data between components (parallel buses and serial buses)
  - input interfaces used for administrative or debugging purposes (serial ports, parallel ports, infrared/optical ports)
- Overarching goal for embedded device testing is to identify vulnerabilities that allow attackers to expand their control of that single device to other devices with limited or no physical access to those other devices

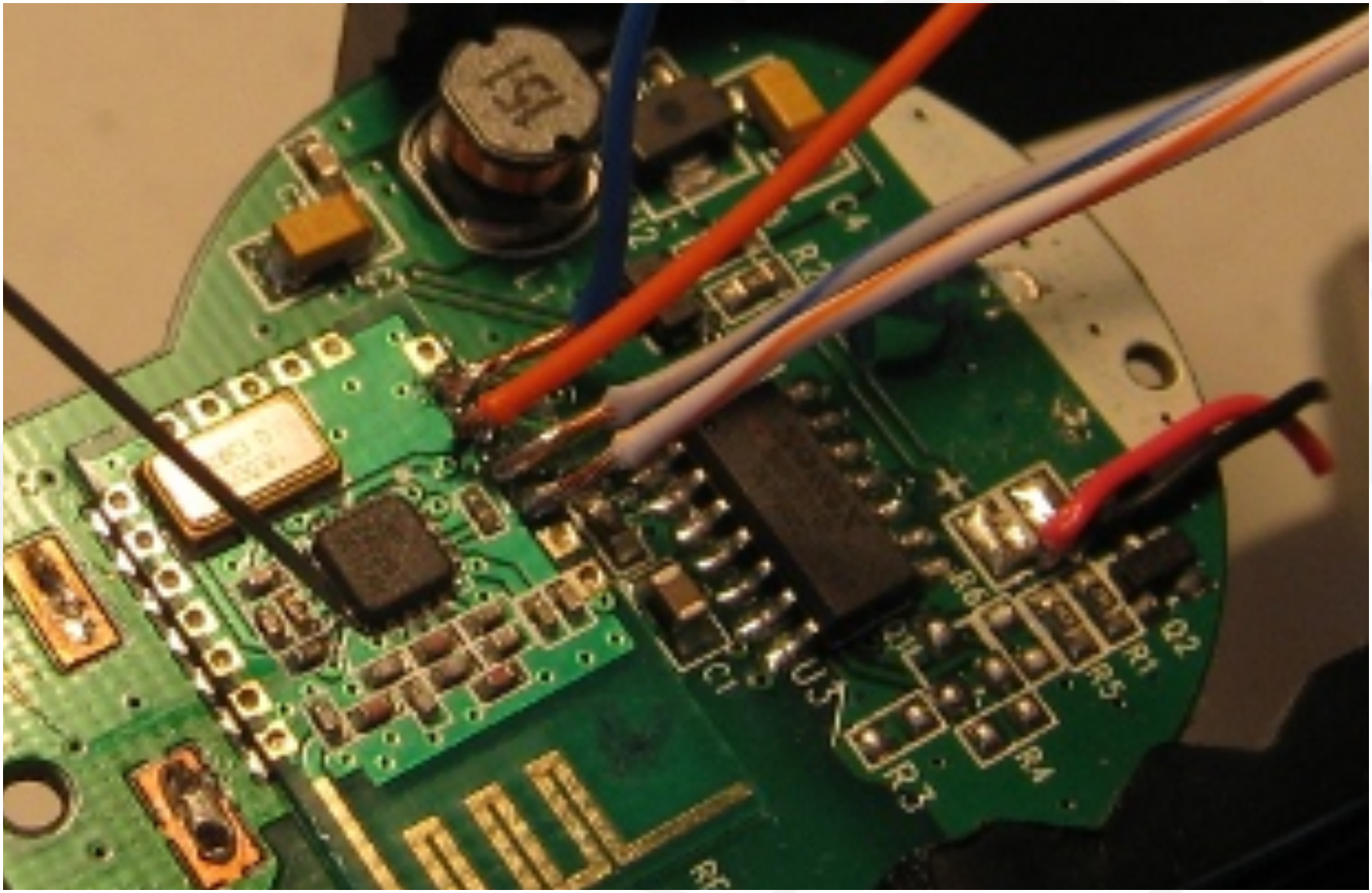
Embedded Device Pentest Tasks



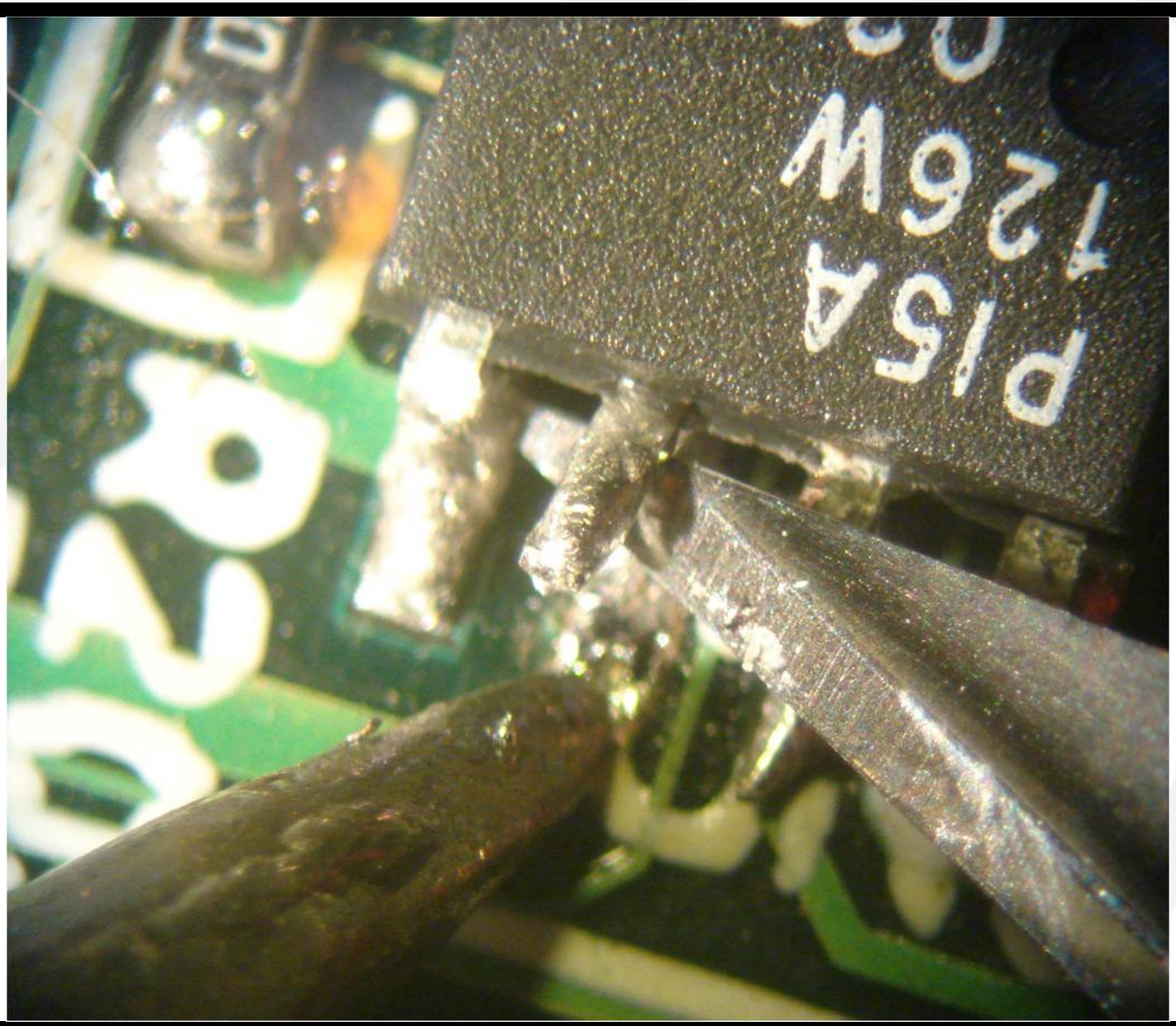
Goals: Key & Firmware Extraction

- Attacking data at rest
  - Power down the device, expose its circuit board, and interact directly with each component
  - Extract contents of accessible RAM, Flash, and EEPROM
  - Identify cryptography keys or firmware
- Attacking data in motion
  - Boot and normally operate the device in a lab, monitoring bus activity between major chips (MCU, Radio, Flash, RAM)
  - Crypto keys can often be found in key load operations between a microcontroller and crypto accelerator
  - Firmware can often be found in boot processes (between Flash and MCU) and firmware updates (between Radio, MCU, and Flash)

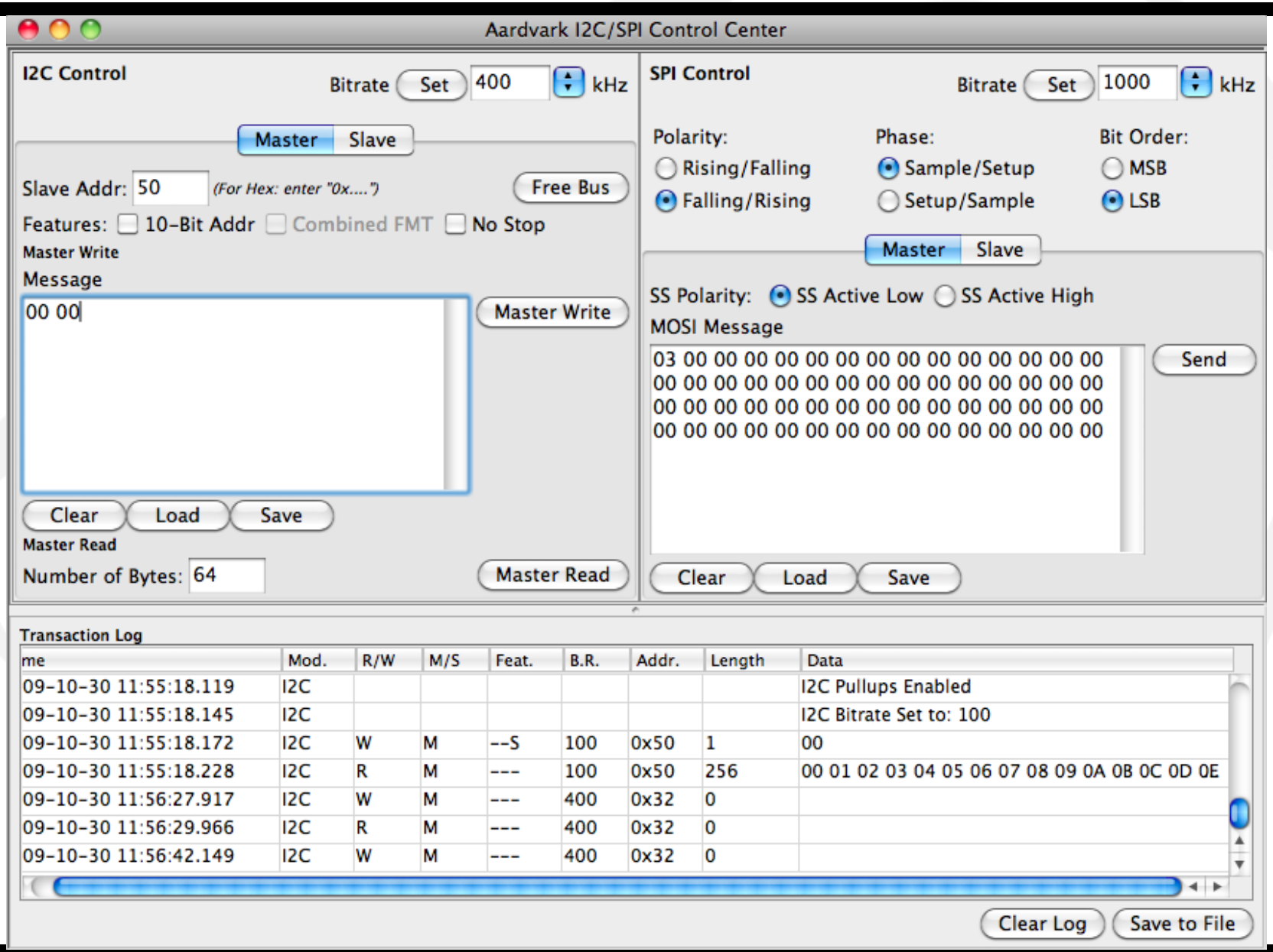
Interfacing with an IC



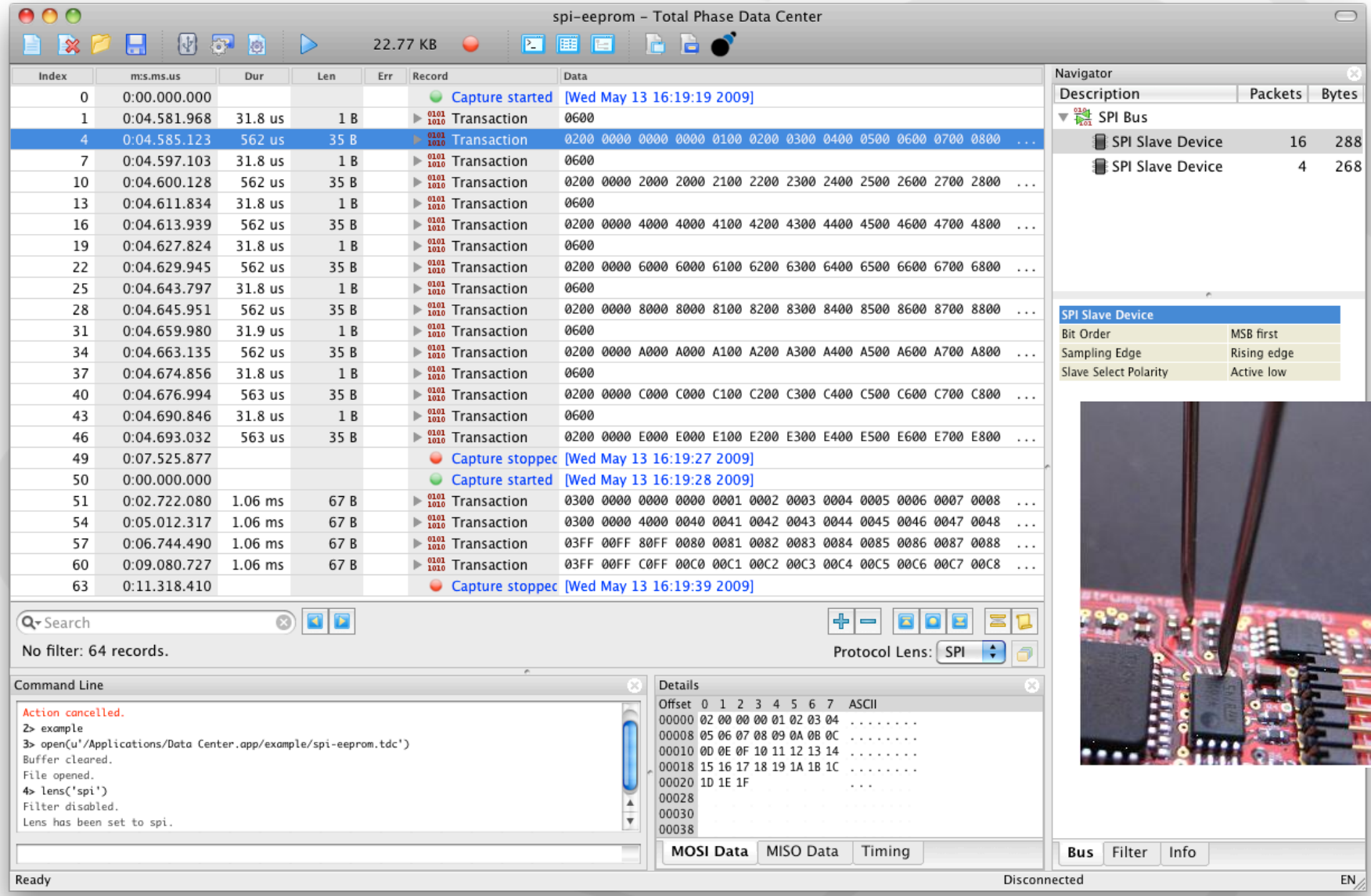
Lifting an IC's Chip Enable (CE) Pin



Task: Dumping Data at Rest



Task: Bus Snooping Data in Motion



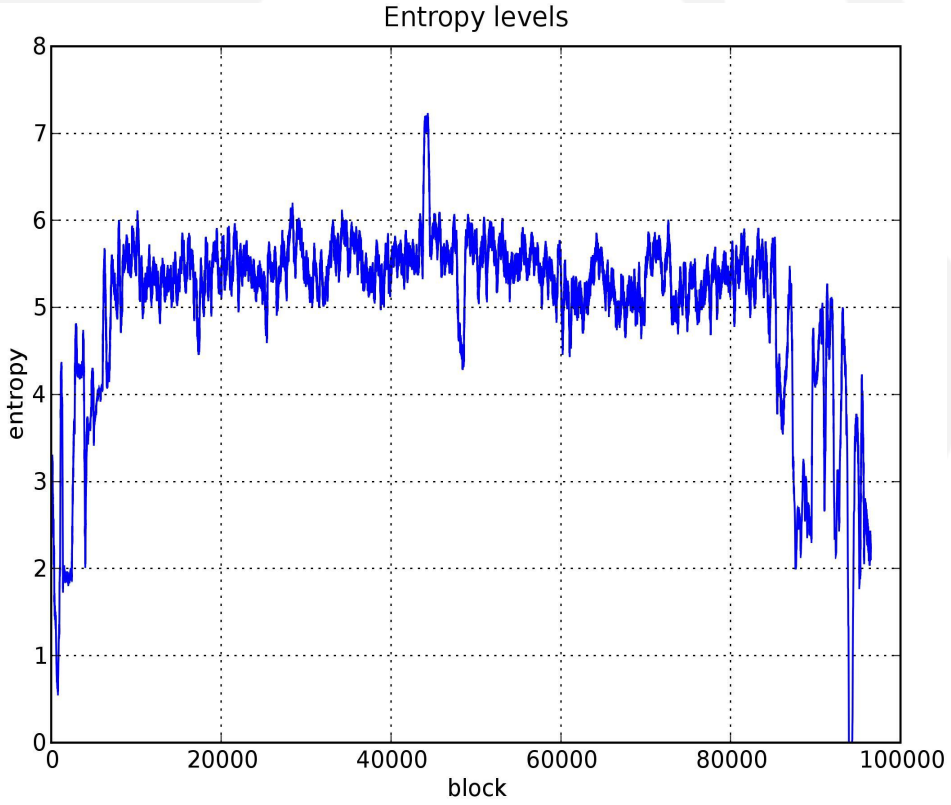
Task: Systematic Key Search

- Perform basic string searches for obvious keys
- Develop custom tools to do more advanced searches:
  - GoodFET: Abuses vulnerability in TI, Ember radios to access RAM even when chip is locked
  - zbgoodfind: Search for ZigBee key using RAM dump as a list of potential keys
  - Combined they can recover the ZigBee network key

```
$ sudo goodfet.cc dumpdata chipcon-2430-mem.hex
Target identifies as CC2430/r04.
Dumping data from e000 to ffff as chipcon-2430-mem.hex.
...
$ objcopy -I ihex -O binary chipcon-2430-mem.hex chipcon-2430-mem.bin
$ zbgoodfind -R encdata.dcf -f chipcon-2430-mem.hex
zbgoodfind: searching the contents of chipcon-2430-mem.hex for
encryption keys with the first encrypted packet in encdata.dcf.
Key found after 6397 guesses:  c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc
cd ce cf
```

Task: Entropy Analysis of Data

- Asymmetric keys have high entropy (very random)
- RAM and Flash is filled with non-random data
- Graphing entropy of flash reveals a spike in randomness
- This spike is the location of the asymmetric key in flash



Demo

Contact Information

www.utilisec.com
sales@utilisec.com

Justin Searle
personal: justin@meeas.com
work: justin@utilisec.com
cell: 801-784-2052
twitter: @meeas