Pentesting Smart Grid Web Apps

Justin Searle
Managing Partner – UtiliSec

Who is UtiliSec

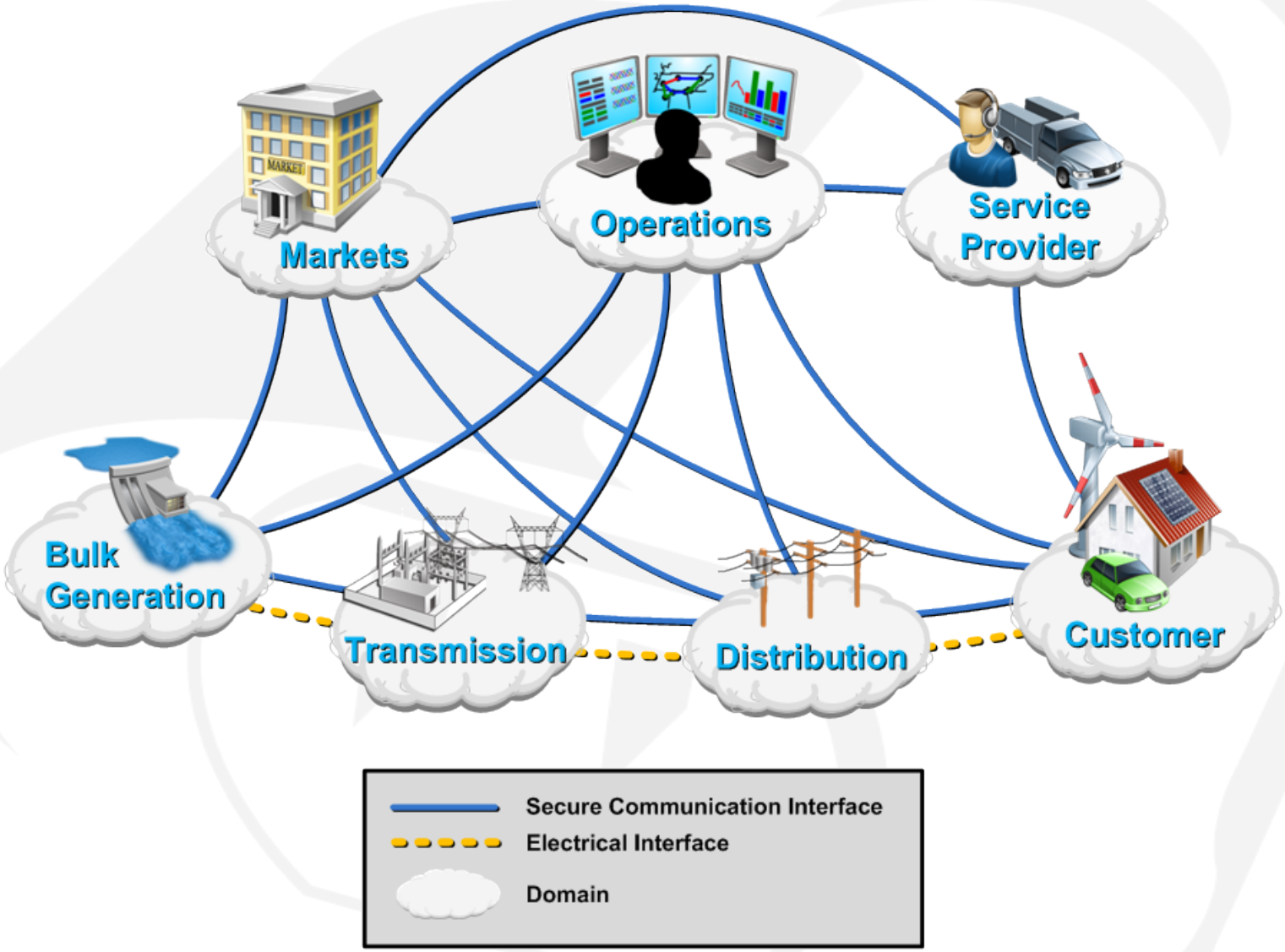
- A security services company specializing in helping electric utilities
- Managing Partners
  - Darren Highfill (darren@utilisec.com)
  - Justin Searle (justin@utilisec.com)
- List of services
  - Critical Functionality in Industry Collaboration
  - Security Architecture Guidance and Review
  - Penetration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

UtiliSec Smart Grid Efforts

- 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:
  - 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).

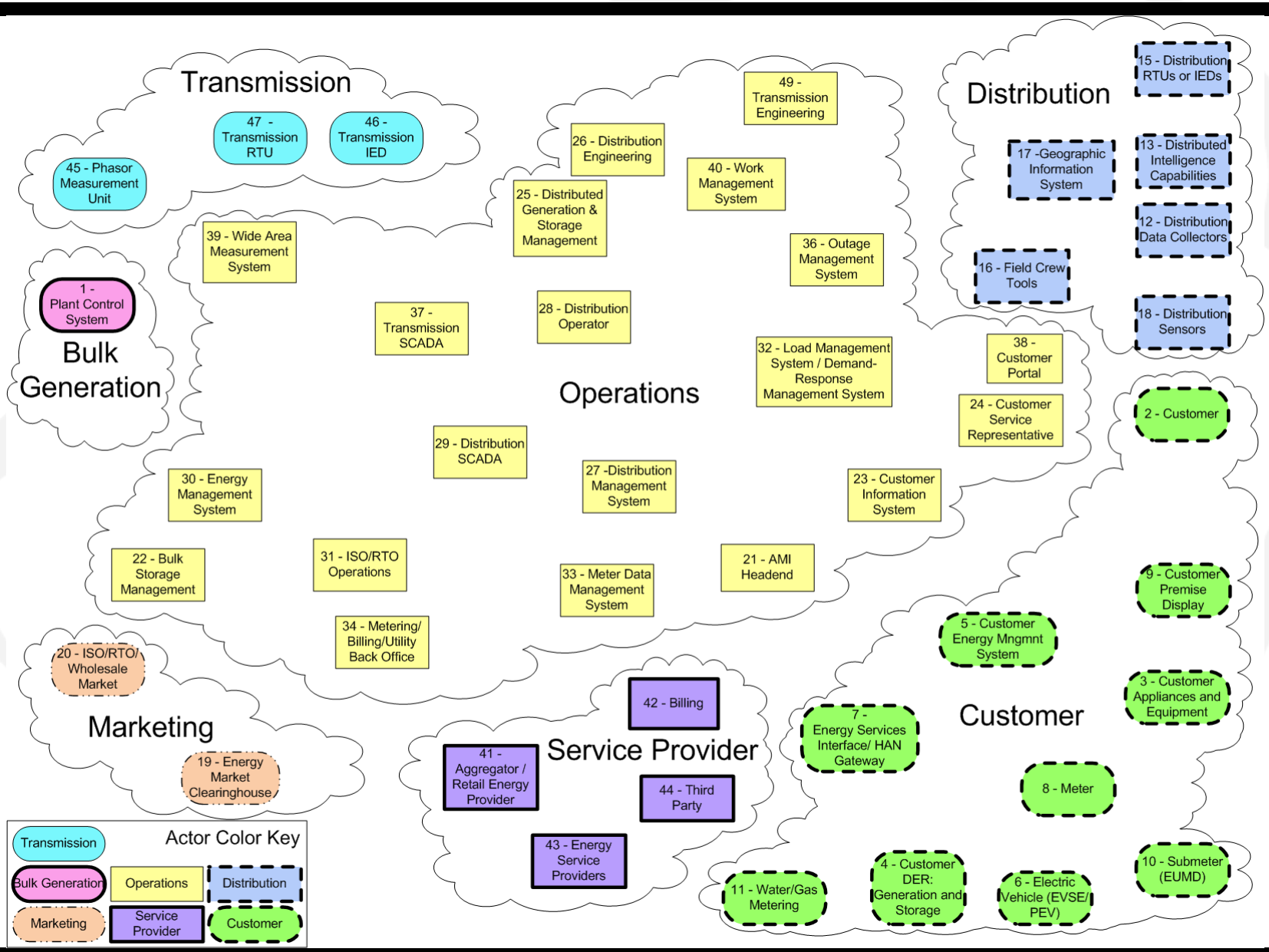
Architectural Overview of the Smart Grid

What is the "Smart Grid"?

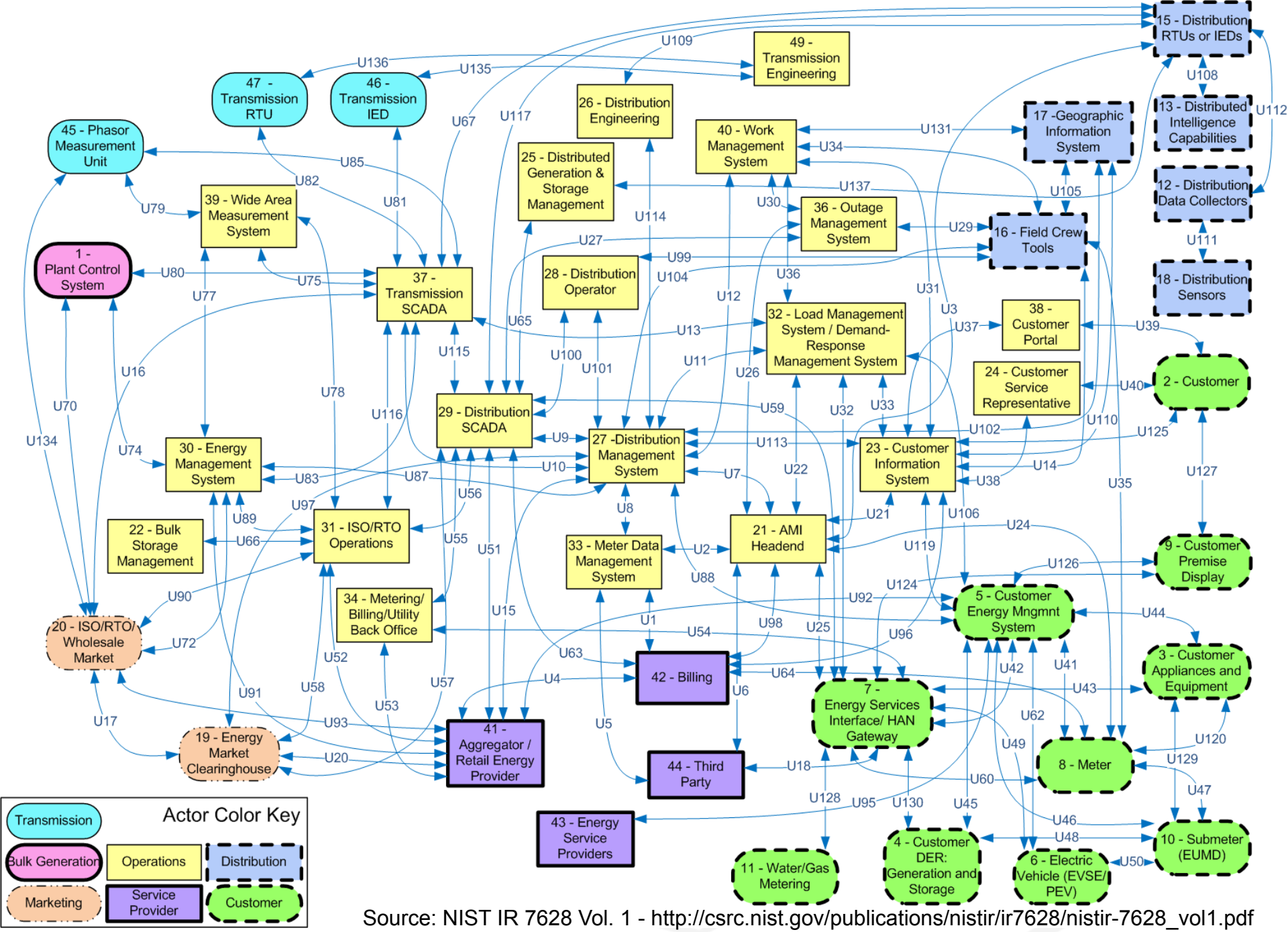


Source: http://www.sgiclearinghouse.org/ConceptualModel

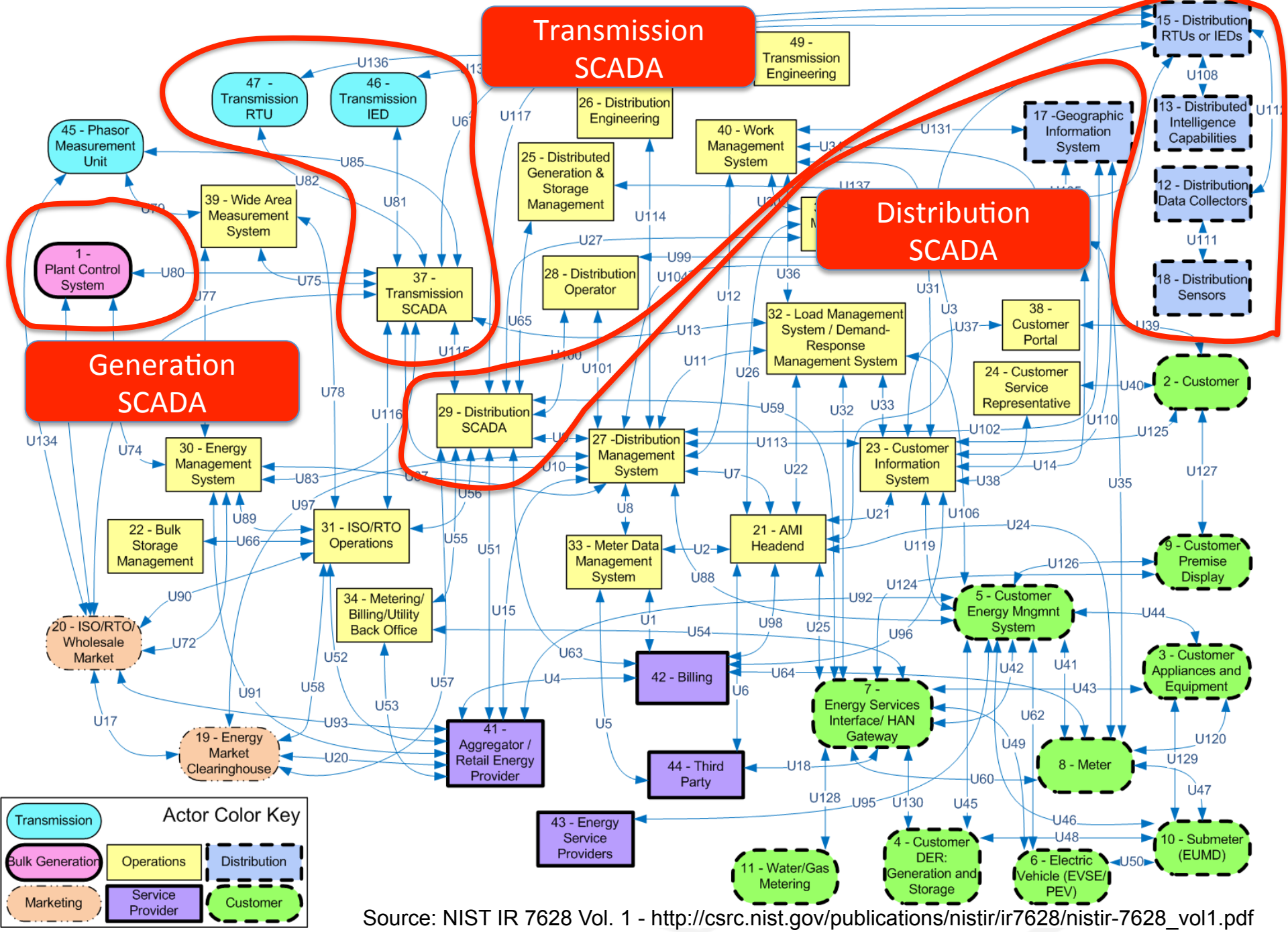
NIST Smart Grid Reference Model



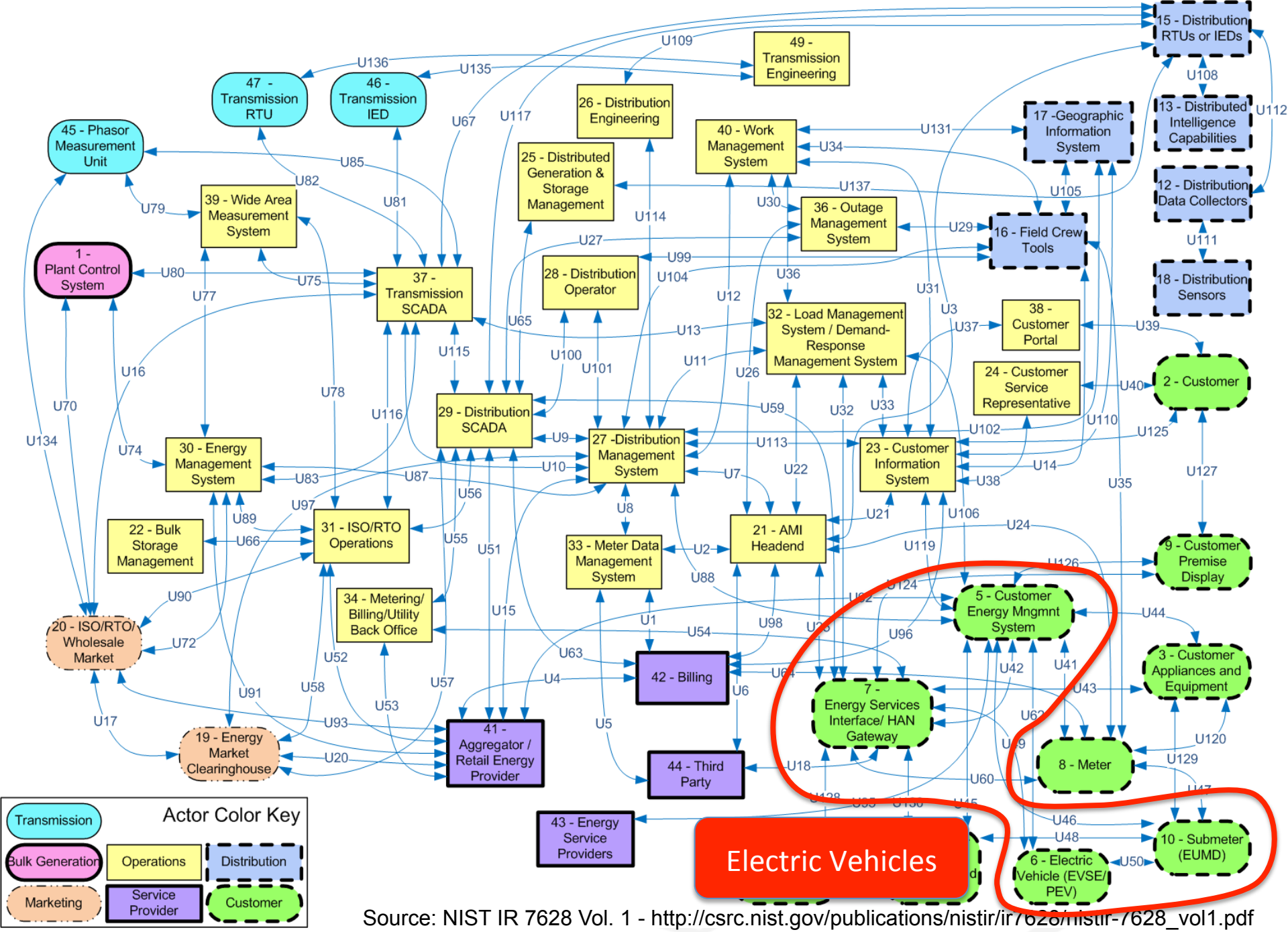
Source: NIST IR 7628 Vol. 1
http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf



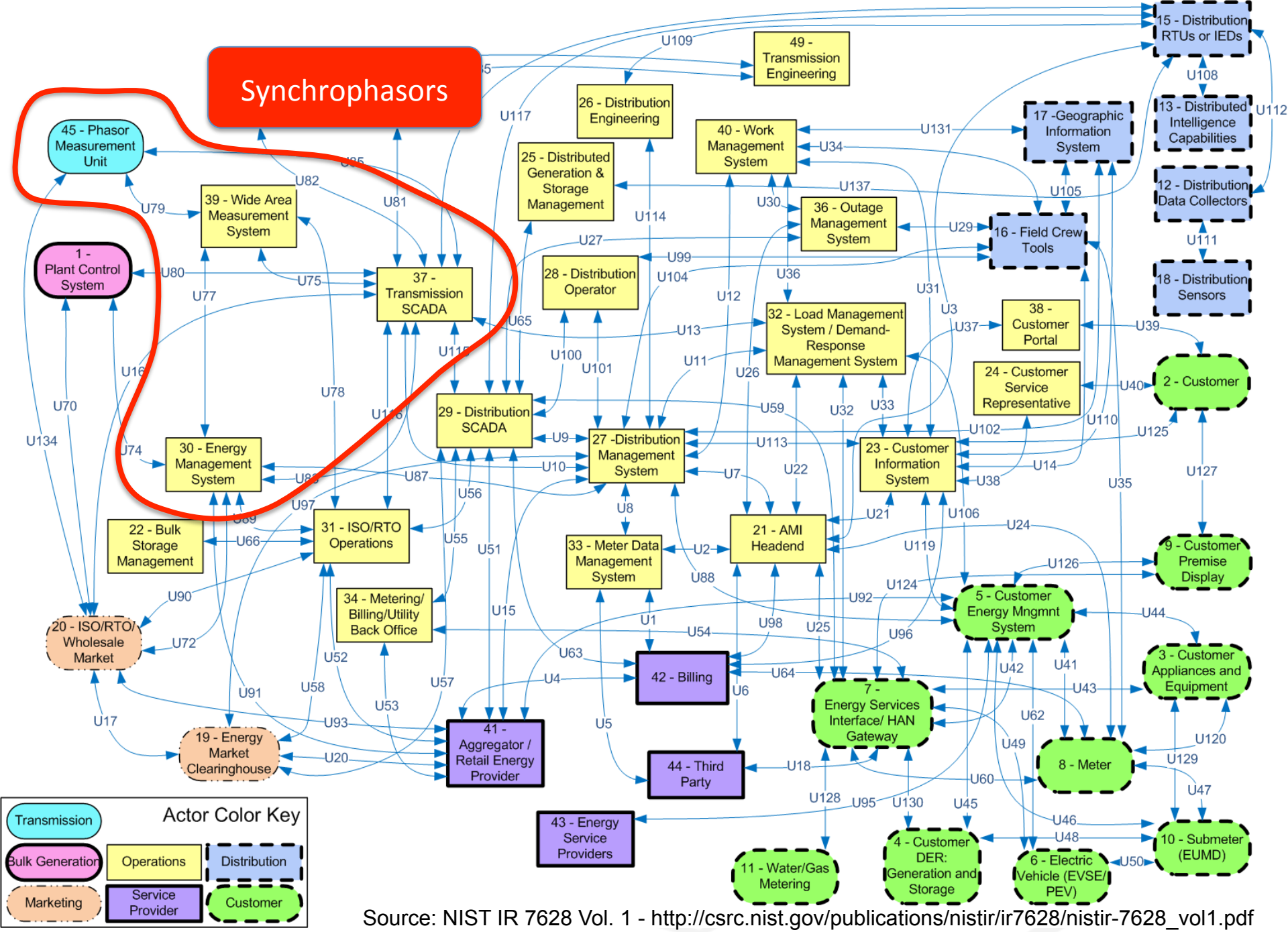
Source: NIST IR 7628 Vol. 1 - http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf



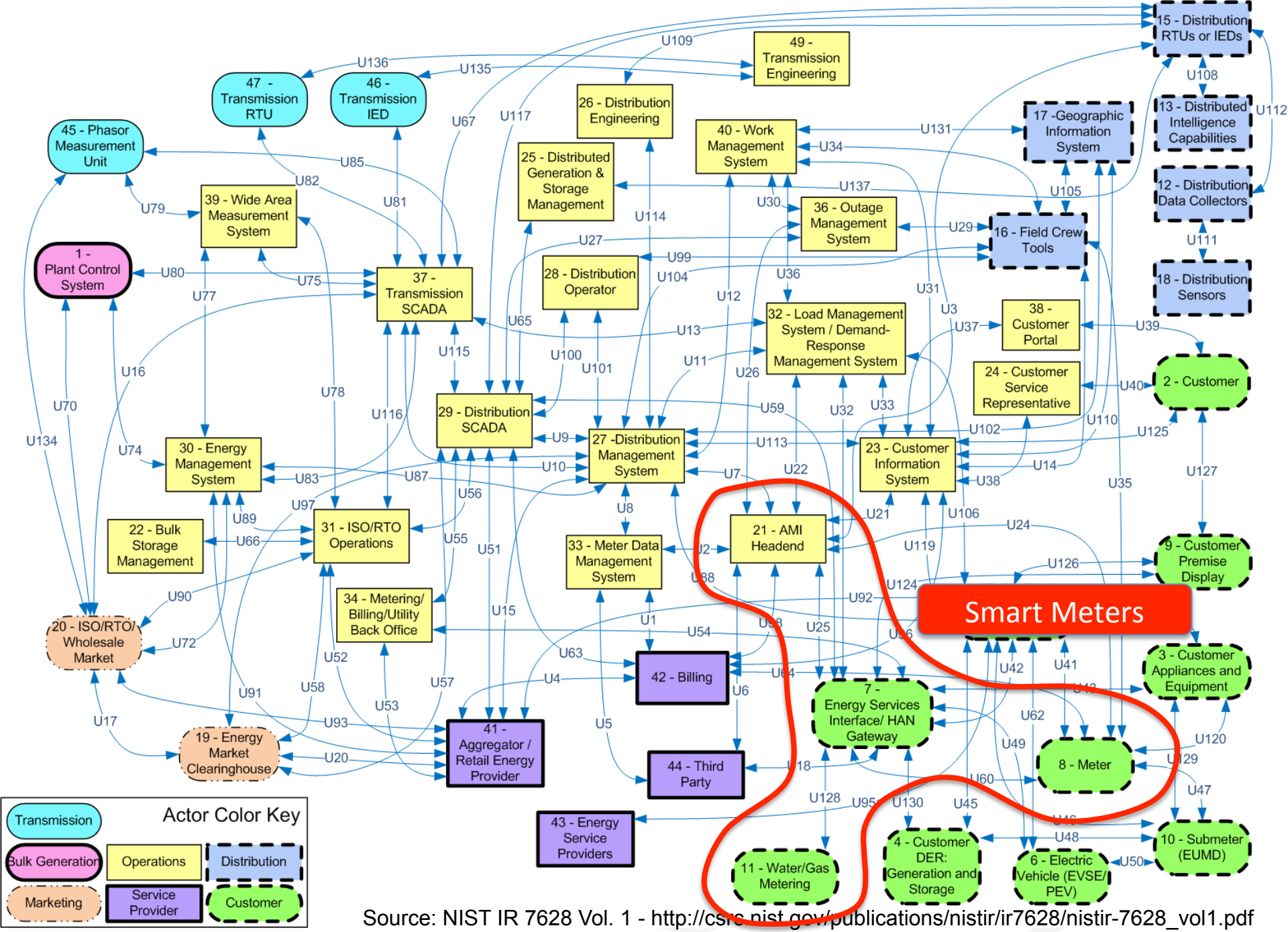
Source: NIST IR 7628 Vol. 1 - http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf



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



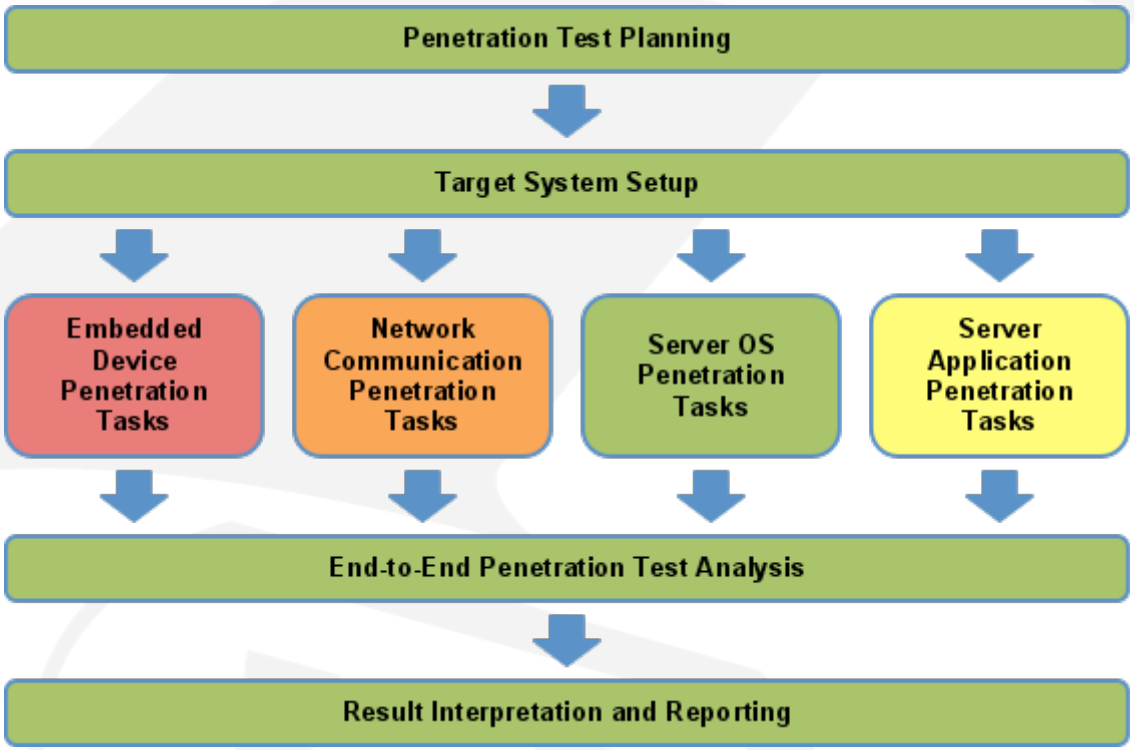
Source: NIST IR 7628 Vol. 1 - http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf



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

Penetration Testing Methodology

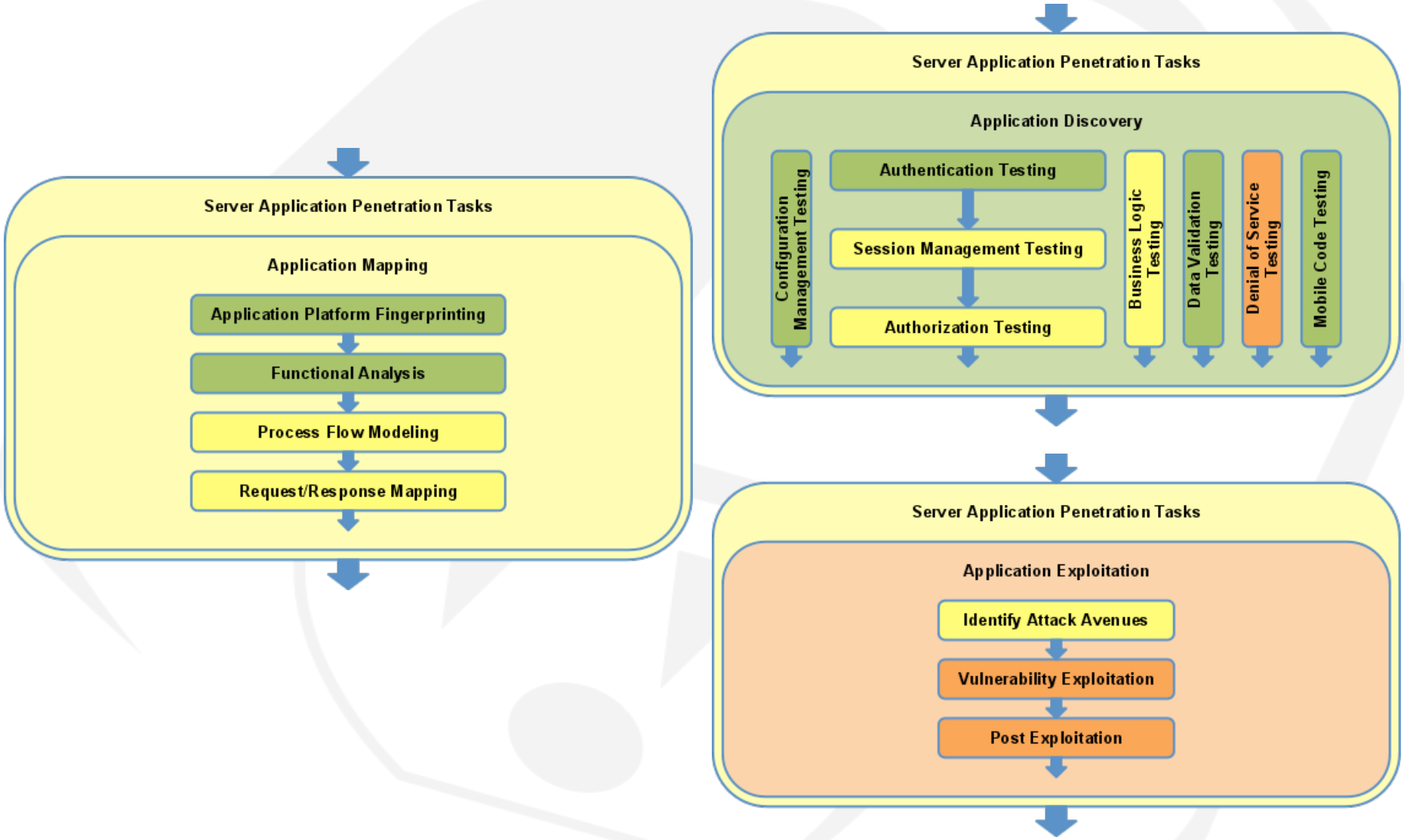
Smart Grid Penetration Test Plan



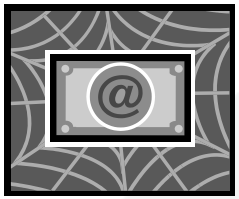
- Green: Tasks most frequently and require the most basic of penetration testing skill
- Yellow: Tasks commonly performed and require moderate penetration testing skill
- Orange: Tasks that are occasionally performed but require higher levels of expertise
- Red: Tasks performed infrequently and require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

White paper found at: http://www.smartgrid.epri.com/NESCOR.aspx

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

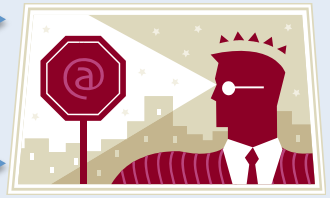
Utility Network

1

Employee using CIS system throughout the day

4

Web browser sends disconnect request to CIS



Customer Information System with Power Disconnect Capabilities

Critical Infrastructure Requirements

- Test in staging or testing environments!
- Under no circumstance, DO NOT BLINDLY RUN AUTOMATED SIPDERING OR SCANNING TOOLS!!!
  - Focus on manual and semi-automated tools
- Intimately know your tools!
- Understand what critical infrastructure is controlled!
- Understand where your requests are going!
- If it controls embedded devices, blacklist:
  - Configuration Updates
  - Firmware Updates
  - Critical Functions (power disconnects, relay state changes...)

Contact Information

www.utilisec.com
sales@utilisec.com

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