CONCEPTUAL SECURITY ARCHITECTURE

Sandy Bacik

July 18, 2011

Architecture as usually practiced

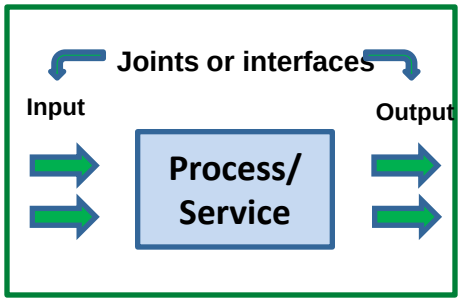
© Scott Adams, Inc./Dist. by UFS, Inc.

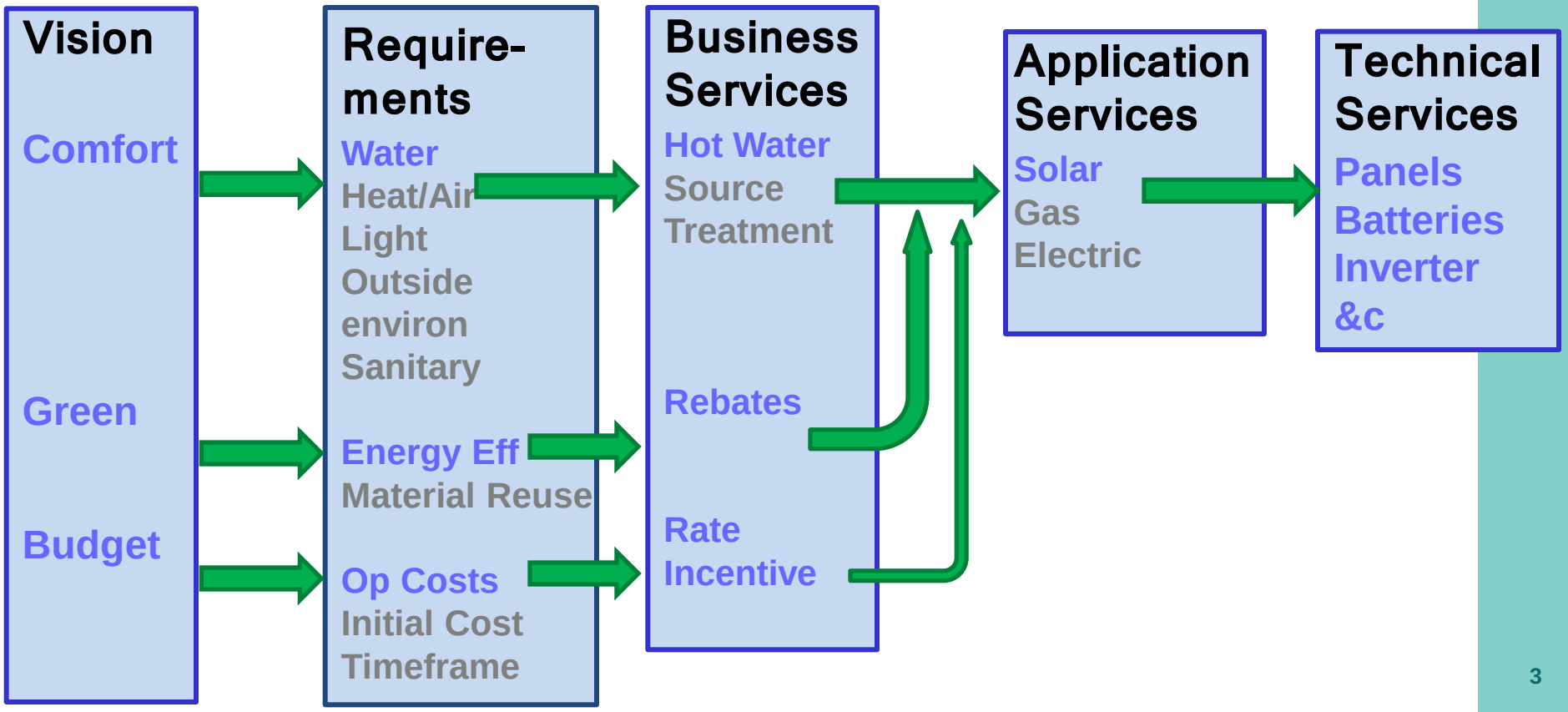
(Apologies to Mr Adams and my fellow architects)

> There is never enough time (or money) to do it right the first time
> There is always enough time and money to fix it over and over again
> -Anonymous

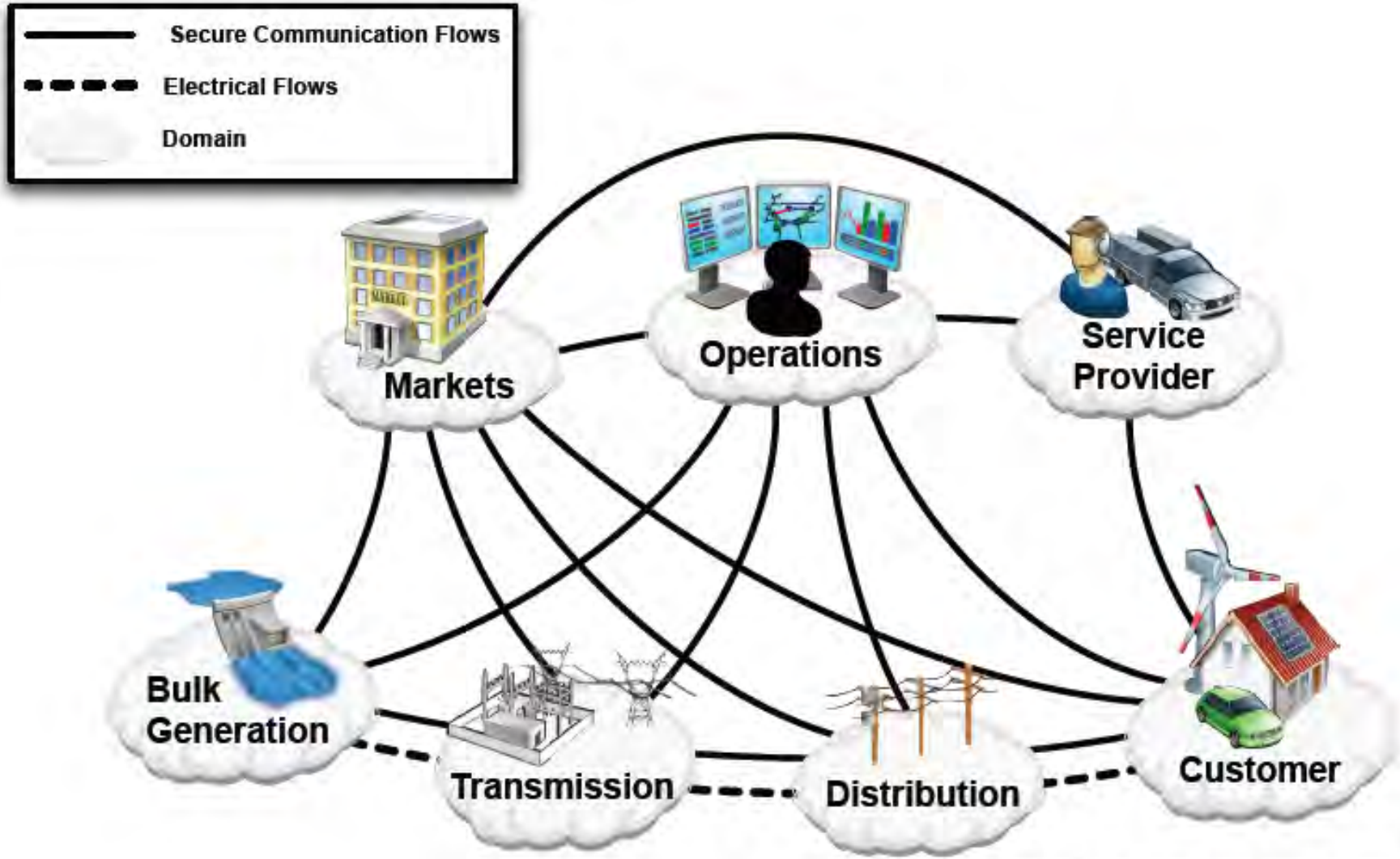
Simple Building Architecture Example

Magic in this case is the ability to infer the options

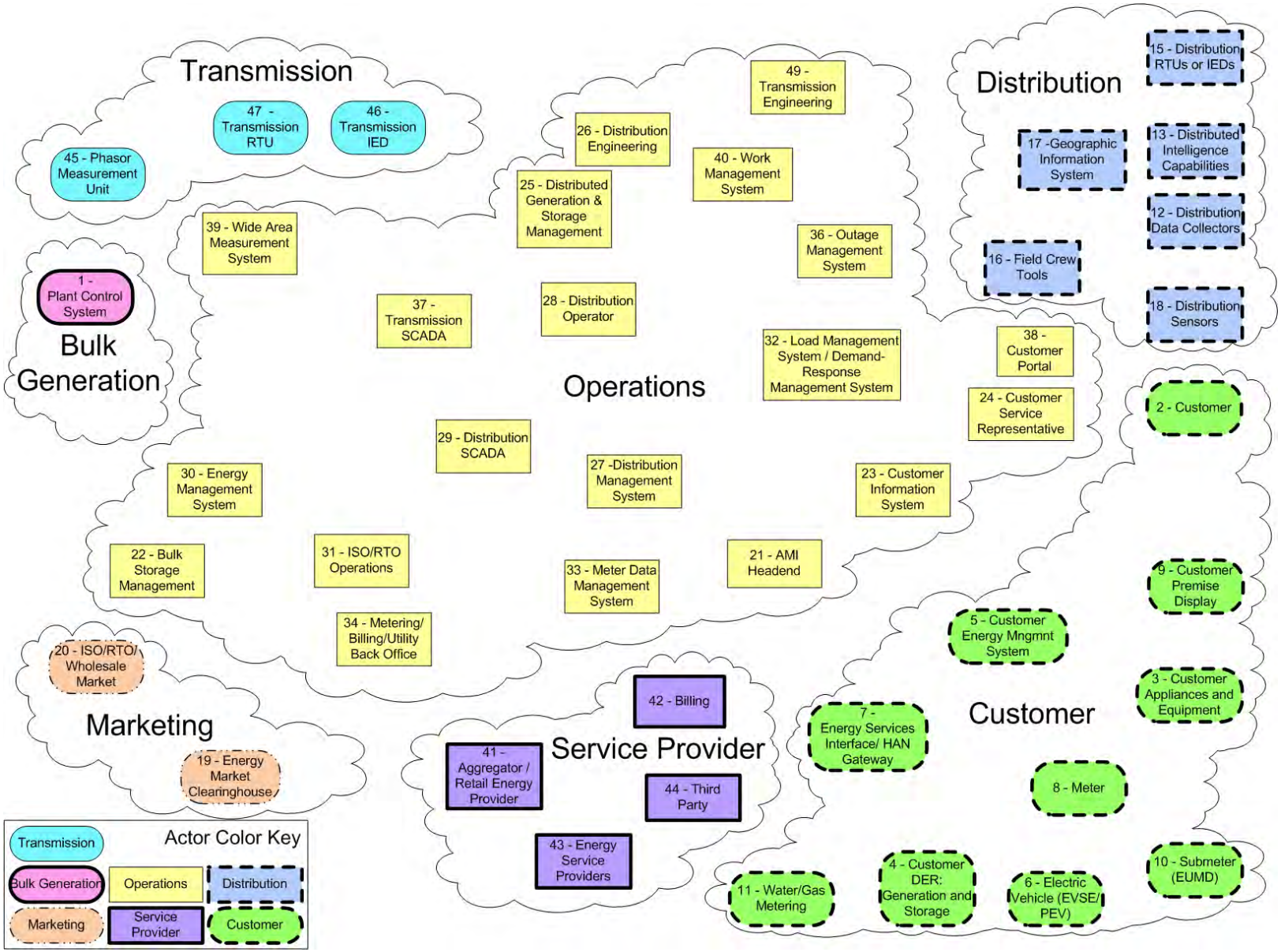




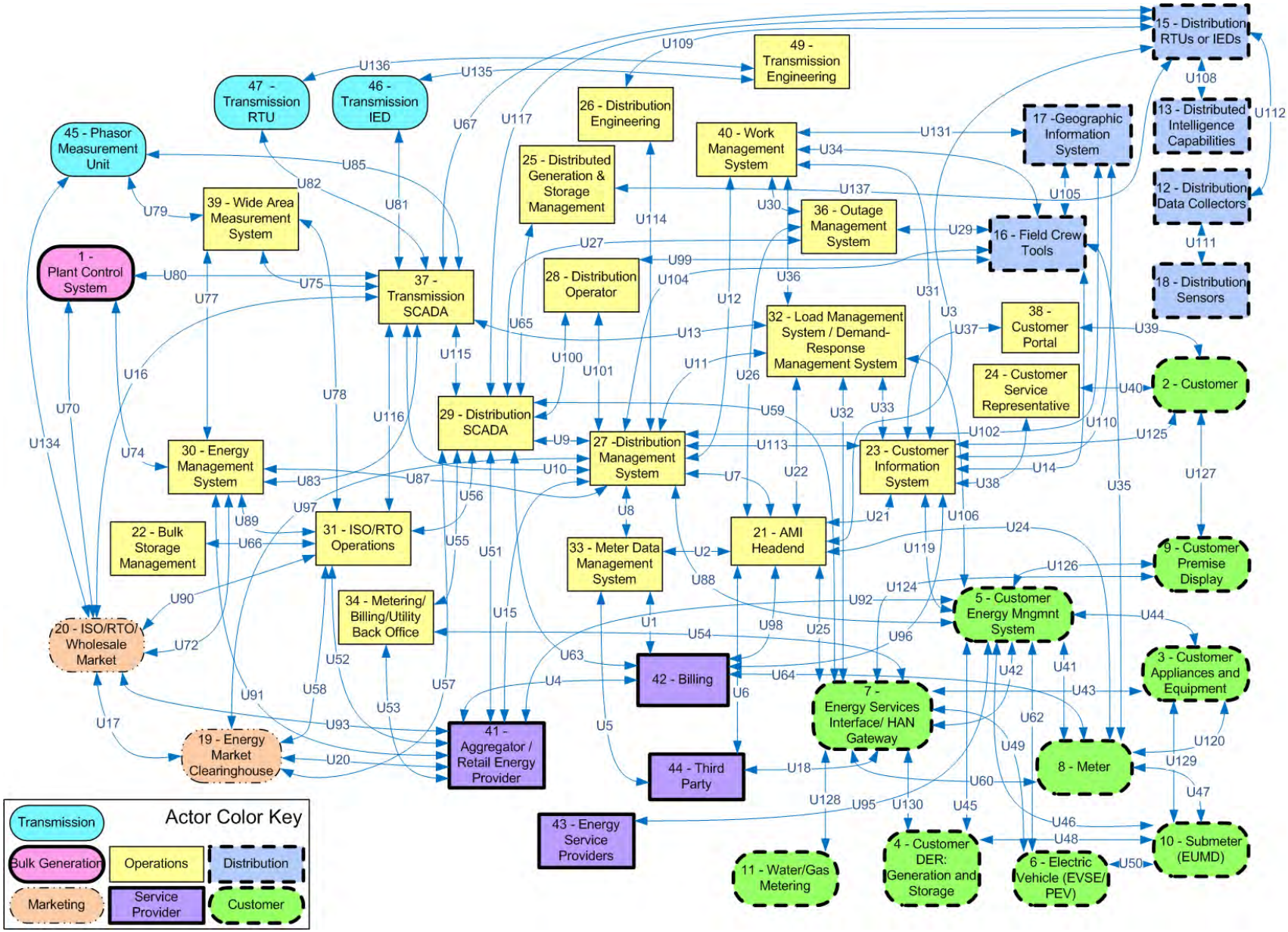
Smart Grid Domains



NIST Smart Grid Framework 1.0 January 2010


Transmission
47 - Transmission RTU
46 - Transmission IED
45 - Phasor Measurement Unit
Distribution
15 - Distribution RTUs or IEDs
17 -Geographic Information System
13 - Distributed Intelligence Capabilities
12 - Distribution Data Collectors
16 - Field Crew Tools
18 - Distribution Sensors
49 - Transmission Engineering
26 - Distribution Engineering
40 - Work Management System
25 - Distributed Generation & Storage Management
36 - Outage Management System
39 - Wide Area Measurement System
1 - Plant Control System
Bulk Generation
37 - Transmission SCADA
28 - Distribution Operator
32 - Load Management System / Demand-Response Management System
38 - Customer Portal
Operations
24 - Customer Service Representative
2 - Customer
29 - Distribution SCADA
27 -Distribution Management System
23 - Customer Information System
30 - Energy Management System
22 - Bulk Storage Management
31 - ISO/RTO Operations
33 - Meter Data Management System
21 - AMI Headend
9 - Customer Premise Display
34 - Metering/ Billing/Utility Back Office
5 - Customer Energy Mngmnt System
20 - ISO/RTO/ Wholesale Market
3 - Customer Appliances and Equipment
42 - Billing
Marketing
7 - Energy Services Interface/ HAN Gateway
Customer
41 - Aggregator / Retail Energy Provider
Service Provider
19 - Energy Market Clearinghouse
44 - Third Party
8 - Meter
43 - Energy Service Providers
10 - Submeter (EUMD)
11 - Water/Gas Metering
4 - Customer DER: Generation and Storage
6 - Electric Vehicle (EVSE/ PEV)
Actor Color Key
Transmission
Bulk Generation
Operations
Distribution
Marketing
Service Provider
Customer

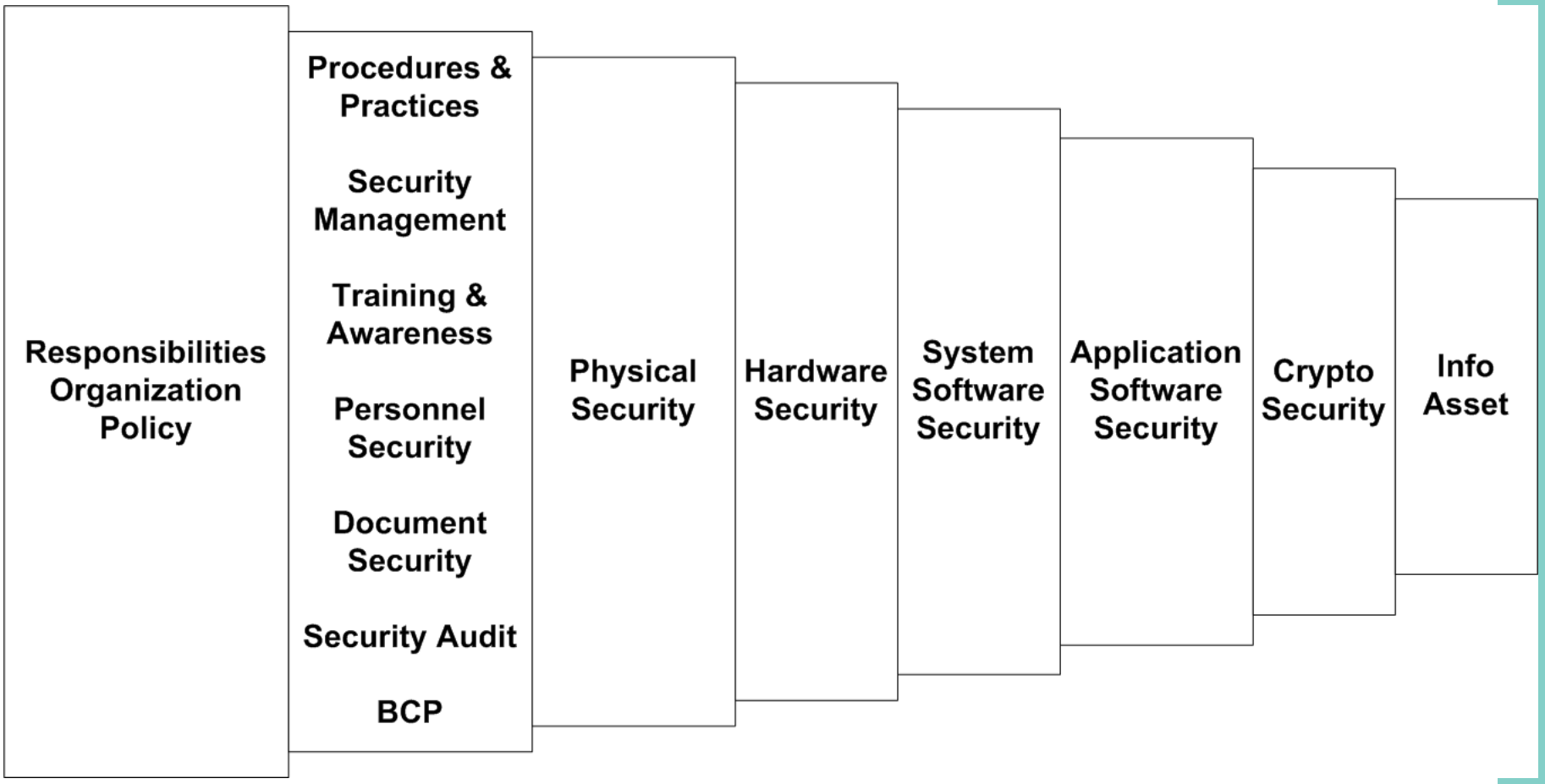
"SPAGHETTI" DRAWING



To Ensure Traceability

- Architecture needs to map to
  - Goals / Objectives
  - Requirements
  - Services

Multi-Layering of Security



Security Tools – More Than Just a Firewall

Management, Audit, Measurement, Monitoring, and Detection Tools
- Log Auditing Utilities
- Virus and Malicious Code Detection Systems
- Intrusion Detection Systems
- Vulnerability Scanners
- Forensics and Analysis Tools (FAT)
- Host Configuration Management Tools
- Automated Software Management Tools

Authentication and Authorization Technologies
- Role-Based Authorization Tools
- Password Authentication
- Challenge/Response Authentication
- Physical/Token Authentication
- Smart Card Authentication
- Biometric Authentication
- Location-Based Authentication
- Password Distribution and Management Technologies
- Device-to-Device Authentication

Filtering/Blocking/Access Control Technologies
- Network Firewalls
- Host-based Firewalls
- Virtual Networks

Physical Security Controls
- Physical Protection
- Personnel Security

Encryption Technologies and Data Validation
- Symmetric (Secret) Key Encryption
- Public Key Encryption and Key Distribution
- Virtual Private Networks (VPNs)

Industrial Automation and Control Systems Computer Software
- Server and Workstation Operating Systems
- Real-time and Embedded Operating Systems
- Web Technologies

Cyber Security Requirements – High Level

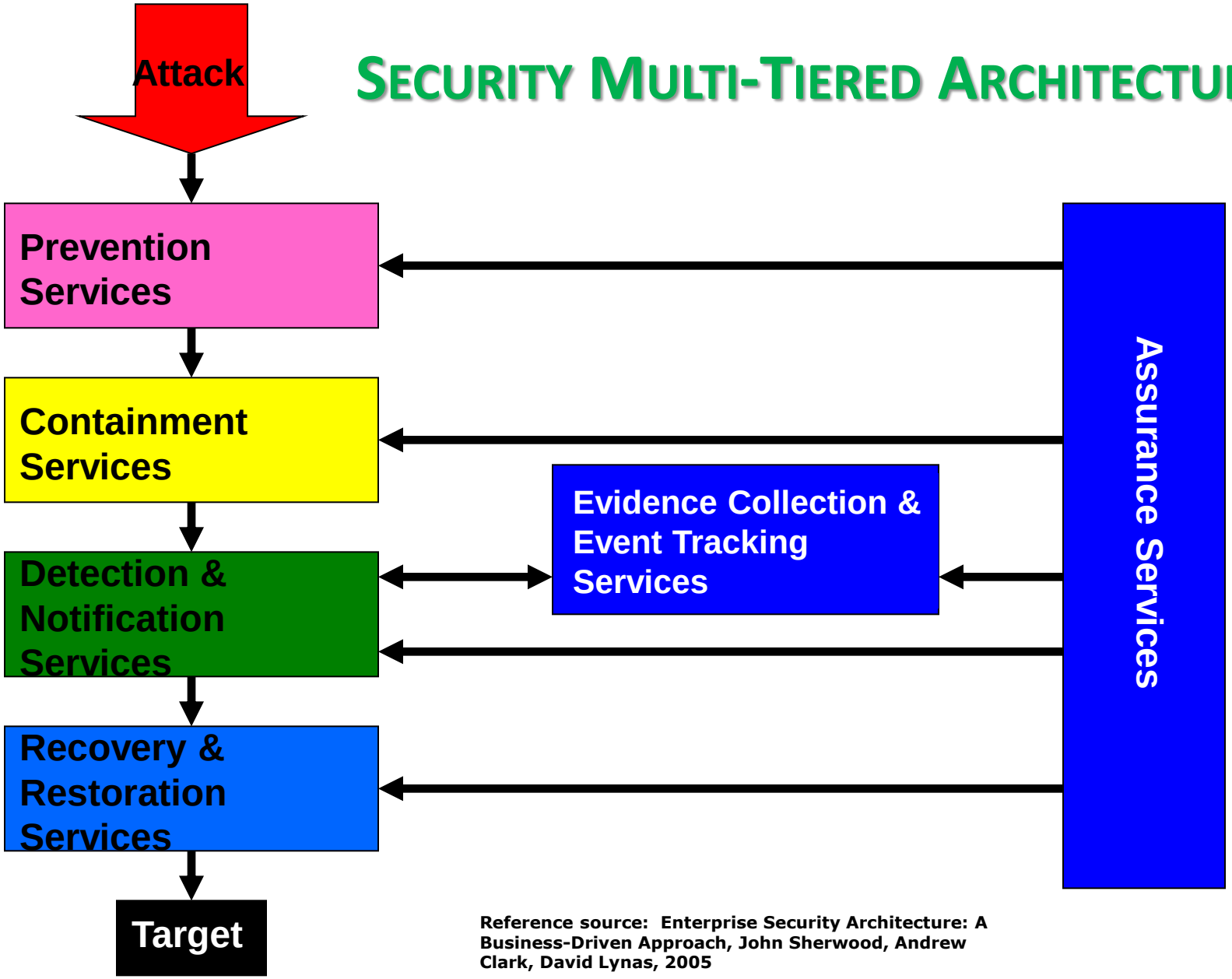
Functional Requirements

- Auditing
- Cryptographic Support
- User Data Protection
- Event Monitoring
- Identification & Authentication
- Functional Management
- Security Event Monitoring
- Physical Protection
- System Configuration
- Resource Utilization
- Trusted Path/Channels

Assurance Requirements

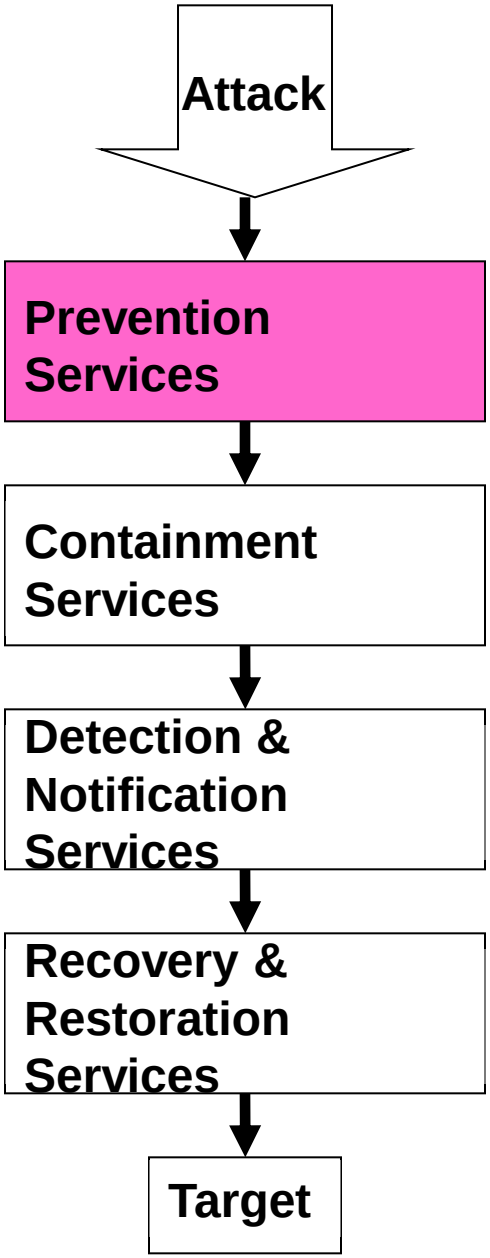
- Configuration Management
- Delivery & Operation
- Guidance Documents
- Life Cycle Support
- Security Awareness
- Operation & Maintenance
- System Architecture
- Testing
- Vulnerability Assessment
- Assurance Maintenance

Security Multi-Tiered Architecture



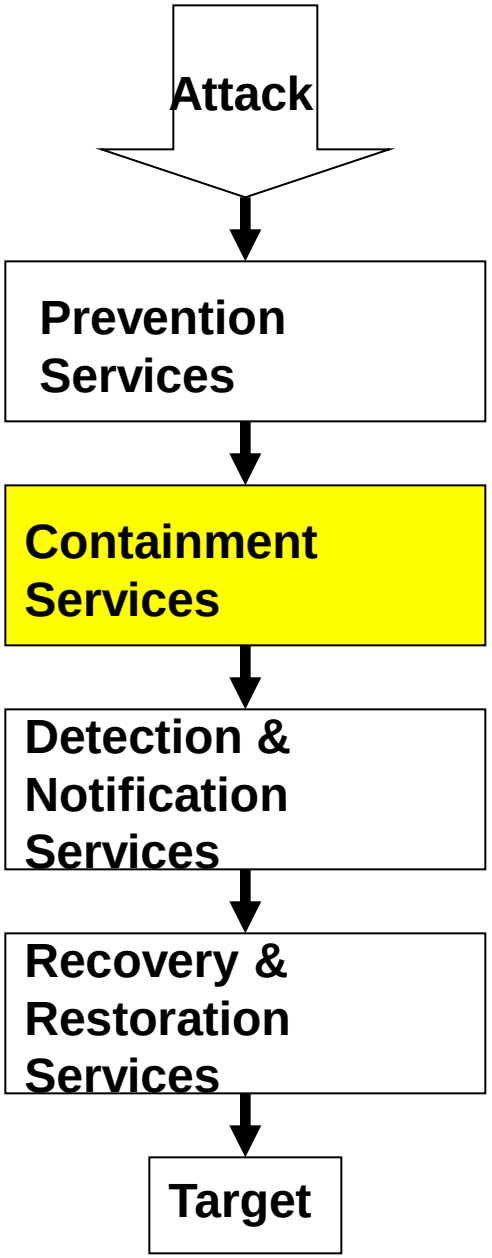
Reference source: Enterprise Security Architecture: A Business-Driven Approach, John Sherwood, Andrew Clark, David Lynas, 2005

Prevention Services



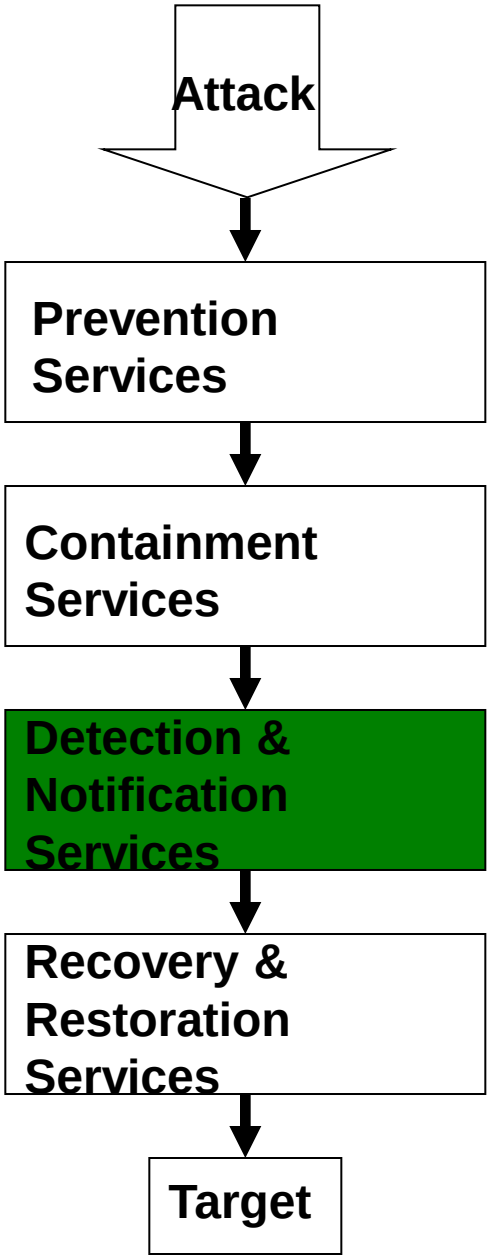
Security Architecture Tier	Security Services	Detail
Prevention	Entity Security Services	Unique Naming
		Registration
		Public Key Certification
		Credentials Certification
		Directory Service
		Authorization
		Authentication
	Communications Security	Session Authentication
		Message Origin Authentication
		Message Integrity Protection
		Message Content Confidentiality
		Measurement & Metrics
		Security Administration
		User Support
		Physical Security
		Environment Security
		Non-repudiation
		Message Replay Protection
		Traffic Flow Confidentiality
	Application & System Security	Authorization
		Logical Access Controls
		Audit Trails
		Stored Data Integrity Protection
		Store Data Confidentiality
		Software Integrity Protection
		Software Licensing Management
		System Configuration Protection
		Data Replication & Backup
		Software Replication & Backup
		Trusted Time
		User Interface for Security
	Security Management	Policy Management
		Training & Awareness
		Operations Management
		Provisioning
		Monitoring
		Measurement & Metrics
		Security Administration
		User Support
		Physical Security Devices
		Environmental Security

Containment Services



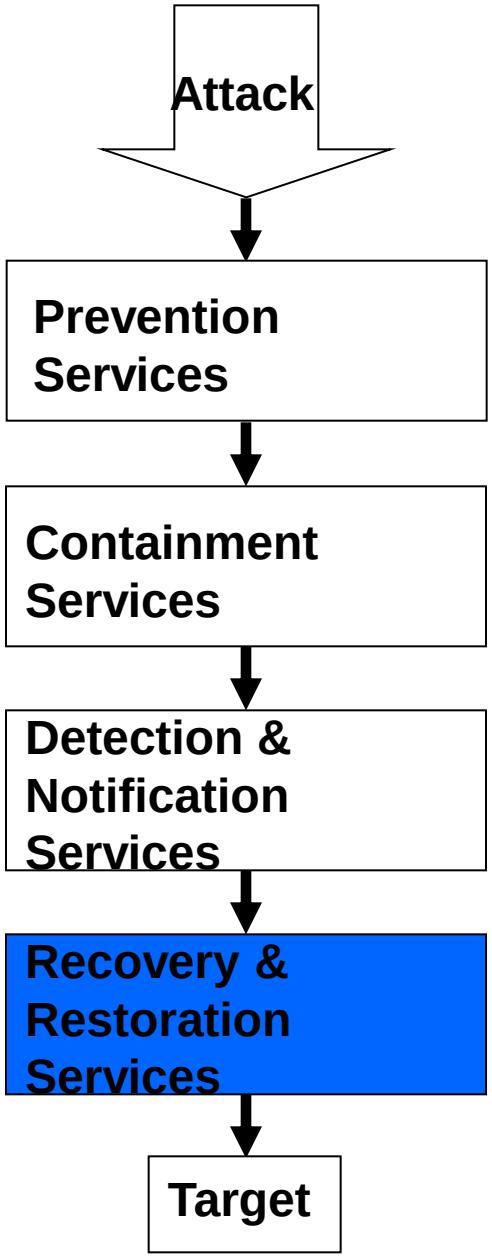
Security Architecture Tier	Security Services
Containment	Entity Authorization
	Store Data Confidentiality
	Software Integrity Protection
	Physical Security
	Environmental Security
	Training & Awareness

Detection & Notification Services



Security Architecture Tier	Security Services
Detection & Notification	Message Integrity Protection
	Store Data Confidentiality
	Security Monitoring
	Intrusion Detection
	Security Alarm Management
	Training & Awareness
	Measurement & Metrics

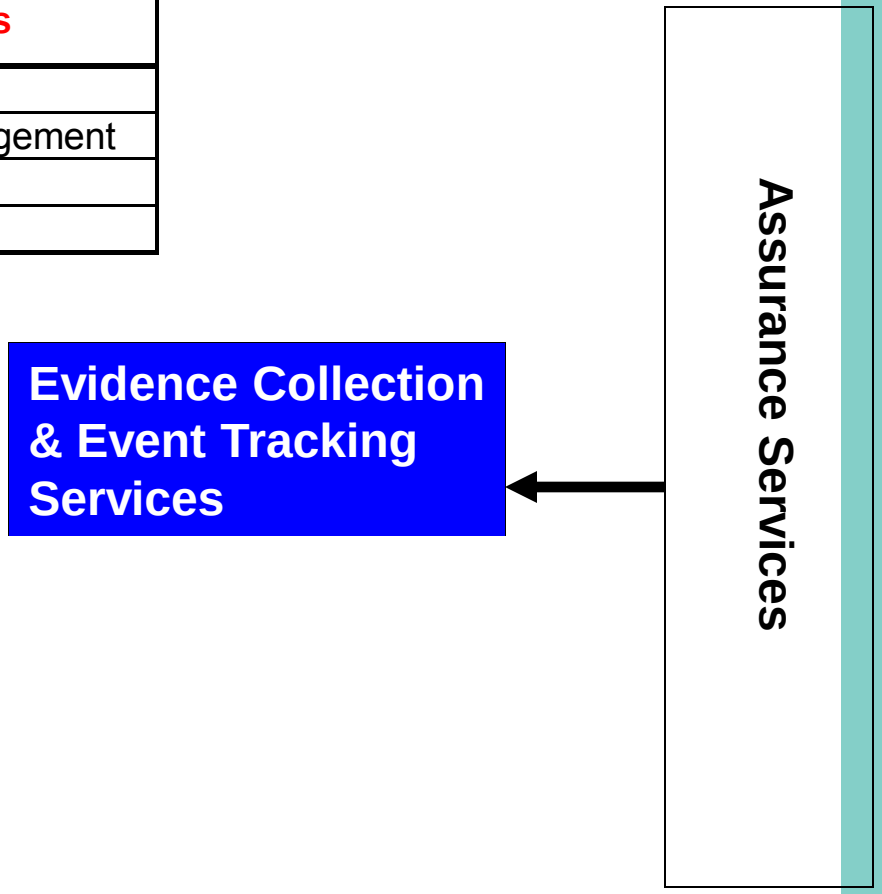
Recovery & Restoration Services



Security Architecture Tier	Security Services
Recovery & Restoration	Incident Response
	Data Replication & Backup
	Software Replication & Backup
	Disaster Recovery
	Crisis Management

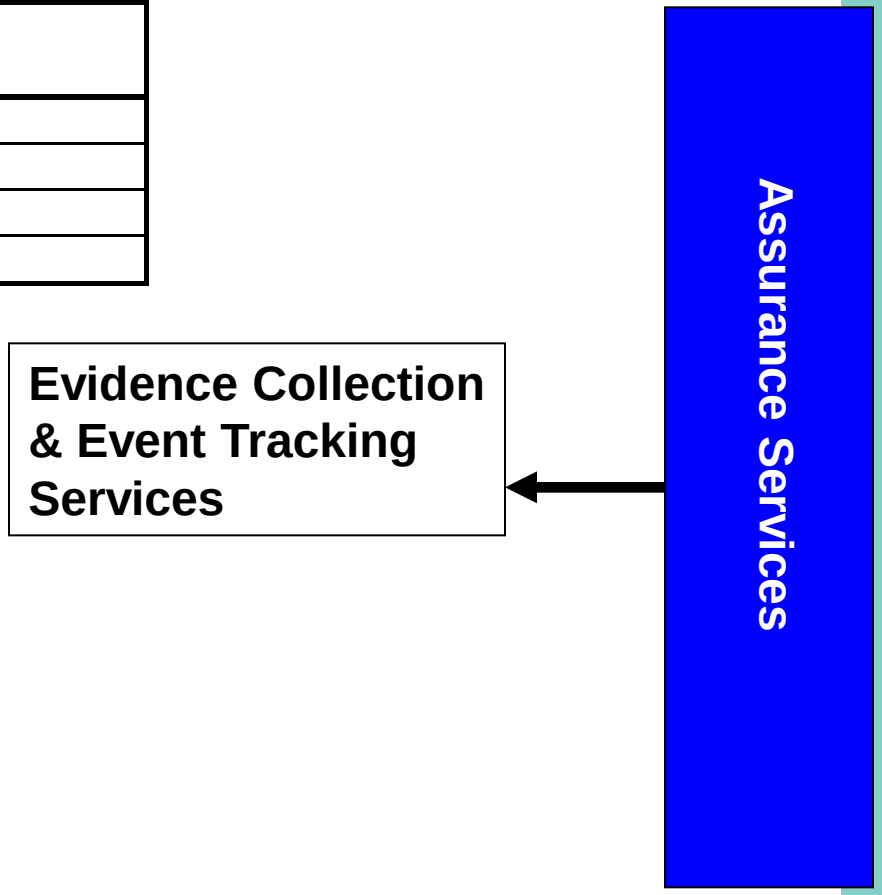
Event Collection & Tracking Services

Security Architecture Tier	Security Services
Event Collection & Event Tracking	Audit Trails
	Security Operations Management
	Security Monitoring
	Measurement & Metrics



Assurance Services

Security Architecture Tier	Security Services
Assurance	Audit Trails
	Security Audit
	Security Monitoring
	Measurement & Metrics



SABSA Overview

- SABSA provides a **holistic** approach to cyber/information security and is baselined against the '*ISO 7498-2:1989, Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*' standard
- Five layer framework that answers the why, how, who, where and when for security architecture
- Five layers are Contextual Architecture, Conceptual Architecture, Logical Architecture, Physical Architecture and Component Architecture
- A sixth layer is added for Service Management Architecture and is synonymous with Operational Security Architecture
- Compatible and complementary to other architecture frameworks, including Zachman, TOGAF, DODAF, etc.

SABSA Framework – Fully Qualified

Business Architecture
Security Architecture
Information Architecture
Application Architecture
Technology Architecture
Risk Management & Information Security

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices & Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Action and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites, Networks and Platforms	Security Operations Schedule

BASIC BACKGROUND INFORMATION

Basic Cybersecurity Objectives

- Availability is the most important security objective for power system reliability. The time latency associated with availability can vary—
  - ≤ 4 ms for protective relaying
  - Subseconds for transmission wide-area situational awareness monitoring
  - Seconds for substation and feeder SCADA data
  - Minutes for monitoring noncritical equipment and some market pricing information
  - Hours for meter reading and longer-term market pricing information; and
  - Days/weeks/months for collecting long-term data such as power quality information.
- Integrity for power system operations includes assurance that—
  - Data has not been modified without authorization
  - Source of data is authenticated
  - Time stamp associated with the data is known and authenticated; and
  - Quality of data is known and authenticated.
- Confidentiality is the least critical for power system reliability. However, confidentiality is becoming more important, particularly with the increasing availability of customer information online—
  - Privacy of customer information
  - Electric market information; and
  - General corporate information, such as payroll, internal strategic planning, etc

Created an initial business attribute list

- **Attribute classes:**
  - **User attributes**
  - **Management attributes**
  - **Operational attributes**
  - **Risk management attributes**
  - **Legal and regulatory attributes**
  - **Technical strategy attributes**
  - **Business strategy attributes**

Defense Strategy of Security Services

- Using a standard attack multi-tier security services and review common security service services
- Review generic message list and apply security services
- http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGArchi/Security_Services-And-MessageList-v0p1.xls

Cannot go all the way to specific implementations

- We cannot go all the way to specific technology and implementations because
  - Do not know organizational objectives
  - Do not know specific organizational requirements
  - Do not know organizational size or scope
- Order – Eat – Pay or Order – Pay – Eat example