



Evolving Toward a High Assurance Smart Grid Through a Distributed Control Architecture



*Smart Grid Cyber Security
is more than just applying IT security
to grid control links*

It is a total System Design approach

*Tom Overman
thomas.overman@boeing.com*

*Brad Cohen
brad.s.cohen@boeing.com*

Agenda

- High Assurance
 - A broad term encompassing dimensions of high security, high availability, high reliability
- Review of threat examples, with Lessons Learned
- Grid integration
- Threat Response:
 - An Architectural Approach to achieve a High Assurance Smart Grid

A definition

- High Assurance Smart Grid (HASG)
≠ Evaluation Assurance Level (EAL) for Smart Grid

- High Assurance Smart Grid (HASG)
≈ “integrated approaches for assuring reliability, availability, integrity, privacy, confidentiality, safety, and real-time performance of complex systems...”

See High Assurance Systems Engineering (HASE) 2010 conference web site at:
<http://web.mst.edu/~hase/hase2010/>

The Threat

Lessons Learned (IT Solutions Approach)

Maroochy Waste Water

Event: More than 750,000 gallons of untreated sewage intentionally released into parks, schools, and hotel grounds.

Impact: Loss of income, public health questioned, 2000,000 in cleanup and monitoring costs.

Specifics: SCADA system had 200 nodes (140 pumping stations) governing sewage and drinking water.

- Used OPC ActixX controls, DNP3, and Modbus protocols.
- Used packet radio communications to RTUs.
- Baden used commercially available radios and stolen SCADA software to make his laptop appear as a pumping station.
- Caused as many as 48 different incidents over a 3-month period (Feb 9 to April 23).

Lessons learned

- Change log-ons after terminations.
- Investigate anomalous system behavior.
- Use secure radio transmissions.

Davis Besse Nuclear Power Plant

Event: Aug 20, 2003 Slammer worm infects plant.

Impact: Complete shutdown of digital portion of Safety Parameter Display System (SPDS) and Plant Process Computer (PPC).

Recovery time:
SPDS - 4 hours 50 minutes
PPC - 8 hours 9 minutes

Specifics: Worm started at contractors site.

- Worm jumped from corporate to plant network and found an unpatched server.
- Patch had been available for 6 months.

Lessons learned

- Secure remote (trusted) access channels.
- Defense-in-depth strategies, FWs and IDS.
- Critical patch installation needs to drive trusted agent status.

Insider Threat

2 deny hacking into L.A.'s traffic light system

2 Los Angeles traffic engineers admit hacking

Lessons learned

- Role based access.
- Data/command integrity.

Polish Trains

Schubert hacks into city's train system

Lessons learned

- Role based access.
- Trusted agents.
- Integrated physical security.

Olympic Pipeline Explosion

Event: 10-inch gasoline pipeline explosion and fire, exacerbated by inability of SCADA system to perform control and monitoring functions.

Impact: 3 fatalities, property damage \$4.6M, matching three of BP's largest loss companies.

Specifics: Erroneous changes to live historical databases caused critical shutdown in system responsiveness (exacerbated by sensor repair rate changing from 3 second post to over 8 minutes).

- Communication links between main computer, field sensors, and controllers with a combination of leased phone lines and frame relay.

Lessons learned

- Identify controls to critical assets.
- Do not use administrative controls to solve system anomalies.
- Do not perform database updates on live systems.
- Apply appropriate security to remote access.

60 Minutes Report of 08 Nov 2009

"It is now clear this cyber threat is one [of] the most serious economic and national security challenges we face as a nation"

President Barack Obama

"They can steal critical infrastructure, wipe databases. We know they can rob banks. So, it's a much bigger and more serious threat."

Jim Lewis, Director, Center for Strategic and International Studies

"I look at this as, like a pre-9/11 moment where we identify a problem, we identify a threat, we know it exists, we know it's real, and we don't move quickly enough to fix the problem"

Congressman Jim Langevin, D-R

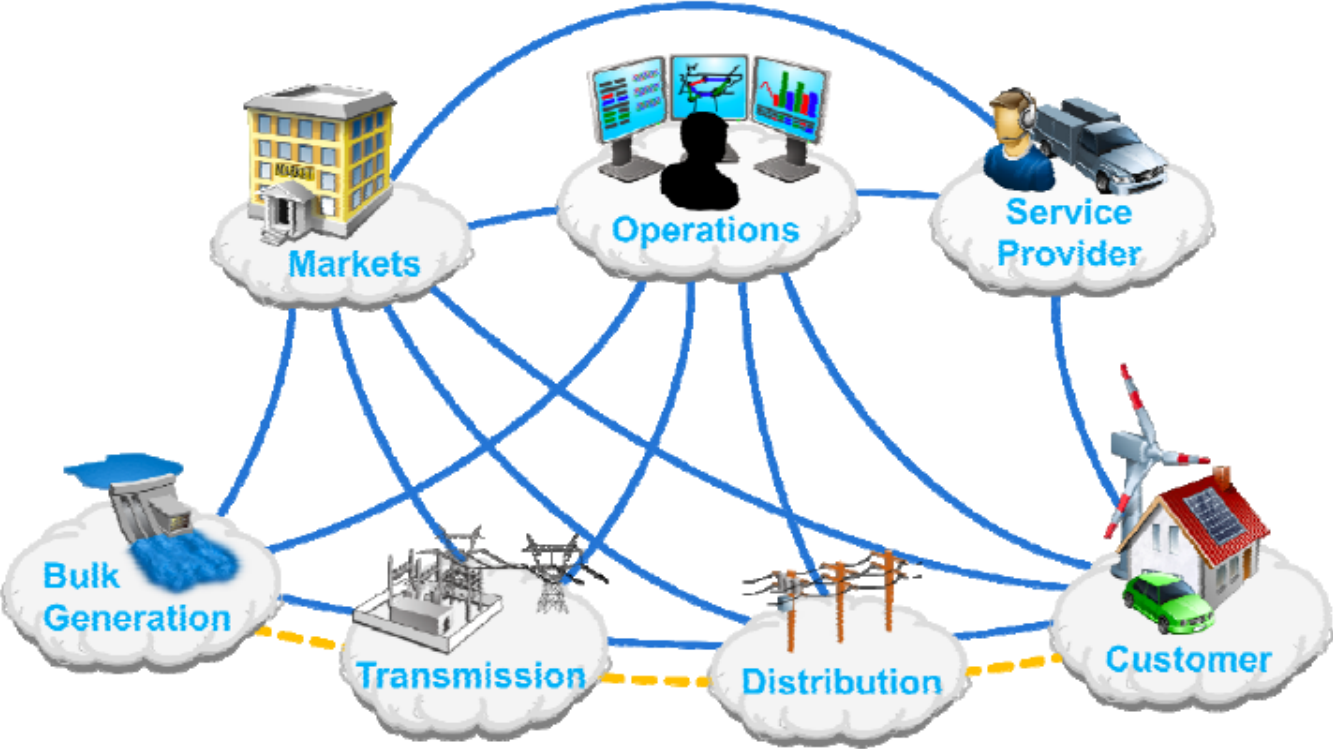
Lessons learned

- Role based access.
- Data/command integrity.
- Trusted agents.
- Integrated physical security.

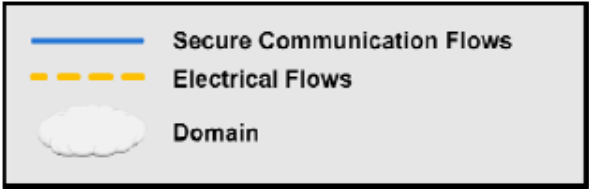
- Apply appropriate security to remote access
- Critical patch installation needs to drive trusted agent status
- Data/command integrity
- Defense-in-depth strategies, Firewalls & IDS
- Delete user accounts after terminations
- Don't perform database updates on live systems
- Don't use administrative controls to solve system anomalies
- Identify controls to critical assets
- Integrated physical security
- Investigate anomalous system behavior
- Role based access
- Secure remote (trusted) access channels
- Trusted agents
- Use secure radio transmissions

All necessary, but not sufficient
these do not address grid control architecture

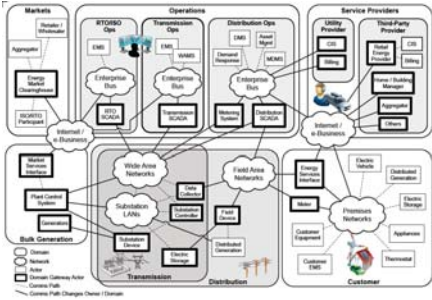
NIST Smart Grid Conceptual Reference Diagram



NIST Smart Grid Framework 1.0 Sept 2009

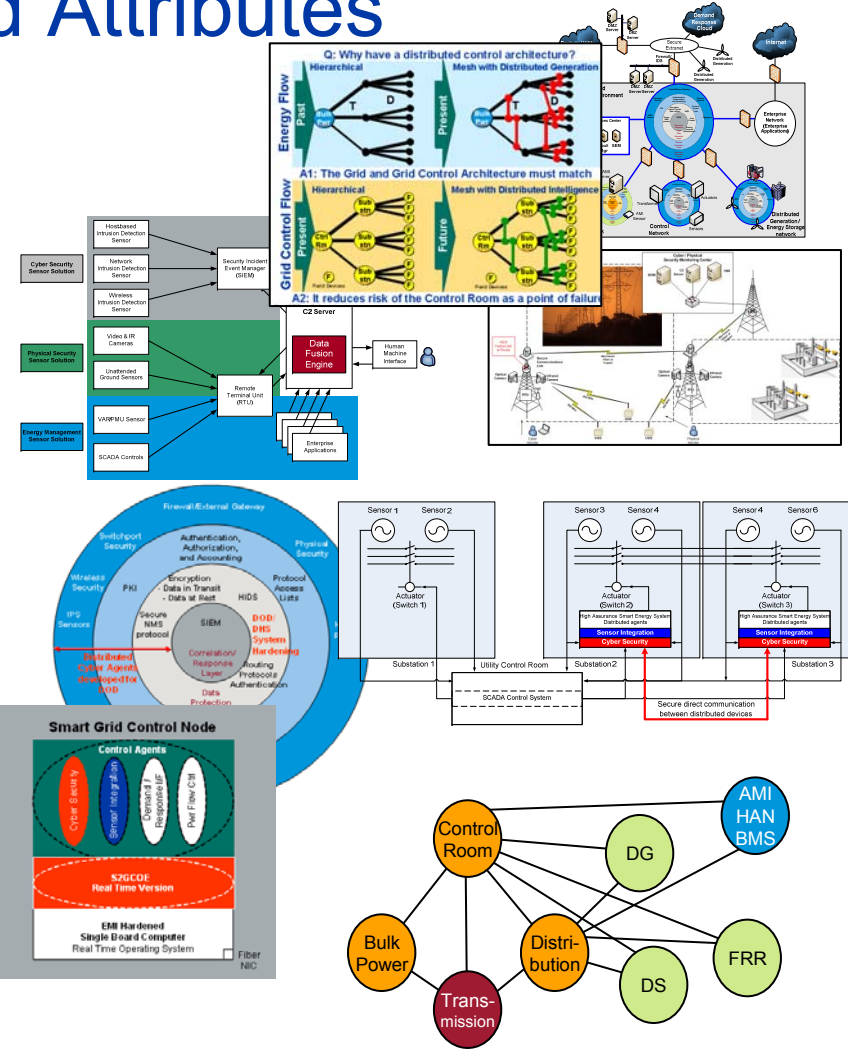


System Details



High Assurance Smart Grid Attributes

- Integrated Energy Management, Cyber Security and Physical Security with Defense in Depth
 - Including strong Role Based Access Control (RBAC) *for people and devices*
- Secure distributed architecture enables autonomy and eliminates single point of failure
- Assume compromise in the system (through accident, malice or system failure) *and engineer energy control systems accordingly*
- Auto-Responsive (AR) Loads
 - if you can't remotely control it, the remote control can't be compromised



Creating a High Assurance Smart Grid requires utilizing the best attributes from multiple disciplines

Defense in Depth Model

See NERC Smart Grid Task Force Report *Reliability Considerations from the Integration of Smart Grid*

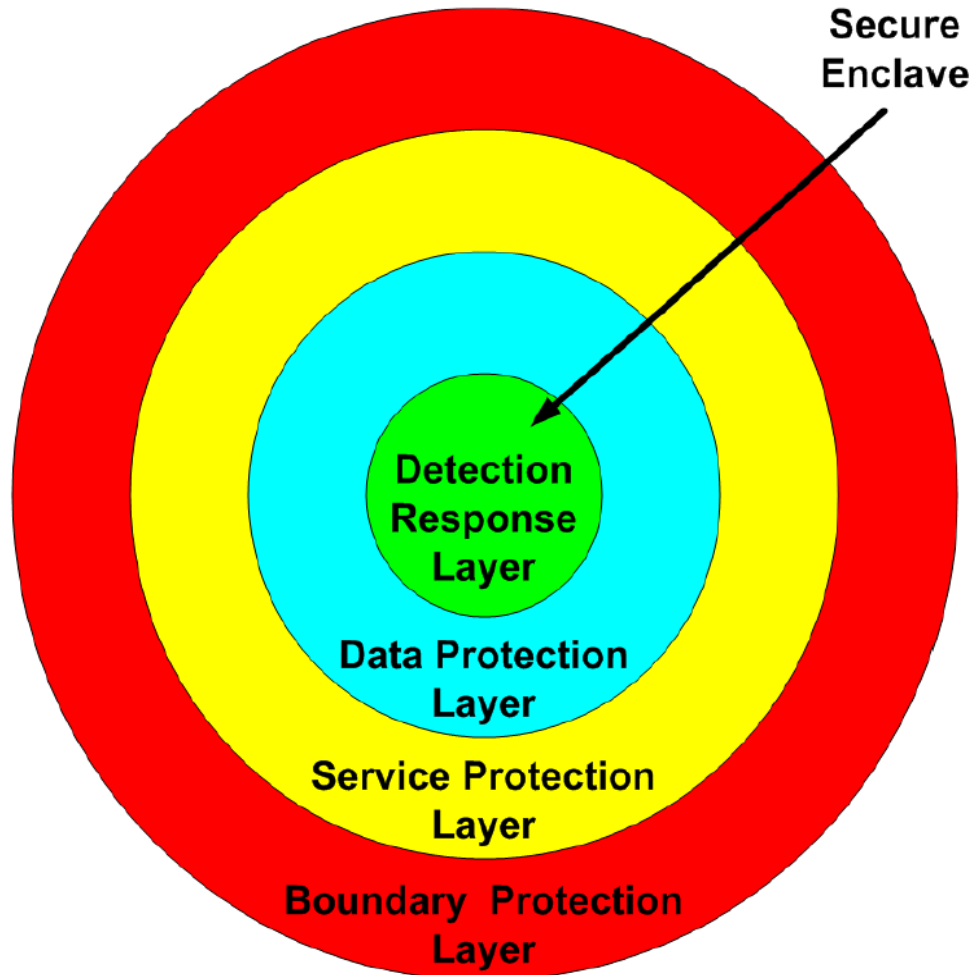
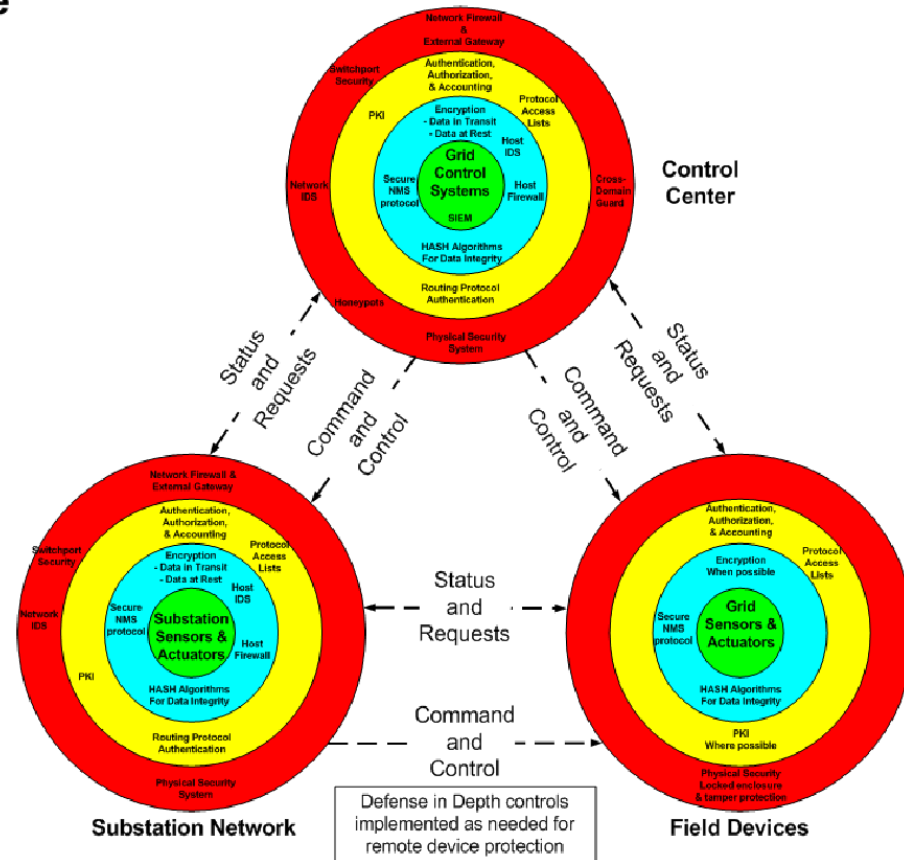


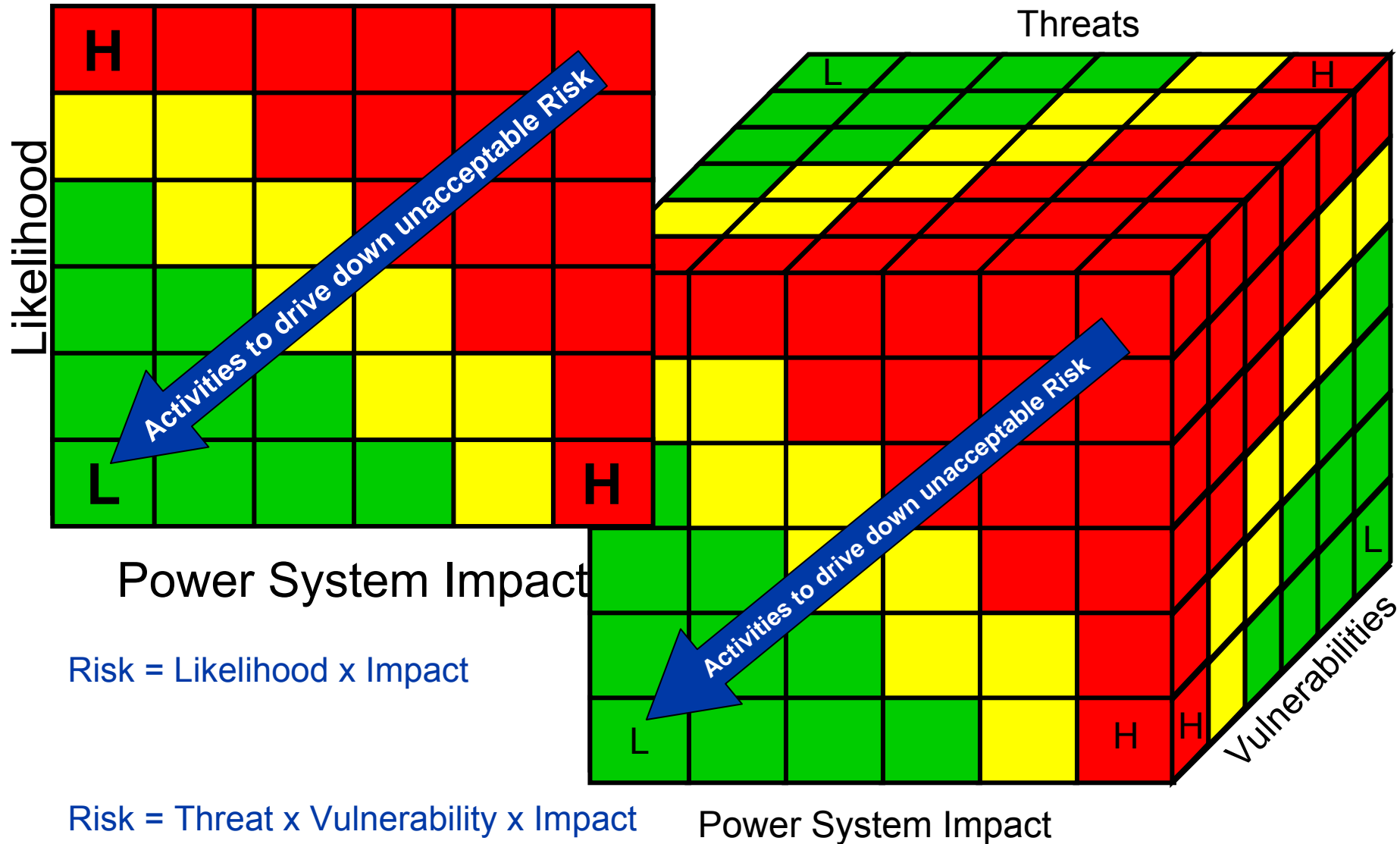
Figure 6: Cyber security defense-in-depth model

Figure 7: Cyber security defense-in-depth example

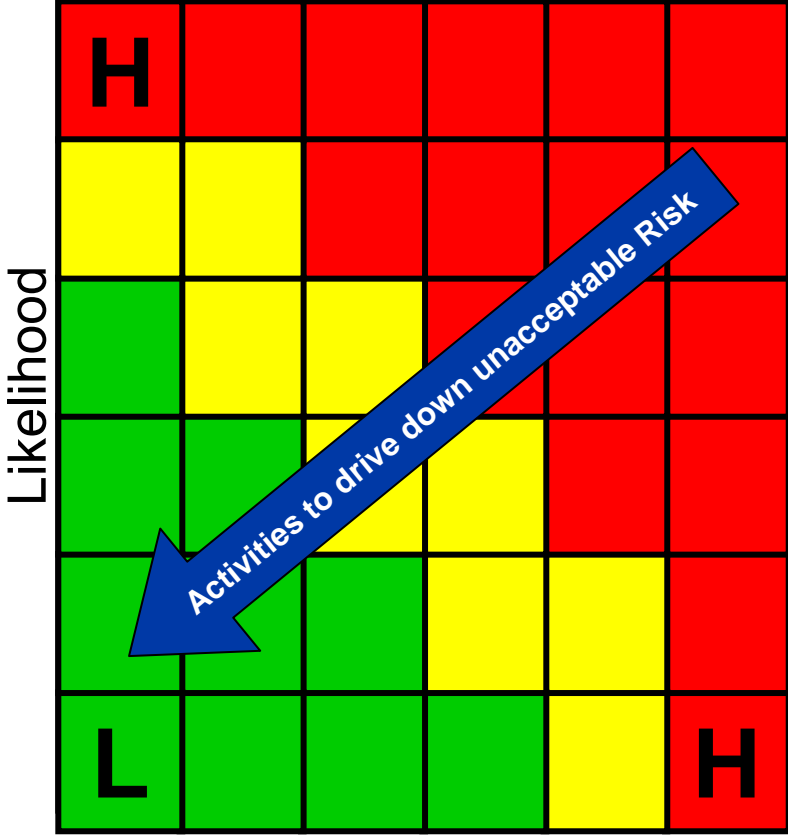
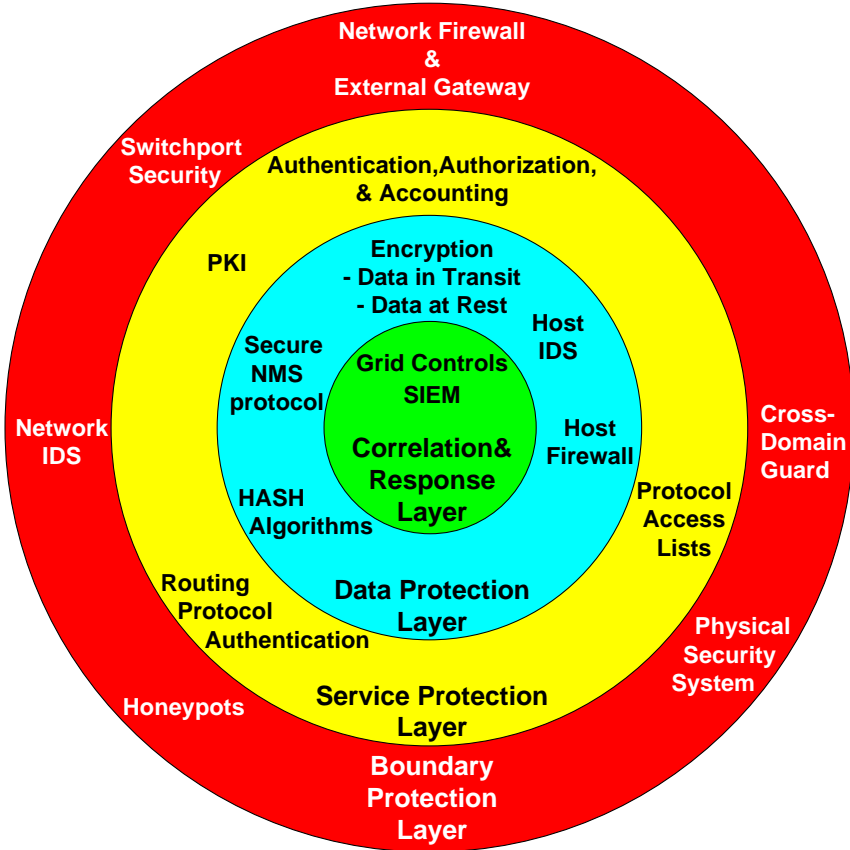


http://www.nerc.com/files/SGTF_Report_Final_posted.pdf

Risk Management Approach to Selecting Security Controls



Cyber Security Defense in Depth & Risk Management

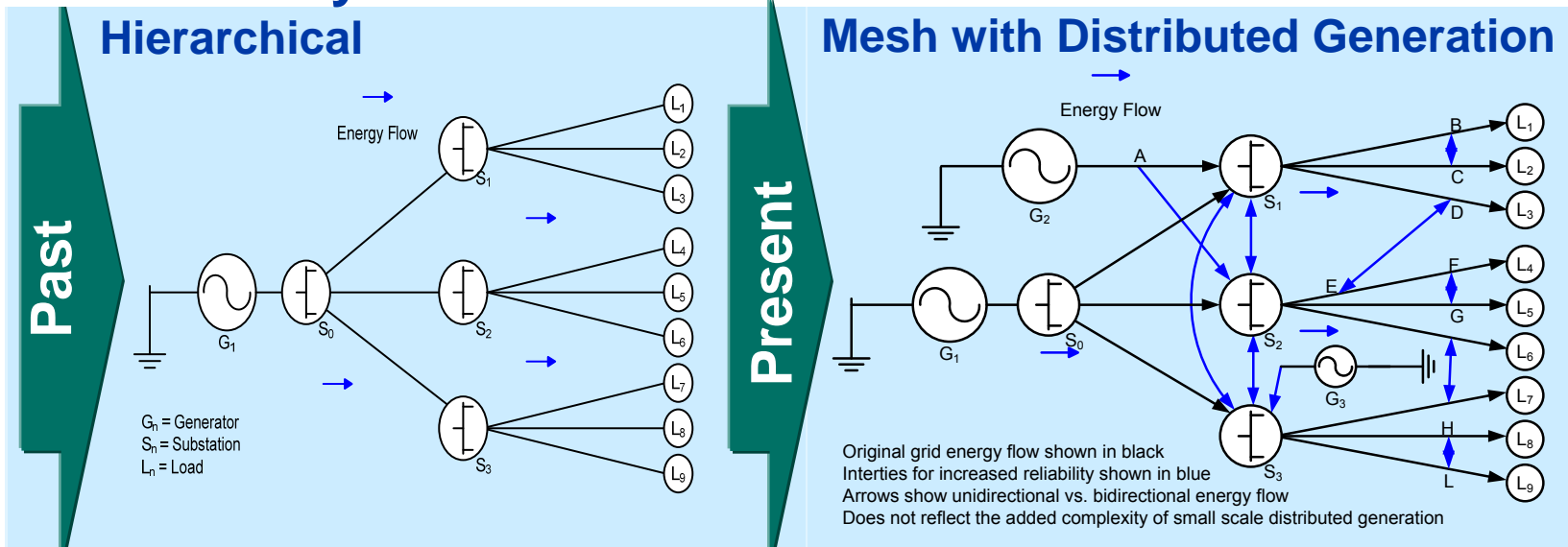


Power System Impact

Defense in Depth & Risk Management Assessment determine which controls are needed at each node or type of node

Q: Why have a distributed control architecture?

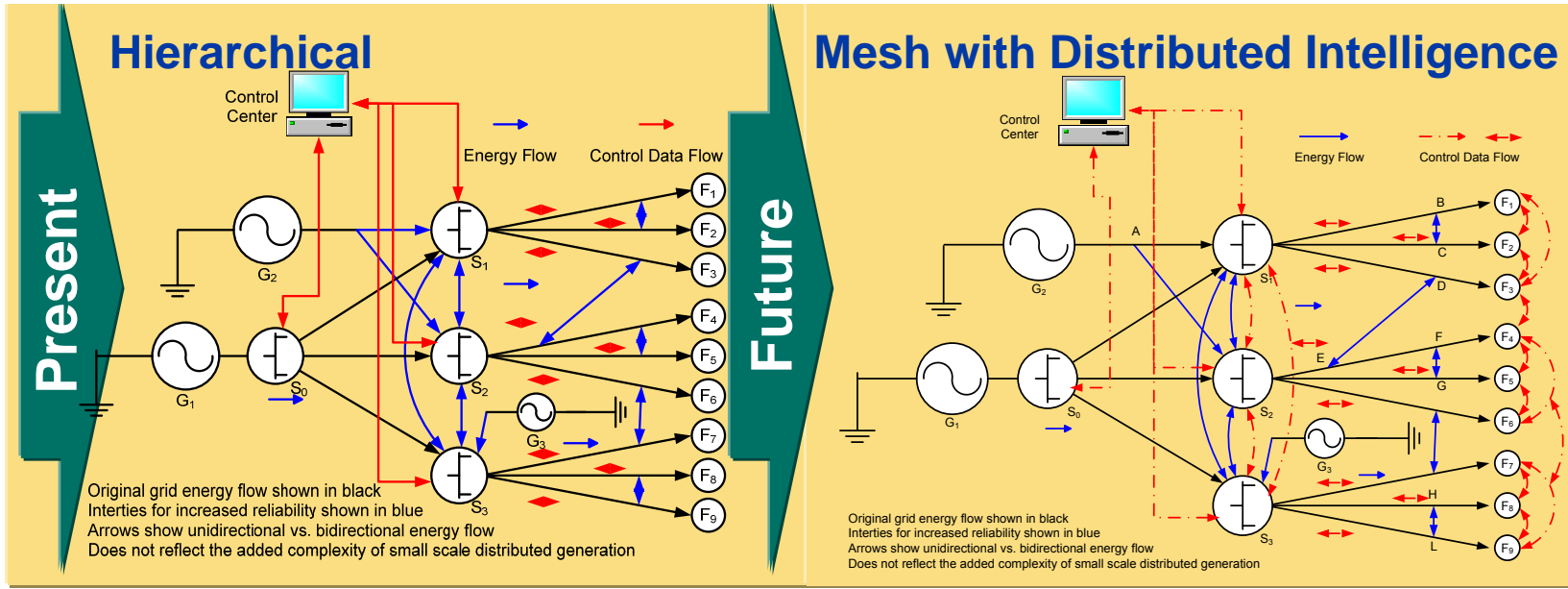
Energy Flow



Energy Distributed Network

A1: The Grid and Grid Control Architecture must match

Grid Control Flow



Control Distributed Network

A2: It reduces risk of the Control Room as a point of failure

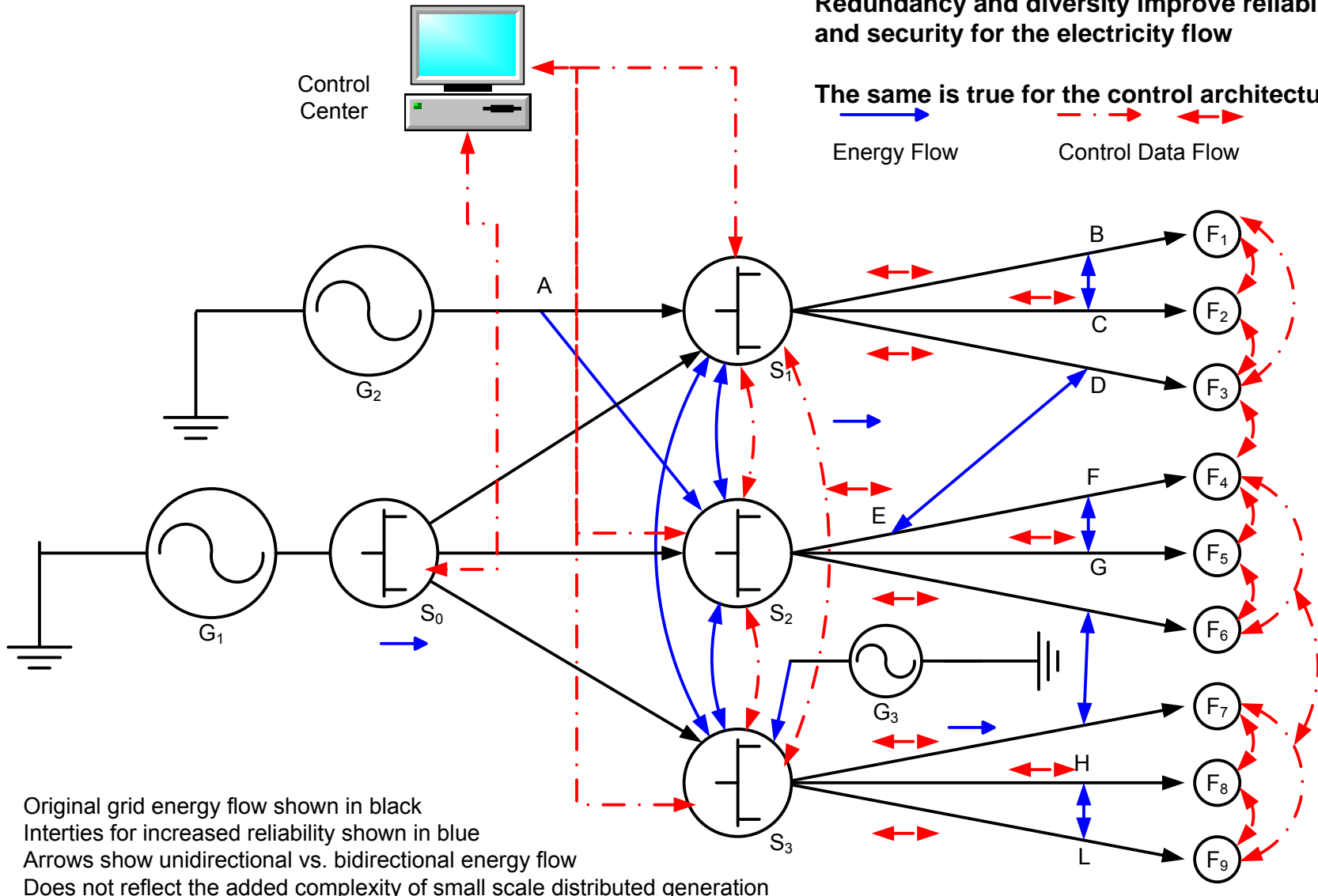
Distributed Energy → Distributed Control

Redundancy and diversity improve reliability and security for the electricity flow

The same is true for the control architecture

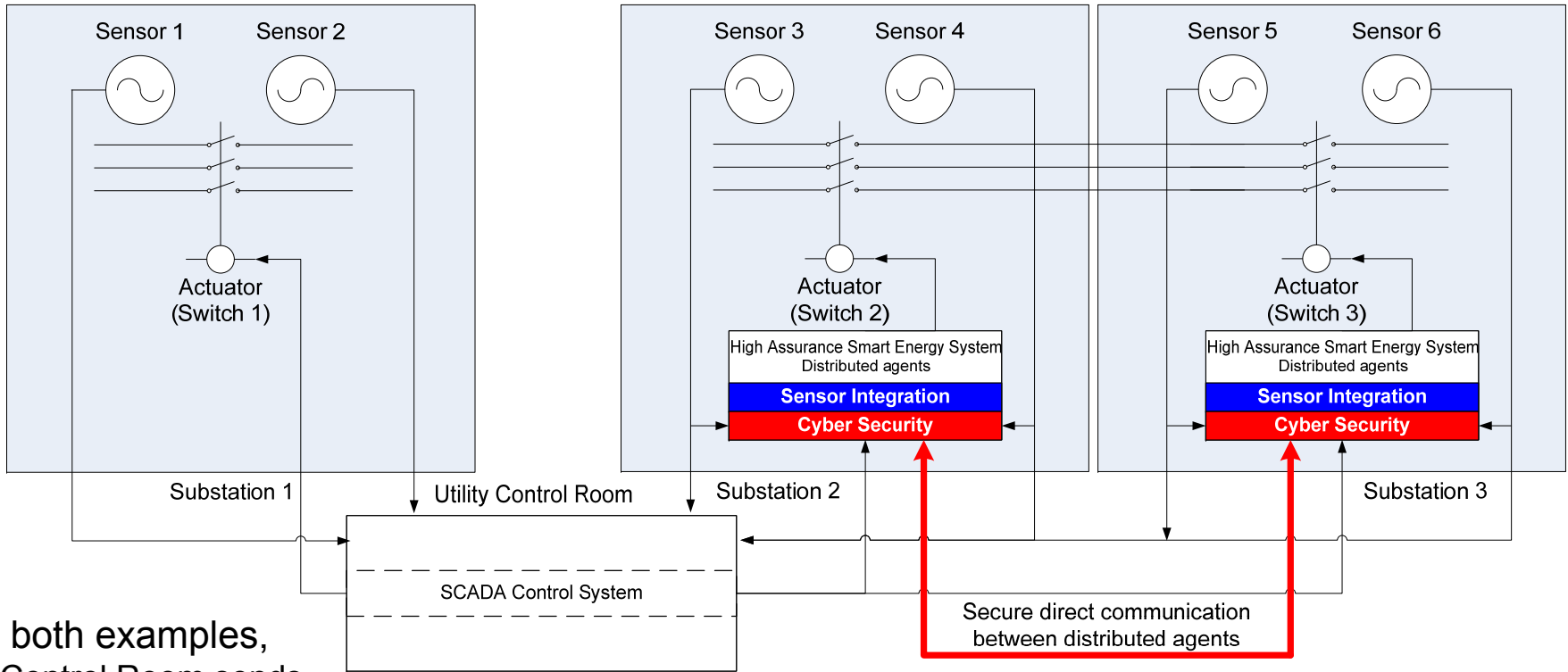
Energy Flow

Control Data Flow



Original grid energy flow shown in black
 Interties for increased reliability shown in blue
 Arrows show unidirectional vs. bidirectional energy flow
 Does not reflect the added complexity of small scale distributed generation

High Assurance Smart Grid Substation Example



In both examples,

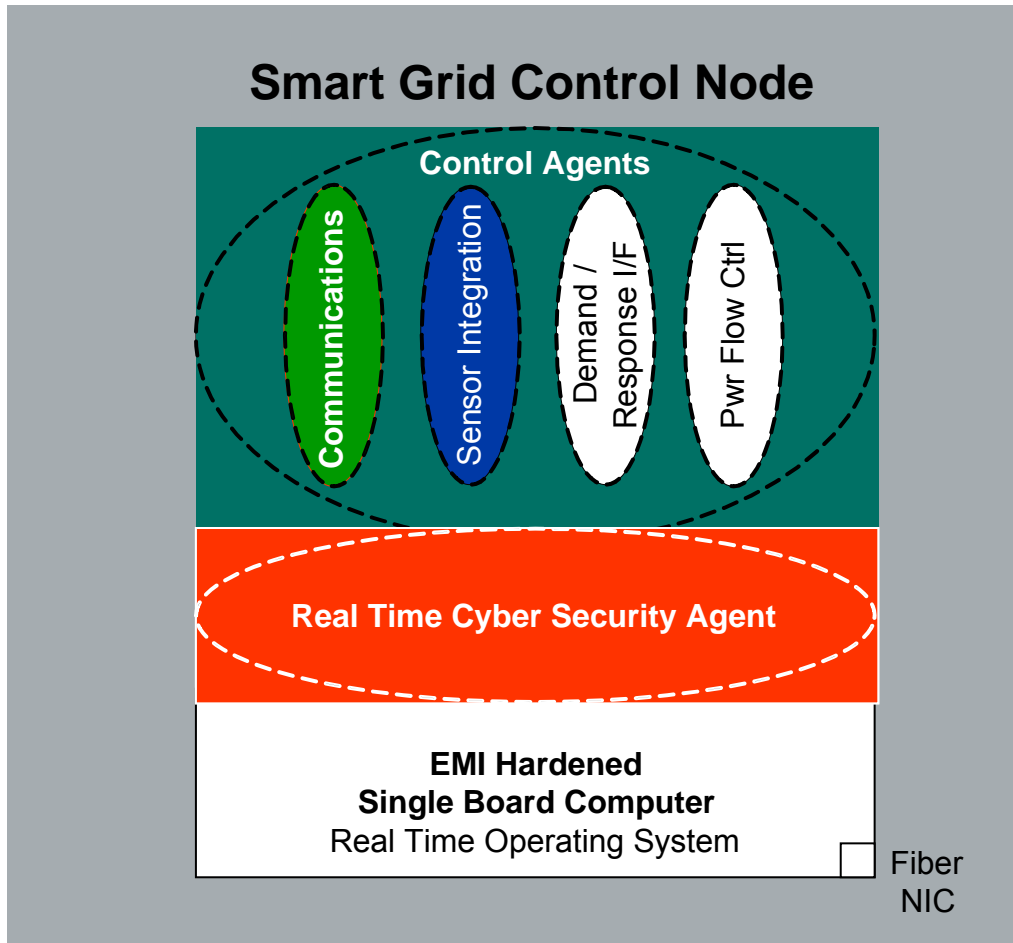
- Control Room sends command to close
- Grid segments are out of phase, which will cause damage if actuator closes

In Substation 1, Actuator 1 trusts the command, activates, resulting in damage

In Substation 2, Actuator 2 receives a command to close, **directly validates of local sensor status and Substation 3 status**, and refuses the command

High Assurance Smart Grid comes only from integrating Cyber Security, Physical Security, and Distributed Energy Management

Strong Distributed Cyber Security Enables Trusted Distributed Intelligence for Energy Control



- Not just “Distributed Agents” but Distributed Intelligence
 - Many Agents are just “Rules-Based”
 - Autonomy requires Distributed Intelligence
- Software Control Agents for:
 - Grid Management
 - Cyber Security
 - Physical Security

Distributed Control Agents assure no action is taken based on a single input HASG leverages distributed cyber agents developed for DOD

Why have Load Control?

- Because Loads are not smart enough to manage themselves

Potential Solutions

- Increase automation and security to achieve load device control over individual devices or groups of devices
- Increase the ability of loads to manage themselves in response to grid conditions

An Ethernet Comparison to the Electricity Network

Shared Attributes

- Shared media: many nodes, one set of ‘network’ wires per ‘subnet’
- Congestion: overloading impacts quality of service
- Non-Deterministic: highly reliable when “over-engineered”, but no guarantee of service
- Peak loads: impacted by predictable but random patterns (predictable random distributions)

Non-shared Attribute

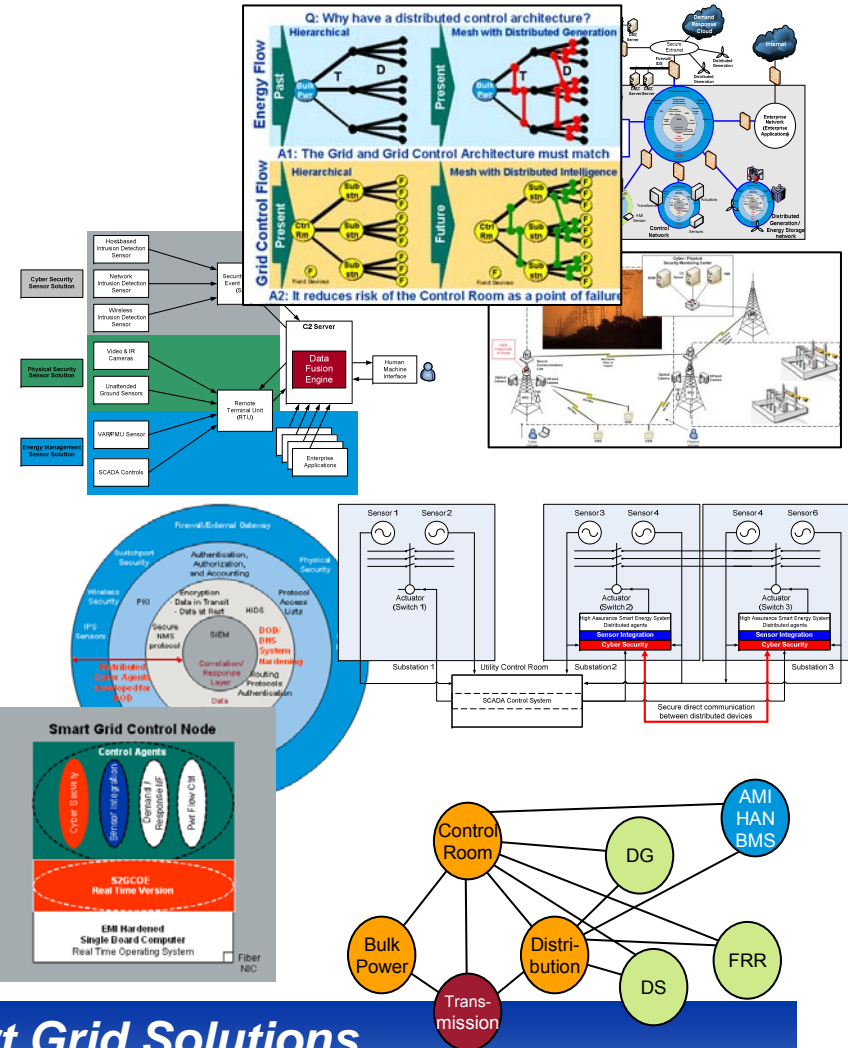
- Ethernet has *randomness* built into controls to increase reliability of data throughput

Auto-Responsive (AR) Load Control

- PNNL Study – load senses grid frequency
 - Reduce Load when frequency is below 59.95Hz (for example)
 - **HOWEVER, use a random function (say, 5-20 minutes) for when to resume load**
 - Avoids creating rapid grid load oscillations
 - Same concept (but different time constraints) as Ethernet Collision Detection & Retry Timing
 - Provides a gradual increase in load after underspeed
 - Increase load when frequency is above 60.05Hz (for example)
 - And drop load immediately when frequency goes back below 60.05Hz
 - Provides a clipping function for overspeed
- AMI Meter Connect/Disconnect Functions
 - Function is service connect/disconnect, not life safety of workforce
 - Use a random function (say, 5-20 minutes, rectangular distribution) for when meter responds
 - Avoids potential for rapid shocks to system if AMI control network is compromised
- Overall, avoids complexity of having to build an expanded control network with hundreds of millions of control nodes on a national basis

High Assurance Smart Grid Attributes

- Integrated Energy Management, Cyber Security and Physical Security with Defense in Depth
 - Including strong Role Based Access Control (RBAC) **for people and devices**
- Secure distributed architecture enables autonomy and eliminates single point of failure
- Assume compromise in the system (through accident, malice or system failure) **and engineer energy control systems accordingly**
- Auto-Responsive (AR) Loads
 - if you can't remotely control it, the remote control can't be compromised



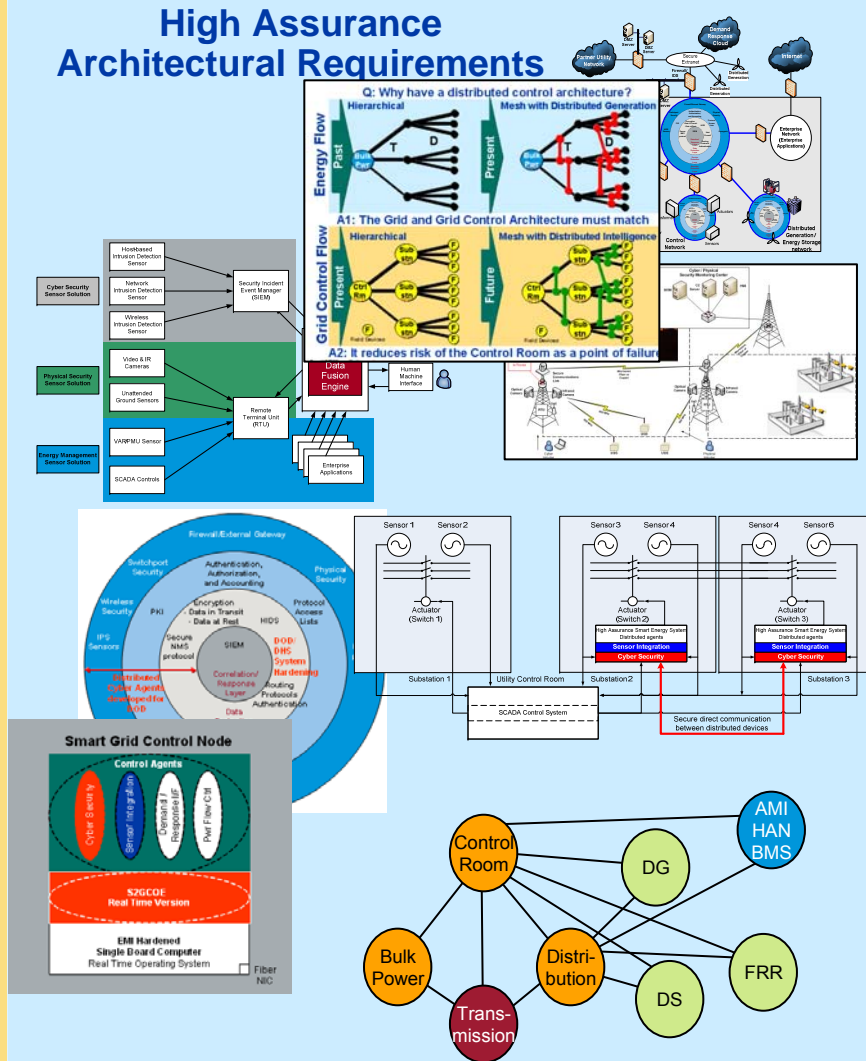
**High Assurance Smart Grid Solutions
utilizing the best attributes from multiple disciplines**

The Solution – A System Design Approach

IT Lessons Learned

- Apply appropriate security to remote access
- Critical patch installation needs to drive trusted agent status
- Data/command integrity
- Defense-in-depth strategies, Firewalls & IDS
- Delete user accounts after terminations
- Don't perform database updates on live systems
- Don't use administrative controls to solve system anomalies
- Identify controls to critical assets
- Integrated physical security
- Investigate anomalous system behavior
- Role based access
- Secure remote (trusted) access channels
- Trusted agents
- Use secure radio transmissions

High Assurance Architectural Requirements



Smart Grid Cyber Security is more than just applying IT security to grid control links – It is a total System design approach

The Integrated Solution for a High Assurance Smart Grid: Energy Management, Cyber Security and Physical Security

1. Engineer energy control systems using High Assurance principles
 - From utility, aviation, space and government systems
2. Defense in depth
 - Best attributes of cyber security in a layered approach
3. Risk management approach to selecting cyber security controls
 - Select from Defense in Depth controls based on Risk Assessment
4. Distributed intelligence
 - For Cyber Security, Physical Security and Grid Management
5. Increase use of Auto-Responsive (AR) load management
 - Enhance grid stability without expansive Command & Control systems
 - If you can't remotely control it, the remote control can't be compromised

***High Assurance Smart Grid Solutions –
An integrated approach across multiple disciplines***

