

Beyond SCADA: Networked Embedded Control for Cyber Physical Systems

Energy System Cyber-Security

Tim Johnson**

Mike Hartman**

Ken Caird*

Ron Larson*

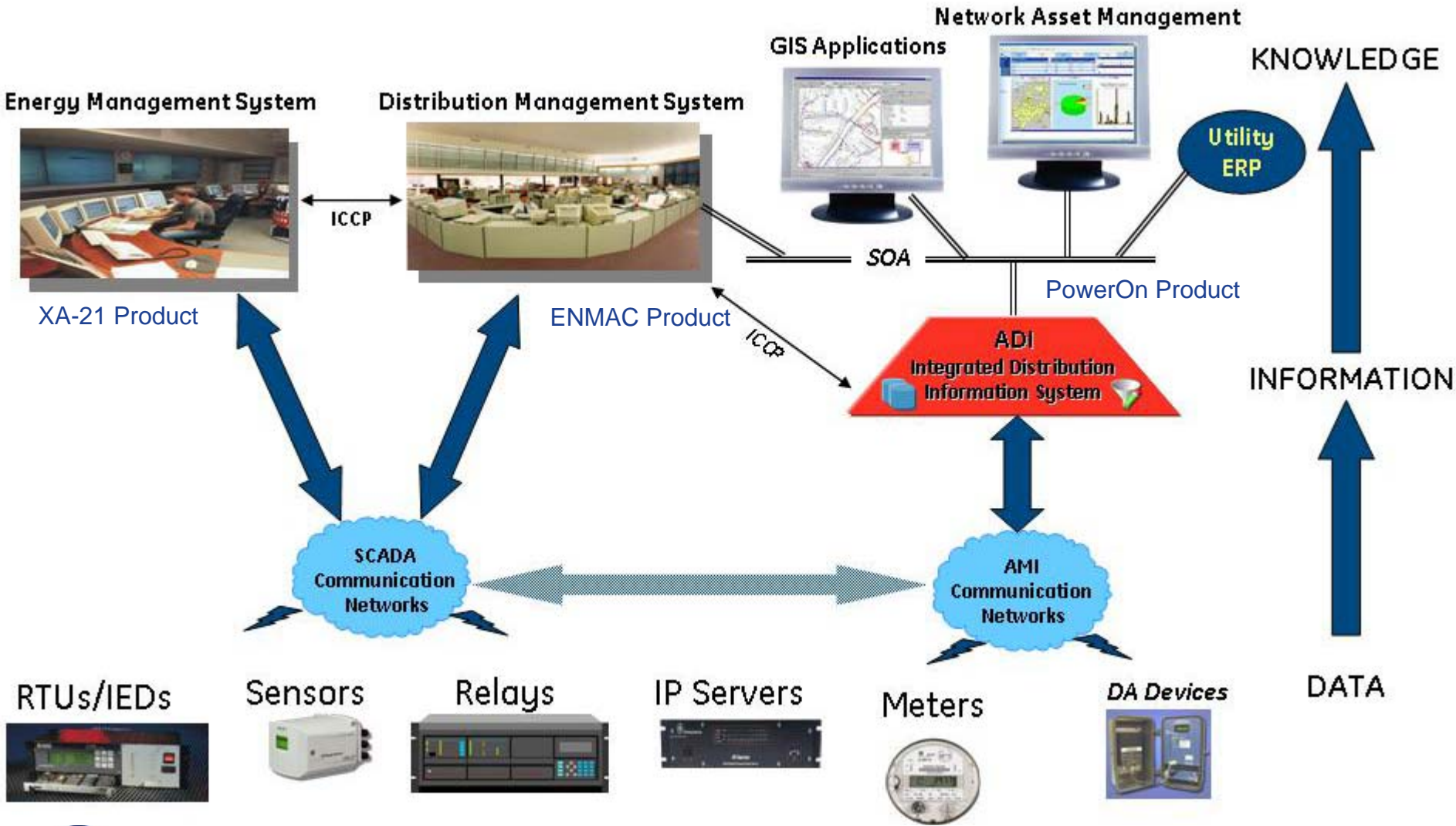
**GE Energy – Network Reliability Products & Services*
& GE Global Research****



imagination at work

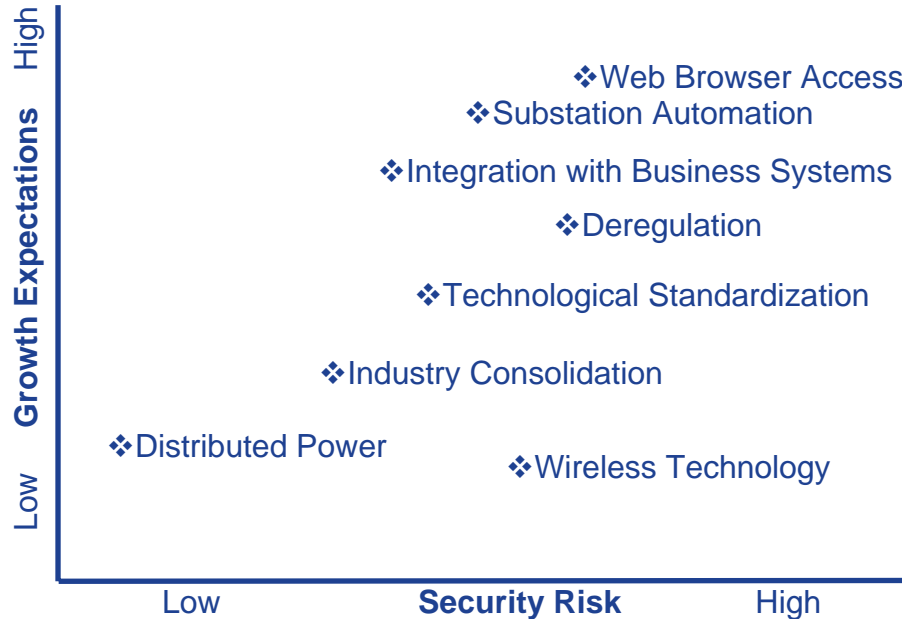


GE Energy Network Reliability Products & Services – Turning data into knowledge



Technology Trends will Increase Security Risks

Growth/Risk Matrix



Decentralization Increases Likelihood Of Security "Holes"

Trends	Security Concerns
Deregulation – Will Require Utilities To Have Better Control of Their T&D Systems; Reintegration Of Separated Functional Components Of The Power Industry	Complex IT Integration With Foreign SCADA Systems May Create Holes for Hackers to Penetrate
Industry Consolidation	Increased Size of SCADA Systems With Diverse Internal Systems Difficult to Secure
Technological Standardization – XML Platforms Facilitate Integration of SCADA Systems; More Scalable	Standard Software Is Easier For Hackers To Break Into
Increasing Substation Automation – Increased Complexity	Expensive to Secure Complex IT Systems
Distributed Power – Increasing Off-site Generation	Remote, Distributed Systems More Difficult to Secure
Integration With Business Systems	More Entry Points For Hackers; "Insider" Threat
Wireless Technology	Difficult To Secure
Energy Trading - Increased Operational Data Necessary	More Access Points; More Complexity

Rank 1: Costs and other barriers to innovation

Challenges

- ***Security Costs*** are a concern to Utility Customers, and greatly impede the rate of adoption of improved technology. What parts of costs will be recoverable?
- Large installed base of *legacy* equipment with non-secure protocols.
- Identify compensating advantages – such as reducing operations and/or servicing costs
- ***Clear standards for conformance and interoperability*** are needed

Technology research needs

- Inexpensive upgrade of hardware and software for existing unsecured legacy power and communications equipment
- Invention of low-cost, effective means of detecting cyber-physical threats or intrusions through newer equipment.
- **Focus on innovations with high benefit/cost opportunities first**

Other Priorities, Challenges,

Rank 2: Systems Issues

- **Challenges** - monitoring systems showing wide area alarm patterns that are difficult to detect
- **Technology Needs** - Active intrusion detection based on joint cyber-physical threats

Rank 3: Software Platforms

- **Challenges** – Secure operations through transitions in heterogeneous systems
- **Technology Needs** – re-usable and trusted software, capable of a layered defense to cyber-threats

Rank 4: Emergent Behaviors

- **Challenges** – System simulation and human interface tools for understanding the global state of the system (including wireless portions) and estimating its future evolution
- **Technology Needs** – Can the decentralized nature of many emergent systems be effective as an active defense mechanism for cyber attack?

Six businesses, each aligned for growth...with

Quality and Cyber-Security!



Infrastructure



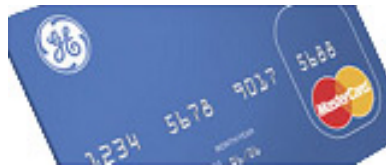
Industrial



Healthcare



Commercial Finance



Consumer Finance



NBC Universal

- Customer security
- Enterprise security
- Infrastructure security
- Asset & facility security
- Network and Information security
- Global remote service security