



## Smart Grid Security

Nadya Bartol, CISSP, CGEIT  
Vice President of Industry Affairs  
and Cybersecurity Strategist  
[Nadya.bartol@utc.org](mailto:Nadya.bartol@utc.org)

# What is Smart Grid?

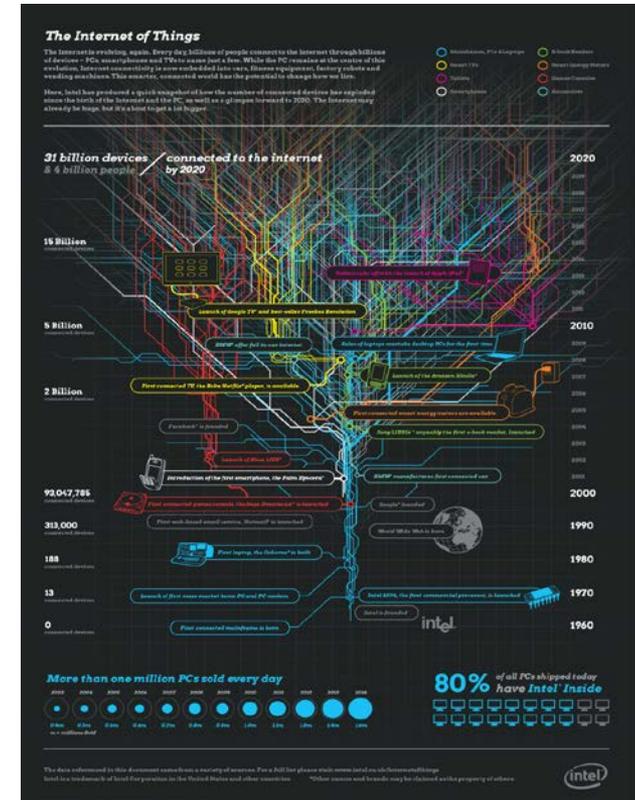
---

- A **smart grid** is a modernized electrical grid that uses analog<sup>[1]</sup> or digital information and communications technology to gather and act on information, such as information about the behaviors of suppliers and consumers, in an automated fashion to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity

# Why is smart grid important?

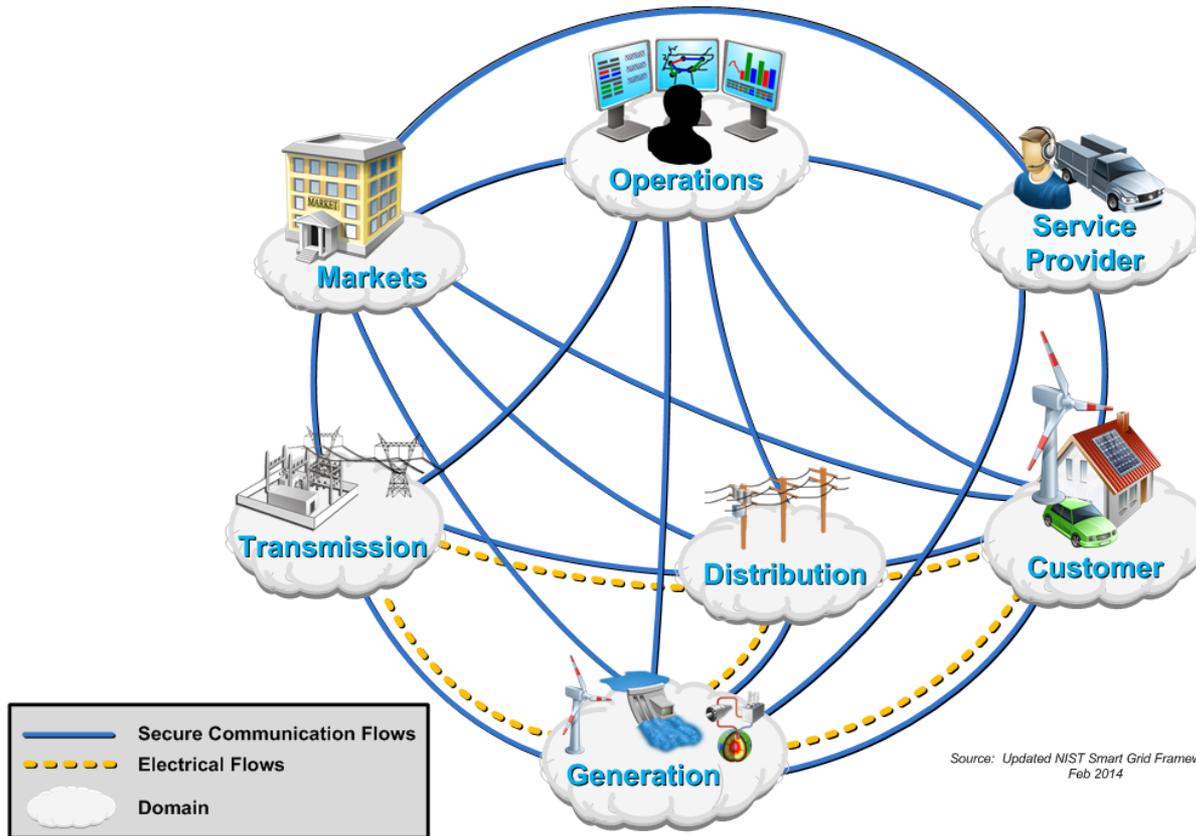
## Devices connected to the Web:

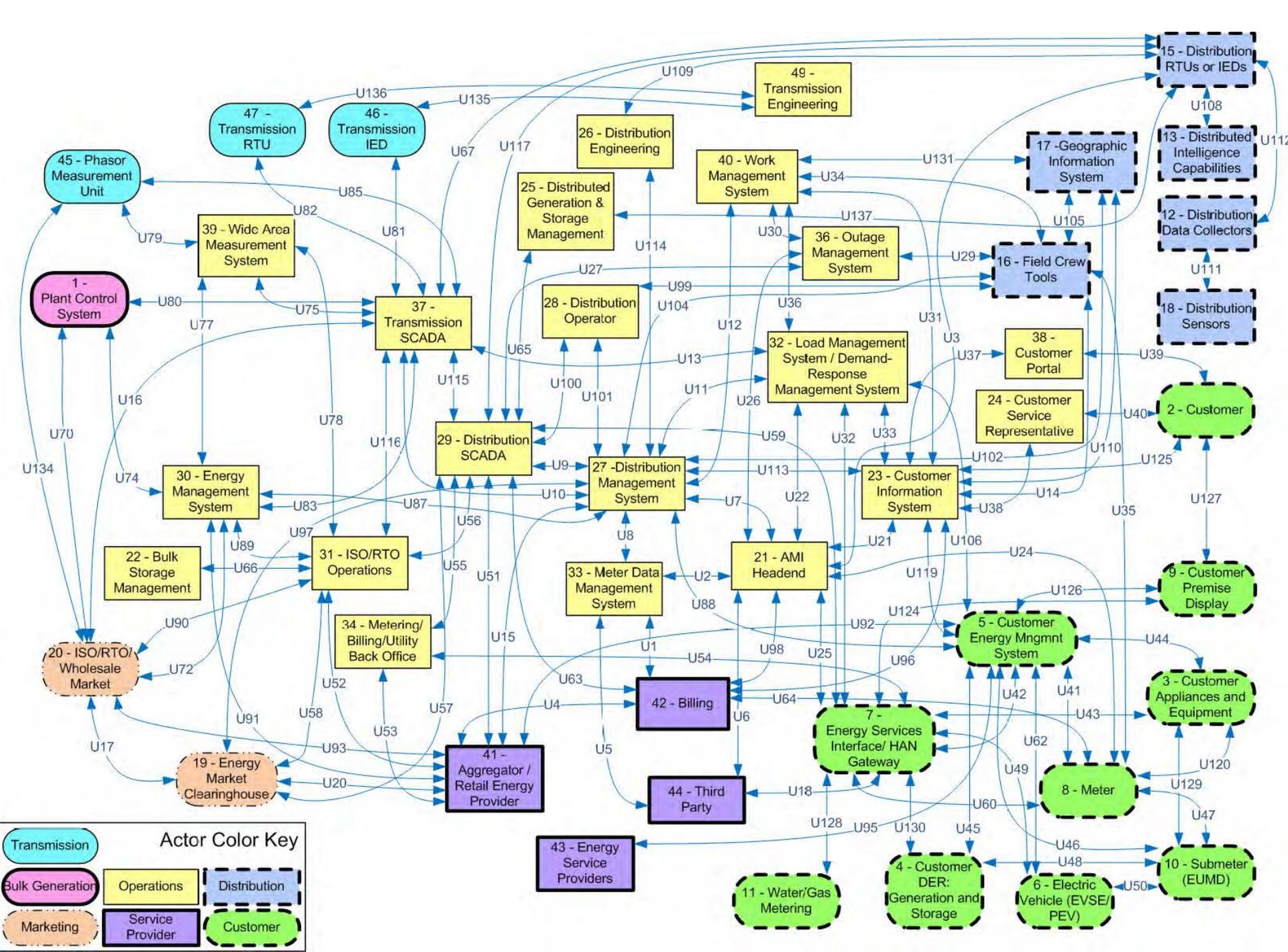
- 1970 = 13
- 1980 = 188
- 1990 = 313,000
- 2000 = 93,000,000
- 2010 = 5,000,000,000
- 2020 = 31,000,000,000



Source: Intel

## Conceptual Model





# Smart Grid Cybersecurity is influenced by a rich environment

## Governance

Executive Order 13636  
 European Network and Information Security Directive  
 Canada Cybersecurity Strategy

## Regulatory

FERC  
 European Commission  
 State PUCs  
 NARUC  
 NRC



NERC

## Public/Private

DHS, DOE, ISACs  
 60+ working groups in North America

## Standards and Guidelines

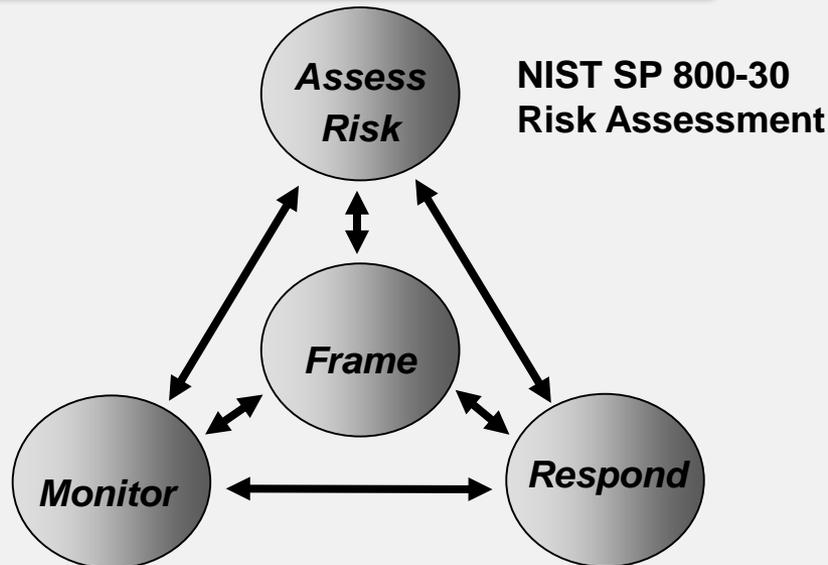
IEC  
 ISO  
 ISA99

NIST  
 ENISA  
 SGIP



## NIST SP 800-39 Information Security Risk Management

PROCESS



NIST SP 800-137  
Continuous  
Monitoring

NIST SP 800-53  
Security Controls  
NIST SP 800-53A  
Security Controls  
Assessment

IMPLEMENTATION

- NIST SP 800-55 – Security Measurement
- NIST SP 800-57 – Key Management
- NIST SP 800-61 – Incident Handling
- NIST SP 800-161 – Supply Chain Risk Management
- NIST SP 800-64 – Security Lifecycle
- **NISTIR 7628 – Smart Grid Security**
- **NIST SP 800-82 – Industrial Control Systems Security**

# ISO/IEC Information Security Management System (ISMS) Family of Standards

Terminology

ISO/IEC 27000 – Overview and Vocabulary

Requirements

ISO/IEC 27001 –  
ISMS Requirements

ISO/IEC 27006 –  
Audit & Certification Requirements

Guidelines

ISO/IEC 27002 –  
Code of Practice

ISO/IEC 27003 –  
ISMS Guidelines

ISO/IEC 27007 –  
Audit  
Guidelines

ISO/IEC 27008 –  
Guidance for auditors  
on ISMS controls

ISO/IEC 27004 –  
Measurement

ISO/IEC 27005 –  
Risk Management

ISO/IEC 27009 – Use of ISO/IEC 27001  
for sector/service-specific Third-  
Party accredited certifications

ISO/IEC 270XX –  
Sector-Specific  
Guidelines

★ ISO/IEC 27019 - Information security  
management guidelines based on ISO/IEC  
27002 for process control systems specific  
to the energy utility industry

## Security Engineering

ISO/IEC 15408 -  
Common Criteria

ISO/IEC 20004-Secure  
software development  
and evaluation under  
ISO/IEC 15408 and  
ISO/IEC 18405

## Implementation

ISO/IEC 27036-  
Supplier  
Relationships

ISO/IEC 27034-  
Application Security

## Identity Management and Privacy Technologies

ISO/IEC 27018-  
Code of practice for PII protection in  
public clouds acting as PII processors

# ISA-62443/IEC 62443 Series

**General**

 <p>ISA-62443-1-1</p> <p>Terminology, concepts and models</p>	 <p>ISA-TR62443-1-2</p> <p>Master glossary of terms and abbreviations</p>	 <p>ISA-62443-1-3</p> <p>System security compliance metrics</p>	 <p>ISA-TR62443-1-4</p> <p>IACS security lifecycle and use-case</p>
--	--	--	--

*Published as ISA-99.00.01-2007*

**Policies & procedures**

 <p>ISA-62443-2-1</p> <p>Requirements for an IACS security management system</p>	 <p>ISA-TR62443-2-2</p> <p>Implementation guidance for an IACS security management system</p>	 <p>ISA-TR62443-2-3</p> <p>Patch management in the IACS environment</p>	 <p>ISA-62443-2-4</p> <p>Installation and maintenance requirements for IACS suppliers</p>
---	--	--	--

*Published as ISA-99.02.01-2009*

**System**

 <p>ISA-TR62443-3-1</p> <p>Security technologies for IACS</p>	 <p>ISA-62443-3-2</p> <p>Security levels for zones and conduits</p>	 <p>ISA-62443-3-3</p> <p>System security requirements and security levels</p>
--	--	--

*Published as ISA-TR99.00.01-2007*

**Component**

 <p>ISA-62443-4-1</p> <p>Product development requirements</p>	 <p>ISA-62443-4-2</p> <p>Technical security requirements for IACS components</p>
--	---

 Published	 In development	 Removed / Canceled
 Published (under review)	 Out for comment/vote	 Planned

# What do utilities say they need?

---

- Utilities-focused cybersecurity workforce
- Secure Vendor Products
- Cultural and Community Awareness
- Architecture, Infrastructure, and State of Practice Diversity
- Information Sharing

# Challenges moving forward

---

- Emerging threat
- Evolving regulation
- Qualified workforce
- IT/OT convergence
- Assurance practices

# Questions

