A smarter grid?
Keep it safe!

Miles Keogh & Michael Jung

USAID / USEA Webcast

June 18, 2020

Who are these guys?

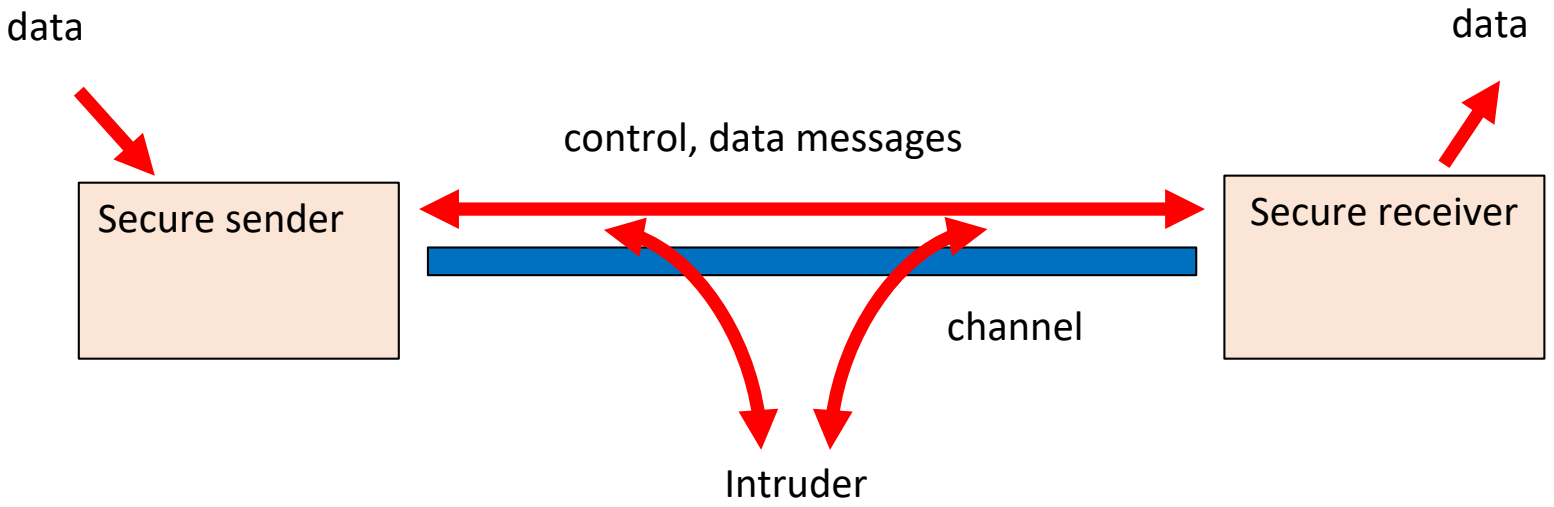
Purpose and Objective of Our Conversation

- We'll explore:
  - The grid: yesterday, today, and your choices for tomorrow
  - Unique risks from grid intelligence
  - What kinds of tools help you manage those risks

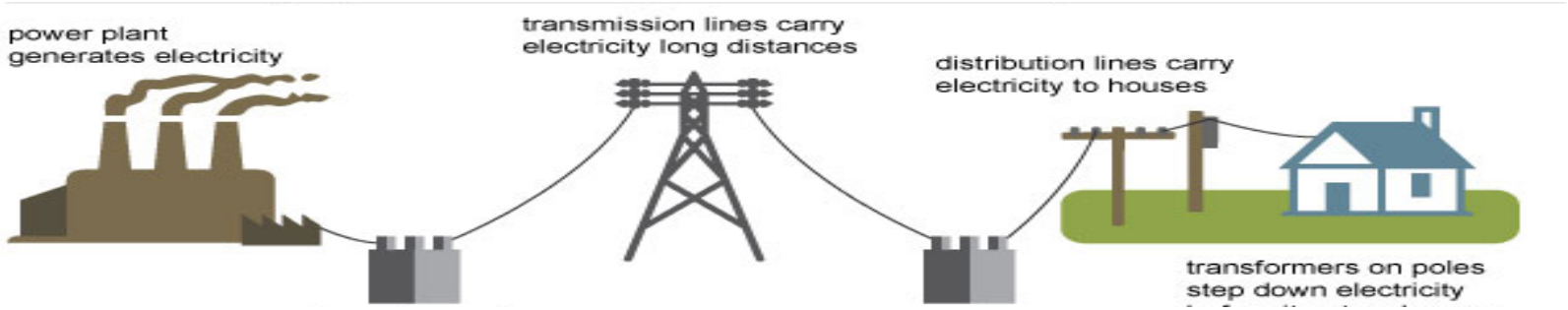
Today’s Grid / A Smarter Grid

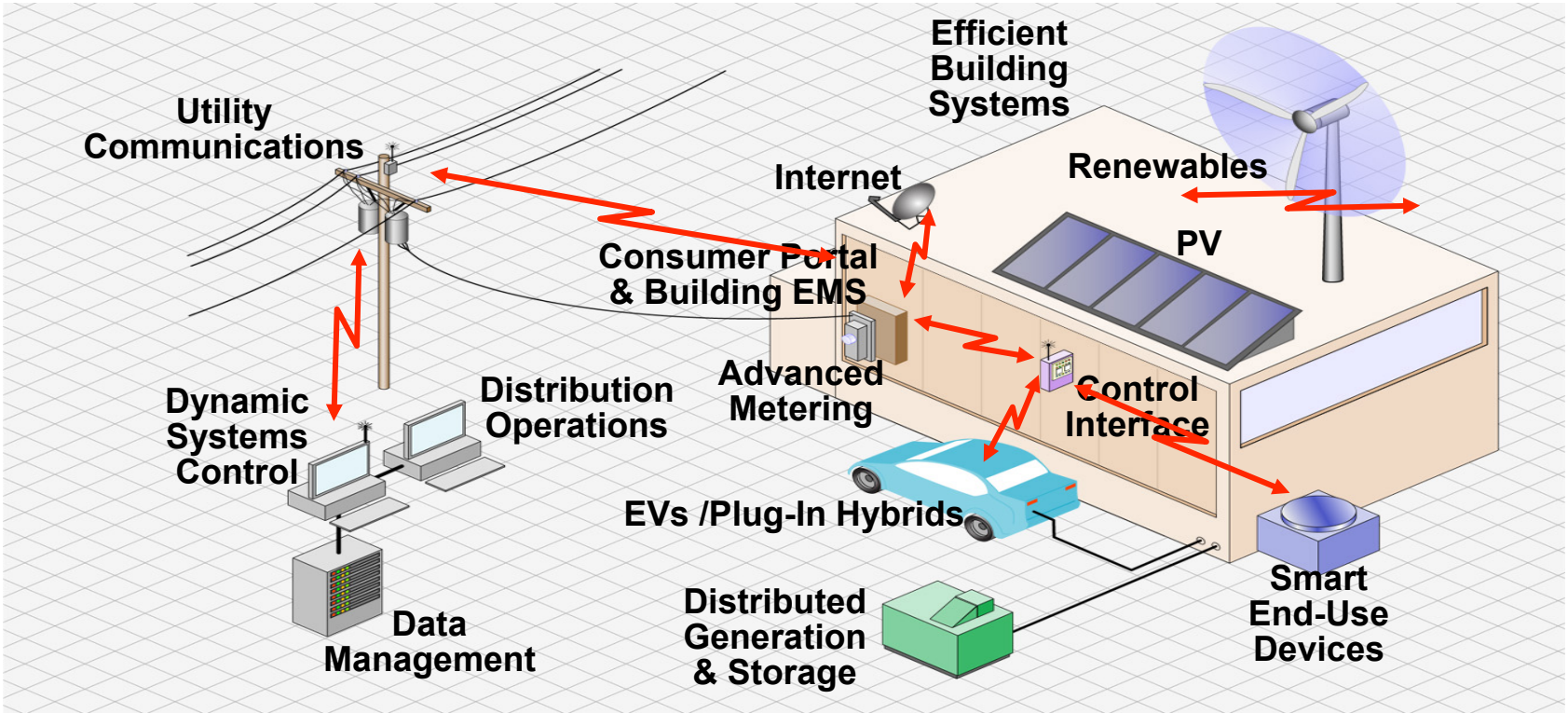
"Cyber" just means "Connected"

- "Cyber" connectivity occurs when devices generate, transmit, and receive data.
- Data becomes intelligence when someone or something takes action based on that data.



Yesterday / Tomorrow





How has digitalization affected other sectors?

- Banking
- Entertainment

- Telecom
- Airlines

What values does digitalization serve?

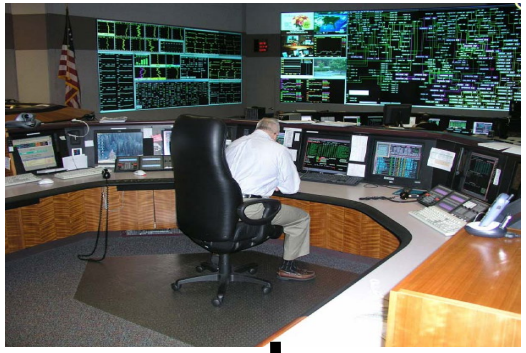
- Before:
  - Reliability... for an analog economy
  - Affordability... for growing consumption
  - Dispatchable generation... for a top-down system

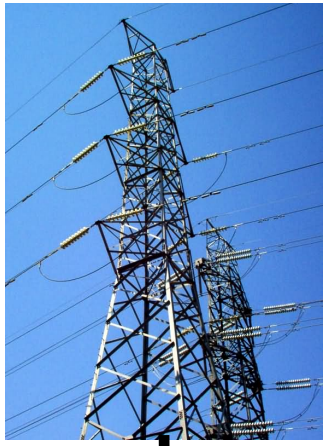
- After:
  - Energy independence by reducing reliance on imported energy resources
  - Sustainability to balance economy and environment
  - Operational efficiency and cost-effectiveness through system visualization
  - Reliability for a *digital* economy
  - Power quality for modern industries
  - Non-dispatchable energy resources
  - Demand response & storage
  - New opportunities and benefits for customers

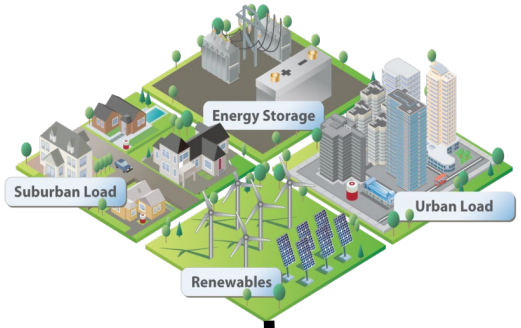
What makes grid security different?

Protect + **Protect** + **Protect** = **Protect**

Conventional IT Systems + **Control Systems** + **Electrical Infrastructure** = **“Smart Grid”**







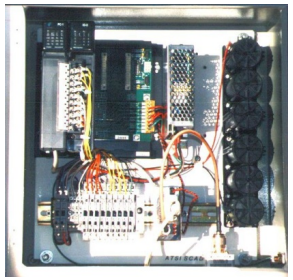
What is a control system?

Devices

Sensor

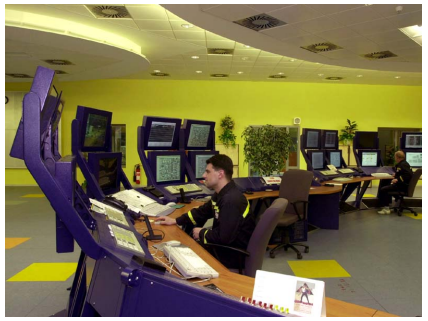
Control Valve

Controllers ("Tiny Brains")



Networks

Humans & Human-Machine Interfaces



Field Devices

Meters
Sensors
Motors
Pumps
Other Devices

Remote

Controller (e.g. Programmable Logic Controller, Remote Terminal Unit).

Comms

Wired
Wireless

Master

SCADA and Human-Machine Interface

FIELD DEVICES ⟷ **CONTROL CENTER**

Control systems Vs. IT systems

IT Security vs. Control System Security

	INFORMATION TECHNOLOGY	**CONTROL SYSTEMS**
Anti-virus/Mobile Code	Common/widely used	*Uncommon/impossible to deploy*
Support Technology Lifetime	3-5 years	*Up to 20 years*
Application of Patches	Regular/scheduled	*Slow (vendor specific)*
Time Critical Content	Generally delays accepted	*Critical due to safety*
Availability	Generally delays accepted	*24 x 7 x 365 x forever*
Physical Security	Secure	*Remote and unmanned*

Integrating Intelligence into Generation

- System visualization improves load following
- Better integrate market actions
- More accurate for market, reliability, and environmental performance
- Integrate variable resources
- Integrate demand response and load-side resources
- Generation may not remain centralized – may become more distributed
  - This may raise the need for a more intelligent system

Integrating Intelligence into Transmission

- System sensors improve system optimization, performance
  - “get more from the grid you have”
- Bigger balancing areas; better seams management
- Enables phasor measurement, synchronization, protective islanding, “self-healing”
- Reduces restart time
- Creates opportunities that enable markets

Making Distribution Intelligent

- Outage detection and management
- Energy theft
- Energy efficiency
- Peak reduction
- Distributed energy resource hosting capacity
- Electric vehicle integration
- Dynamic pricing
- Customer engagement

Adding Intelligence to Business Operations

- Online billing
- Customer management
- Reducing friction between G/T/D by creating opportunities for benefitting from cross-silo cooperation
  - Example: Using peak demand response (D) to reduce transmission capacity needs (T) and defer/avoid new power plant costs (G)

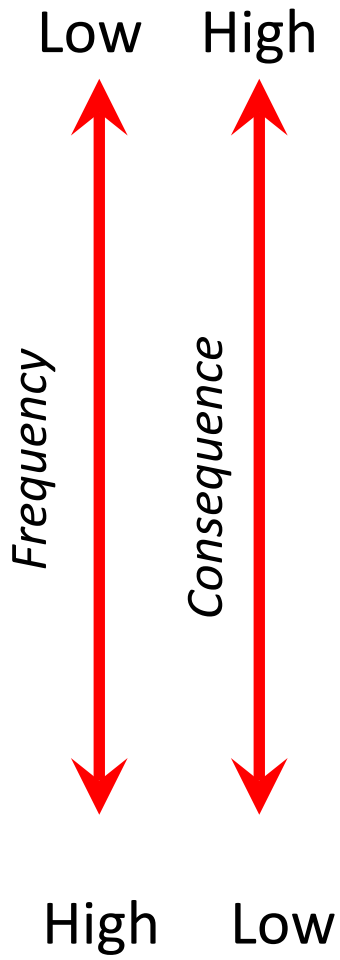
- We've known how to deal with these risks since the 70's
  - Techniques like blacklists/whitelists, antivirus, segmentation, access control

Adding Intelligence to End-Use

- A mix of control systems and information technology systems
- But customer experience is still mostly flipping a light switch
- Transactive energy
  - A: Using less/getting off the grid
  - B: Selling back to the grid
  - C: Dynamic pricing
  - A+B+C: Buying low and selling high

- EVs – reduce dependence on fossil fuel imports and improve human health through air quality improvement (e.g., blue skies during COVID)

Types Of Cyber Intrusions

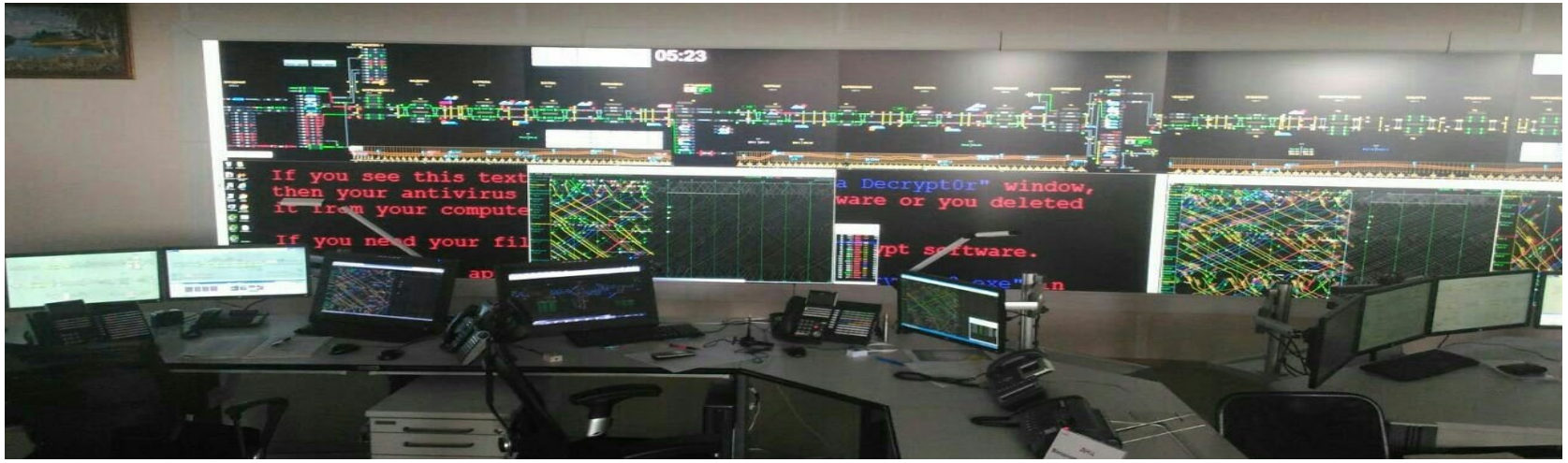


- *Overt attacks* – Objective: to disrupt, destroy, frighten. Terrorists, Nation States, Disgruntled current or former employees.
- *Gain System Control* – Remotely modify and operate the system as a vehicle for attack.
- *Extortion* – Criminal motivation to make money.
- *Theft* – Objective: make money and not be discovered (stealth). Organized crime, US, International and individuals.
- *Intrusion* – Unauthorized access to information and the potential to use information to do harm.

Simple attacks can still be devastating

- Easy to do / easy to defend against ----- > difficult to do / hard to defeat
- Most entry points are still the “click the link”, because it works
- Denial of service, “man in the middle”, encryption attacks, remote access attacks, data corruption attacks (SQL injection), “social engineering” – all old tricks, still most-often used

- Trojans, viruses, worms, root kits – all are “malware”
- Ransomware shows that nation-state capabilities get out for use by criminals in 2-3 years
- Visualization means an attack doesn’t need to affect operations, just what you think you see



Are the risks manageable? How?

- It works better if you manage risks from the start!
- Tools to manage risk:
  - Planning frameworks (e.g., NIST Cybersecurity Framework)
  - Risk assessment tools (e.g., ESC2M2)
  - Standards for compliance (e.g., NERC Cyber Standards)
  - Best practices (e.g., SCADA procurement standard language)

Questions To Guide Your Choices

- How will you manage Risk?
  - What risks would this investment decrease? What risks would increase? Are those risks manageable?

- What investments are worth the money?
  - P<D<A: cost of **Protection** should less than value of the **Data**, which should be less expensive than the price of a successful **Attack**
    - Protect paperclips like paperclips and diamonds like diamonds
  - Defense in depth / redundancy
- You're in the right place at the right time!

Any Questions?

Miles Keogh, Alexandria Virginia
Michael Jung, Portland Oregon

(contact Johanna Koolemans-Beynen,
jkoolemans-beynen@usea.org)