

The “Engineer’s” Perspective on Cybersecurity

nationalgrid

DIGITAL
SUBSTATION 

We bring
energy
to life

Mark Thompson

*Director – Digital Delivery –
Electric System Engineering*

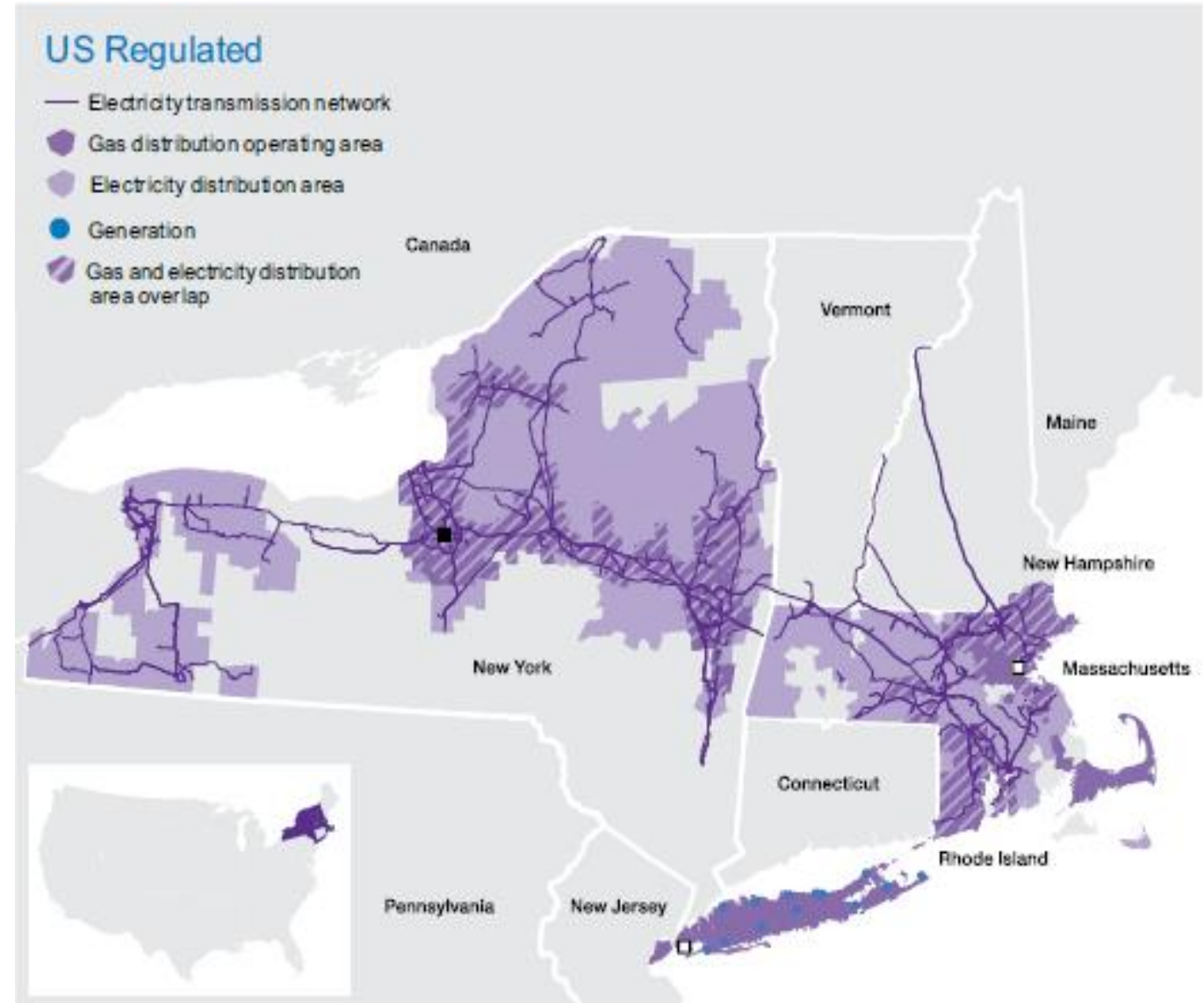
March 2021

National Grid in the US

In the US, National Grid is primarily a gas and electric utility, providing gas to over 3.5 million customers and electricity to over 3.4 million customers across Massachusetts, New York, and Rhode Island.

We operate the largest transmission network in the northeast US, including an interconnector providing Canadian hydro power to New England.

- ... based in the UK and northeastern US
- Approximately 19 million industrial, commercial and domestic customers
- Almost 28,000 employees
 - 63% work in the US; 37% work in the UK



Digital Substation Program @ National Grid



- ~150 sites in the next 10 years
- Technology: IEC 61850 & Online Monitoring
 - Enhanced use of intelligent microprocessor-based devices to optimize our systems
 - Network-connected operational technology
 - Enhanced data acquisition & remote access
- Embracing new ways of working
 - Upfront capital efficiencies
 - Operational/maintenance efficiencies
 - Enabling future innovation
- Data-driven investment & maintenance decisions




*National Grid is a leader in Digital Substations,
with a first-of-its-kind installation in North America*


OT Cybersecurity Challenges

 Views of explicitly those of an engineer – NOT a security expert 

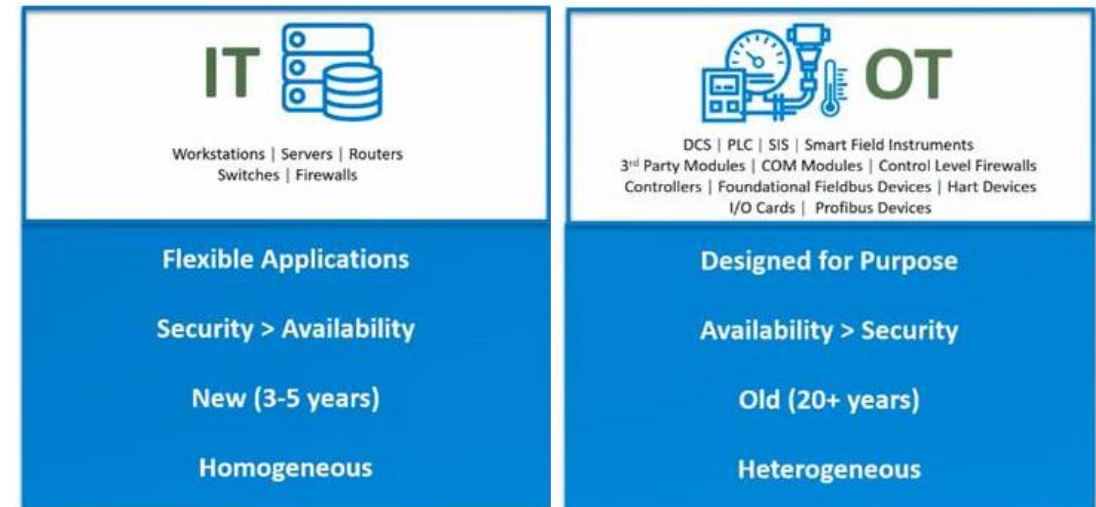
 Resource (Security Architect) availability and experience in OT systems

 Over-reliance on existing security baseline requires (BSR), which were designed for enterprise solutions

 Disparate project processes, systems, and tools between the business (delivering capital projects) and IT/Security (delivering new solutions)



 Security Testing: Pen tests which rely on consultants to scope/execute and not testing the operational impacts of events

Differing Missions



* Graphic was borrowed from unknown presentation*

OT Cybersecurity – Key to Success

 Views of explicitly those of an engineer – NOT a security expert 

True collaboration between Security & Business

Forcing Discussions

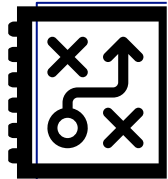
Stepping up to Support

Don't know what we don't know

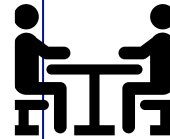
Stress test systems & designs

Engineering can help develop documentation for projects

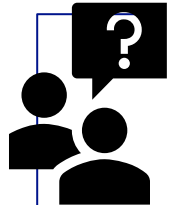
Security needs to be flexible



IT/Security Scope Document – Drafted by a PM based on the IT/Security design to document scope/schedule/budget during preliminary engineering



OT/Security Playbook – Aligned expectations “Rosetta stone” based on OT equipment type & connectivity (e.g. protection relay vs. Windows-based VM in substation)



Asking why 3 times if something doesn't seem right. Examples of security testing results that were successfully questioned by the business: CA SSL certs required for intra-substation comm and the use of unsecured protocols on OT devices

nationalgrid

