NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Integration

Integrating Security with Engineering Practices

Ryan D. Quint, PhD, PE
Director, Engineering and Security Integration
North American Electric Reliability Corporation
U.N. 19th Session of Group of Experts on Cleaner Electricity Systems
October 2023

RELIABILITY | RESILIENCE | SECURITY




NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

What is Security Integration?

Security Integration: *The integration of cyber and physical security aspects into conventional planning, design, and operations engineering practices.*

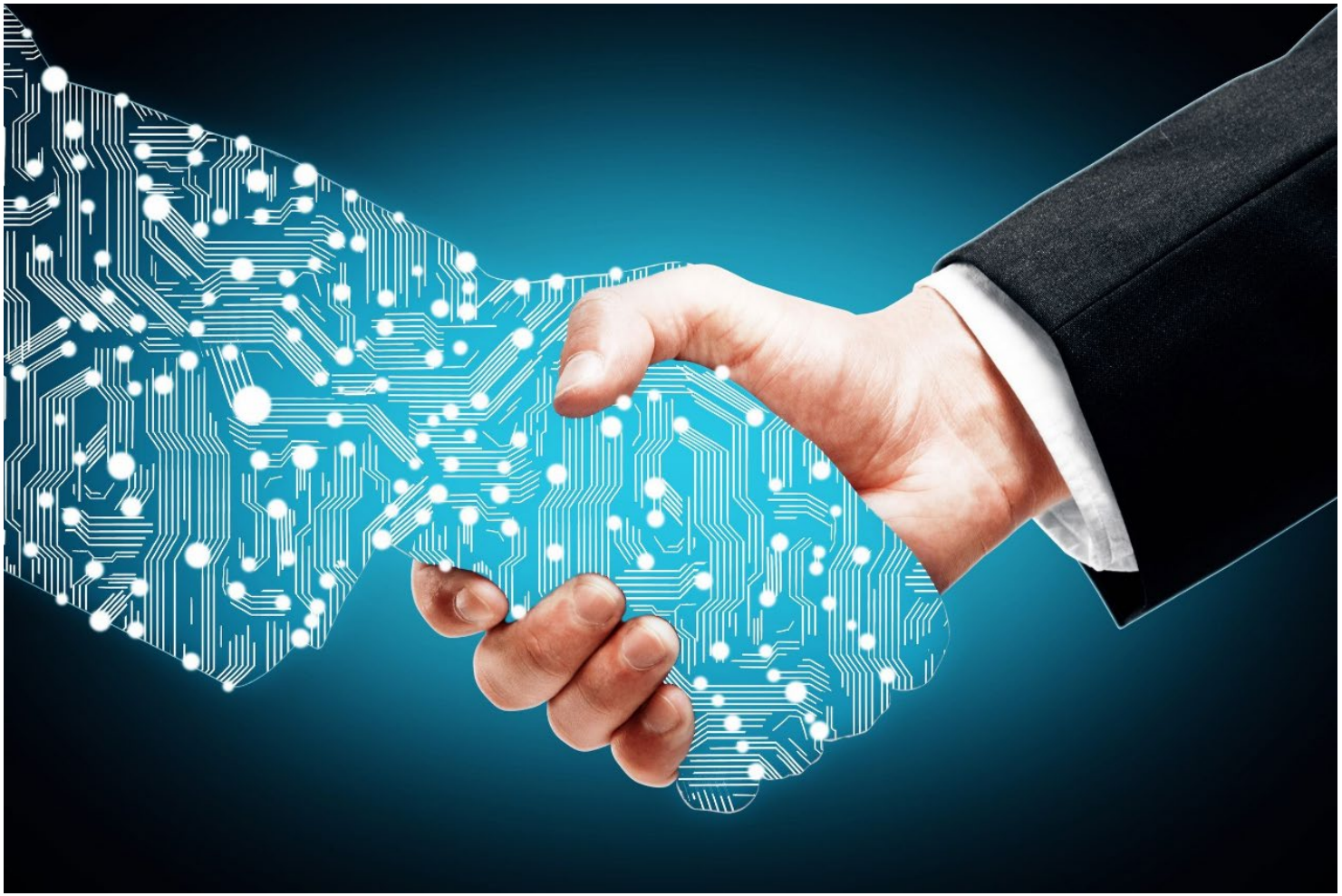
- Can we *plan* a grid more resilient to cyber and physical attack?
- Can we *design* a grid with security as a critical consideration up front rather than at the end?
- Can we *operate* the grid in a way that can easily identify, detect, and respond to security incidents?
- Can we *restore* the grid effectively following any compromise?
- No more “bolt on” security measures – integrate them up front

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Historically…

[Source: National Review]

Today…



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC Security Integration Strategy

Cyber-Informed Transmission Planning

- Cyber Contingency Mapping
- Cyber Informed Studies and Modeling
- Coordinating Risk Mitigation
- Adequate Level of Reliability and Security

Security Integrated Design and Operations

- Cyber Security Investments
- Technological Challenge Assessments
- Defense in Depth
- Securing Blackstart Plans

Grid Transformation

- Assessments of Aggregate Risks
- DER and DER Aggregator Cybersecurity
- Securing the Changing Resource Mix
- Infrastructure Interdependence and Fuel Supply

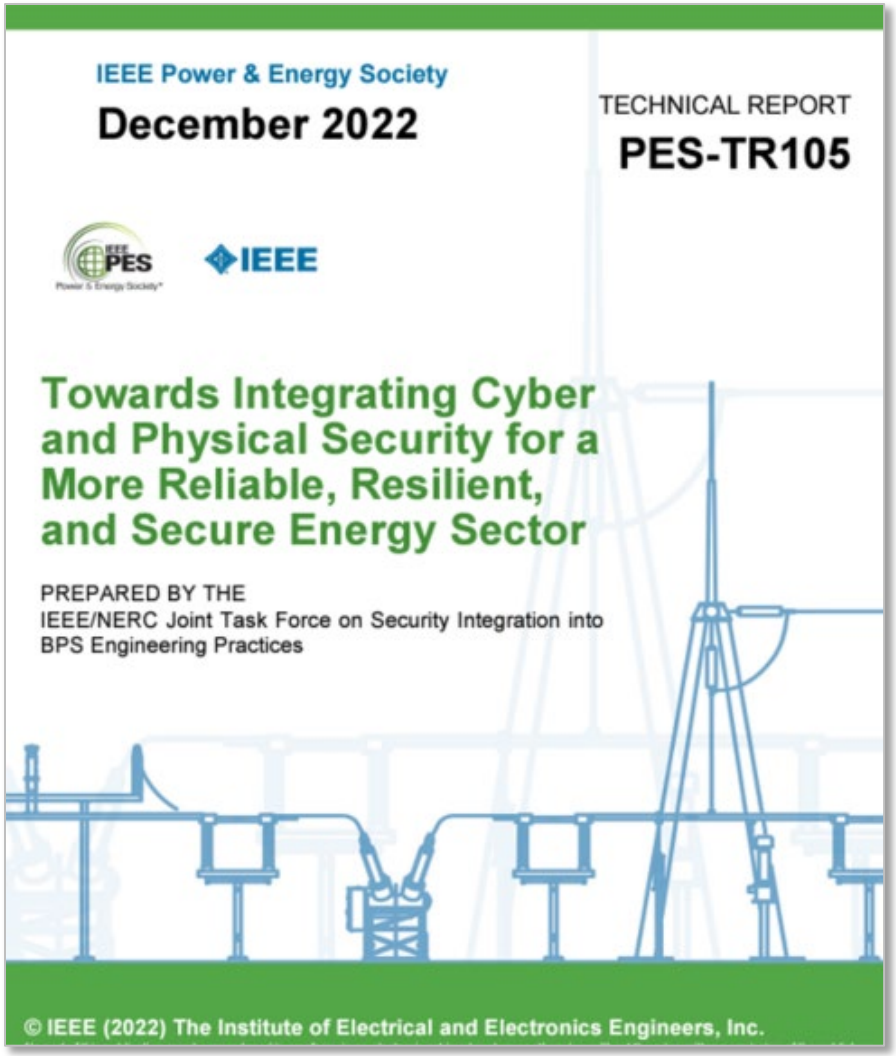
Emerging Technologies and Security Practices

- Identifying Emerging Technology Risk Areas
- Cloud Technology in OT Space
- Advanced Security Concepts

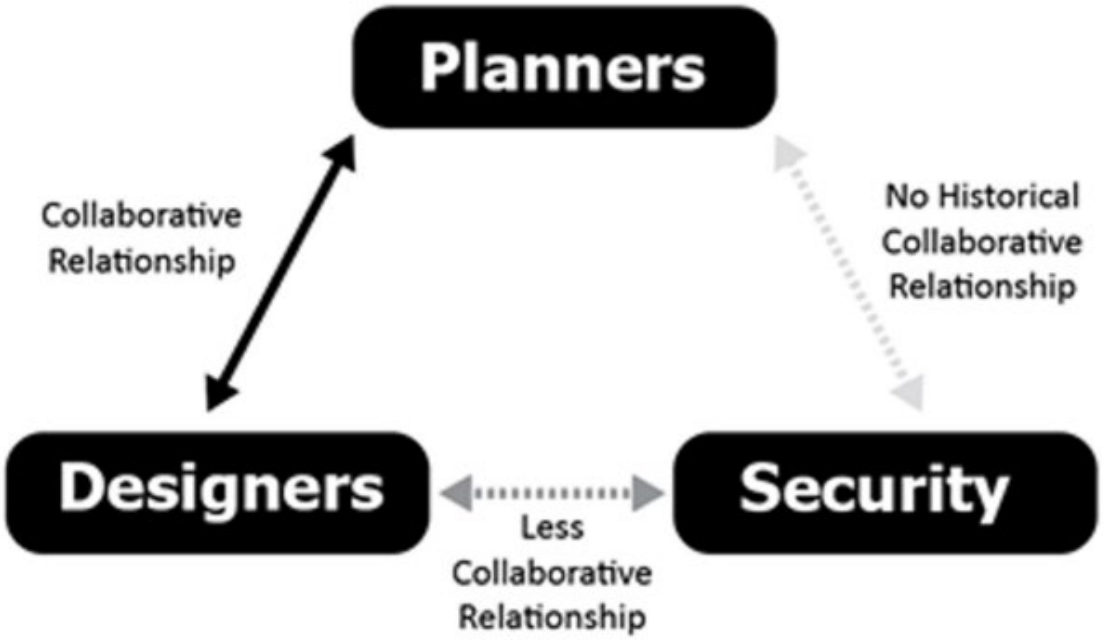
Guidance and Industry Support through Collaboration

Internal: E-ISAC / RSTC / Technical Sub-Groups
External: Industry Forums / Stakeholder Engagements / Federal and Private Partners

Foundational Documents of Security Integration

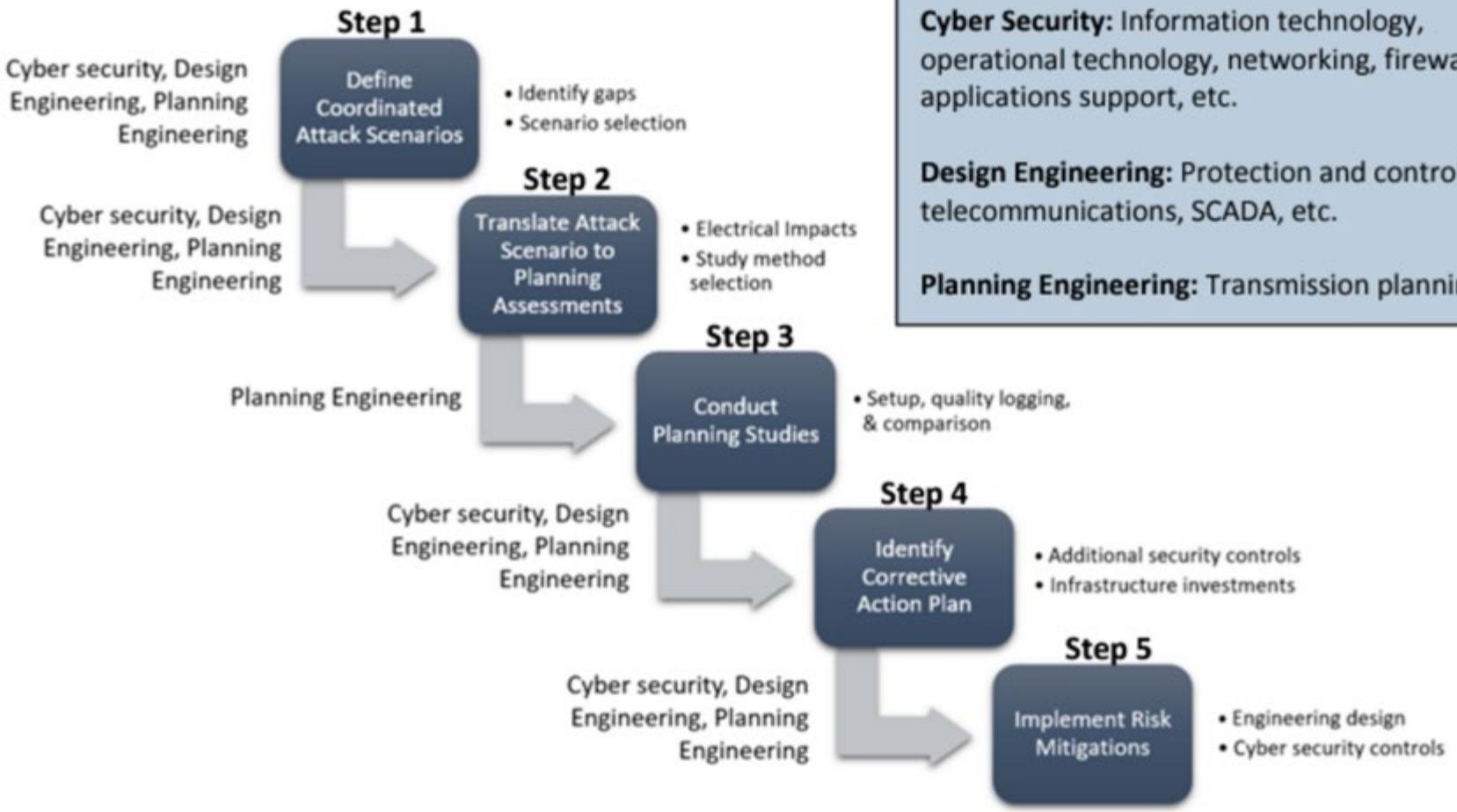


Historical Planning-Design-Security Relationship



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber-Informed Transmission Planning Framework



Cyber Security: Information technology, operational technology, networking, firewalls, applications support, etc.

Design Engineering: Protection and controls, telecommunications, SCADA, etc.

Planning Engineering: Transmission planning

Concept of Eliminating "Critical" Facilities

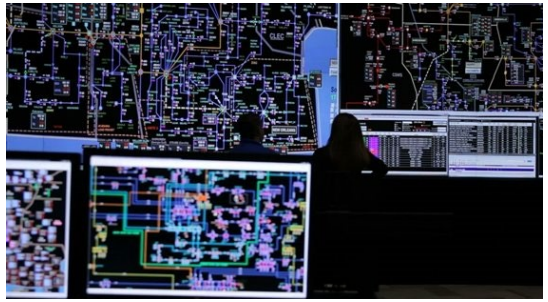
- Leverage multi-value projects that help reduce the number *critical* facilities on the grid
  - Critical = those facilities that could result in instability, uncontrolled separation, or cascading outages
  - Challenges with confidentiality across regulatory spectrum
- Combination of protecting the "crown jewels" and eliminating their criticality in the first place
- Requires concerted "cyber-informed planning" rather than focusing solely on environmental contingencies in the planning horizon

Security Considerations for Inverter-Based Resources

- Scaling of attack surface
  - More distributed assets on bulk power grid
  - Internet-connected assets on the distribution system
- Decentralized control
  - Remotely accessibility and controlled, unmanned facilities – by operator, contractors, equipment manufacturers, etc.
- Predominately power electronic-based response (room for risk)
- Need coordinated effort to secure resources from cyber attack
  - Equipment standards (IEEE, IEC, etc.) and operational security standards

[Source: SMA]

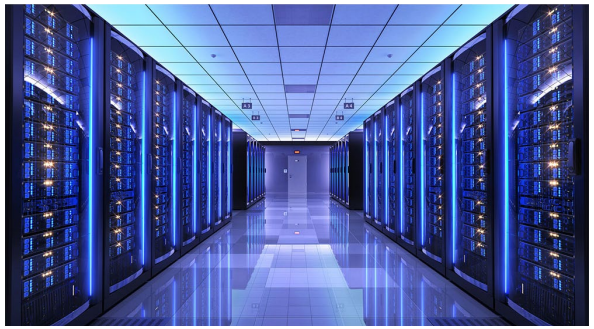
[Source: GE]

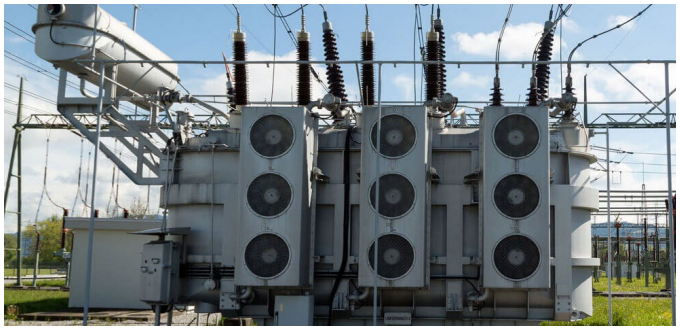


[Source: MISO]

Complexity and Rigidity of Existing IT and OT Systems

- Differentiate security by design for new systems versus managing security risk for existing systems
  - Conflict of new security controls, tools, and practices versus complexity and rigidity of existing systems
- Inherent risks moving from serial-based systems on private networks to IP-based protocols with new technologies
  - Virtualization, cloud computing, IoT devices, emerging technologies
- Growing security vulnerabilities requires both IT and OT resources – from monitoring to mitigation





[Source: Omicron]

Notable Security Concerns from an Engineering Perspective

- Grid edge devices = Internet-connected
  - Internet of Things
  - Smart thermostats
  - Electric vehicles
  - Building management
  - Microgrids
  - Energy storage and DERs
- Virtual power plants and distributed energy resource (DER) aggregators
- Growth of large power consumption loads – both aggregate and individual
  - Aggregate impact of electric vehicles
  - Individual impact of data centers and crypto mining facilities
- Lack of standards (equipment or performance) across the board

[Source: Home Appliances World]

[Source: Electrive]

Securing the Energy Transition

- Rapidly increasing penetration of inverter-based resources
- Growth of distributed energy resources (DERs)
- Introduction of DER Aggregators and virtual power plants
- Large load interconnections – data centers, crypto mining, etc.
- Rise of electric vehicles
- Continued connectivity of end-use loads to Internet

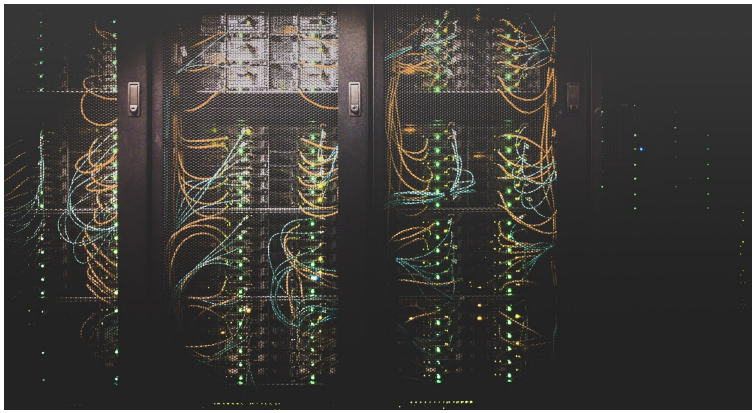
Securely Enabling Emerging Technologies

- Wide range of emerging technologies
  - Virtualization
  - Cloud computing
  - Zero trust network access
  - Artificial intelligence
  - Grid edge technology
  - 5G communications
  - Blockchain
  - Mobile resources
  - Virtual power plants
  - Quantum computing

[Source: QAD]

- Present boundary-spanning risks – span multiple organizations and segments of the energy sector
- Require coordinated efforts to fully leverage benefits yet mitigate risks
- Some we will have ability to “manage” the emergence; others we will be driven by external factors

Securely Leveraging Cloud Technology



- Operational benefits
  - Redundancy and reliability of data
  - Remote vendor support and services
  - Increased resilience and reduced costs
- Operational concerns
  - Availability and reliability
  - Communications links
- Potential risks and challenges
  - Compliance audits of cloud service providers
  - Layered complexity of cloud service offerings (understanding dependencies)
  - Roles and responsibilities of provider versus customer
  - Ensuring sufficient security controls in the overlay
- Great for offline applications and services (e.g., system studies)
- Technology readiness and maturity for real-time operational critical infrastructure

Existing and Future OT Security Workforce Development

- Need to upskill and train existing workforce
- Need blended security/engineering curricula in academia ("cyber engineering)
- Need workforce expertise in:
  - OT network security, not just IT expertise
  - Utility experience and understanding of engineering practices
  - Blended cybersecurity and engineering background
  - Protocols, network architectures, tools, engineering needs
- Covers the full spectrum – generation, transmission, distribution; system operators, utilities, regulators, policymakers, government agencies
- Need range of experience levels; build a strong bench

References

- NERC Security Integration Strategy
- ERO Enterprise Cyber-Informed Transmission Planning Paper
- IEEE Technical Report 105 on Security Integration
- INL Cyber-Informed Engineering (CIE)
- Consequence-Driven, Cyber-Informed Engineering
- ISA/IEC 62443 Series of Standards
- NIST SP 800-82 Rev. 3

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions and Answers

Ryan D. Quint, PhD, PE
Director, Engineering and Security Integration
ryan.quint@nerc.net