



Cyber Security and Critical Infrastructure Protection

William Lucas

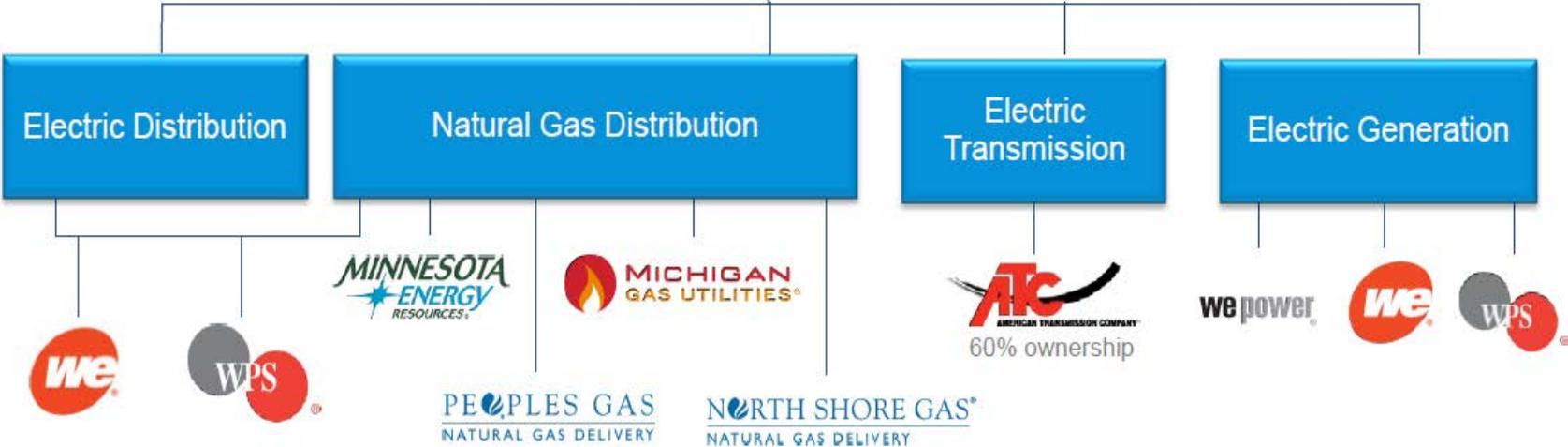
Director, IT Security and Compliance

July 21, 2016

Outline

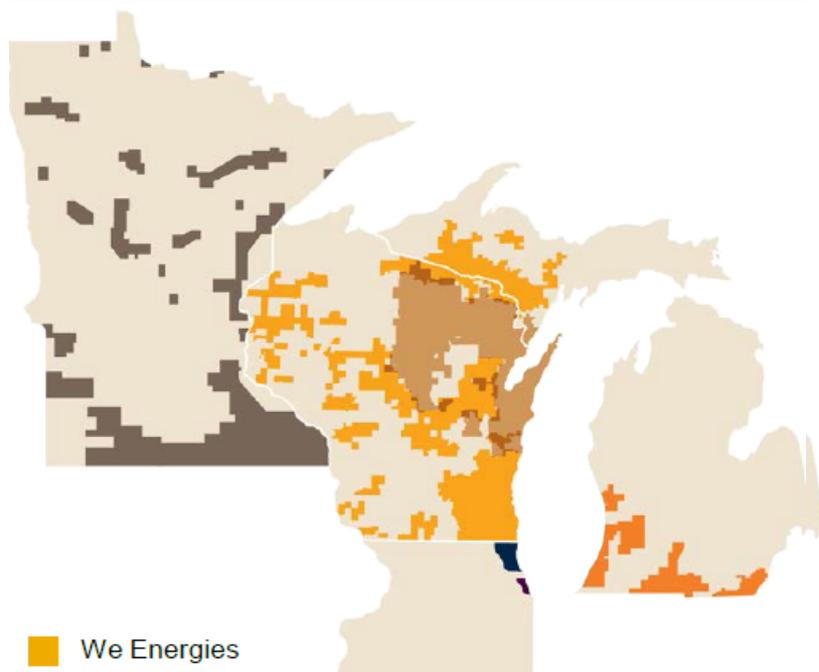
- Company Overview
- Industry Terms
- WEC Energy Group SCADA
- Cyber Attack Types
- Cyber Threats and How We Address Them

Company Overview



WEC Energy Group

Service Territory



- We Energies
- Michigan Gas Utilities Corporation
- Minnesota Energy Resources Corporation
- North Shore Gas Company
- The Peoples Gas Light and Coke Company
- Wisconsin Public Service Corporation

Company Statistics

- \$19 billion market cap ⁽¹⁾
- 1.6 million electric customers
- 2.8 million gas customers
- 60% ownership of ATC
- 70,000 miles electric distribution
- 44,000 miles gas distribution
- \$17 billion of rate base ⁽²⁾

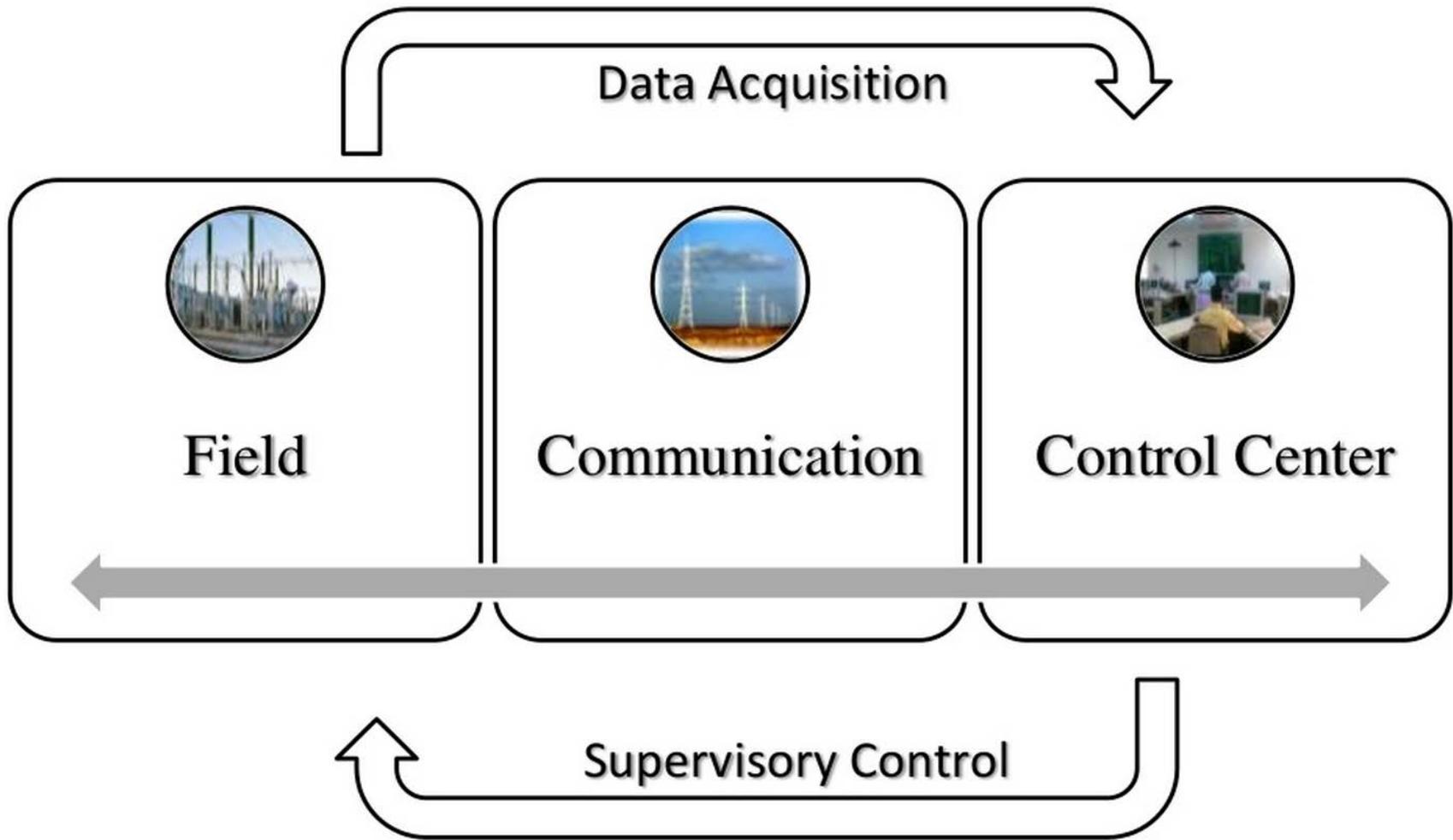
(1) As of 3/31/16

(2) Actual year-end 2015

Terms Unique to the Utility Industry

- FERC (Federal Energy Regulatory Commission)
- NERC (North American Electric Reliability Corporation)
- CIP (Critical Infrastructure Protection)
- EEI (Edison Electric Institute)
- ES-ISAC (Energy Sector Information Sharing and Analysis Center)
- ICS-CERT (Industrial Control System Computer Emergency Response Team)
- DoE-C2M2 (Department of Energy Cybersecurity Capability Maturity Model)
- CRISP (Cybersecurity Risk Information Sharing Program)
- SCADA (Supervisory Control and Data Acquisition)

Gas and Electric SCADA



WEC Energy Group SCADA Systems

- Power generation station control systems
- Substation monitoring and protection
- Electric distribution and transmission system monitoring and control
- Gas distribution station and storage facility monitoring and control
- Customer load and energy usage controls

Threat Actors and Impacts to the Industry

Threat Actors

- Organized criminals
- Nation states
- Hacktivists
- Terrorism



Impacts

- Financial theft
- Theft of customer data
- Business disruption
- Destruction of critical infrastructure
- Reputation damage
- Threats to life and safety

The Threat is Real



- Ukraine distribution grid blackout (BlackEnergy)
- Lansing Board of Water and Light (BWL) computing systems shut down due to ransomware attack
- German Nuclear plant in Bavaria infected with malware, logins compromised
- Cyber security concerns over Smart Grid
- DDoS/phishing attacks on utilities increasing
- PLC and control system vulnerabilities/exploits increasing

How Industry is Addressing the Threat

- The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
- NIST Cybersecurity Framework
- GridEx (NERC power grid exercise)
- EEI Cyber Mutual Assistance
- The National Infrastructure Advisory Council (NIAC)
- Adoption of mandatory and enforceable cyber security standards (NERC CIP)

How Industry is Addressing the Threat

- Threat Information Sharing (ES-ISAC, ICS-CERT, AGA Cyber Security Group)
- Collaboration with DOE, DHS, FBI, NERC and FERC
- Established mandatory critical infrastructure protection standards
- State PUC's and emergency government collaboration
- Collaboration with security leadership across the nation's electric utility industry

How WEC Energy Group Addresses the Threat

Risk Governance

- Board of Directors Audit Oversight
- Enterprise Risk Steering Committee (ERSC)
- Information Security Steering Committee (ISSC)
- NERC CIP Steering Committee
- Sarbanes Oxley (SOX) security controls - Internal Audit
- Compliance with all mandatory standards

Cyber Security Framework and Maturity

- DoE Cybersecurity Capability Maturity Model (C2M2) conducted for multiple areas
- Maturity levels determined for 10 NIST security domains
- Improvement areas determined and reviewed/approved by ERSC
- Progress reviews and status tracked

Incident Response and Information Sharing

- Electricity Information Sharing and Analysis Center (EISAC)
- AGA alerts
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- Member of EEI cross-utility mutual aid and assistance team for cyber attacks
- FBI and DHS
- Conduct annual cyber incident response exercises (includes participation in GridEx)

Cyber Security Controls

- Isolated critical control systems from corporate network
- Implemented strong identity and access management controls including two factor authentication for remote access
- Perform secure code reviews for software purchased/developed prior to implementation

Cyber Security Controls

- Mature security configuration management program
- Use layered security model (AV, malware detection, advanced persistent threat, intrusion prevention, network segmentation)
- Security patch management program including governance and audit

Protecting Sensitive Information

- Policy and education
- Sensitive information defined
- Data loss prevention
- Encryption
- Audit sensitive information use and storage
- Data loss incident response
- Discovery

Third Party Security Support Services

- Denial of service mitigation services
- Cyber incident assistance and remediation
- 24x7 security incident and event monitoring
- FBI/DHS incident assistance and investigation
- Conduct periodic third party audits of our cyber security controls, policy and overall maturity levels

Policy and End User Education

- User education (phishing, suspicious activity, acceptable use)
- Cyber Security Policy
- Information Security Policy
- Acceptable Use Policy
- Annual cyber security policy reviews