Water and Wastewater Supervisory Control and Data Acquisition (SCADA) Security Program

The Evolution of York Region's Collaborative Approach to SCADA Security

November 14, 2023

Introduction

Saurabh Mahajan

Projects Manager, SCADA Security, The Regional Municipality of York

- Develops and maintains cybersecurity program for Process Control Systems (PCS)/SCADA assets
- Over 15 years of information technology and cybersecurity experience
- Managed cybersecurity in healthcare and higher education
- Certified Information Systems Security Professional (CISSP) and a Certified Information Security Manager (CISM)

Mike O'Meara

Process Control Systems (PCS)/SCADA Manager, Water and Wastewater, The Regional Municipality of York

- Through his team, he supports York Region’s SCADA-related infrastructure, process automation, control and monitoring of the Region's water and wastewater systems
- Over 20 years of information technology experience and 13 years of operational technology (OT) experience
- Certified in Advanced Cyber Security at York University, Project Management Professional (PMP) and CISSP

Agenda

- York Region introduction
- SCADA System overview
- Why implement a SCADA Security Program
- Our path and milestones
- Lessons learned
- Questions

York Region

- Almost 1.2 million residents call York Region home

- One of the largest municipalities in Canada

- Our geography – about 1,800 square kilometres over nine different municipalities –beautiful, interesting and diverse as our people

AURORA

EG East Gwillimbury

GEORGINA

KING

MARKHAM

Newmarket

Richmond Hill

VAUGHAN

TOWN OF WHITCHURCH-STOUFFVILLE

York Region SCADA Facts

1500 Instruments monitored and controlled by SCADA

350 Pumps controlled by SCADA

230 Process Automation Controllers (PACs) form the SCADA system

250 Switches deployed to support the SCADA network

7 SCADA Data Centres are highly available and distributed throughout the system

180 Operator Interface Terminals (OITs) provide localized monitoring and control interfaces

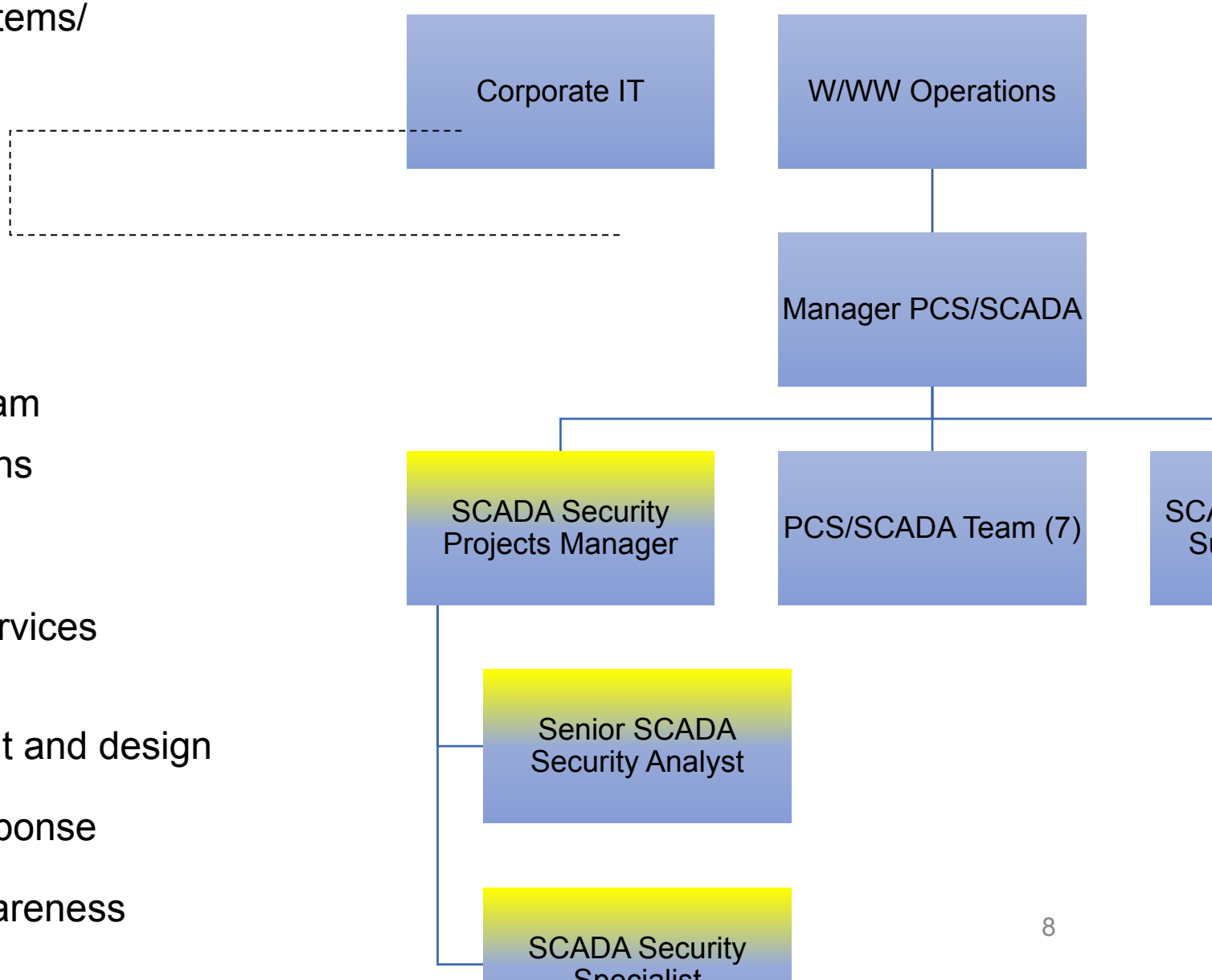
200 Active users

240 Uninterruptible Power Supplies (UPS) handle power interruptions

STAND ALONE NETWORK AND INFRATSRUCTURE

Our Team

- The PCS/SCADA (Process Control Systems/ SCADA) team
  - IT/OT security professionals
  - PCS/SCADA team
  - Systems, Data and Network team
- Embedded SCADA-focused security team in Water/Wastewater (W/WW) Operations
- Formalized SCADA Security Program
- Dotted line reporting to Corporate IT Services



Our Roles

- Guide SCADA architecture development and design
- Manage vulnerabilities and incident response
- Promote and monitor staff and user awareness

Why Implement a SCADA-centric Security Program?

People

- An increased need for remote access
- Understanding of cybersecurity and unique OT requirements
- Shift of focus to availability then confidentiality and integrity
- Reduced reliance on others for security needs

Process

- Digital transformation
- Distributed system
- SCADA systems being targeted
- Potential of physical impacts
- Unique SCADA-specific threat and vulnerability management
- Specific incident response needs

Technolog y

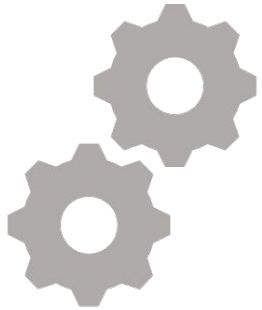
- Systems may not have been designed for security
- SCADA systems adopting IT technologies and protocols
- Physical security/access concerns
- Equipment lifecycles

Why Implement a SCADA-centric Security Program?

People

- An increased need for remote access
- Understanding of cybersecurity and unique OT requirements
- Shift focus to availability then confidentiality and integrity
- Reduced reliance on others for security needs

Why Implement a SCADA-centric Security Program?



Process

- Digital transformation pressures
- Facilities cover relatively large area with various communication options
- SCADA systems have become viable targets
- Potential physical impacts to an incident
- Unique SCADA-specific threat and vulnerability management
- Inconsistent incident response (R and R, priorities, etc.)

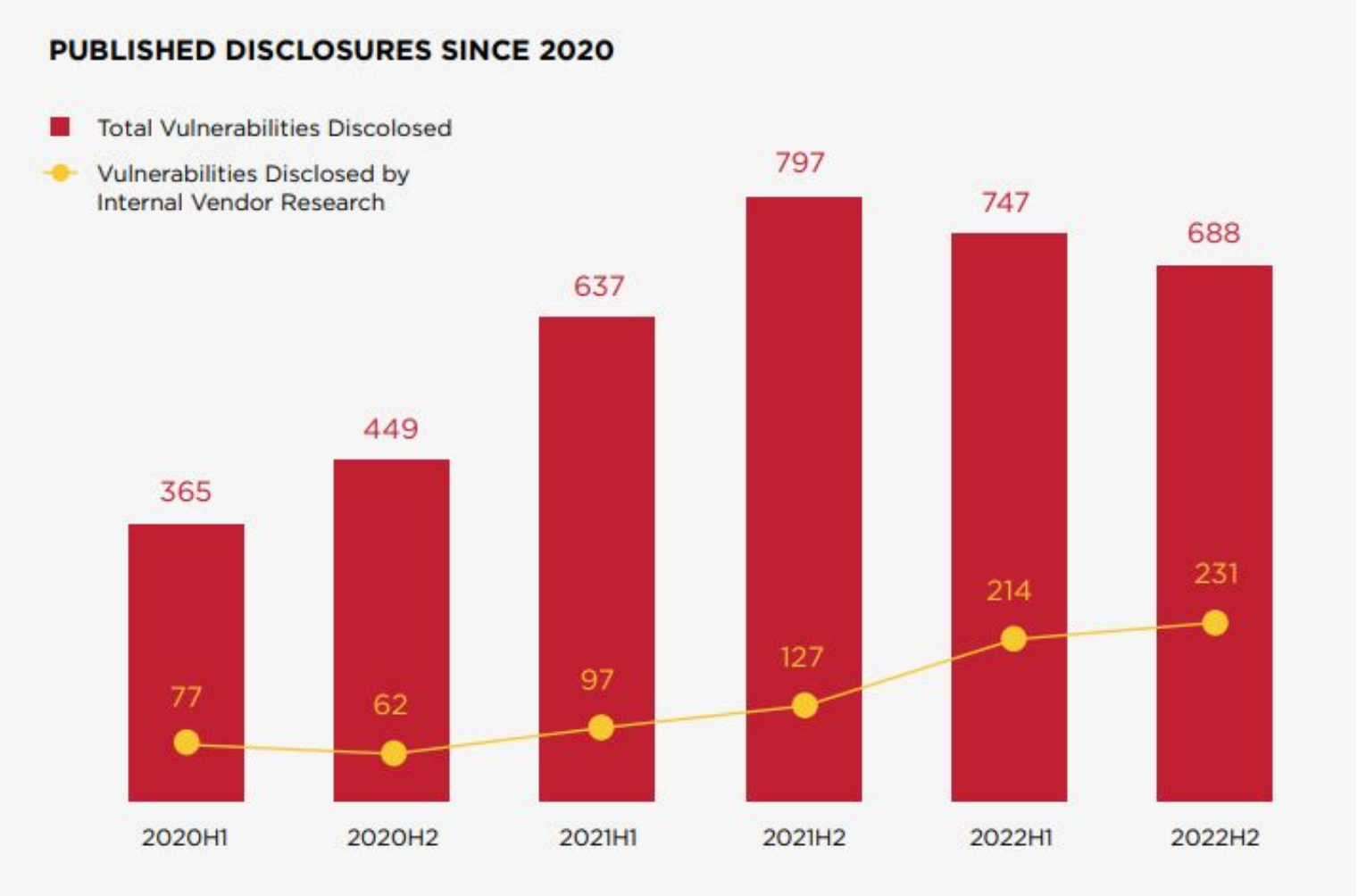
Why Implement a SCADA-centric Security Program?

Technology

- Most SCADA systems were not initially designed for security – security through obscurity
- SCADA systems have adopted IT technologies and protocols (IT/OT convergence)
- Physical security/access concerns
- Need to consider OT equipment lifecycles and application of IT technologies in an OT environment

Current Security Landscape

- Industrial Control System (ICS) vulnerabilities continue to be identified at an alarming rate
- Critical industrial sectors, including water and wastewater, were the most impacted by vulnerabilities disclosed during 2020, 2021 and 2022
- Ransomware and malware remain the top security risks, and destructive malware incidents are on the rise



Source – Claroty State of XIoT Report 2022 2h

Our Path and Major Milestones

SCADA focus	Senior management support	Working with Corporate IT	Security assessments
Leveraged IMS/DWQMS (drinking water quality management standard)	SCADA Master Plan	SCADA security team	Education and awareness
Physical security	SCADA Risk Register	Development of SCADA incident response plans and playbooks	SCADA tools and technologies

Focus on OT/SCADA Security

IT/OT Convergence

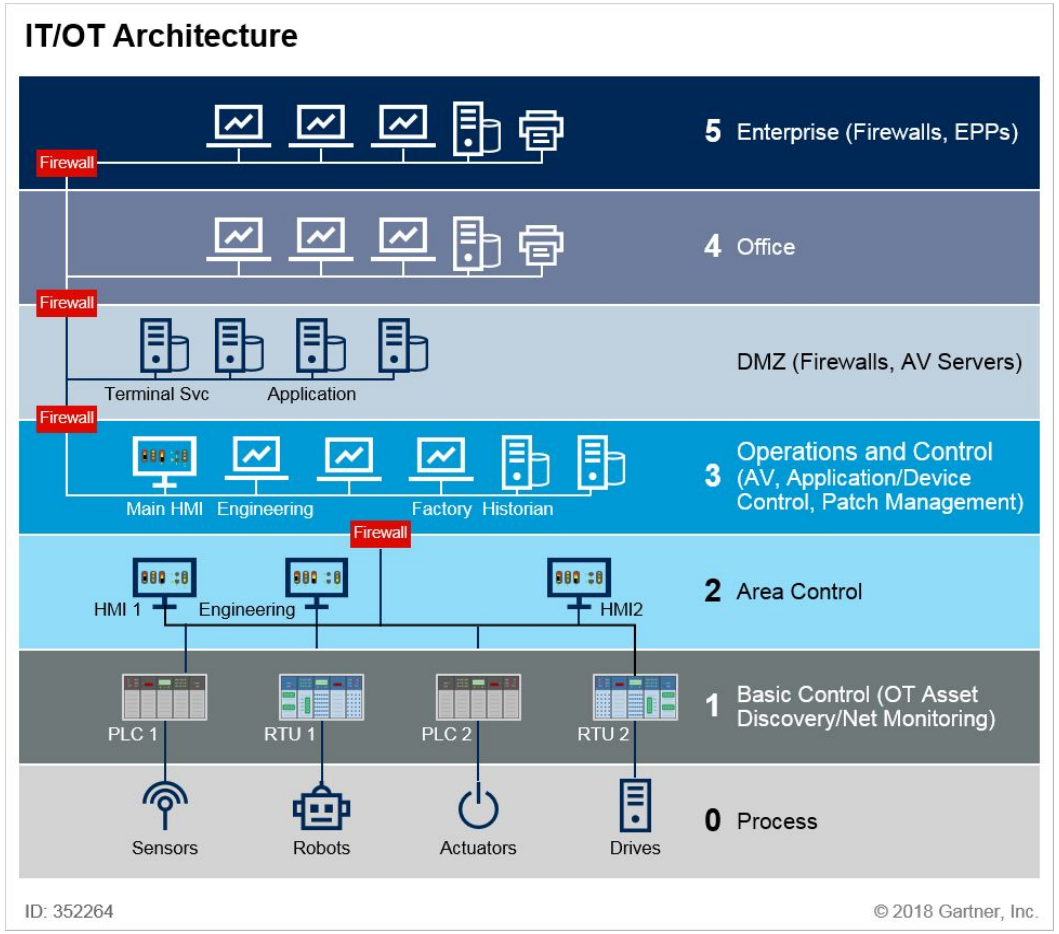
- OT systems increasingly leverage IT technologies
- OT specific controls to protect industrial environments with a defense in-depth approach

IT Priorities

- Prevent and minimize the impact of breaches
- Secure the data (personal, identifiable information and protective health information)

OT Priorities

- Human safety
- Continuous availability



Focused on OT/SCADA Security

SCADA cybersecurity program

Identify, develop and implement:

- SCADA security policies and procedures, standards and baselines
- Cybersecurity roles and responsibilities
- SCADA team RACI (responsible, accountable, consulted and informed)
- Patch and vulnerability and patch management program
- Security awareness program

Senior Management Support

Working with the Senior Management Team (SMT) is essential in the development and advancement of the SCADA Cybersecurity Program. This is achieved by:

- Leveraging internal and external assessments
- Informing SMT of emerging risks and mitigations
- Gaining support to advance the SCADA security program
- Ongoing risk assessments of OT systems based on standard frameworks
- Receiving Council approval of SCADA standards and equipment

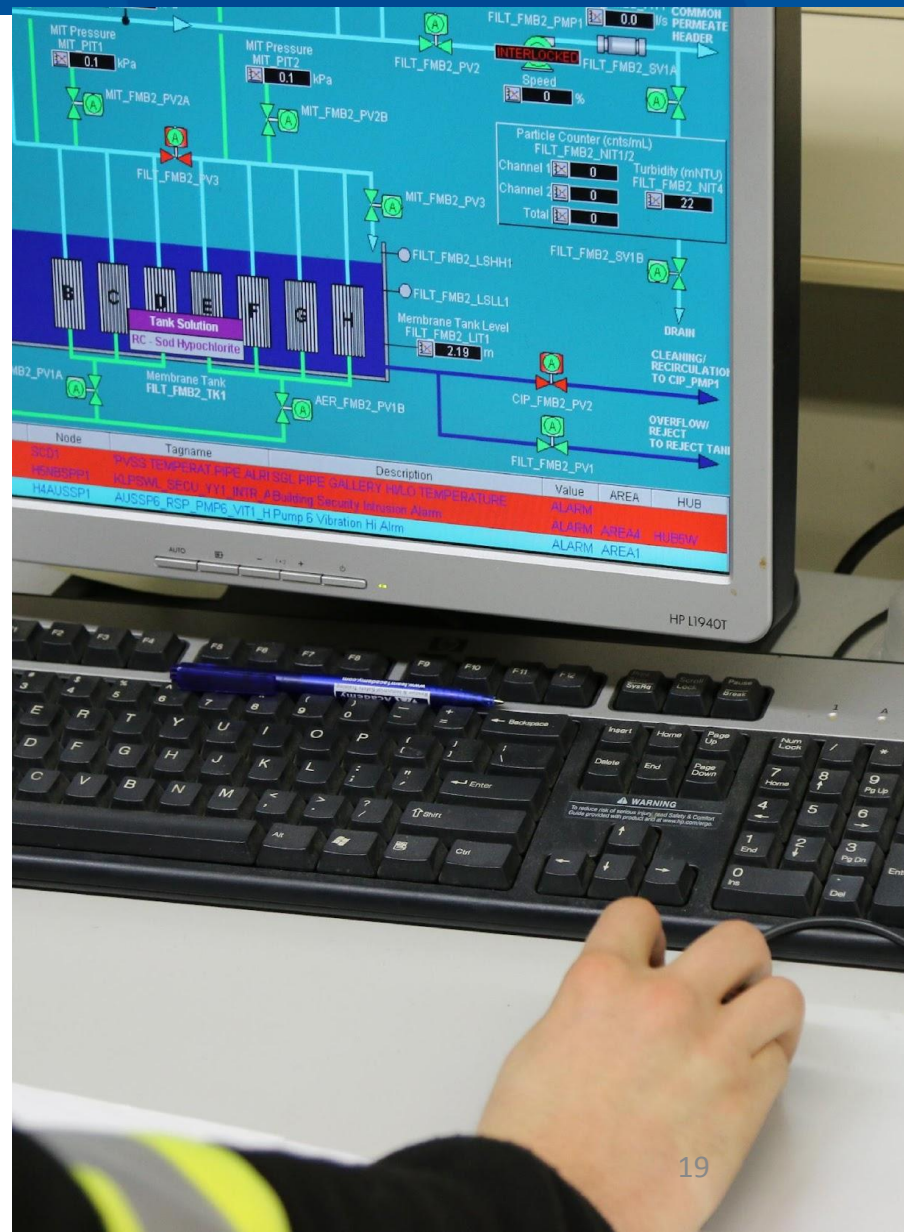
Working With Corporate IT

Ongoing collaboration with Corporate IT and organizational structure changes

- Standardization of common security tools across IT/OT
- Review common security vulnerabilities
- Alignment of cybersecurity roles and responsibilities
- Dotted line reporting structure to ensure accountability and authority
- Open dialogue and collaboration
- Coordinated training response and support
- Not reinventing the wheel – align and reuse where possible

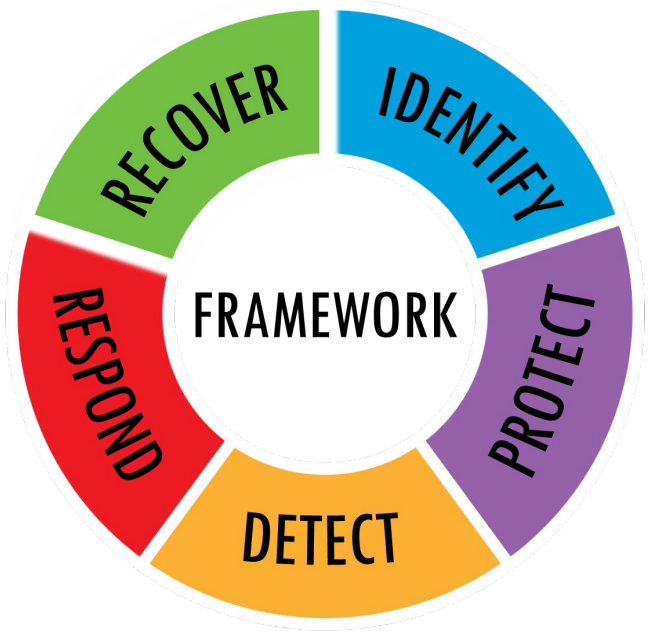
Leveraged Internal and External Assessments

- Facilitated assessment from Public Safety Canada
- IMS reviews and audits
- Ongoing internal assessments
- External audits
- Tabletop exercises
- Annual breach exercise
- Internal audits and evaluate security controls



Leveraged the IMS and DWQMS

NIST cyber security framework



Continual improvement cycle

Management of Physical Access To SCADA Infrastructure

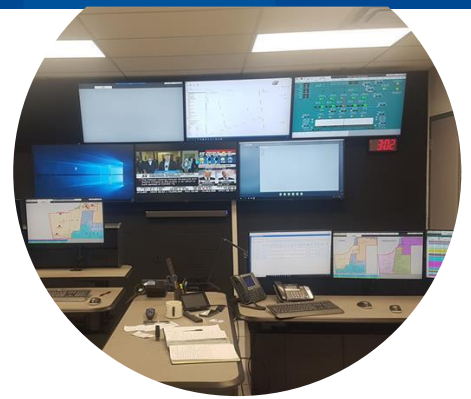
- Physical security being managed by a corporate partner
- Developed access lists for SCADA Data Centres and audit reports (limited access for non-SCADA staff)
- Reduced co-location and generalized access to SCADA equipment
- Developed procedure for after-hours access
- Weekly audits of card activity to SCADA infrastructure
- Implemented eKey solution for programmable automation controller (PAC) and Network Access Cabinets (NAC) panels
- York Region-issued laptops for contractors
- Asset inventory

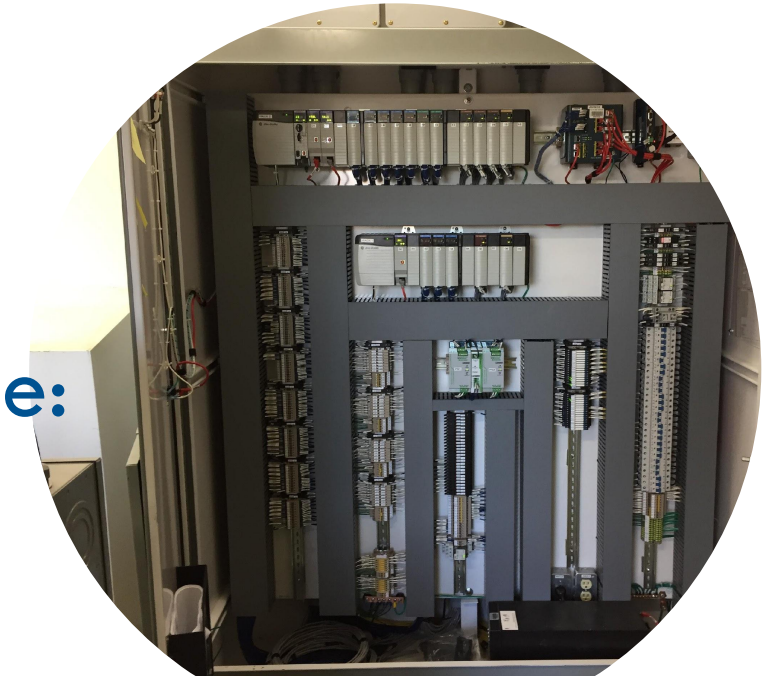
Development of SCADA Master Plan

- Completed in late 2020
- 10-year plan ensures the SCADA system meets future needs
- This led to the appropriate use of SCADA technology guideline – identifies what the SCADA system can and cannot be used for
- Formalized security-centric system architecture and approach
- Detailed required projects and resources required to deliver

Development of SCADA-Focused Security Team

- The team was built gradually – no big bang
- Security roles and responsibilities were shifted from general staff to security specialists
- Developed SCADA-specific cybersecurity job descriptions
- Defined RACIs





SCADA Security Roles Now Include:

- SCADA Security Projects Manager
- SCADA Security Analyst

Education and Awareness

- Added cybersecurity as an agenda item in all staff meetings
- Implemented mandatory cyber training for all SCADA users
- Customized phishing campaigns for SCADA user group
- Monthly cyber talks to discuss new vulnerabilities and/or threats
- Worked with other support groups (Property Services, IT, Capital) to understand SCADA-specific needs and risks

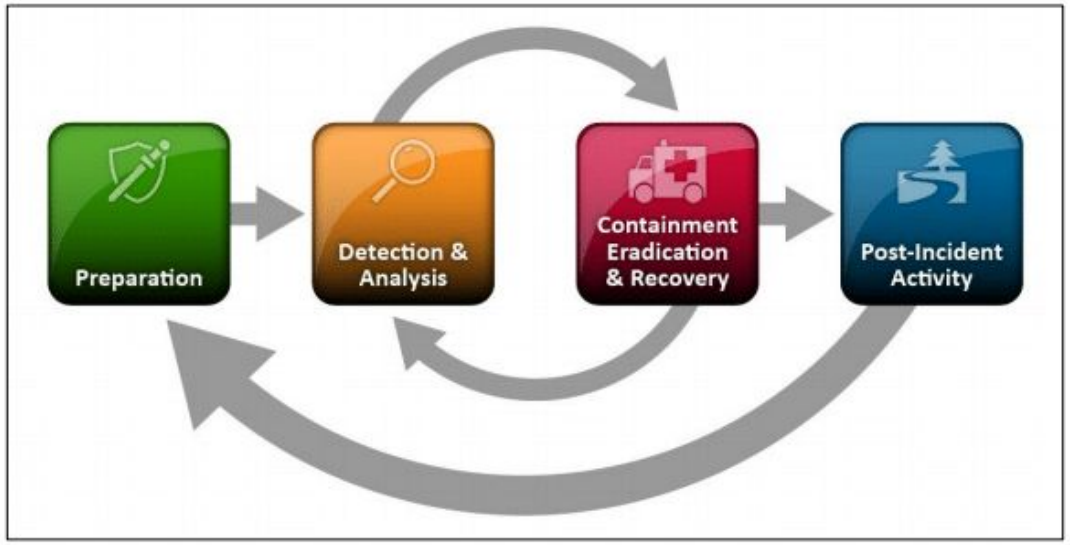
Deployment of SCADA Risk Register

- Developed a formal process for managing SCADA cyber risks and vulnerabilities
- Assess and remediate risks
- Prioritized risks based on impact
- Qualitative and quantitative risk analysis
- Follow-up with changing landscape

Risk Matrix		Severity				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Almost Certain	Medium	High	Very High	Very High	Very High
	Likely	Medium	High	High	Very High	Very High
	Possible	Low	Medium	High	High	Very High
	Unlikelyh	Low	Low	Medium	Medium	High
	Rare	Low	Low	Low	Low	Medium

Development of SCADA Incident Response Plans and Playbooks

- Developed malware and ransomware playbooks
- Created incident roles and responsibilities
- Determined incident severity levels
- Set up alerts for incident notifications and escalation process
- Implemented automated incident response
- Implemented cybersecurity tabletop exercises



SCADA Tools and Technologies

- Endpoint security
- Endpoint detection and response
- Patch management tool
- Multi-factor authentication
- Centralized logging
- Vulnerability scanning tool
- Security baselines
- Application and device control
- Network segmentation
- Dot1x authentication
- Zero trust network architecture
- Integrating cybersecurity monitoring

Lessons Learned

1. A clear focus and understanding of OT security is needed
2. Don’t rely on someone else for a system’s security. Just like safety, security relies on all involved
3. Engage SMT/C-Level early and often
4. Work closely with partners (IT, Legal, Risk, HR, Property)
5. Start small and keep going – continual improvement, it will never be done
6. Leverage outside opinions/input and resources
7. Ask lots of questions – be curious
8. Practice!
9. Work with what you have first
10. Have a plan – be proactive about security

Thank You