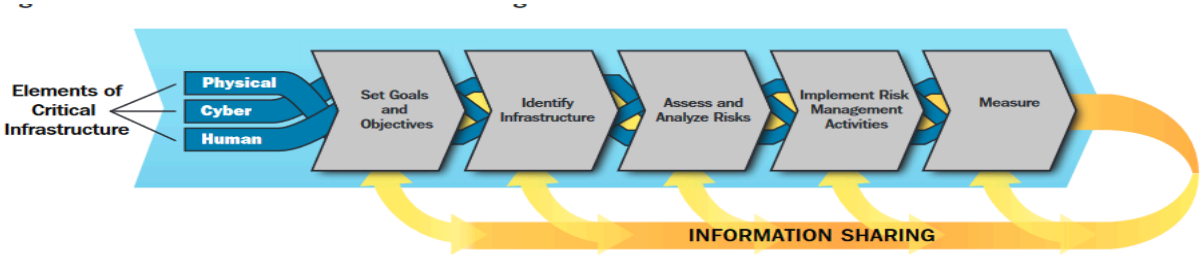
Prepared by Christopher Wilson- Cyber Operations

1. Introduction

In my risk assignment report, We will evaluate the cybersecurity implications of a proposed City operations system. This is a very ambitious project funded and maintained by a third-party entity called stakeholders. This project aims for the city operating system to integrate with cutting-edge AI/machine learning algorithms to maintain and monitor all of the city's infrastructure segments and close a gap in information technology and operational technology.

Our commitment extends beyond merely enhancing city management capabilities. We aim to set a benchmark in security standards and compliance, ensuring that our city operations systems are not just efficient but also robustly secure against emerging cyber risks. This comprehensive approach to integrating advanced technologies with a strong cybersecurity framework will position our city at the forefront of secure and innovative urban management."



OT

Traffic Controls system

- Stakeholders- city planners, taxpayers, commuters
- Concerns - Energy supply constraints/concerns
- Interest-: Efficient incident management, real-time traffic data

Electrical grid control systems

- Stakeholders - Utility companies, residents, businesses, Emergency services
- Concerns- Energy supply stability, Safety, Cost-efficiency

- Interest- Operational efficiency, Affordable rates, Renewable energy options

2. Description

1. ***Traffic control systems***
    - **Function** - with the functionality of these systems, they can manage the flow of not only vehicular traffic but also the flow of pedestrian traffic, being able to reduce the amount of congestion and enhance road safety and pedestrian safety
    - **Components** - Traffic control safety systems include road signs, surveillance cameras, and sensors that you can activate in an emergency, such as emergency response services(EMS) if needed to respond to emergencies.
    - **Connectivity and Data Handling** - This system is supposed to connect to a centralized data facility, often to process real-time data, by establishing dynamic adjustments to traffic flow based on current conditions.
2. ***Electrical Grid Control Systems***
    - **Function** - This system manages the generation, transmission, and distribution of electrical power across the city. It ensures the reliability and stability of power to residential commercial. And industrial consumers.
    - **Components -** It includes substations, transformers, and power distribution across the city to all the different power consumers. These advanced systems may incorporate. Innovative grid technology for a more energy-efficient management system.\
    - **Connectivity and Data Handling**: These systems use real-time monitoring and control to balance supply and demand, prevent outages, and facilitate rapid response to faults or disruptions in the grid.

3. **OT Systems Protocol Overview**

1. ***Traffic control systems***

- **Protocol Name** - NTCIP (National Transportation Communications for ITS Protocol)
- **Ports that are used** - The ports that would be used inside of an application would be port number 19200 because NTCIP uses this port for all of their communications with other control modules and SNMP ports.

- **Security Issues -** With using NTCIP, the security challenges that we face are due to open standards and the widespread use of NTCIP throughout the centralized data systems, which can be a vulnerability issue and lead to unwanted

2. **Electrical Grid Control Systems**

- **Protocol Name - IEC 61850**
- **Port Used -** with the power grid, it is typical to use port number 102
- **Security Issues -** The main concerns with using protocol IEC 61850 also include the risk of unauthorized access and the potential for cyber-physical attacks disrupting the grid operations.

4. **Threat Analysis and Historical Malware Impact on Traffic Control Systems**

1. **BlackEnergy and Traffic control systems**

Impact: BlackEnergy's adaptability makes it a significant threat to traffic control systems. A successful attack could compromise traffic light control control systems. With a successful attack it could lead to city wide traffic jams, accidents, and potental gridlock. Overall would lead to a delay in EMS response and union disruption.

ICS Kill chain stage:

Infiltration: Infiltration often through spear-fishing attacks that target system operators/ technicians

Propagation: Spread within the network, often leveraging known vulnerbillties inside of windows-based systems.

Control system Discovery: Identification and the mapping of a networks assets and layout that includes traffic control interfaces.

Control systems manipulation: An execution of malicious payloads to disrupt traffic chaos to due to gaining access to signal operations or gaining remote control

Action on Objectives:Creating real-world disruption, from causing traffic chaos to impeding ems response.

2. **Mirai Botnet and traffic control systems**

Impact: Mirai, exploiting IoT vulnerabilities, could hijack internet -connected traffic control devices, causing causing signal malfunction or failures. This could results in uncoordinated traffic lights, increasing the risk of collisions and severely impeding urban mobility.

ICS kill Chain Stage

Initaition: Exploting weak security in IoT devices, like default passwords in traffic control systems.

Propagation: Rapid spread by autonomously searching for other vulnerabilities devices

Control System Discovery: Identifying the capabilities and limattions of compromised traffic systems.

Control System Manipulation: Overloading the devices with requests or altering control functions.

Action on Objectives: Disruption of Normal traffic flow, potential creation of a botnet for a larger scale attacks.

3. **Havex and Traffic Contol Systems**

Impact: Havex, focusing on Indusral control systems, could compromise the integrity of and reliability of traffic control operations .This might lead to incorrect signal timings, and escalating urban traffic challenges.

ICS Kill Chain:

Initation: Deployment via Phishing or compromised legitament software used by traffic control system

Propagation and Foothold Establishment: Scanning for and infecting other networked devices within the traffic control infrastructure

Control System Discovery: Gathering information on the network configuration and connected traffic control devices

Control system manipulation: Interfering with the operational logic of traffic control systems, altering timings or signals.

Action On Objctives: Achieving disruption of the traffic flow, data manipulation, or long-term access for sustained interference.

5. ***Electrical Grid Systems: Malware Threats and Security Analysis***

1. ***Stuxnet and electrical grid control systems***

Impact: Stuxnet, Originality was designed to sabaitage Iraian nucular program, could if adapted, cause significant harm to electrical grid infrastructure. Its ability to manipulate industrial

control systems could lead to the malfunction of critical components like transformers or circuit breaker, causing physical damage. This could results in widespread power outages, overloads in parts of the grid, and potentially long-term damage to infrastructure.

ICS Kill chain stage

Initation : infilltration through removable media, such as a USB drive, especailly in isolated and segmented networks thought out a system.

Propagation: Spread within the network, seeking out specific PLCs responsible for grid control.

Control System Discovery: Identification of specific software and hardware configurations of PLCs used in grid operations.

Control system manipulation: Altering PLC code to cause Physical damage to grid infrastructure, like opening/closing breakers inappropriately.

Action on Objectives: Executing the payload to disrupt grid operations, leading to the intended physical damage.

2.***Industroyer and Electrical grid control systems***

Impact: Industroyer, or CrashOverride, specifically target power grid systems. It could manipulate control settings of electrical substations, leading to disconnections and equipment failure. Its capabllites to intract directly with grid control protocols means it could cause blackouts and damage equipment, Leading to prolonged restoration times.

Initiation: Network infiltration, potentially through phishing or exploiting network vulnebillities.

Establishment of Foothold: gaining persistent access within the network

Control system manipulation: Sending unauthorized commands via inustral communication protocol (like IEC 61850 or OPC)

Control System Discovery: Mapping out the network, identifying critical components in the electrical grid.

Action on Objectives: Executing operations that lead to blackouts and potential physical damage.

Triton and Electrical Grid Control Systems

- **Impact**: Triton, targeting safety instrumented systems (SIS), represents a significant threat to grid safety mechanisms. It could reprogram or disable SIS, leading to the removal of critical safety barriers. This could result in uncontrolled grid operations, risking severe accidents or infrastructure damage, potentially even leading to hazardous conditions for workers and the public.
- **ICS Kill Chain Stage**:

  Initiation: Infiltration, possibly through spear-phishing or network breaches.

  Propagation and Foothold Establishment: Moving within the network to target systems related to safety controls.

  Control System Discovery: Identifying and understanding the safety system's operations and defenses.

  Control System Manipulation: Altering or disabling the safety logic, making the grid operate without safety constraints.

  Action on Objectives: Causing unsafe operational conditions, potentially leading to catastrophic failures or accidents.

6. mitigation plan

1. **BlackEnergy Mitigation**

   Prevent: Enhance network security, conduct anti-phishing training.

   Detect: Use IDS for traffic monitoring.

   Respond: Isolate and cleanse infected systems.

   Recover: Restore from backups, update security protocols.

2. **Mirai Botnet Mitigation**
   - **Prevent**: Strengthen IoT device passwords, network segmentation.
   - **Detect**: Monitor for traffic anomalies.
   - **Respond**: Disconnect and reset infected devices.
   - **Recover**: Update IoT firmware, conduct network audits.
3. **Havex Mitigation**
   - **Prevent**: Verify software sources, keep systems updated.
   - **Detect**: Use industrial-specific antivirus solutions.
   - **Respond**: Analyze and quarantine affected systems.
   - **Recover**: Restore from backups, review security measures.

Electrical Grid Control Systems

1. **Stuxnet-like Threats Mitigation**
    - **Prevent**: Control physical access, application whitelisting.
    - **Detect**: Monitor for PLC anomalies.
    - **Respond**: Isolate and analyze affected systems.
    - **Recover**: Restore PLC configurations, reinforce security.
2. **Industroyer Mitigation**
    - **Prevent**: Implement robust firewalls, access controls.
    - **Detect**: Use grid-specific IDS.
    - **Respond**: Disconnect and investigate affected systems.
    - **Recover**: Train staff, update response plans.
3. **Triton Mitigation**
    - **Prevent**: Harden SIS, regular security assessments.
    - **Detect**: Monitor SIS for unauthorized changes.
    - **Respond**: Shut down operations if compromised.
    - **Recover**: Conduct regular drills and backup SIS configurations.

7. ***Pentest Recommendation/Remediation***

Traffic Control Systems

1. **Frequency of Testing**: Bi-annual. Traffic control systems are critical and dynamic, requiring regular checks to ensure security integrity.
2. **Remote or In-Person Testing**: Combination. Remote testing for network vulnerabilities; in-person for physical security and hardware checks.
3. **Testing Type**: Gray-box. A mix of white-box (understanding of internal structures) and black-box (external testing) offers a comprehensive view.
4. **Special Considerations**: Ensure testing doesn't disrupt traffic flow. Tests should be scheduled during low-traffic hours to minimize impact.

Electrical Grid Control Systems

1. **Frequency of Testing**: Quarterly. Given the critical nature and potential high-impact risks, more frequent testing is advisable.
2. **Remote or In-Person Testing**: Mostly remote for network vulnerabilities, but in-person testing is essential for physical security and system controls.
3. **Testing Type**: White-box. Given the complexity and importance of these systems, an in-depth understanding of internal workings is crucial.
4. **Special Considerations**: Testing should not compromise grid stability. Coordinate with grid operators to schedule tests during low-risk periods.

8. *Threat Recommendatios.*

Traffic Control Systems

1. **Analysis Method:** Combination of Fuzzing and Dynamic Analysis.
    - **Fuzzing:** Randomly testing the system inputs to identify potential vulnerabilities, especially useful for uncovering unknown bugs in software components of the traffic control system.
    - **Dynamic Analysis:** Monitoring the system in real-time to understand how it behaves under normal and stress conditions, which helps in identifying potential security flaws during its operational state.
2. **Frequency of Research:** Semi-annually.
    - Given the dynamic nature of traffic control systems and their exposure to evolving threats, conducting semi-annual research is recommended to keep up with the latest vulnerabilities and ensure system resilience.

Electrical Grid Control Systems

1. **Analysis Method:** Combination of Static Analysis and Dynamic Analysis.
    - Static Analysis: Examining the system's codebase without executing it to identify potential vulnerabilities. This is crucial for complex systems like the electrical grid, where changes can have significant impacts.
    - **Dynamic Analysis:** Observing the system during runtime to identify vulnerabilities that manifest only when the system is operational, essential for systems that are often targeted by sophisticated cyber threats**.**
2. **Frequency of Research: Quarterly.**
    - The electrical grid's criticality and the high stakes of potential disruptions necessitate more frequent threat research. Quarterly analyses align with the fast-evolving landscape of cybersecurity threats targeting such critical infrastructure.

9. *Appendices*

Appendix A: Compliance standards

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

https://www.standards.its.dot.gov/Factsheets/Factsheet/23

https://www.speedguide.net/port.php?port=19200

https://www.ntcip.org/about/

https://www.gegridsolutions.com/multilin/journals/issues/spring09/iec61850.pdf

https://isc.sans.edu/survivaltime/port/102

https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01