MANAGING CRITICAL OPERATIONS RISKS-CYBERSECURITY PERSPECTIVE, IIOT APPROACH

ASHRAF SABRY

SECURICIP

Ashraf.sabry@list.ru

INTRODUCTION

There is no doubt that cybersecurity now is a very important and essential function for any organization, and the reason for this is the risks that organization may have due to lack of proper cybersecurity practices, those risk could affect the organization reputation, cause severe financial losses, possible regulatory and legal consequences, and in case of presence of control systems such as SCADA, DCS, BMS. etc.. the risks may even be safety and environmental.

Cybersecurity operations need to be effective, and to be effective it requires to be based on having effective procedures, competent team, and reliable technology.

There are essential policies and procedures that should exist to support the effective cybersecurity operations such as: General Cybersecurity Policy, Cybersecurity Risk Management Policy, Vulnerability Management Policy, Incident Management Policy, etc. Incident Management Procedure, Vulnerability and Patch Management Procedures, Backup and Restore Procedures…etc. The competent team require to ensure it has specific expertise and skills such as: ICS (Industrial Control System) / OT (Operational Technology) cybersecurity experience and certification -Cybersecurity Incident Handling Cybersecurity- Risk Management Effective communication and coordination skills-

INTRODUCTION

- **Operations technology (OT) is the term used in industrial operations. It comprises control systems, networks, and other industrial automation components that control physical processes and assets. Control systems are at the heart of the nation’s critical infrastructure, which includes electric power, oil and gas, water and wastewater, manufacturing, transportation, agriculture, and chemical factories. ICSs, which are a part of the OT environment in industrial enterprises, encompass several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and other smaller control system configurations such as programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices (IEDs) and other field devices. Industrial Control Systems (ICS) is a general term for several types of command-and-control systems, which are used in industry and critical infrastructure**

INDUSTRIAL CONTROL SYSTEMS (ICS)

INDUSTRIAL CONTROL SYSTEMS DESCRIBE ANY SYSTEM THAT CAN GATHER INFORMATION IN AN INDUSTRIAL PROCESS AND MODIFY, REGULATE, AND MANAGE THE PROCESS TO THE DESIRED STATE.

1-Supervisory Control and Data Acquisition (SCADA)

- A communication-based system that enables control, control, and process control. This is by sending dedicated commands to controllers. These processes are usually production, production, refining, energy generation and product assembly. The systems include a computerized layer for monitoring and controlling the accessories. Industry processes include, among others, production, production, refining, energy generation and product assembly processes. Processes in public or private infrastructures include inter alia, outdoor lighting systems (urban and inter-urban), water supply systems, wastewater collection and purification systems, oil, and gas transmission pipeline monitoring, electricity grid, alarm systems, and large communications systems. Processes in public or private

INDUSTRIAL CONTROL SYSTEMS (ICS)

INDUSTRIAL CONTROL SYSTEMS DESCRIBE ANY SYSTEM THAT CAN GATHER INFORMATION IN AN INDUSTRIAL PROCESS AND MODIFY, REGULATE, AND MANAGE THE PROCESS TO THE DESIRED STATE.

2-Distributed Control System (DCS)

3-Process Control System (PCS)

4-Energy Management System (EMS)

5-Structural Control Systems (BMS)

6-Automation System (AS)

7-Safety Instrumented System (SIS)

INDUSTRIAL CONTROL SYSTEMS (ICS)

INDUSTRIAL CONTROL SYSTEMS DESCRIBE ANY SYSTEM THAT CAN GATHER INFORMATION IN AN INDUSTRIAL PROCESS AND MODIFY, REGULATE, AND MANAGE THE PROCESS TO THE DESIRED STATE.

- Any other automated control system used to transport processes which include oil, gas, water, electricity, and people. DCS is used in refineries and chemical plants whereas PCS is usually used in manufacturing facilities as well as in small chemical plants. ICS systems improve the quality of these products and services by ensuring lower costs and an increase in safety ICS systems provide valuable business making decisions as they can implement real-world actions making them very powerful but also very dangerous. ICS/SCADA systems are different from IT systems and unlike IT systems, they lack standard security guidelines. It is the responsibility of companies to create, maintain and manage system-specific ICS cybersecurity practices which should be documented, enforced, and updated on a regular basis.

INDUSTRIAL CONTROL SYSTEMS VS IT SYSTEMS

1- First, ICS are typically used to control critical processes.

- . Key priorities are continuity and the ability for operations to view and control the processes. ICS triggered disruption of the production or critical functions, which may affect the organization's profit and reputation. This causes a strong reluctance to apply any system changes that could harm the continuity of the production and its performance. Security controls common in regular IT, including regular patching and antivirus updates, therefore, pose a risk to the monitored and controlled production processes

INDUSTRIAL CONTROL SYSTEMS VS IT SYSTEMS

2- Secondly, ICS and (office) IT have historically been managed by separate organizational units.

- . ICS people do not consider their ICS to be IT. ICS is just monitoring and control functions integrated into the process being operated. ICS people lack cybersecurity education. The IT department, on the other hand, is unfamiliar with the peculiarities and limitations of ICS technology. They do not regard the control of processes to have any relationship with IT. Only a few people have the knowledge and experience to bridge both domains and define an integrated security approach. Organizations that have brought the personnel from These two diverse domains together, have successfully bridged the gap and
- improved the mutual understanding of both their IT and ICS domains. Their security posture has risen.

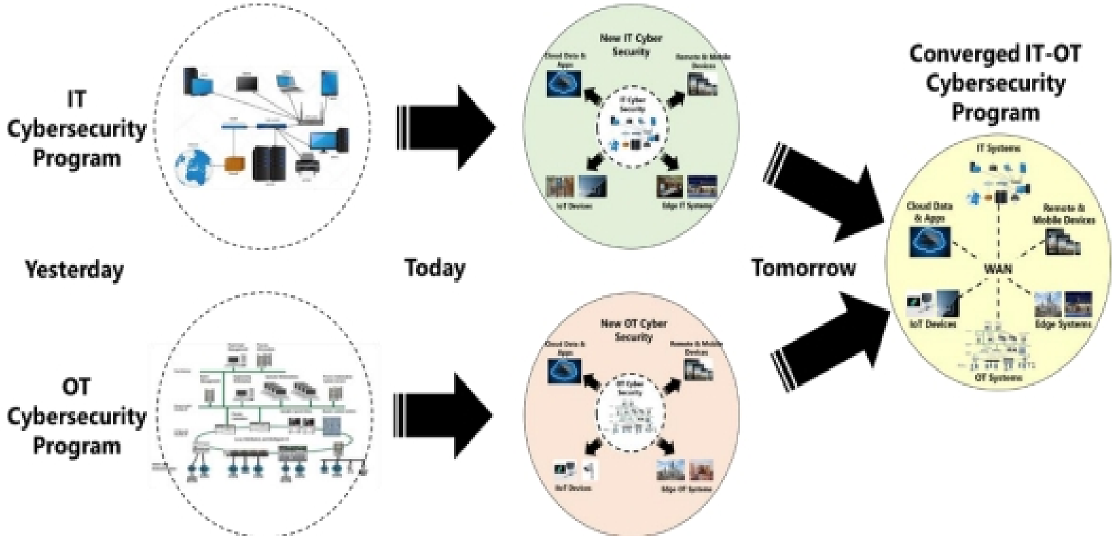
INDUSTRIAL CONTROL SYSTEMS VS IT SYSTEMS

3- A final characteristic of ICS is its long lifespan.

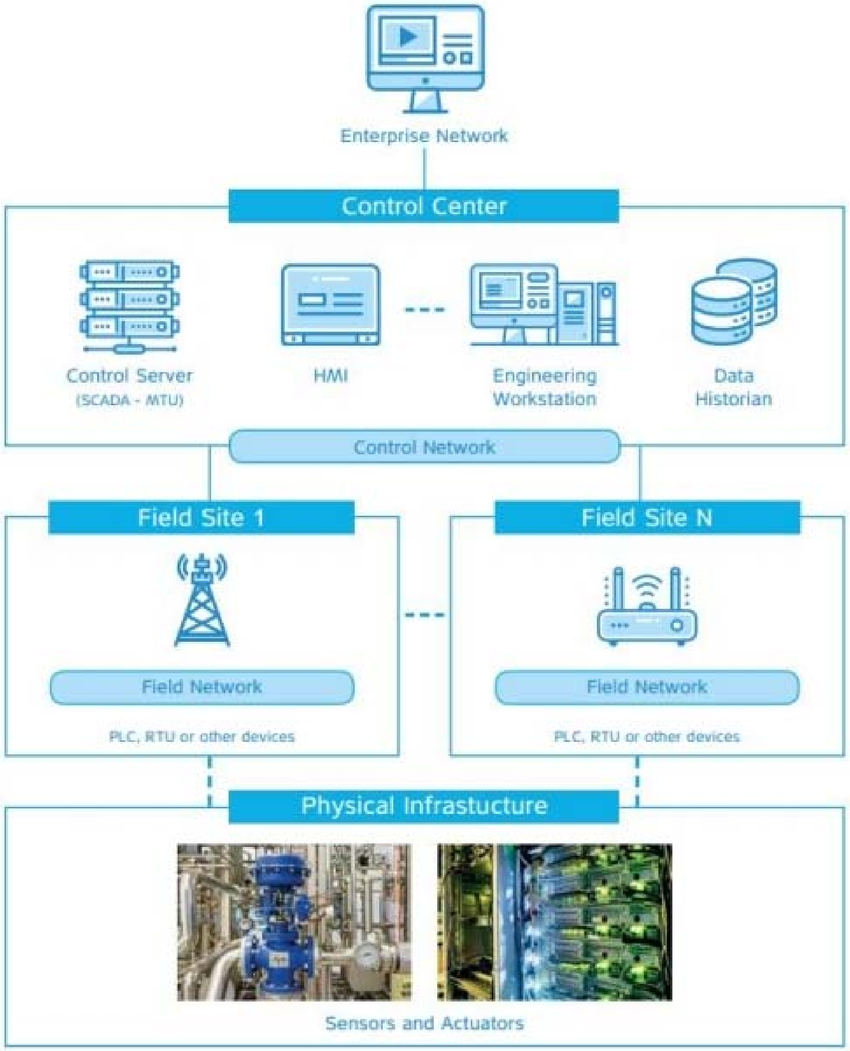
- Whereas regular IT is renewed Every few years, ICS tends to stay in place for decades. One reason is the high cost involved in migration, especially when ICS is at many geographically dispersed field sites. As ICS components have asynchronous lifecycles, a coherent security approach can only be gradually implemented. Most ICS environments and their cyber security, therefore, must cope with legacy. In practice, the opportunity for a coherent cybersecurity approach is often missed when decisions about security requirements for new ICS components are made autonomously in projects and constrained by project budgets.

IT&OT (YESTERDAY-TODAY-TOMORROW)

- The data from these devices are to be collected and analysed by inferring new knowledge both online and offline through data analytics and machine learning techniques. Finally, there is the application layer that implements business. operational decisions based on data acquired and inferred from the devices



IT-OT CYBERSECURITY CONVERGENCE



INTERNET OF THINGS (IOT)

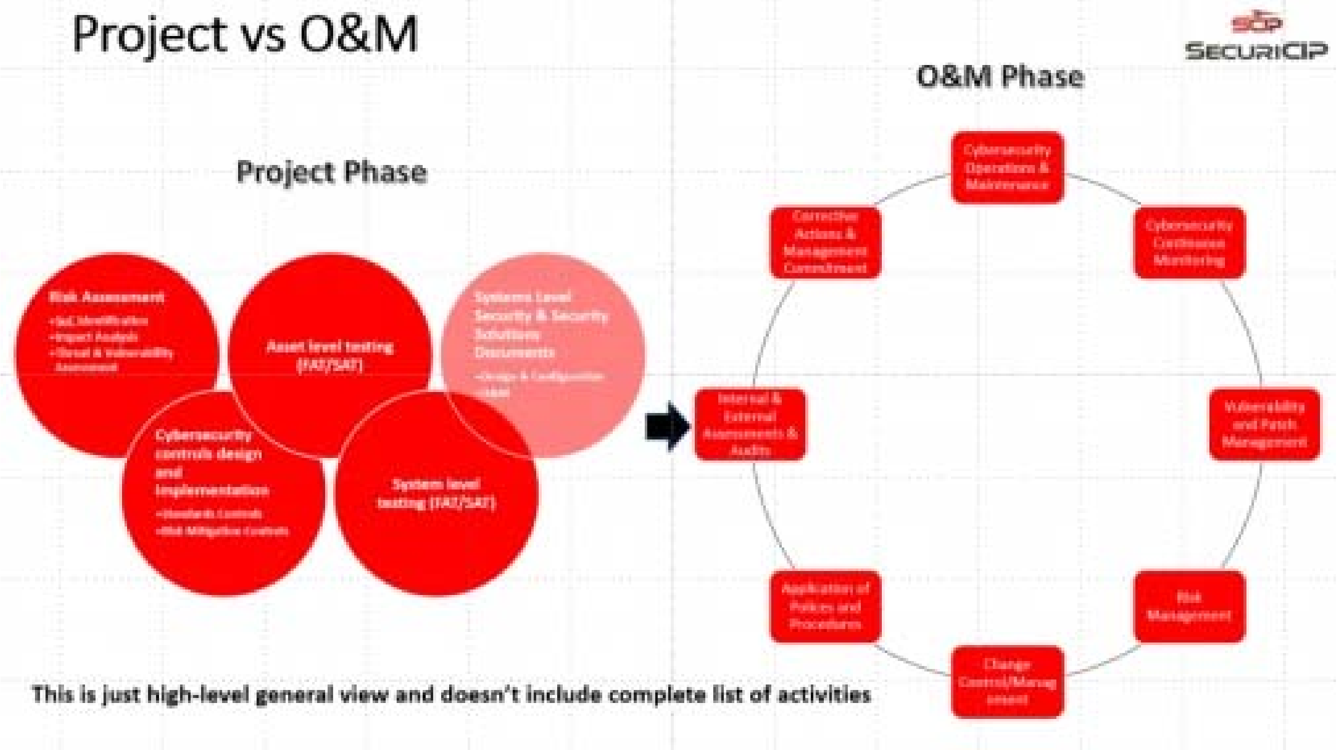
It is described as the physical devices like mobiles, Pc's, home appliances and many more electronic devices that are embedded with sensors, software's and other technologies to transmit the data and to communicate among the devices through the Internet.

For example: air conditioners, sensors, smart watches, mobile phones etc.

INDUSTRIAL INTERNET OF THINGS (IIOT)

It is described as using the internet of things in industrial applications and sectors. The IIOT refers to inter-connected sensors and other networked devices together with computer's industrial mainly used in manufacturing. For example: smart robotics, Air bus etc.

CYBERSECURITY MAINTENANCE



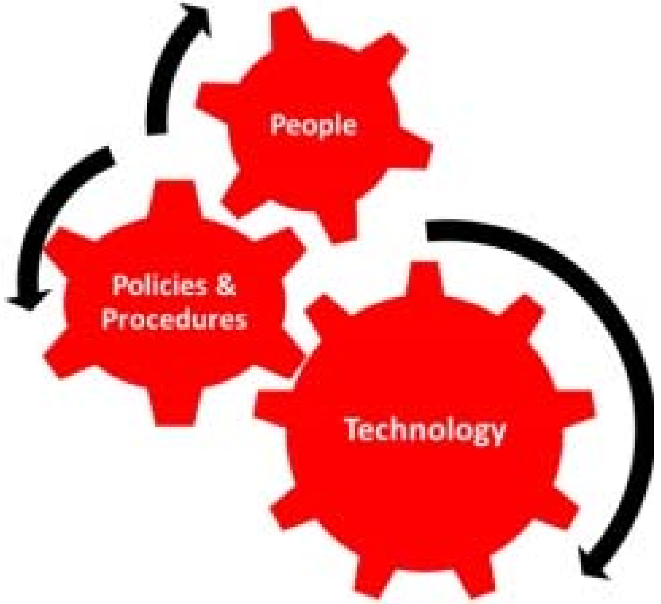
Project vs O&M

SECURICIP
Project Phase
Risk Assessment
•SuC Identification
•Impact Analysis
•Threat & Vulnerability Assessment
Asset level testing (FAT/SAT)
Systems Level Security & Security Solutions Documents
•Design & Configuration
•O&M
Cybersecurity controls design and implementation
•Standards Controls
•Risk Mitigation Controls
System level testing (FAT/SAT)
O&M Phase
Cybersecurity Operations & Maintenance
Cybersecurity Continuous Monitoring
Vulnerability and Patch Management
Risk Management
Change Control/Management
Application of Policies and Procedures
Internal & External Assessments & Audits
Corrective Actions & Management Commitment

This is just high-level general view and doesn't include complete list of activities

CONSIDERATIONS FOR O&M

- Effective cybersecurity is a conscious effort from all individuals that work with or around networked systems. Computerized maintenance management systems (CMMSs), connected controls, O&M personnel information, advanced and smart meters, and building or equipment access are examples of systems considered for O&M cybersecurity.



RECOMMENDATIONS:

1. **Conduct OT/ICS Cyber security risk Assessment to identify cyber security risks & its possible consequences on safety, financial, reputation …etc.**
2. **Ensure Implantation of OT/ICS cyber security Program Consistent with local regulations &International relevant standards to maximize output from People, policies & Procedures, technology.**

SUMMARY

- **Industrial Control Systems (ICS)**

  - What is ICS?

  - Which sectors depend on ICS?

  - Benefits of using ICS

- **Industrial Control Systems vs IT systems**

  - Physical Link

  - Safety Aspect

  - Availability & Integrity vs Confidentiality

  - Realtime requirements

- **Cybersecurity effective O&M for ICS systems**

  - Cybersecurity Operations

  - Cybersecurity Operation Team

  - Cybersecurity Operations Functions

  - Cybersecurity Continuous Monitoring

    1- Supporting Tools

    2- Supporting Procedures

SUMMARY

- Cybersecurity Incident Response

- Cybersecurity Vulnerability & Patch Management

- Cybersecurity Risk

- **Cybersecurity Maintenance**

- Maintaining Security Systems

1- Licenses Tracking and Management

2- Systems regular checks

3- Vendor/supplier support

- Integrating security maintenance activities within system maintenance

1- Security agents on systems

2- Security logs on systems

THANK YOU

ASHRAF SABRY
SECURICIP
Ashraf.sabry@list.ru / +201158555475