ISA/IEC 62443 Compliance Strengthen ICS Cyber Defense

Daniel Ehrenreich,
SCCE - Secure Communications and Control Experts

28-8-2020

……. Presenter Introduction

- 1976 -1990 Tadiran Inc.
- 1991 - 2011 Motorola Ltd
- 2011 - 2013 Siemens Ltd
- 2014 - 2014 Waterfall Security Ltd
- 2014 - SCCE Consulting
- 2014 - SCCE Training
- 2018 - ISO 27001 Auditor

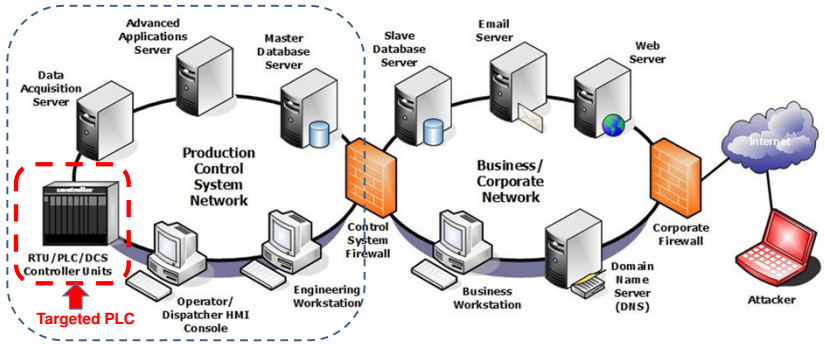
Over 44 years of Industrial Activity

Daniel Ehrenreich
SCCE
Secure Communication and Control Experts
Tel: +972-54-9151594
Daniel@Scce.co.il

Industrial Applications targeted for Cyber attacks

- Targeted Industrial sectors for cyber attacks
  - Chemicals, Oil and Gas
  - Food and Beverage
  - Buildings and Energy
  - Pharmaceuticals
  - Water and sewage
  - Manufacturing
  - Transportation
  - Industrial suppliers
  - Government
  - Public safety

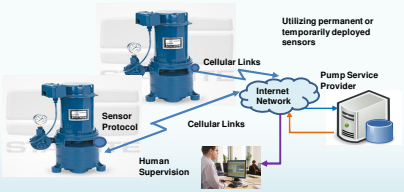
Organization architecture including IT & ICS

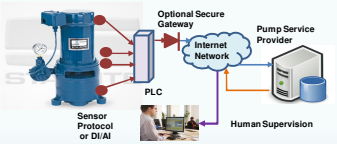


Not permitted for training purposes

Industrial IoT Sensors – Stand alone configuration

- **Ecosystem architecture**
  - Each sensor is acting as an IIoT Endpoint device
- **True cyber risks to industrial operations**
  - Each sensor increase the cyber attack surface
  - The risk are operation outage or damage to the mechanical equipment





The Cyber attack surface comprise of 3 main vectors

- **Internally Generated Cyber Attacks**
  - Start with breaching the physical perimeter
  - Attacker can be: employee, visitor or a hacker

Conducted by:
- Determined attacker
- Disgruntled employee
- Any person by intention
- Unintentional action

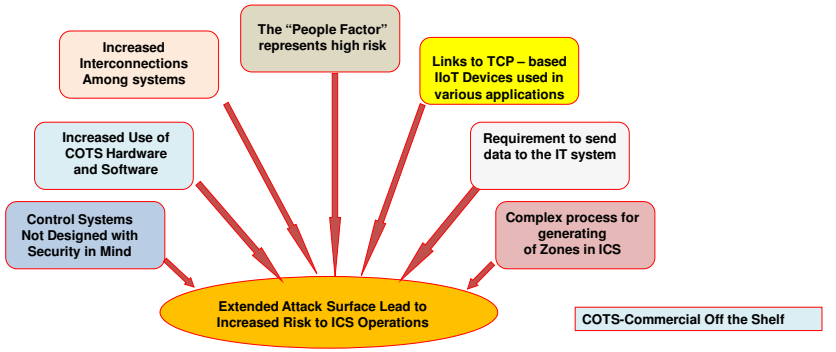
- **Externally Generated Cyber attack**
  - Starts through internet with Social Engineering
  - Gradual compromising of safety barriers
  - May operate 100-200 days prior it is detected

Conducted by:
- Determined attacker
- Disgruntled employee
- Hostile country Action
- Crime action

- **Supply Chain Cyber Attack**
  - Vendors of products and supply services
  - Expert service personnel (in country or abroad)

Conducted by:
- HR Service suppliers
- Vendors of HW and SW
- Servicemen unintentionally
- Intentional-planned attack

ICS-Related Cyber Security Risks and Concerns



Corporate Risk matrix as per ISA/IEC 62443

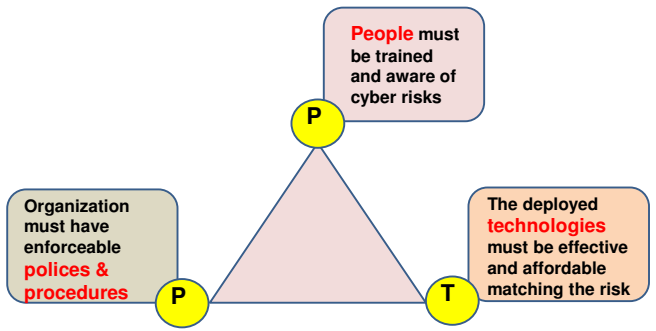
Risk=Likelihood * Impact

Risk = P * I

Impact \ Likelihood	1 Remote	2 Unlikely	3 Possible	4 Likely	5 Certain
1 Trival	1	2	3	4	5
2 Minor	2	4	6	8	10
3 Moderate	3	6	9	12	15
4 Major	4	8	12	16	20
5 Critical	5	10	16	20	25

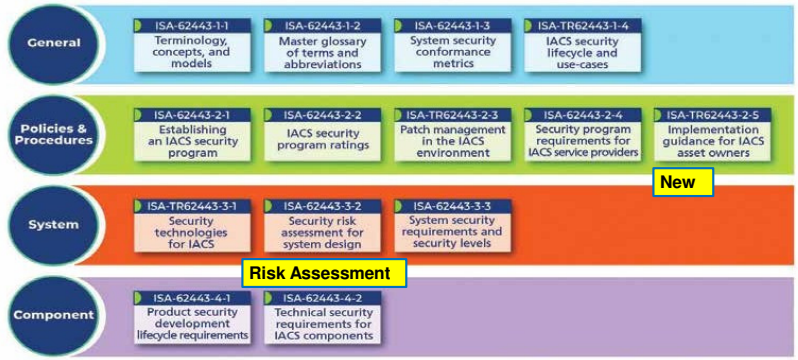
IEC 62443-3-2 Example table for mapping Cyber Risk Reduction Factor to Target Security Level

Cyber Defense through the PPT Triad



9

Risk assessment int he ISA/ICS 62443 Standard 1/2



10

The ISA99 committee created the ISA/IEC 62443 standard

- Constitutes the main international reference framework for cybersecurity related to ICS
  - The Safety, availability and integrity are the most important factors for the adoption of protective measures against cyber threats
- The ISA99 committee that developed the IEC 62443 is composed of owners, equipment and service providers
  - Manufacturers and integrators, governments, educational institutions and various research groups.
- Other international and regional standards and regulations
  - NA: NIST 800-82, 800-53, NIST Framework 1.1, NERC-CIP, etc.
  - Israel: 2 NCD docs and 1 doc of Ministry of Environment Protection

11

The ISA/IEC 62443 key principles

- A "collection of processes, personnel, hardware and software to assure the secure and reliable ICS operation
  - The cybersecurity as an ongoing process and not as goal
  - It requires utilizing "secure-by-design principles" for the ICS
- The key standards in the IEC 62443 series are:
  - IEC 62443-2-4, The policies and practices for system integration
  - IEC 62443-4-1, The secure development lifecycle requirements
  - IEC 62443-4-2, The ICS components security specifications
  - IEC 62443-3-2 Focus on the process of assessing the risk of an ICS
  - IEC 62443-3-3 Defines the security requirements and security levels

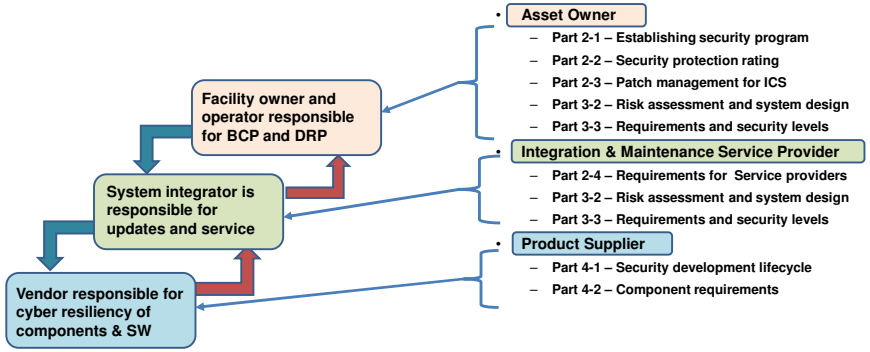
12

ISA/IEC 62443 Standard Security Level (SL)

- **SL 1**
  - Prevent the unauthorized disclosure of information via casual exposure.
- **SL 2**
  - An entity using simple means with low resources, generic skills and low motivation.
- **SL 3**
  - An entity using sophisticated means with moderate resources, specific skills and moderate motivation.
- **SL 4**
  - An entity using sophisticated means with extended resources, specific skills and high motivation.

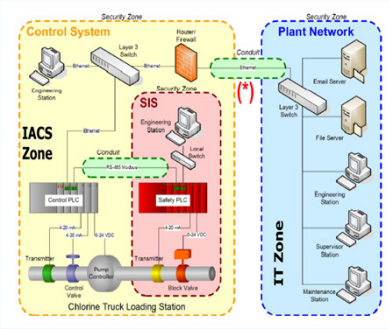
Who Might Attack us?

The cyber defense is achieved by 3 Stakeholders



Addressing ICS Zones and Conduits per ISA/IEC 62443

- **Main principle of Segregation**
  - How different systems interact within the ICS zone
  - Where information flows between systems
  - What form that information takes
  - What data-type devices communicate each to other
  - How fast/often those devices communicate
  - The security differences between system components



ISA/IEC 62443 Series for Asset Owners

- **Asset Owner activities:**
  - Establish a Security Program that includes specific requirements
  - Define the partition of Zones and Conduits
  - Request to conduct Risk Assessments
  - Document ICS requirements in the Cybersecurity Specification
  - Procure the service for a qualified integrator
- **ISA/IEC 62443 standards:**
  - ISA/IEC 62443-2-1, Establishing an ICS security program
  - ISA/IEC 62443-2-2, Security Program ratings
  - ISA/IEC 62443-3-2, Security risk assessment for system design
  - ISA/IEC 62443-3-3, Security risk requirements as per security levels
- **Just to know….**
  - ISA/IEC 62443-2-3, Patch management

ISA/IEC 62443 Series for Integration Providers

- **Service providers activities:**
  - Establish a Security Program for ICS
  - Implement a process that meet the Cybersecurity Requirements Specification (CRS)
  - Apply security patches during the integration phase of the ICS lifecycle
  - Purchase the products and software from qualified vendors
- **ISA/IEC 62443 standards:**
  - ISA/IEC 62443-2-4, Requirements for ICS service providers
  - ISA/IEC 62443-3-2, Security risk assessment for system design
  - ISA/IEC 62443-3-3, System security requirements and security levels
- **Just to know….**
  - ISA/IEC 62443-4-1, Product security development lifecycle requirements
  - ISA/IEC 62443-4-2, Technical security requirements for ICS Components

17

GTACS 2020 ISACA Singapore Chapter

ISA/IEC 62443 for Maintenance Service providers

- **Maintenance service activities:**
  - Establish and sustain a Security Program for maintenance services
  - Provide services and capabilities that meet the ICS security policies
- **ISA/IEC 62443 standards:**
  - ISA/IEC 62443-2-4, Requirements for ICS service providers
- **Just to know….**
  - ISA/IEC 62443-3-3, System security requirements and security levels
  - ISA/IEC 62443-3-2, Security risk assessment for system design

19

GTACS 2020 ISACA Singapore Chapter

ISA/IEC 62443 Series for Product Suppliers

- **Product Suppliers activities:**
  - Establish and sustain a Security Development Lifecycle
  - Provide ICS related software that meet defined SL capabilities
  - Provide Component products that meet the defined SL capabilities
  - Provide ongoing lifecycle support for their ICS related products
- **ISA/IEC 62443 standards:**
  - ISA/IEC 62443-4-1, Product security development lifecycle requirements
  - ISA/IEC 62443-4-2, Technical security requirements for ICS Components
- **Just to know….**
  - ISA/IEC 62443-3-3, System security requirements and security levels

18

GTACS 2020 ISACA Singapore Chapter

Takeaways from this Session

Put Security Goals into your specifications

Deal with Vendors who Take Security Seriously

Do Not Compromise on Security Requirements

Always Be Ready for Tomorrow's Challenges

GTACS 2020 ISACA Singapore Chapter

GTACS 2020 GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY ISACA Singapore Chapter