Your presenter: Glenn A. Merrell, CAP

An **ISA Certified Automation Professional**

INDUSTRIAL CONTROL SYSTEMS SECURITY

Lafayette, CO USA

Mr. Glenn Merrell, CAP is a senior industry consultant applying extensive experience in Industrial Control Systems (ICS), automation, safety, Critical Infrastructure Protection (CIP) and industrial security. Mr. Merrell is an ISA Certified Automation Professional with over 45 years of cutting edge *cross-sector* multi-discipline expertise in industrial control systems, possessing a wide expertise base in real-time control systems including but not limited to electrical, Nuclear Power, instrumentation, process, manufacturing, machine and factory automation / Robotics, Safety Instrumented Systems (SIS), industrial networks, SCADA, ICS Cyber Security and many others.

RISK! (-3-2)

Why you *must* treat "*Operational Technology*" '*Control System*' ***risk*** and *its' SECURITY differently* than *INFORMATION Technology risk*

Virtual

meets

Physical

October 2022

What is Risk? (-1-1)

Within ISA 62443, risk is defined as :

- expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence.

The following are definitions of key terms used in this MLM:

- Threat – 62443 series definition of "risk"
- Vulnerability – 62443: flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy
- Consequence – 62443 definition of "risk"

**(-n-n) are work products that coprise ISA99/IEC62443*

What is Risk, *to you*? (-3-2)

Noun

A situation involving exposure to danger.

Source: Oxford Dictionary

RISK then is a "term of art" when used in different professions or fields or practice, the term holds far different weights of meaning conceptualized / understood by each person.

HOW is Risk determined? (-3-2)

RISK = THREAT Multiplied times Vulnerability Multiplied times Consequence

If any are zero, there is zero risk, *but* …

Risk and Loss: *Cognizance / Awareness*

? When was the last time someone in your organization was killed by a laptop?

If your personnel do not understand – comprehend, and are "cognizant" of **unique risks**,

- they cannot be "aware" of *unique risk "threats" or "consequences"*.

Business aspects discussion

- Within your organization, where does the responsibility for
  - Security live?
  - Safety live?

Risk - in a Business model

- What are your Critical control systems assets?
- HOW does compromise of those assets cause physical risk impacts?

F.A.I.R. tool *(Factor Analysis of Information Risk*, https://www.fairinstitute.org/) relates asset to result of or reduction of loss (ROL) to financial risk

- Links workforce development / cognizance / competency deficiencies to ***loss*** figures 3 *trillion* USD
- Cognizance: awareness – train for total understanding and knowledge of the related risks, tasks and recognizing "*vulnerabilities*".

ISA 99 Scope - *why ANSI/ISA/IEC62443?* *(-1-1)*

"…control systems whose compromise could result in any or all of the following RISK situations: "types of risk" (-3-2)

- "endangerment of public or employee safety" (not covered by IT)
- "environmental protection" (not covered by IT)
- "equipment / infrastructure damage" (not covered by IT)
- "loss of public confidence" (shared concept) but which is MORE VISIBLE, an explosion or virtual bits/bytes
- "loss of Production" risks here are defined by industry
- "violation of regulatory requirements" (only covered by IT in "data" protection")
- "loss of proprietary or confidential information" (shared concept)
- "economic loss" (shared concept) but …"you CANNOT reboot an explosion or death"
- "impact on entity, local, state, or national security" Critical Infrastructure

What is different between IT and OT risk?

Example: "toggle a single binary bit from a value of 1 to 0

- IT Risk (data "CIA") vs.
  - The bit is MSB
    - THE QUANTITY CHANGES FROM

      TRUE TO FALSE -
  - Risk:
    - Someone suddenly gets/looses a lot of money in their bank account
    - Confidentiality and Integrity
  - Typically No death, no dismemberment, no physical injury
  - Restoration
    - Verify program
    - Restore system

- **OT Risk** (*functions* of ***control*** "RRAS")
  - 1 = **safe to enter or open a valve**
  - **0= NOT SAFE TO ENTER or close a valve**
    - ***A safety door, gate or safety function is disabled***
  - **Risks**
    - HIGH PROBABILITY OF **DEATH**, DISMEMBERMENT, INJURY, damage,
    - **S**AFETY
  - Restoration
    - Redundancy, logic state checks, hardened purpose built controllers for reliability – availability - Safety, access level restrictions with MoC, abnormal condition monitoring – *plausibility checks*, specific control functions training

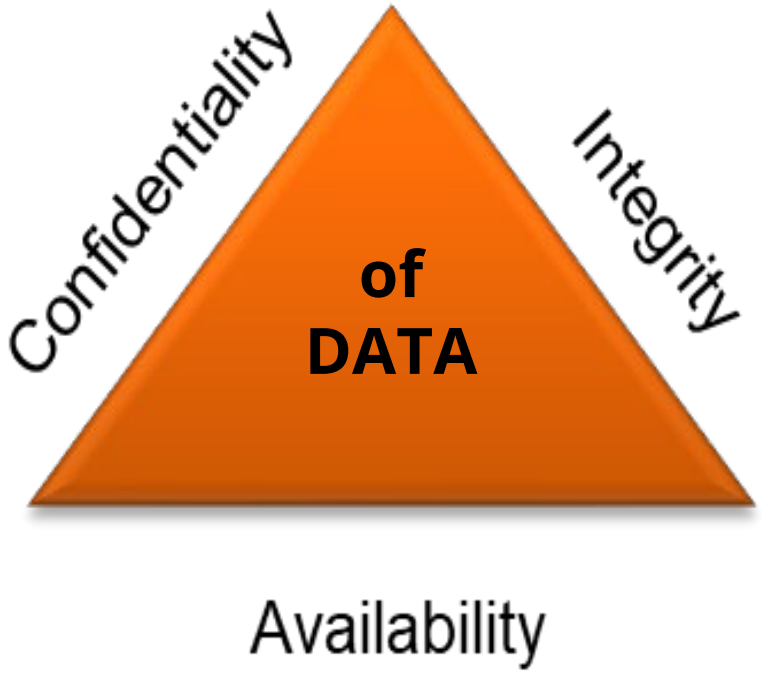
Information Technology Security Triad

IT Cybersecurity is focused on "*Data*" security, an "*INFORMATION*" protection concept

IT Cybersecurity Triad

- **C**onfidentiality
- **I**ntegrity
- **A**vailability
- … *of "Data"* - bits/bytes/files
- Least Privilege
- Role Based

- **IT Security** *may be in fact* ***dangerous*** misapplied to control systems, creating unpredictable results in a Control System Operation – WHY?



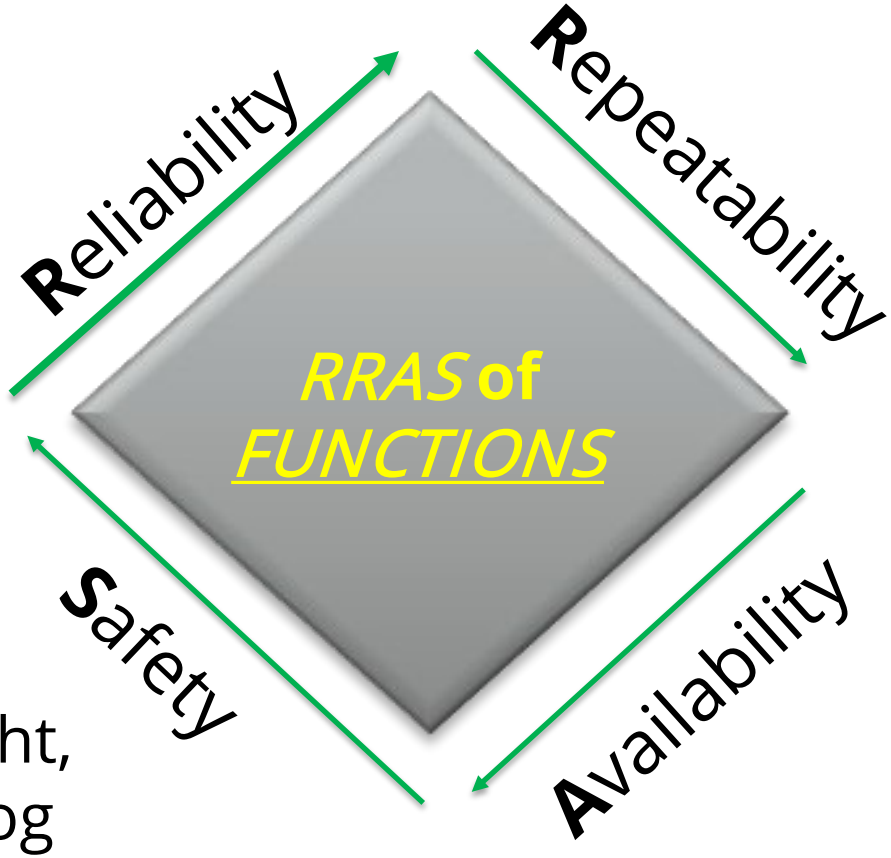
ENGINEERING requires applications of *Physical Sciences*

ENGINEERING is focused on the *Physical Science of functions*

Engineering Resilience Diamond

Reliability
Repeatability
Availability
Safety

*applying **physical** variables*:
Flow, Pressure, Temperature, Level, Acceleration, time-of-flight, distance, speed, position, analog / digital, etc.

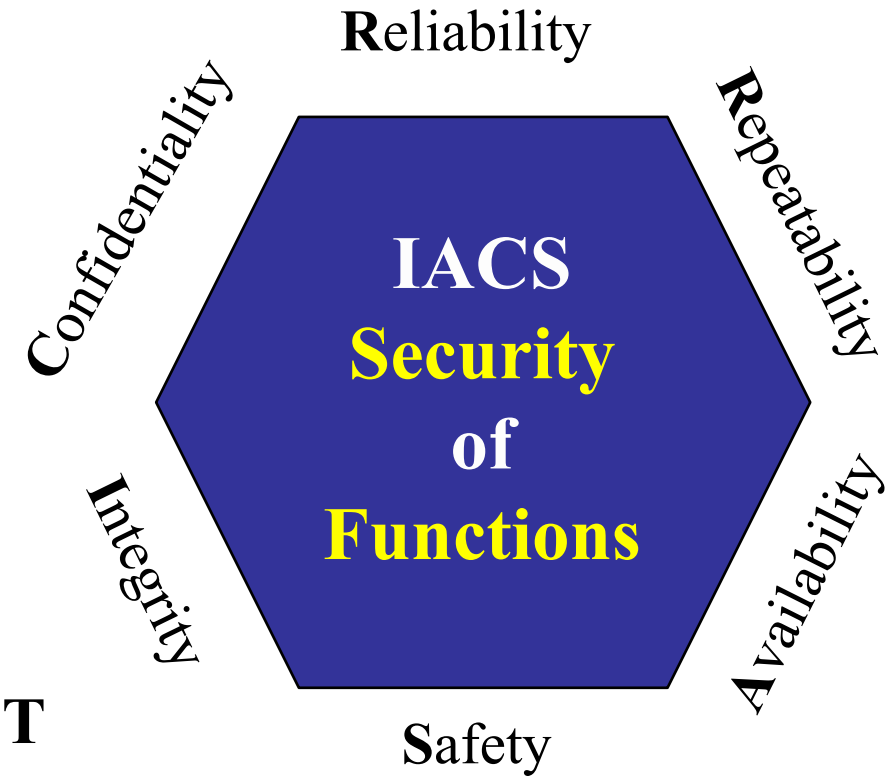


Securing Control Systems requires *ALL considerations, MODIFIED*

Securing **a Control System *requires* guaranteeing the "*as designed*" *FUNCTIONS***

IACS / Control System
Security **Hexagon**
- **R**eliability
- **R**epeatability
- **A**vailability
- **S**afety
- *Role Based*
- *Least Privilege*
- **I**ntegrity
- **C**onfidentiality

of "**CONTROL**" ***functions***,
… *Control is not **data** !* IT ≠ **OT**



Applying Secure-By-Design
Secure Development Life Cycle *to reduce risk*

TRAINING

Requirements

Design

Development

Testing

REVIEW

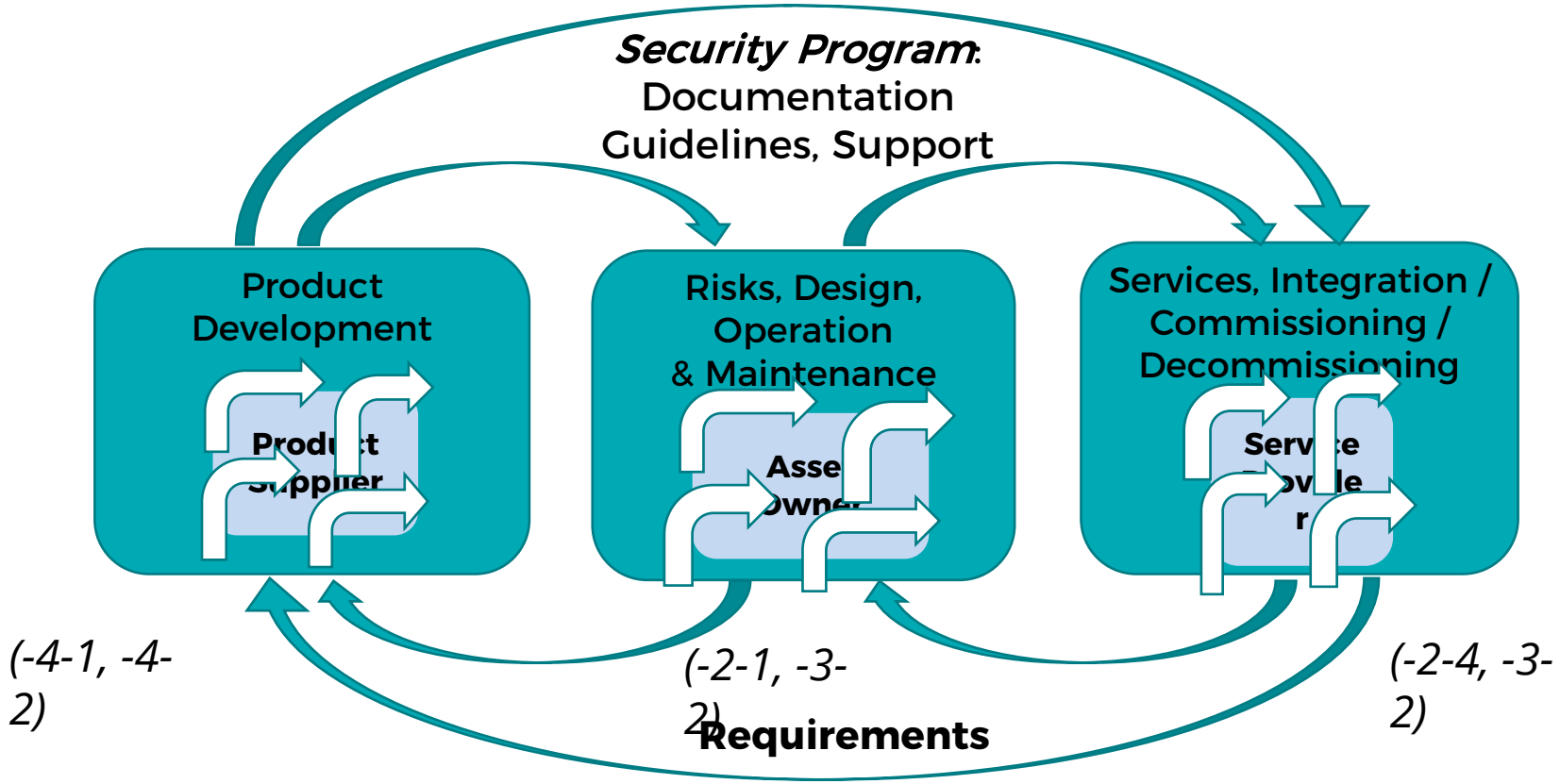
Operate

Maintain

Decommission

Security Life Cycles – an *Iterative* process within a Security Program to reduce *RISKs*

(-1-1, -1-4, -2-1, 2-3, -3-2, -4-1)



* (-n-n) work products that comprise ISA99/IEC62443

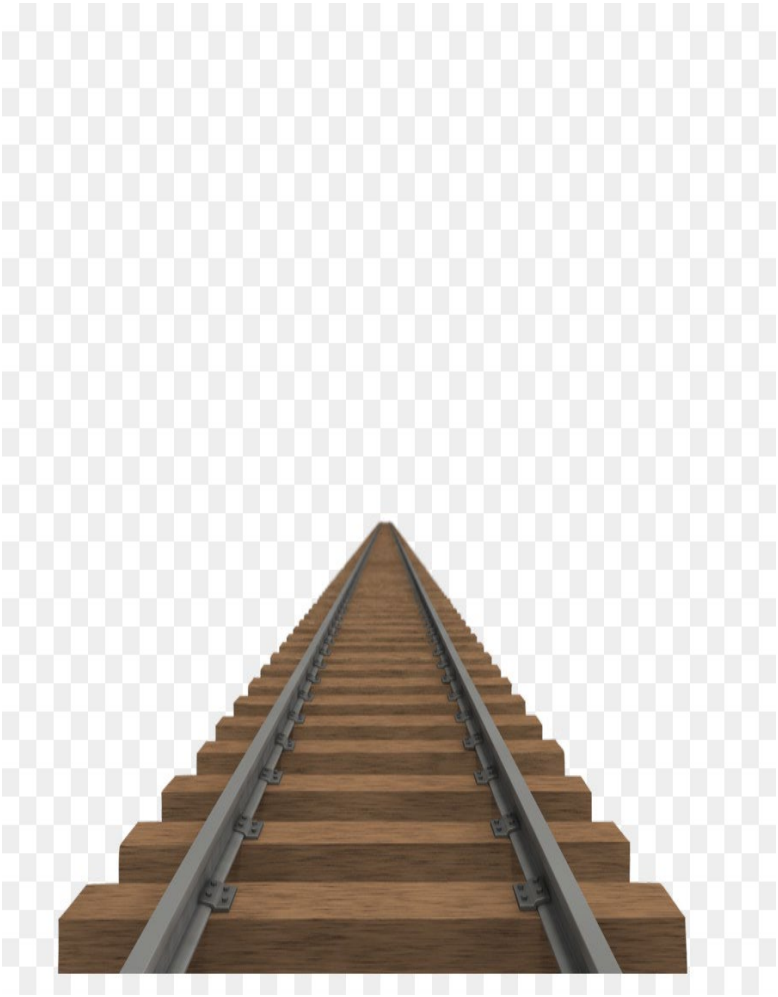
ANSI/ISA TR62443-1-4
Programs, Lifecycles, Use Cases

- **Purpose**
  - Identify the Programs, Lifecycles and Use Cases applied across the standard series
- **Scope**
  - The “how to” application of the standard series through;
- **Construction**
  - *Identifying* requirement groups, relating to
    - Roles referenced in the series;
    - Generic professional titles responsibilities
  - *Identifying* critical actions and deliverables connected to requirement groups, such as
    - *ORG*.n.n specifies that the Organizational parts of a Security Management System for
      - Assembling teams (ORG1.3)
      - TRAINING those teams to be cognizant and competent (ORG1.4)
      - ASSIGNING ROLES AND RESPONSIBILITIES to those trained (ORG1.5)
      - Performing Risk Assessments (ORG2.1)
    - *REFERRING* those ACTIONS and Deliverables “HOW TO’s” to key TARGETED awareness tools
      - Micro Learning Modules
      - Learning Paths
      - Use Cases

***RISK*: Is it Convergence, or *Collaboration*?**

When you envision in your minds-eye a pair of Railway tracks traveling straight towards the horizon, the artists concept of a vanishing point in a disappearing perspective occurs where it appears as though those two parallel tracks meet or "converge" somewhere in the distance.

Many say that IT and OT are "converging" but in reality, the two disciplines, IT and OT are like those railway tracks--- each always remaining precisely parallel to the other in collaboration to support the trains functions of weight, movement and direction. In a collaboration manner then IT and OT are not "converging" but they are always running in parallel while collaborating toward securing asset owner systems functions from risk.



Takeaway key points

- ***Differences in Risk*** must be mitigated differently deploying a properly trained and risk aware team;
- ***Mitigation of ICS / IACS RISKs also requires unique CONTROL SYSTEM training***
- ANSI/ISA TR62443-1-4 Programs, Lifecycles, Use Cases targets the how-to linking
  - **M**icro **L**earning **M**odules to build the Concepts in the Standard
  - ***Learning Paths*** to various organizational types and personnel titles
  - ***Use Cases*** directly to ANSI/ISA/IEC62443 series requirements
  - **FOCUSED Training** encompassing the necessary Control System knowledge is CRITICAL

Further Information

Related MLMs

- MLM-018-B, IACS Cybersecurity Risk Management Concepts
- MLM-018-C, IACS Cybersecurity Risk Mitigation

References

- Requirements in ISA/IEC 62443-3-2 Risk
- ISA Micro Learning Modules Series
- ISA99 62443 use case examples
- Third-party articles, standards, papers, etc.

Please click here to provide feedback on this module.

Continue your learning journey with these related resources from ISA.

- ANSI/ISA/IEC62443 Security for Industrial Automation Control Systems
- ISA99 White Papers
- ISA GCA White Papers and Articles
  https://isaautomation.isa.org/cybersecurity-alliance/

- ISA/IEC62443 Cybersecurity Certificate training IC32, IC33, IC34, IC37

ISA Global Cybersecurity Alliance is a collaborative forum to advance cybersecurity awareness, education, readiness, and knowledge sharing. Learn more

Credits

Role	Contributor
Author	Glenn A. Merrell, CAP
Subject matter experts	Glenn A. Merrell, CAP
Editor	Glenn A. Merrell, CAP
Reviewers	
Instructional designer	
Originating work group co-chair	