Don't Overshoot Your Target Security Level

Understanding ISA 62443 Security Levels and Mitigating Business Risks

Alan J. Raveling

OT Security Architect

Areas of Expertise

- OT Cybersecurity Assessments
- Infrastructure Design
- Risk Mitigation Strategies
- Training and Program Development

Industry Vertical Experiences

- Consumer Manufactured Goods
- Value-Added Agriculture
- Pharmaceuticals
- Automotive

Certifications | ISA 62443 Cybersecurity Expert | CISSP |GICSP | VCP DCV

Education | B.S. Computer Science | M.S. Cybersecurity | DCS – Cybersecurity & Information Assurance

ISASecure®

INTERSTATES

Today's **Game Plan**

During the next 45 minutes, we will cover...

- Introduction to ISA/IEC 62443 - Zones & Security Levels
- Benefits & Considerations of Levels
- Selecting the Correct Level(s) for Your Facility
- Summary and Takeaways

ISASecure®

INTERSTATES

What is **ISA / IEC 62443**?

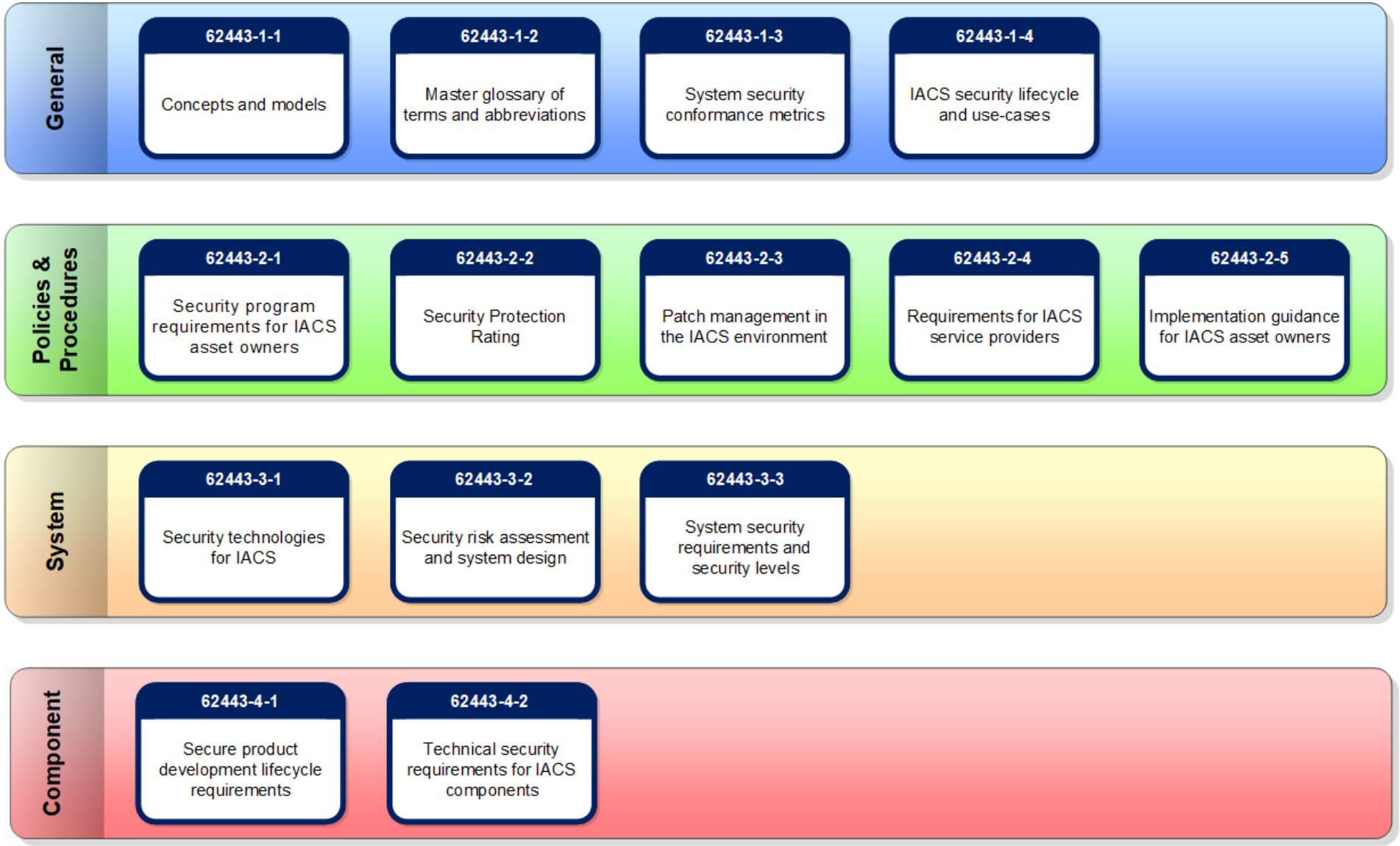
Provide guidance that includes:

- Defining common terms, concepts, and models that can be used by all stakeholders responsible for control systems cybersecurity
- Helping asset owners determine the level of security required to meet their unique business and risk needs
- Establishing a common set of requirements and a cybersecurity lifecycle methodology for product developers, including a mechanism to certify products and vendor development processes
- Defining the risk assessment processes that are critical to protecting control systems

ISASecure®

INTERSTATES

What is **ISA / IEC 62443**?



What is a **Security Level?**

A measure of confidence that the System Under Consideration, Zone, or Conduit is free from vulnerabilities and functions in the intended manner.

Part 3-3 further defines the Security Level in terms of the means, resources, skills, and motivation of the threat actor.

Security Level Use: It is used as a means to discriminate between requirement enhancements for systems (Part 3-3) and Components (Part 4-2).

There are three types of Security Levels that are used throughout the ISA/IEC 62443 Series:
Capability Security Levels (SL-C) | Target Security Levels (SL-T) | Achieved Security Levels (SL-A)

ISASecure®

INTERSTATES

ISA / IEC 62443 Security Levels

Security Level	Attack Type			
	Violation Type	*Means type*	*Resource Level*	*Motivation*
SL-1	Coincidental	N/A	N/A	N/A
SL-2	Intentional	Simple	Low	Low
SL-3	Intentional	Sophisticated	Moderate	Moderate
SL-4	Intentional	Sophisticated	Extended	High

- ISA Security Compliance Institute (ISCI) is now recommending that suppliers certify to level 2 or higher. ISCI SL-1 certifications still ensures that the supplier's Software Development Lifecycle is at maturity level 3 or higher.
- OPAF (Open Process Automation Forum) standardized on level 2 or higher for their OPA Specification.

ISASecure®

INTERSTATES

62443 Zones & Conduits

ZONES

Grouping of logical or physical assets based upon risk or other criteria such as criticality of assets, operational function, physical or logical location, required access, or responsible organization.

CONDUITS

Logical grouping of communication channels that share common security requirements connecting two or more zones.

RISK ASSESSMENT PROCESS

A key step is to partition the System Under Consideration into separate Zones and Conduits.
The intent is to identify those assets which share common security characteristics in order to establish a set of common security requirements that reduce cybersecurity risk.

ISA / IEC 62443 Security Levels

- Not all IACS zones within a facility or organization need to be at the same Security Level
- Moving between zones with different Security Levels is allowed but focus should be given to these data and communication conduits
- Getting alignment on the desired Security Level from all stakeholders is important when developing a plan to address gaps and remediate issues

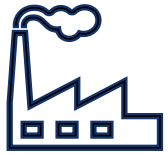
ISASecure®

INTERSTATES

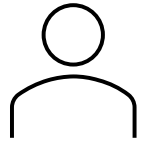
What Should You Consider When Determining Risk?

Consequences

Threats



Industry Vertical



Clients

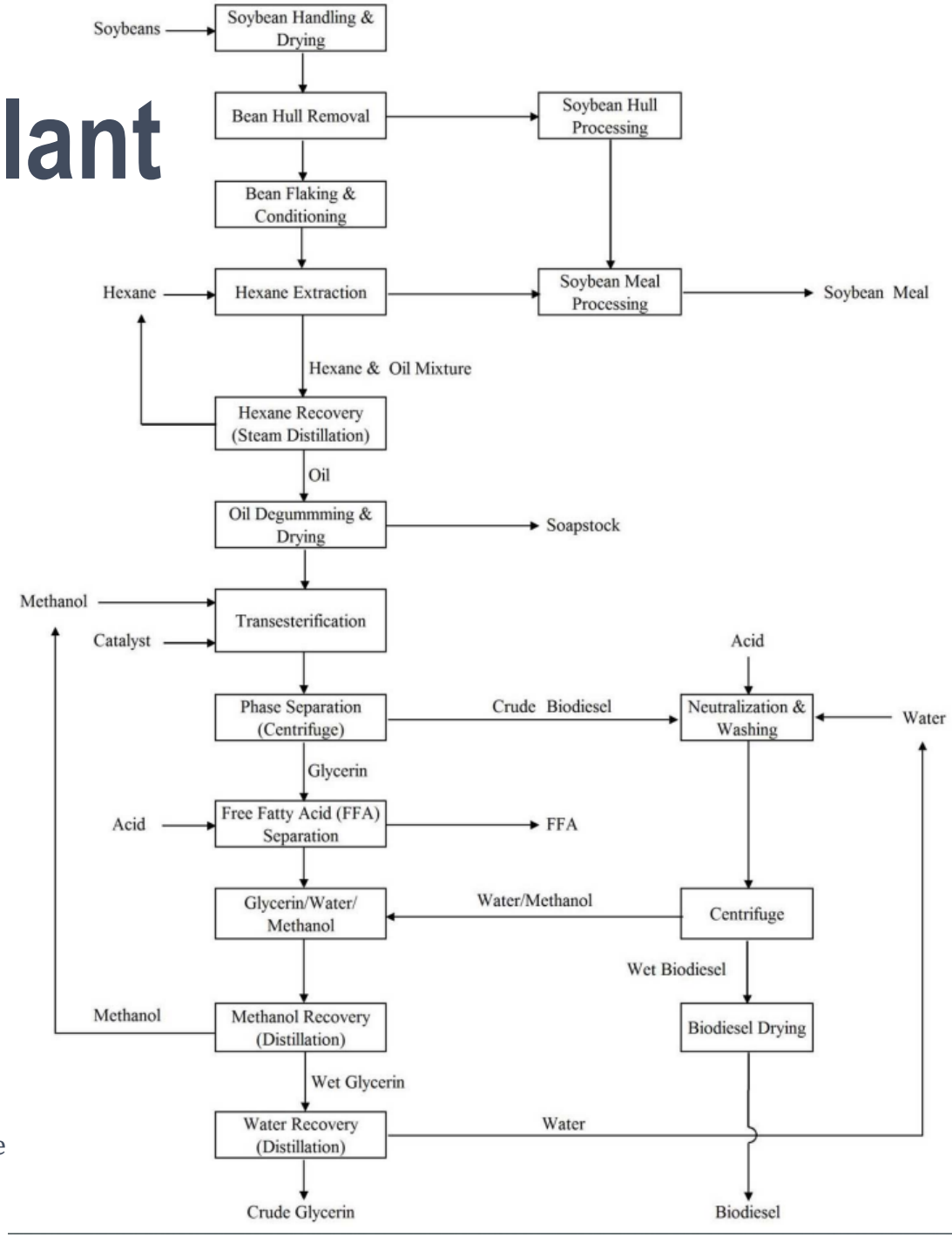
1. What's the worst-case consequence of a successful IACS attack?
2. What threats have industry peers experienced or discussed?
3. What is the industry vertical of the organization?
4. What clients or customers is the organization serving?

ISASecure®

INTERSTATES

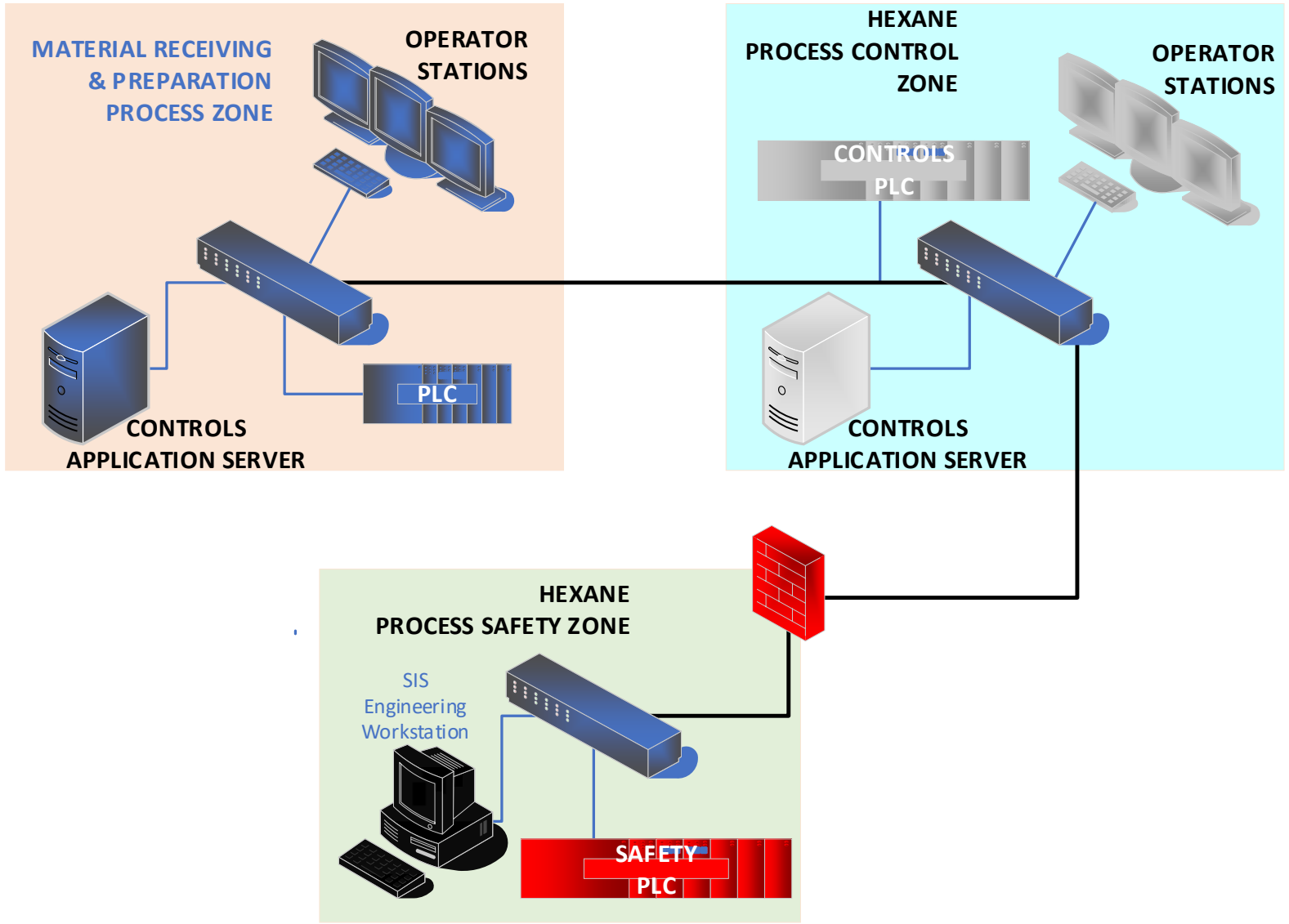
Case Study – **Biodiesel Plant**

- Complex process with many steps
- Many steps are very low risk / simple action
- Some steps involved very hazardous processes
- Breaking down into multiple zones will help right-size the Security Level to be applied in each part of the process



A. Pradhan, D. S. Shrestha, A. McAloon, W. Yee, M. Haas, & J. A. Duffield. (2011). Energy life-cycle assessment of soybean biodiesel revisited. *Transactions of the ASABE*, *54*(3), 1031-1039. https://doi.org/10.13031/2013.37088

Create **IACS Zones** from Physical Processes



Case Study – **Biodiesel Plant**

Examples of real consequences | (not cybersecurity related)

Explosions

La Rioja, Spain - May 26, 2022 – two killed

Dieppe, France – February 17, 2018 – two killed, eleven injured

New Albany, Mississippi - January 22, 2014 - complete destruction

Fires

Orange Mound, Tennessee - March 18, 2016 – nearby home evacuations

Claypool, Indiana – February 15, 2022 – minimal damage

ISASecure®

INTERSTATES

Determining Low / Medium / High Consequences

	Health Safety Environment		
Category	**People onsite**	**People offsite**	**Environment**
A (High)	Fatality	Fatality or major community incident	Citation by regional agency or long-term significant damage over large area
B (Medium)	Loss of work day or major injury	Complaints or local community impact	Citation by local agency
C (Low)	First aid or recordable injury	No complaints	Small, contained release below reportable limits

Excerpt from ISA/IEC 62443-3-2:2020 Annex B Table B.3

- Similar tables exist for Operational and Financial consequences
- Determining the correct choices will require collaboration with many parts of the organization
- Exercise is an excellent opportunity to discuss organizational risks and risk tolerance levels

ISASecure®

INTERSTATES

From Risk Levels to **Security Levels**

- Converting identified risk level to 62443 Security Level is not a one-size-fits-all formula
- Organizations should strive to create a mapping which can be applied across entire IACS
- Different organizations may have different levels of risk tolerance due to industry or physical location
- Assess if the requirements associated with a security level lower identified risk to tolerable level

Example Mapping

Risk Level	62443 Security Level
Low	SL-1
Medium Low	SL-2
Medium	SL-3
Anything Above Medium	SL-4

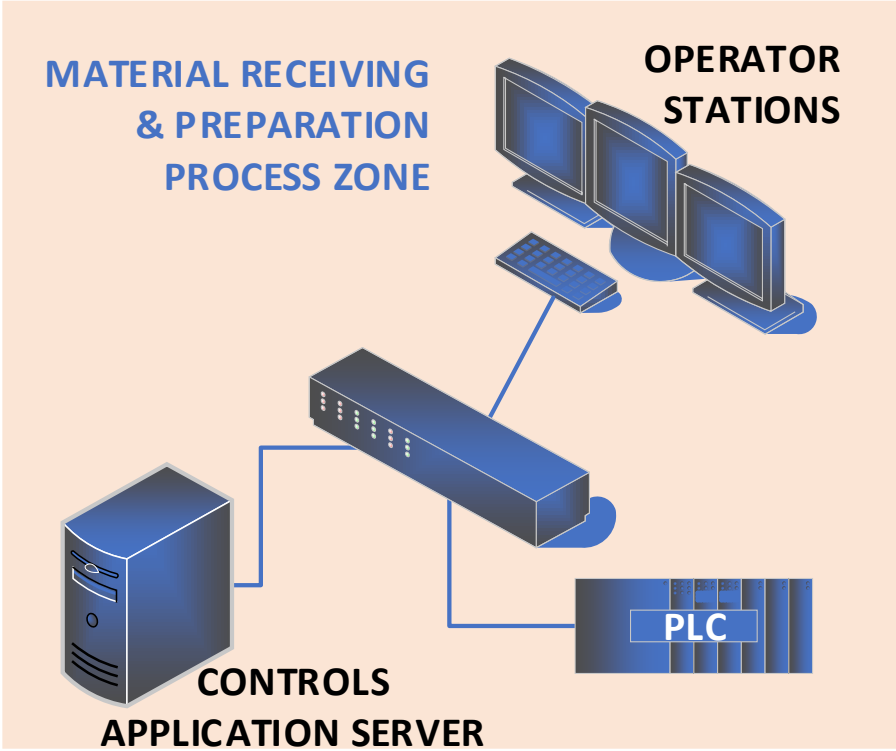
ISASecure®

INTERSTATES

Case Study – Biodiesel Plant

Which Security Level is applicable?

- ✓ Perform risk assessment
  - Low risk
  - Minimal consequences
- ✓ Determine 62443 Security Level
  - SL1



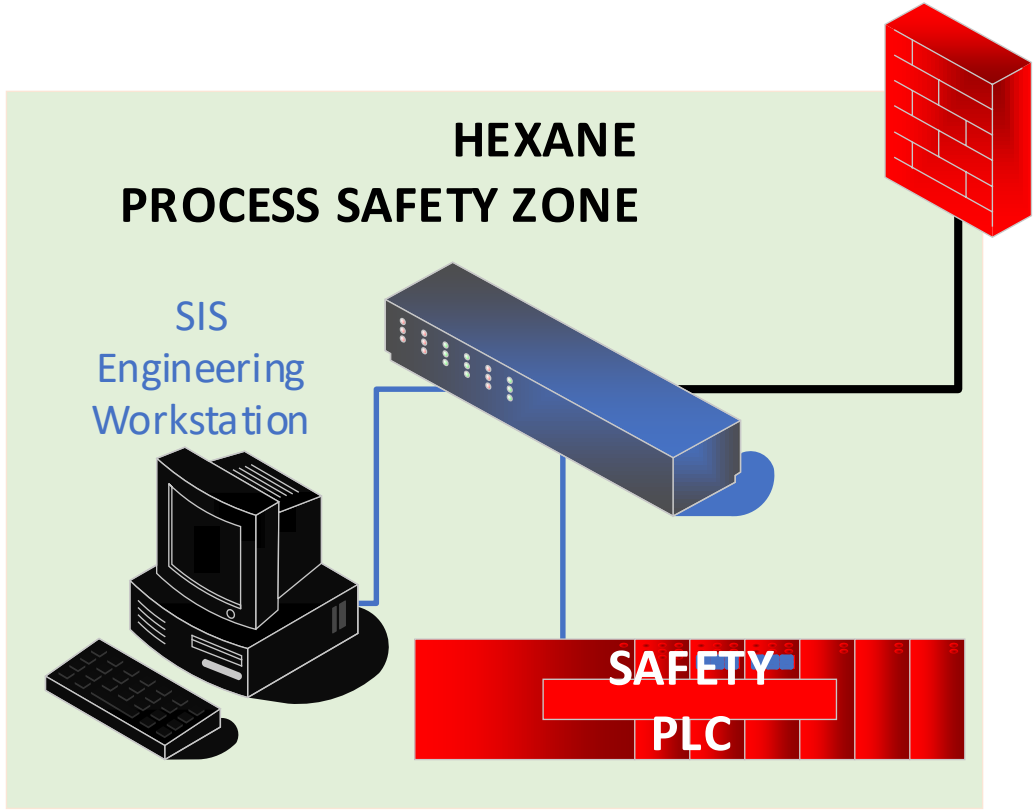
ISASecure®

INTERSTATES

Case Study – Biodiesel Plant

Which Security Level is applicable?

- ✓ Perform risk assessment
  - High risk
  - Significant consequences
- ✓ Determine 62443 Security Level
  - SL4



ISASecure®

INTERSTATES

Examples of Security Requirements **Escalation**

Identity & Access Management		
Different levels of capability / permissions	Named accounts for each individual to enable logging and accountability	Mandatory role-based access to defined IACS resources

Endpoint Protection		
Prevent malware from executing	Only allow pre-approved applications to execute	Systems are hardened to defend against advanced attack techniques

Refer to the Foundational Requirements section of 62443-3-3 for additional details

ISASecure®

INTERSTATES

Overshooting Your **Target**

Why not make the entire IACS the same Security Level?

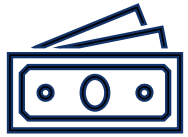
Resources

- Expending resources to address unrealistic risks
- May require training/education that is not relevant to job responsibilities

Effectiveness

- Trying to take on too many controls may lead to poor implementation
- Personnel ignore controls when they are overkill and eventually, everywhere (crying wolf)

Costs



- TCO increases due to elevated ongoing support / maintenance
- Initial project costs increase due to additional time by vendors to implement & procurement of hardware / software which can meet required security level

ISASecure®

INTERSTATES

Overshooting Your **Target**

Consequences of higher Security Level

Time to Resolution

- Change management takes longer due to additional checks, review, and additional approvals necessary to align with requirements
- Troubleshooting may take longer if technicians do not have required access on pre-approved devices

Future Upgrades / Expansions

- Carrying security requirements forward may unduly increase future project costs
- Choices in vendors, integrators, and equipment may be artificially restricted to those which can meet security requirements

ISASecure®

INTERSTATES

In **Summary**

- ISA / IEC 62443 Security Levels help organizations protect themselves against different classifications of threats and risks
- Organizations should evaluate their facilities to determine the risks associated with each zone
- Work with all stakeholders to align on the Security Level which best aligns with the real risks, potential threats, and resource costs

ISASecure®

INTERSTATES

Key **Take Aways**

- Determine the current Security Level and compare against the Target Security Level to create plans which remediate any gaps
- Re-evaluate the desired Security Level as changes in the technology and facility processes occur
- Ensure your personnel receive the proper training and education to ensure a mastery of the ISA / IEC 62443 concepts and materials

ISASecure®

INTERSTATES

CONNECT WITH **US**

www.facebook.com/InterstatesCo

www.linkedin.com/company/interstates

@InterstatesCo


ISASecure®


INTERSTATES