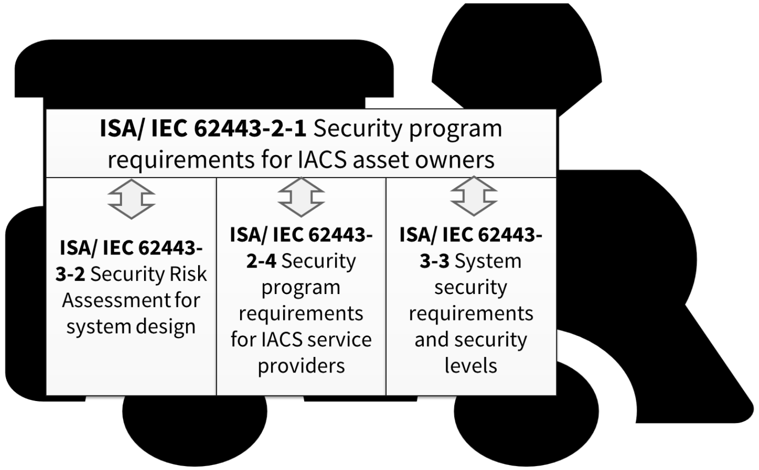
All Aboard the ACSSA, First Stop – Risk Assessment

Patrick C. O’Brien, CFSP, CACS

- Assistant Director of Engineering
- B.S. Chemical Engineering from Pennsylvania State University
- Experience in various roles supporting:
  - Cybersecurity Consulting
  - Process Safety Consulting
  - Machine Safety Consulting
- Coauthor: *Implementing IEC 62443: A Pragmatic Approach to Cybersecurity*
- Project Leader: *Managing Cybersecurity in the Process Industry- A Risk-based Approach*
- *Member of ISA Global Cybersecurity Alliance*
- pobrien@exida.com

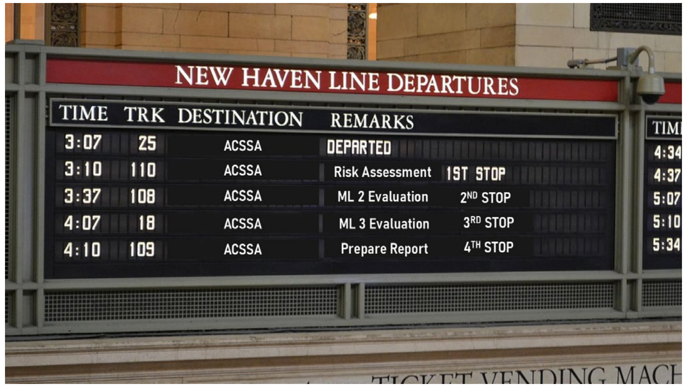
This presentation will introduce ACSSA, cybersecurity risk assessments, and the best ways to get started.



ISA/ IEC 62443-2-1 Security program requirements for IACS asset owners

ISA/ IEC 62443-3-2 Security Risk Assessment for system design	**ISA/ IEC 62443-2-4** Security program requirements for IACS service providers	**ISA/ IEC 62443-3-3** System security requirements and security levels

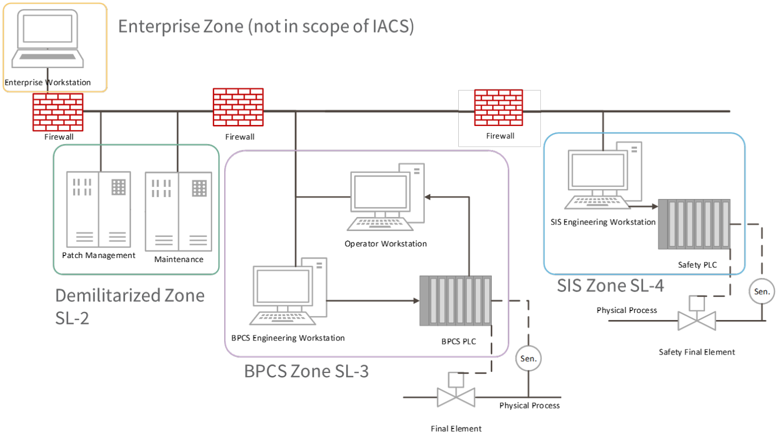
What is ACSSA?



NEW HAVEN LINE DEPARTURES

TIME	TRK	DESTINATION	REMARKS
3:07	25	ACSSA	DEPARTED
3:10	110	ACSSA	Risk Assessment 1ST STOP
3:37	108	ACSSA	ML 2 Evaluation 2ND STOP
4:07	18	ACSSA	ML 3 Evaluation 3RD STOP
4:10	109	ACSSA	Prepare Report 4TH STOP

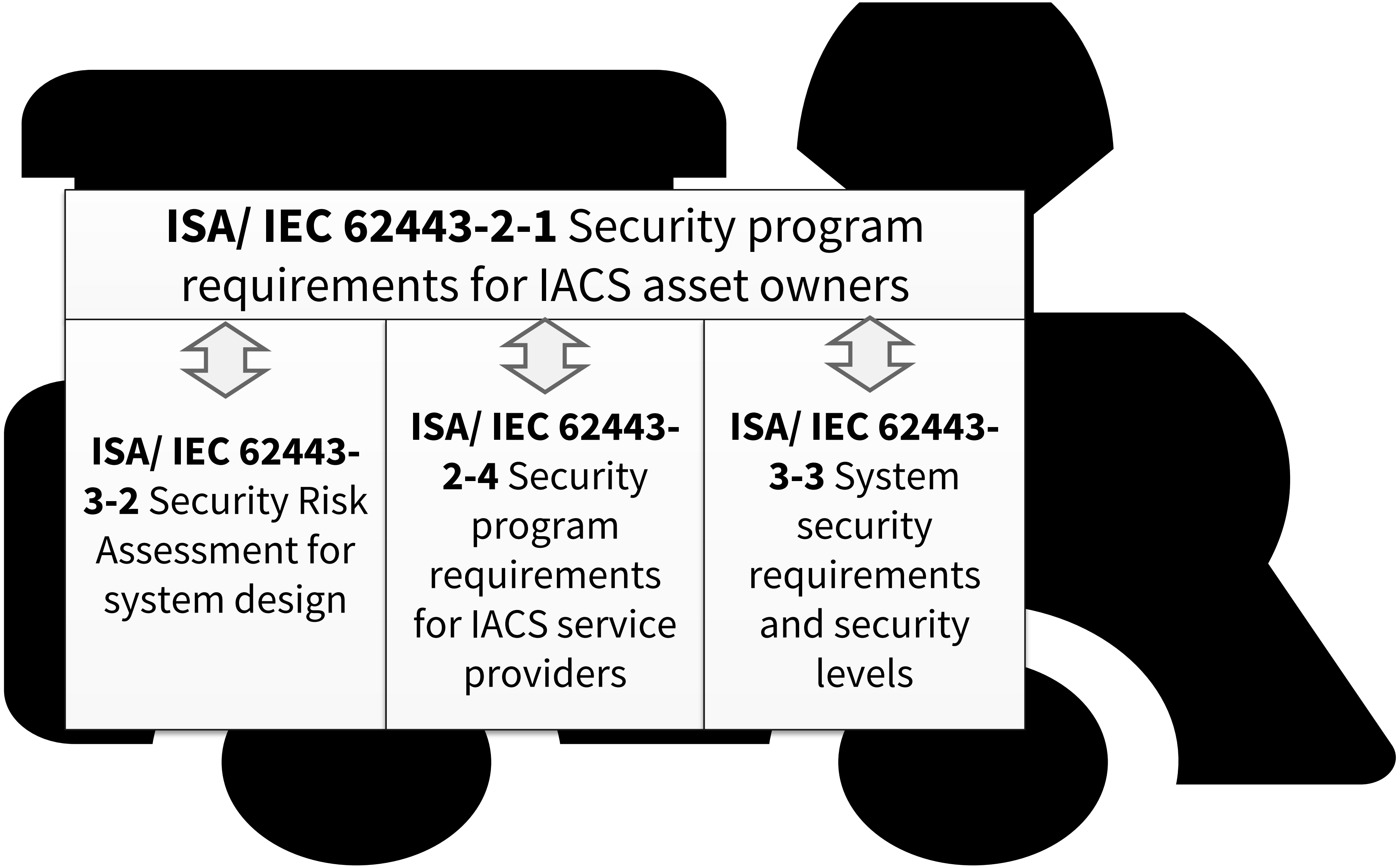
Why is the risk assessment the first step towards ACSSA?



What are the steps in a Cybersecurity Risk Assessment?

Automation and Control System Security Assurance (ACSSA)

ACSSA Standards



ISA/ IEC 62443-2-1 Security program requirements for IACS asset owners

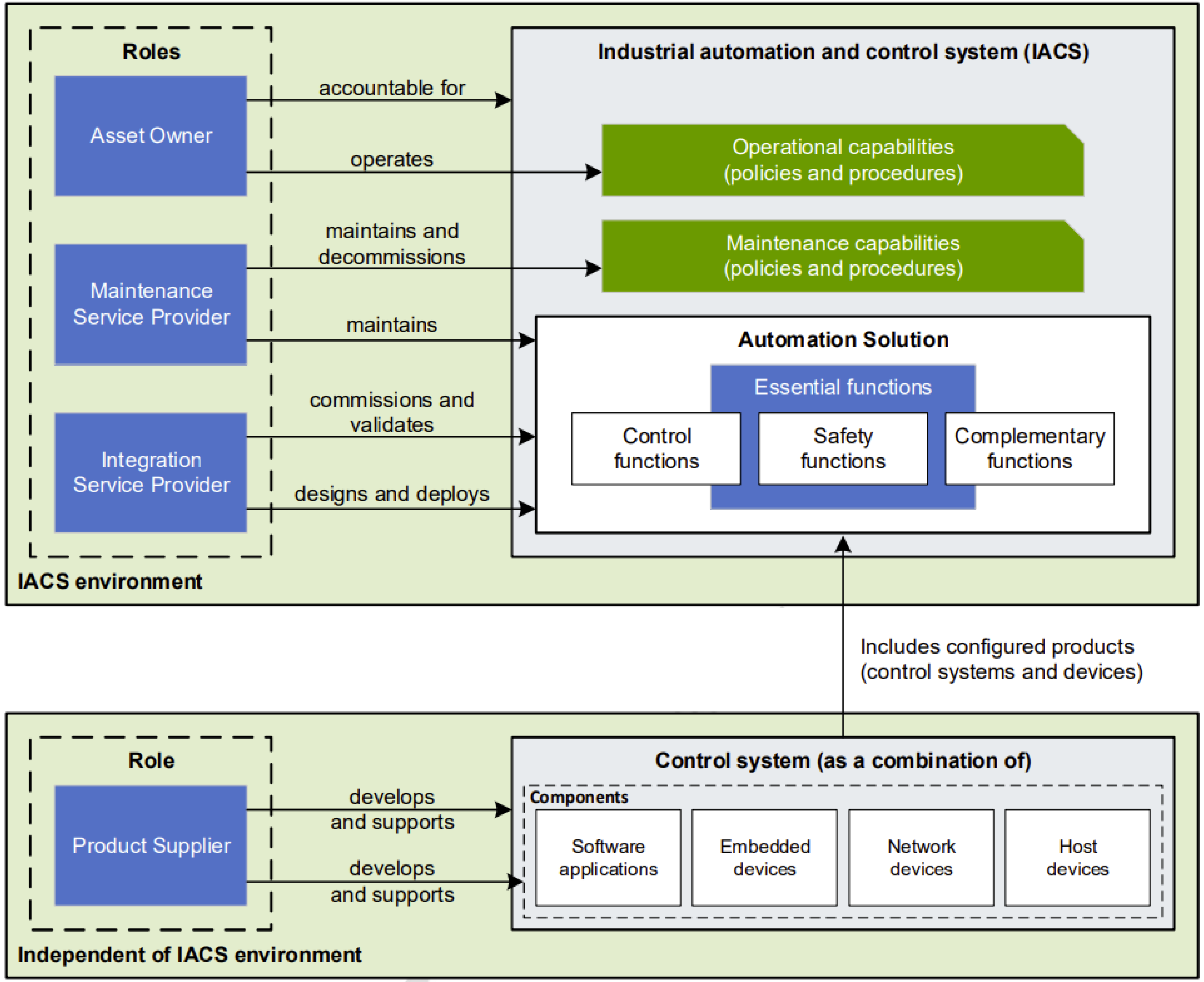
ISA/ IEC 62443-3-2 Security Risk Assessment for system design

ISA/ IEC 62443-2-4 Security program requirements for IACS service providers

ISA/ IEC 62443-3-3 System security requirements and security levels

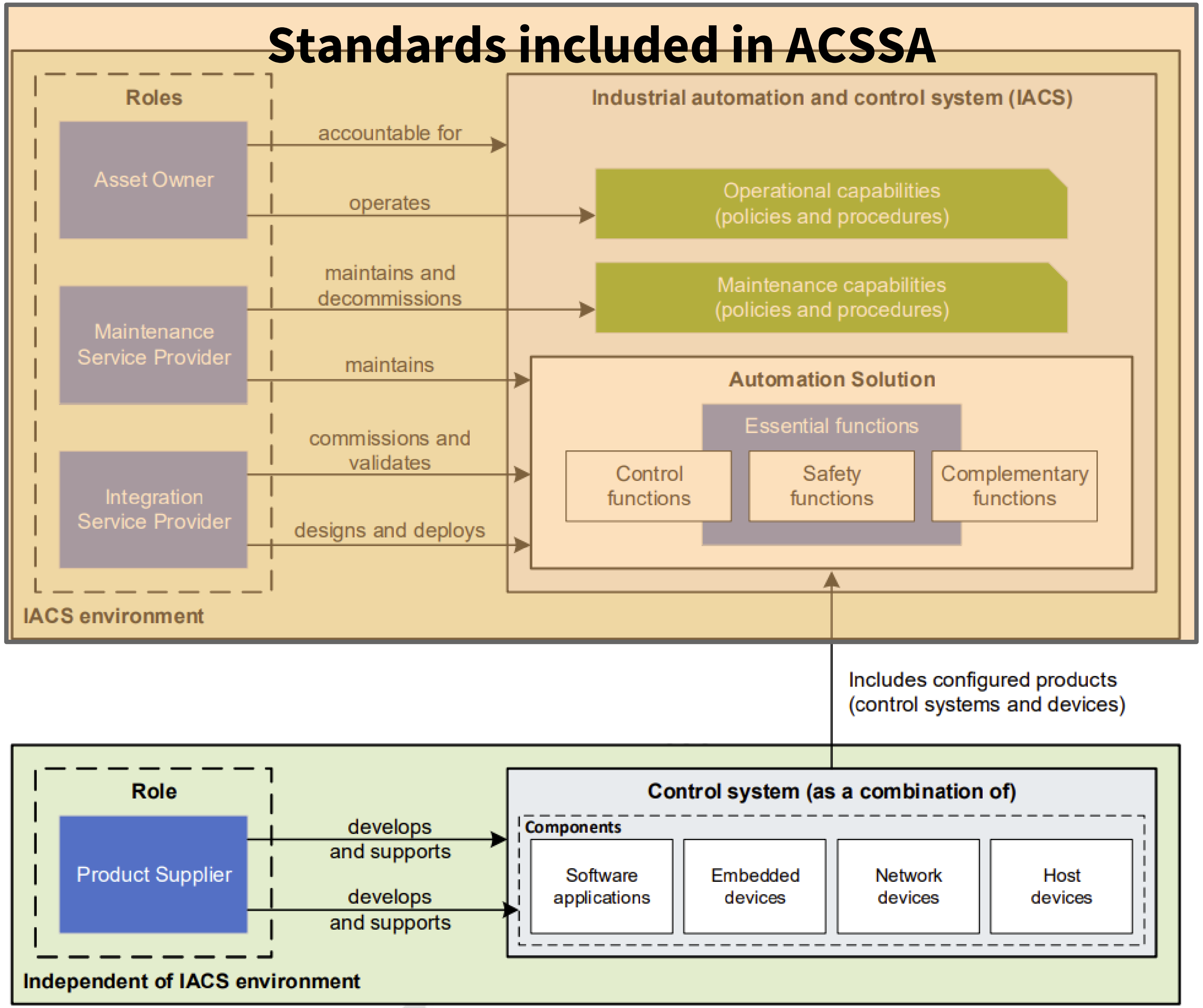
Adapted From: ACSSA 100 Figure 1

Logical view of ISA/ IEC 62443 Standards


Roles
Asset Owner
Maintenance Service Provider
Integration Service Provider
accountable for
operates
maintains and decommissions
maintains
commissions and validates
designs and deploys
Industrial automation and control system (IACS)
Operational capabilities (policies and procedures)
Maintenance capabilities (policies and procedures)
Automation Solution
Essential functions
Control functions
Safety functions
Complementary functions
IACS environment
Includes configured products (control systems and devices)
Role
Product Supplier
develops and supports
develops and supports
Control system (as a combination of)
Components
Software applications
Embedded devices
Network devices
Host devices
Independent of IACS environment

Excerpted From: ACSSA 101 Figure 1

Logical view of ISA/ IEC 62443 Standards



Standards included in ACSSA
Roles
Asset Owner
Maintenance Service Provider
Integration Service Provider
accountable for
operates
maintains and decommissions
maintains
commissions and validates
designs and deploys
Industrial automation and control system (IACS)
Operational capabilities (policies and procedures)
Maintenance capabilities (policies and procedures)
Automation Solution
Essential functions
Control functions
Safety functions
Complementary functions
IACS environment
Includes configured products (control systems and devices)
Role
Product Supplier
develops and supports
develops and supports
Control system (as a combination of)
Components
Software applications
Embedded devices
Network devices
Host devices
Independent of IACS environment

Excerpted From: ACSSA 101 Figure 1

Eligibility for ACSSA

- IACS is in operation or “Near transition to operation”
- Required submissions are prepared
  - Asset Inventory
  - Risk Assessment according to ISA/ IEC 62443-3-2
  - Security Policies and Procedures in accordance with ISA/ IEC 62443-2-1
- ACSSA is for a defined IACS at a specified physical location

Adapted From: ACSSA 100 Section 4.1

Scope of an ACSSA Evaluation

- Named organization that fills the role of asset owner for IACS
- Hardware and software inventory for IACS
- Equipment under control for the IACS
- List of service providers providing integration or maintenance support for the IACS
- Personnel assigned to interact with the IACS
- Documented Policies and Procedures for the IACS

Adapted From: ACSSA 300 ACS.R1

Inspection vs. Certification

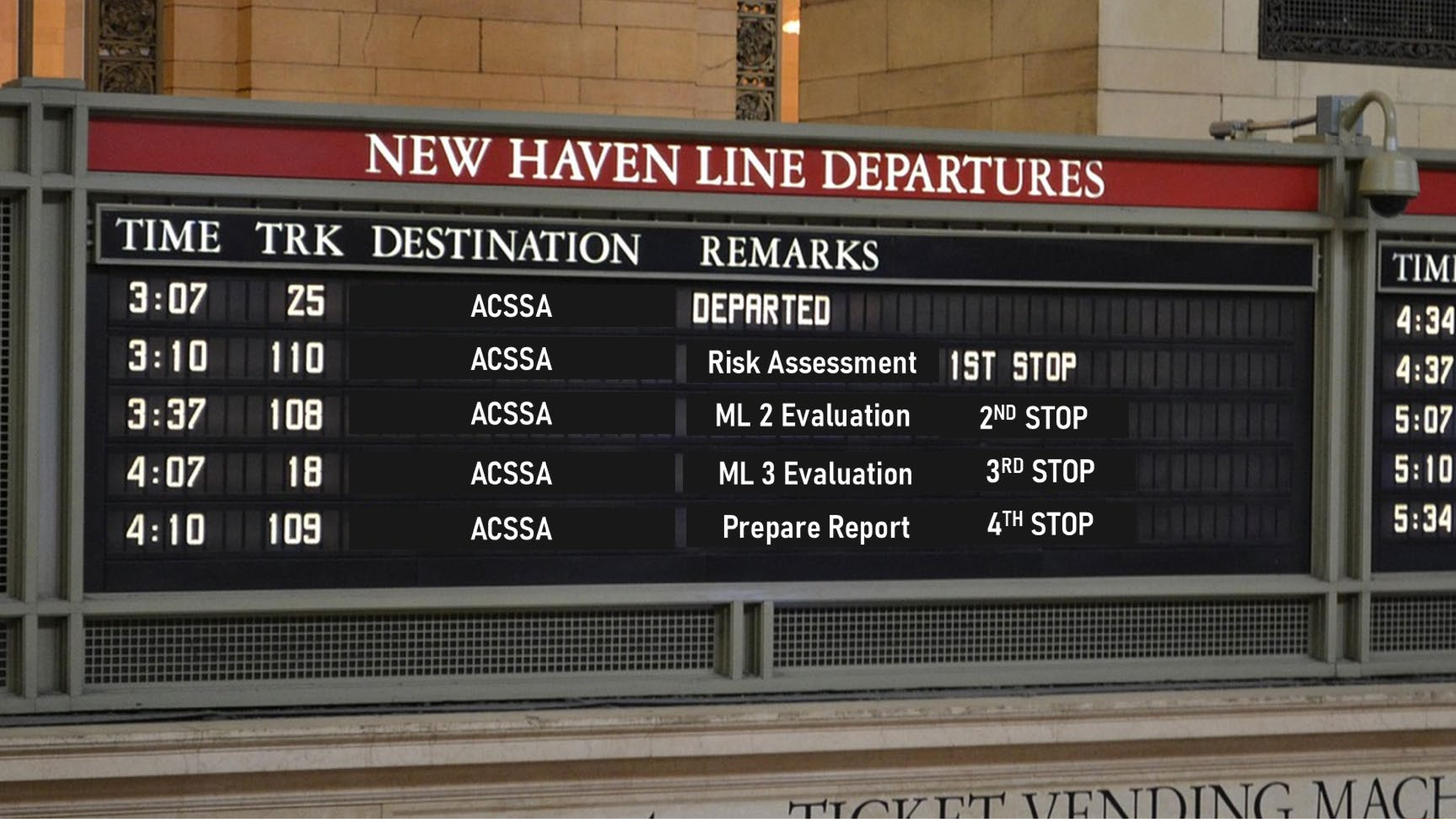
Assessment Type	Conformity Statement	Use Cases
Inspection	Attests conformity of the IACS to individual requirements in the ISA/ IEC 62443 standards but no formal designation for passing inspection.	Typically for internal purposes, e.g., gauge security posture/ readiness, provide independent review of security activities.
Certification	Certification of conformity if all process requirements met (at maturity level 3) and all capabilities in ISA/ IEC 62443-3-3 necessary to achieve the target security level are present and used for each zone or have a documented risk rationale.	Typically for a long-term public commitment to maintain the security program, or because an external entity (customer, insurance provider, regulator, etc.) offers a benefit for certification.

Adapted From: ACSSA 100 Section 4.2

Benefits of ACSSA Inspection/ Certification

- Addresses four parts of 62443 standard in a systematic, unified manner
- Evaluators are confirmed to be qualified and impartial by accreditors held to international standards for conformity assessment programs
- Consistent evaluation of organization security posture/ readiness
- Independent 3rd Party Review of Security Program and Technical Controls
- Opportunity to increase maturity within the organization
- Attestation of conformity that can be shared with external parties (if desired)

Why should a Risk Assessment be my first stop?



NEW HAVEN LINE DEPARTURES

TIME	TRK	DESTINATION	REMARKS	
3:07	25	ACSSA	DEPARTED	
3:10	110	ACSSA	Risk Assessment	1ST STOP
3:37	108	ACSSA	ML 2 Evaluation	2ND STOP
4:07	18	ACSSA	ML 3 Evaluation	3RD STOP
4:10	109	ACSSA	Prepare Report	4TH STOP

1^{ST} Stop - Risk Assessment Evaluation

- Evaluate risk assessment policies and procedures
- Evaluate Zone & Conduits documentation
- Evaluate initial risk assessment process and results
- Evaluate detailed risk assessment process and results
- Confirm completeness of submission for ACSSA

Adapted From: ACSSA 304 Figure 2

Why assess the risk assessment first?

- Risk assessment outcomes are the basis for ACSSA evaluation
- ACSSA determines whether a risk assessment complies with 62443-3-2 and then whether asset owner security program is consistent with the results of risk assessment
- ACSSA is not itself a risk assessment
- If a thorough risk assessment is not done, the organization will fail to meet many other ACSSA requirements

Why assess the risk assessment first?

- Named organization that fills the role of asset owner for IACS
- Hardware and software inventory for IACS
- Equipment under control for the IACS

Defined in Cyber Risk Assessment

- List of service providers providing integration or maintenance support for the IACS

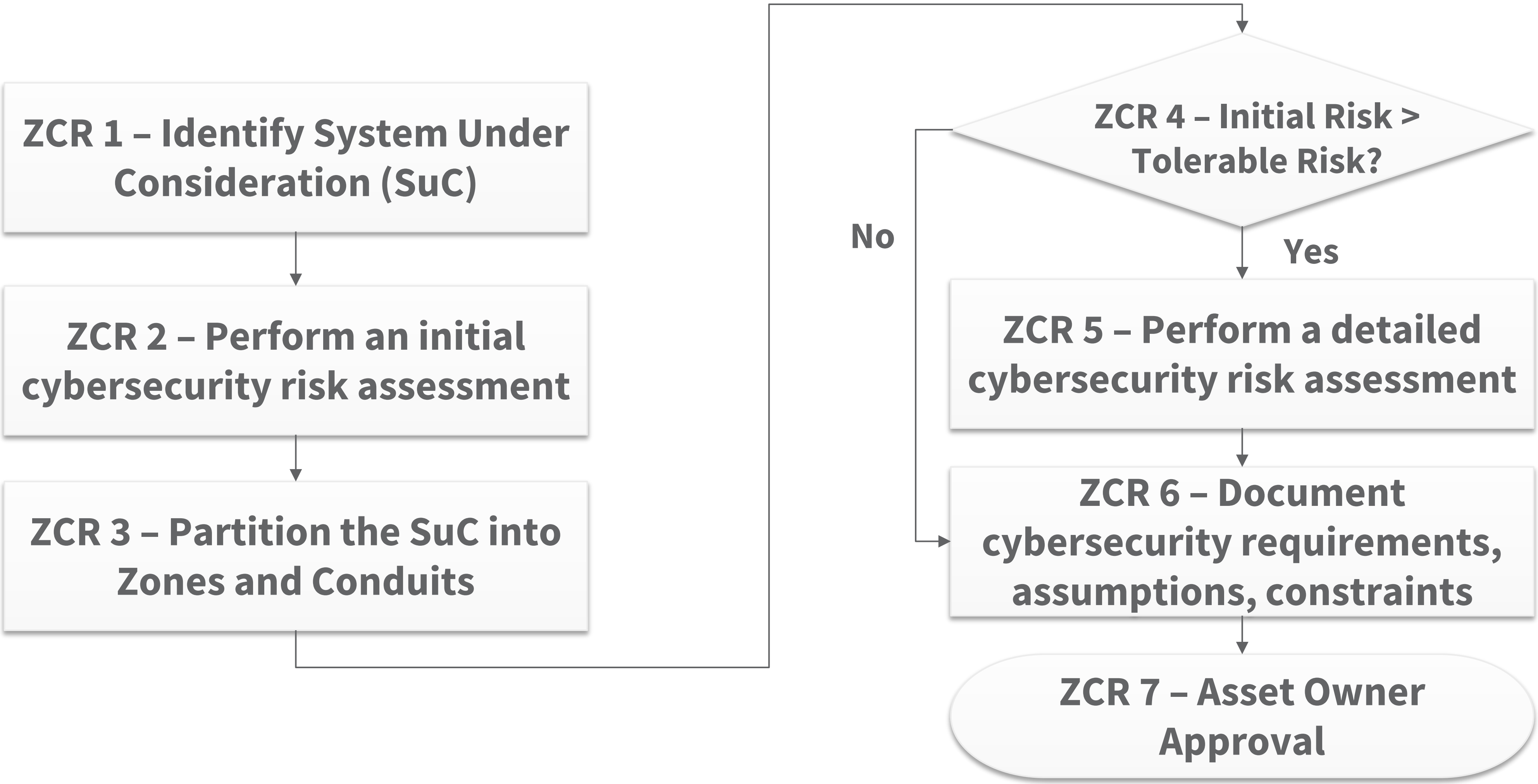
Partly Defined in Cyber Risk Assessment

- Personnel assigned to interact with the IACS
- Documented Policies and Procedures for the IACS

Adapted From: ACSSA 300 ACS.R1

What is involved in the Cybersecurity Risk Assessment Process?

ISA/ IEC 62443-3-2 Risk Assessment



ZCR 1 – Identify System Under Consideration (SuC)

ZCR 2 – Perform an initial cybersecurity risk assessment

ZCR 3 – Partition the SuC into Zones and Conduits

ZCR 4 – Initial Risk > Tolerable Risk?

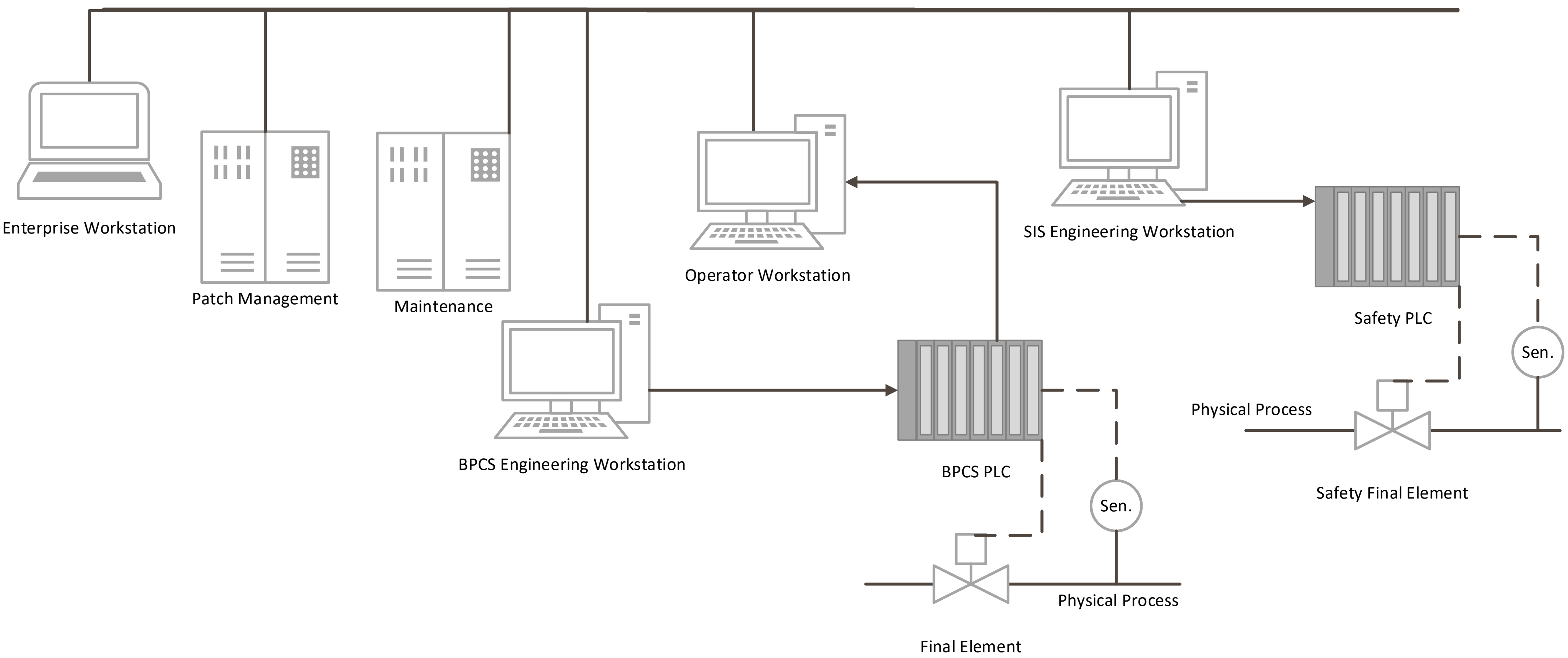
ZCR 5 – Perform a detailed cybersecurity risk assessment

ZCR 6 – Document cybersecurity requirements, assumptions, constraints

ZCR 7 – Asset Owner Approval

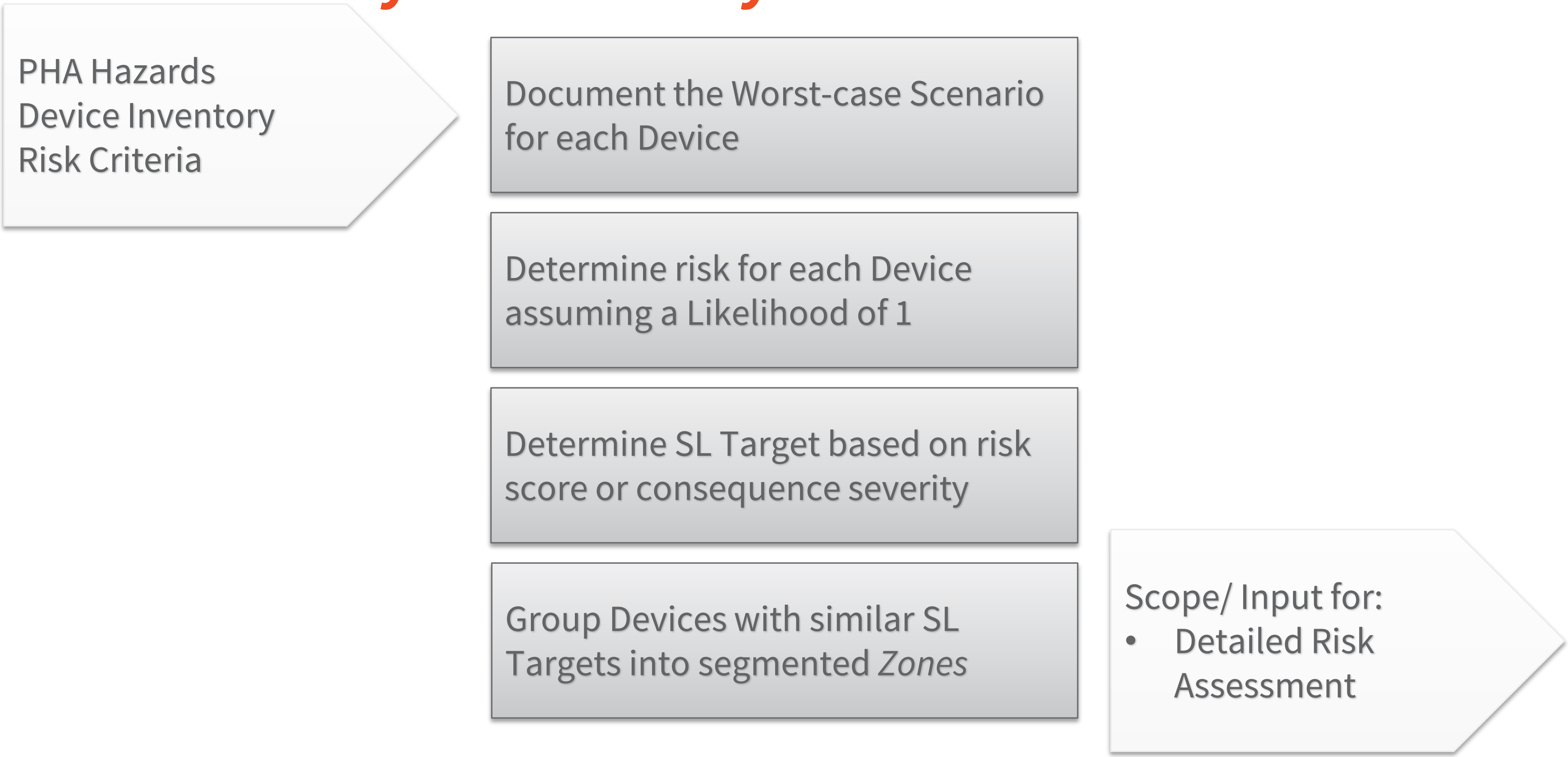
Adapted From: ACSSA 101 Figure 2

ZCR 1 – Identify System Under Consideration



ISA/ IEC 62443-3-2 excerpt 4.2.1.2: *"System inventory, architecture diagrams, network diagrams and dataflows can be used to determine and illustrate the IACS assets that are included in the SUC description."*

ZCR 2 – Perform an initial cybersecurity risk assessment



PHA Hazards
Device Inventory
Risk Criteria

Document the Worst-case Scenario for each Device

Determine risk for each Device assuming a Likelihood of 1

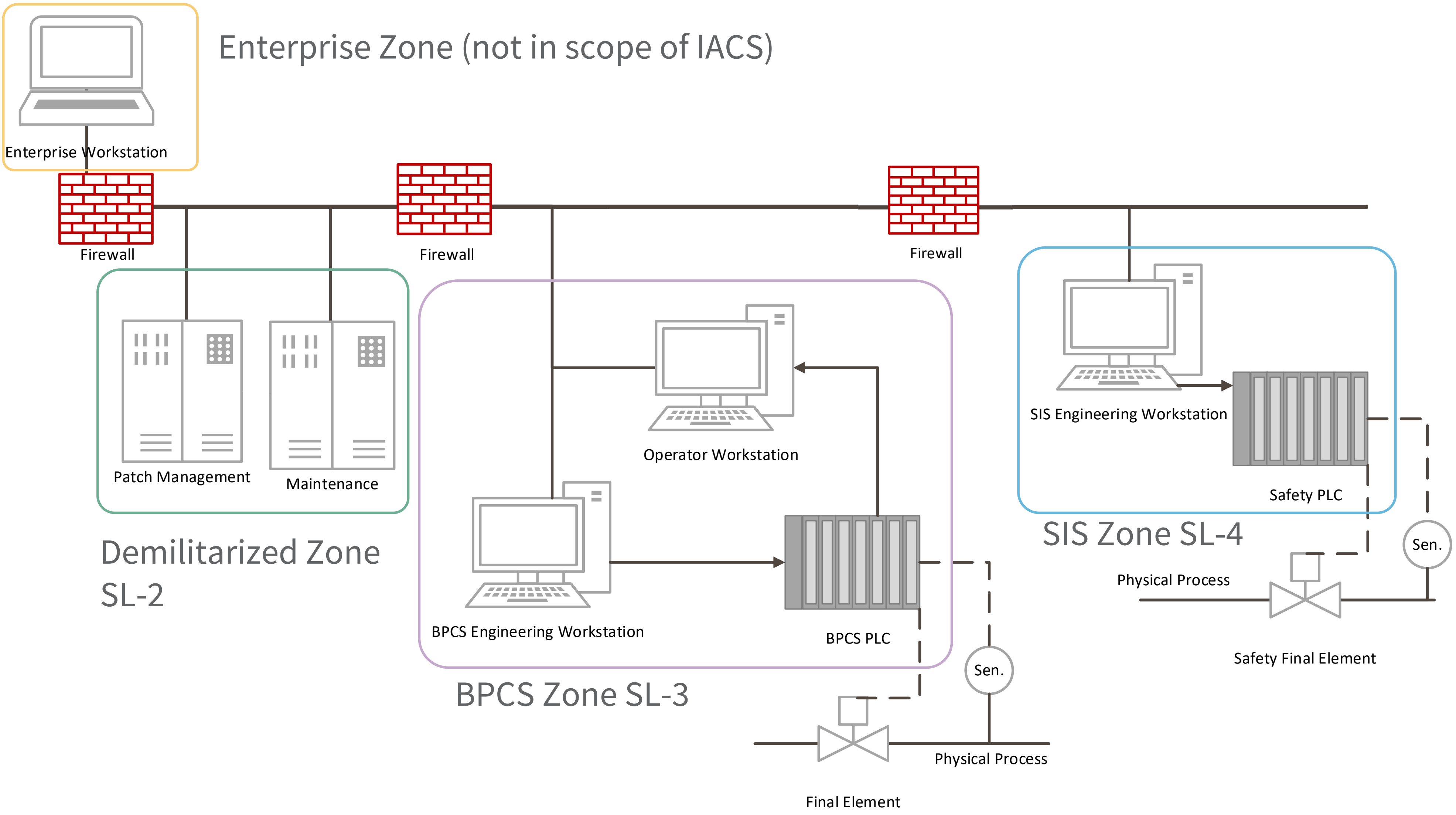
Determine SL Target based on risk score or consequence severity

Group Devices with similar SL Targets into segmented *Zones*

Scope/ Input for:

- Detailed Risk Assessment

ZCR 3 – Partition the SuC into Zones and Conduits

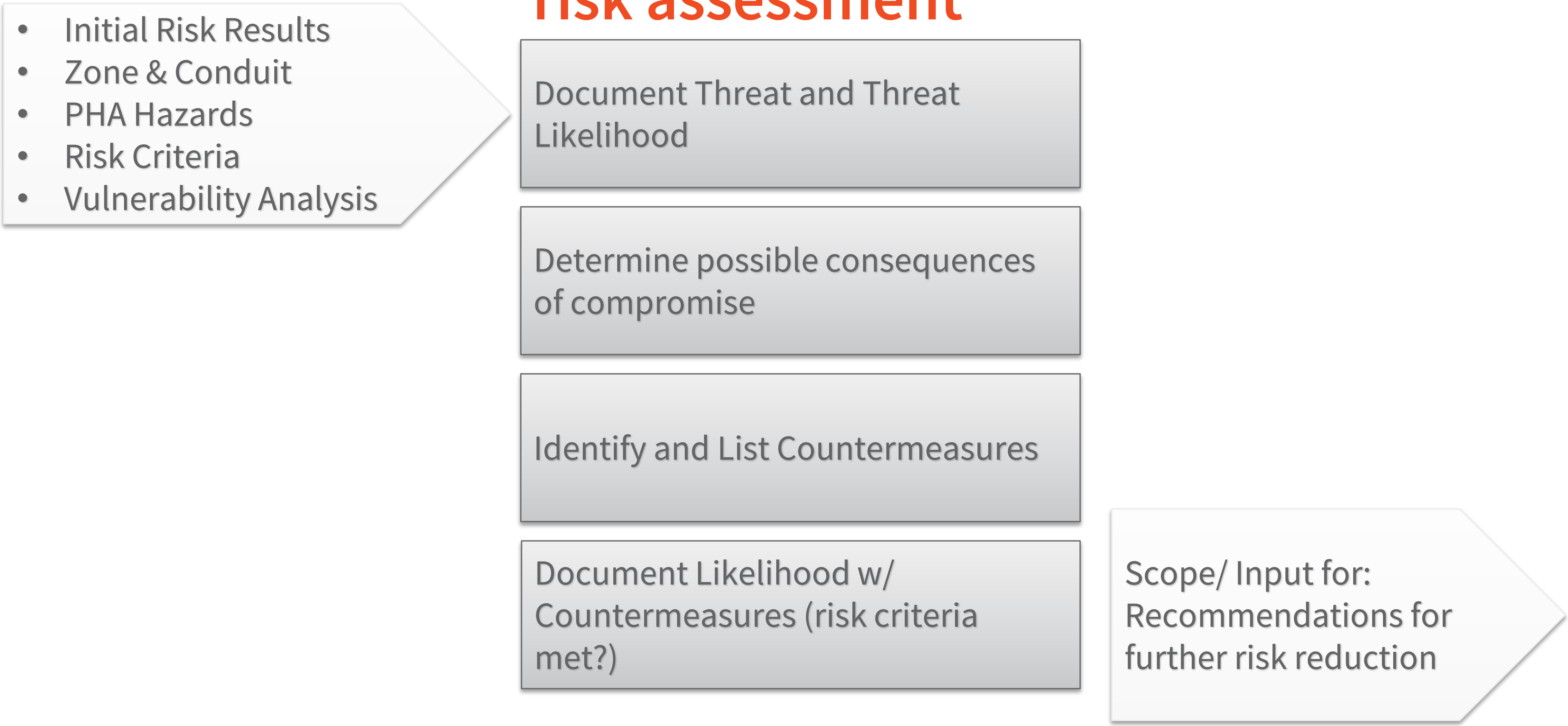


ZCR 4 – Initial Risk > Tolerable Risk?

Zone	Security Level Target	Risk Tolerable?
DMZ	SL-2	No
BPCS	SL-3	No
SIS	SL-4	No

After defining the worst-case cybersecurity consequence for each zone, do any exceed my tolerable risk criteria?

ZCR 5 – Perform a detailed cybersecurity risk assessment



- Initial Risk Results
- Zone & Conduit
- PHA Hazards
- Risk Criteria
- Vulnerability Analysis

Document Threat and Threat Likelihood

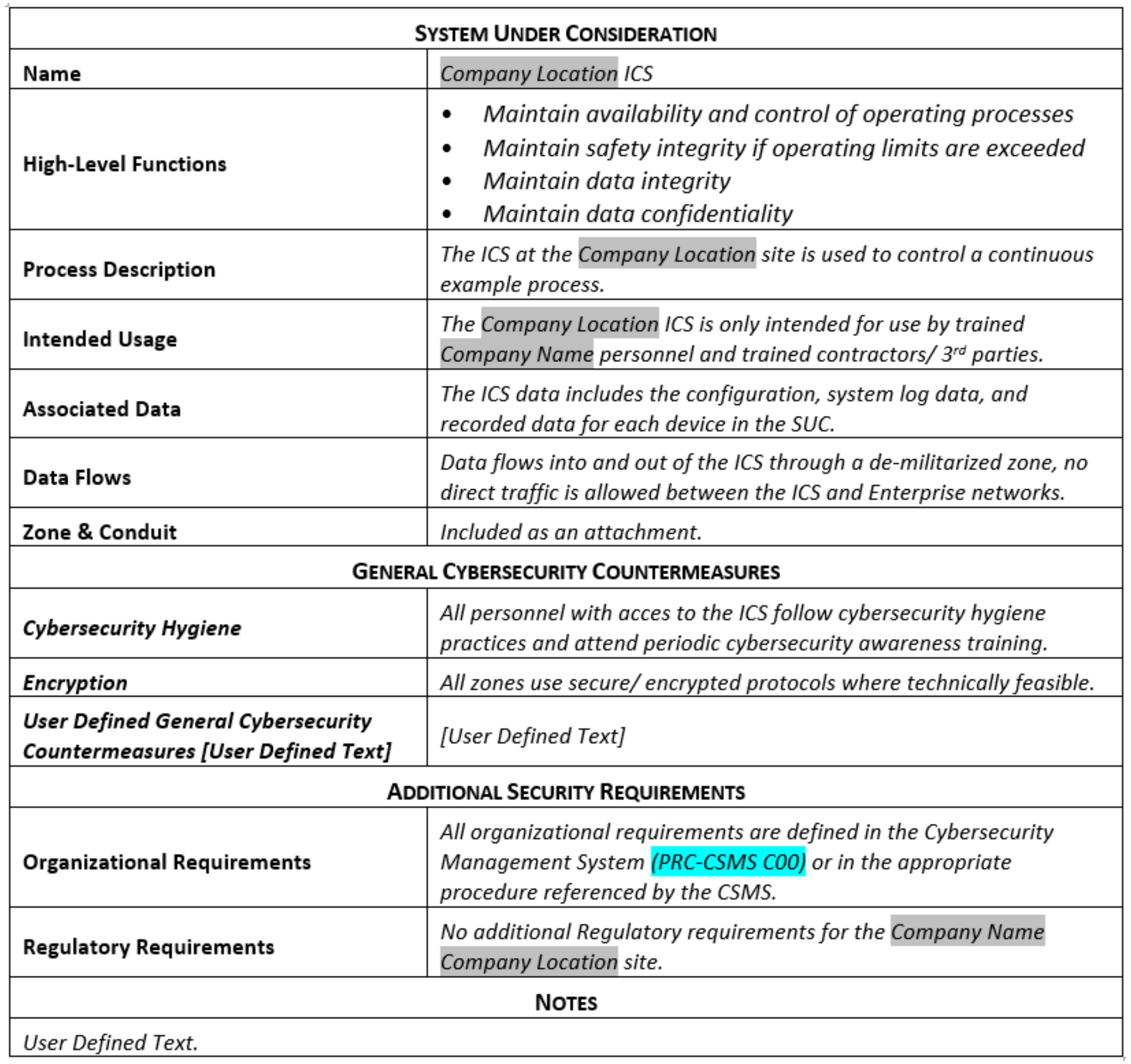
Determine possible consequences of compromise

Identify and List Countermeasures

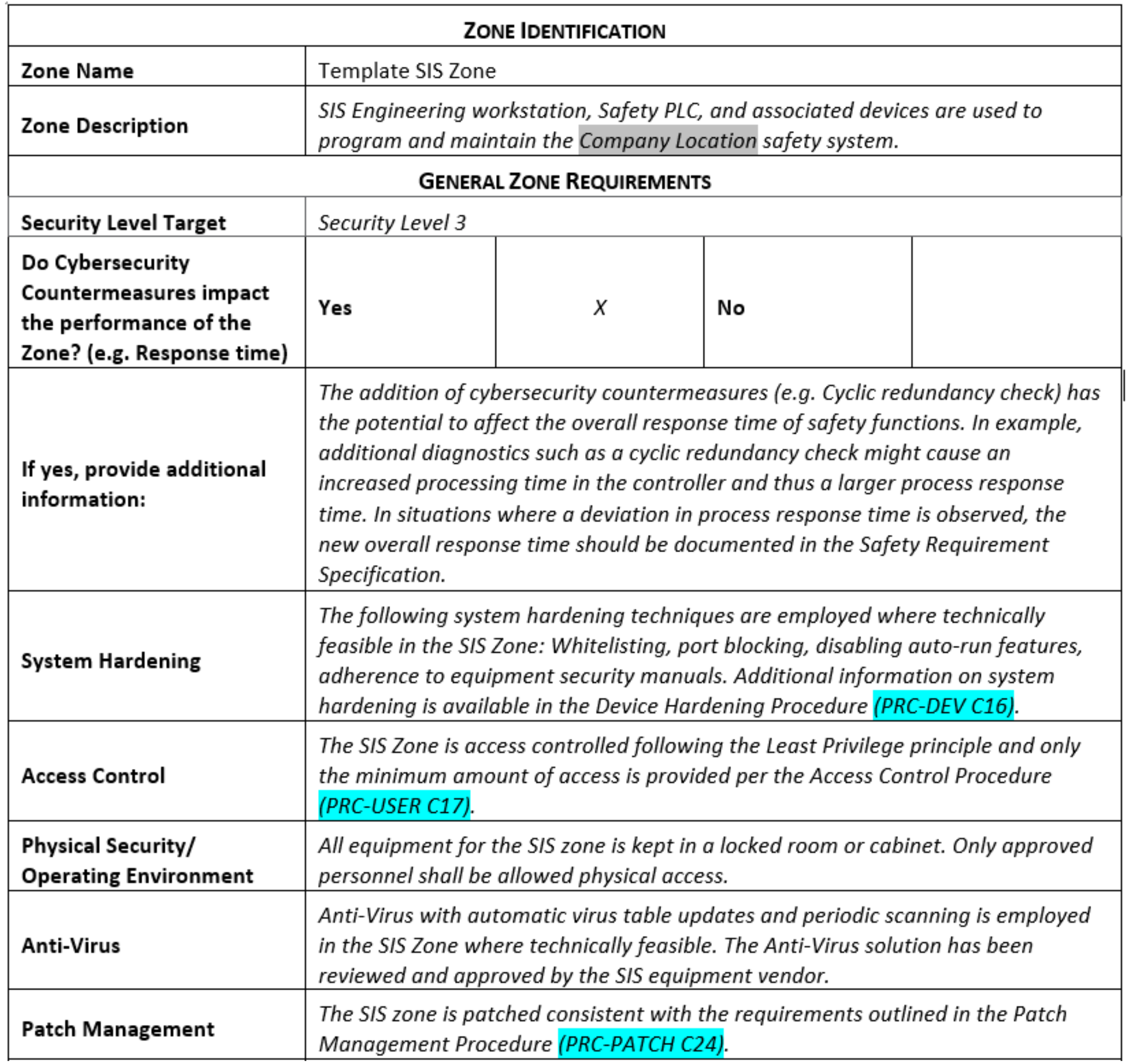
Document Likelihood w/ Countermeasures (risk criteria met?)

Scope/ Input for: Recommendations for further risk reduction

ZCR 6 – Document cybersecurity requirements, assumptions, constraints



System Under Consideration	
Name	*Company Location ICS*
High-Level Functions	- *Maintain availability and control of operating processes* - *Maintain safety integrity if operating limits are exceeded* - *Maintain data integrity* - *Maintain data confidentiality*
Process Description	*The ICS at the Company Location site is used to control a continuous example process.*
Intended Usage	*The Company Location ICS is only intended for use by trained Company Name personnel and trained contractors/ 3rd parties.*
Associated Data	*The ICS data includes the configuration, system log data, and recorded data for each device in the SUC.*
Data Flows	*Data flows into and out of the ICS through a de-militarized zone, no direct traffic is allowed between the ICS and Enterprise networks.*
Zone & Conduit	*Included as an attachment.*
General Cybersecurity Countermeasures	
Cybersecurity Hygiene	*All personnel with acces to the ICS follow cybersecurity hygiene practices and attend periodic cybersecurity awareness training.*
Encryption	*All zones use secure/ encrypted protocols where technically feasible.*
User Defined General Cybersecurity Countermeasures [User Defined Text]	*[User Defined Text]*
Additional Security Requirements	
Organizational Requirements	*All organizational requirements are defined in the Cybersecurity Management System (PRC-CSMS C00) or in the appropriate procedure referenced by the CSMS.*
Regulatory Requirements	*No additional Regulatory requirements for the Company Name Company Location site.*
Notes	
User Defined Text.	



Zone Identification				
Zone Name	Template SIS Zone			
Zone Description	*SIS Engineering workstation, Safety PLC, and associated devices are used to program and maintain the Company Location safety system.*			
General Zone Requirements				
Security Level Target	*Security Level 3*			
Do Cybersecurity Countermeasures impact the performance of the Zone? (e.g. Response time)	**Yes**	*X*	**No**	
If yes, provide additional information:	*The addition of cybersecurity countermeasures (e.g. Cyclic redundancy check) has the potential to affect the overall response time of safety functions. In example, additional diagnostics such as a cyclic redundancy check might cause an increased processing time in the controller and thus a larger process response time. In situations where a deviation in process response time is observed, the new overall response time should be documented in the Safety Requirement Specification.*			
System Hardening	*The following system hardening techniques are employed where technically feasible in the SIS Zone: Whitelisting, port blocking, disabling auto-run features, adherence to equipment security manuals. Additional information on system hardening is available in the Device Hardening Procedure (PRC-DEV C16).*			
Access Control	*The SIS Zone is access controlled following the Least Privilege principle and only the minimum amount of access is provided per the Access Control Procedure (PRC-USER C17).*			
Physical Security/ Operating Environment	*All equipment for the SIS zone is kept in a locked room or cabinet. Only approved personnel shall be allowed physical access.*			
Anti-Virus	*Anti-Virus with automatic virus table updates and periodic scanning is employed in the SIS Zone where technically feasible. The Anti-Virus solution has been reviewed and approved by the SIS equipment vendor.*			
Patch Management	*The SIS zone is patched consistent with the requirements outlined in the Patch Management Procedure (PRC-PATCH C24).*			

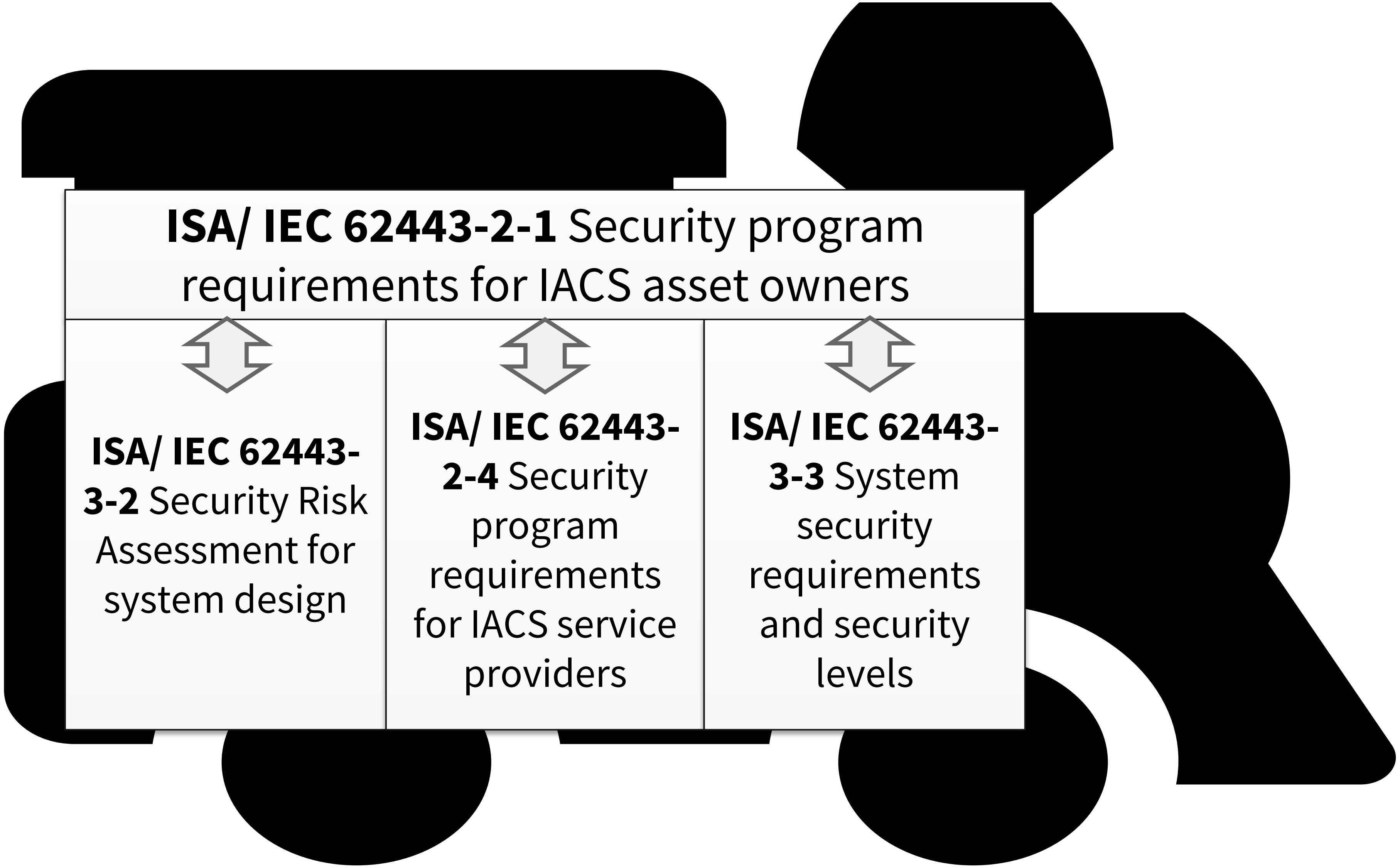
ZCR 7 – Asset Owner Approval

- The cybersecurity risk assessment can be done by the asset owner or by a designated third party
- The results of the risk assessment must be reviewed and accepted by the asset owner

How does the risk assessment impact ACSSA?

- Zone & Conduit provides clear delineation of scope for evaluation
- Security level targets identified in the risk assessment determine applicability of IEC/ ISA 62443-3-3 requirements
- In some cases, a risk justification can be provided to demonstrate that a specific control is not needed because other compensating countermeasures are in place
- If IACS1 and IACS2 are exactly the same in every way except for risk environment, one could pass ACSSA certification and one not pass

ACSSA Leaving the Station



ISA/ IEC 62443-2-1 Security program requirements for IACS asset owners

ISA/ IEC 62443-3-2 Security Risk Assessment for system design

ISA/ IEC 62443-2-4 Security program requirements for IACS service providers

ISA/ IEC 62443-3-3 System security requirements and security levels

Adapted From: ACSSA 100 Figure 1

Questions?