An Approach for Data Security in the Era of Industry 4.0

keeping data safe

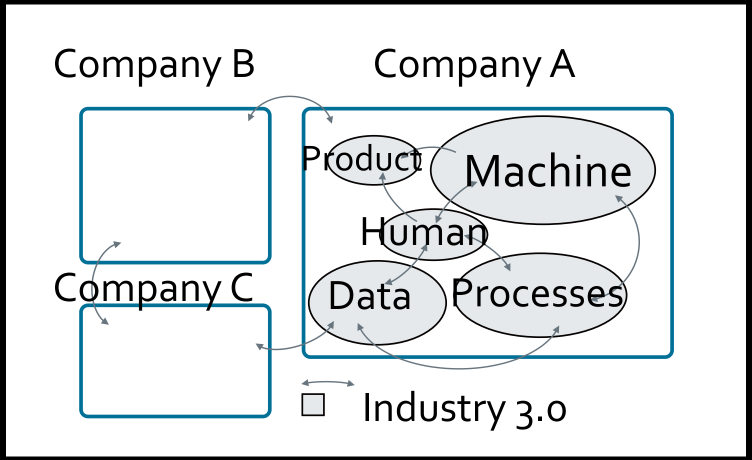
Masao Ito
NIL Software Corp.
email: nil@nil.co.jp

7/Sep/2017

Introduction

- In the Industry 4.0 era, there is the difference between the physical and logical view of the factory. For example, a machine owned by a company, but it might be controlled by another company.
- As for safety and security, it might be desirable to analyse the system (of systems) by a single approach. Focusing on the early phase of system development, we try to conider the possibility of an approach.

Industry 3.0 to 4.0

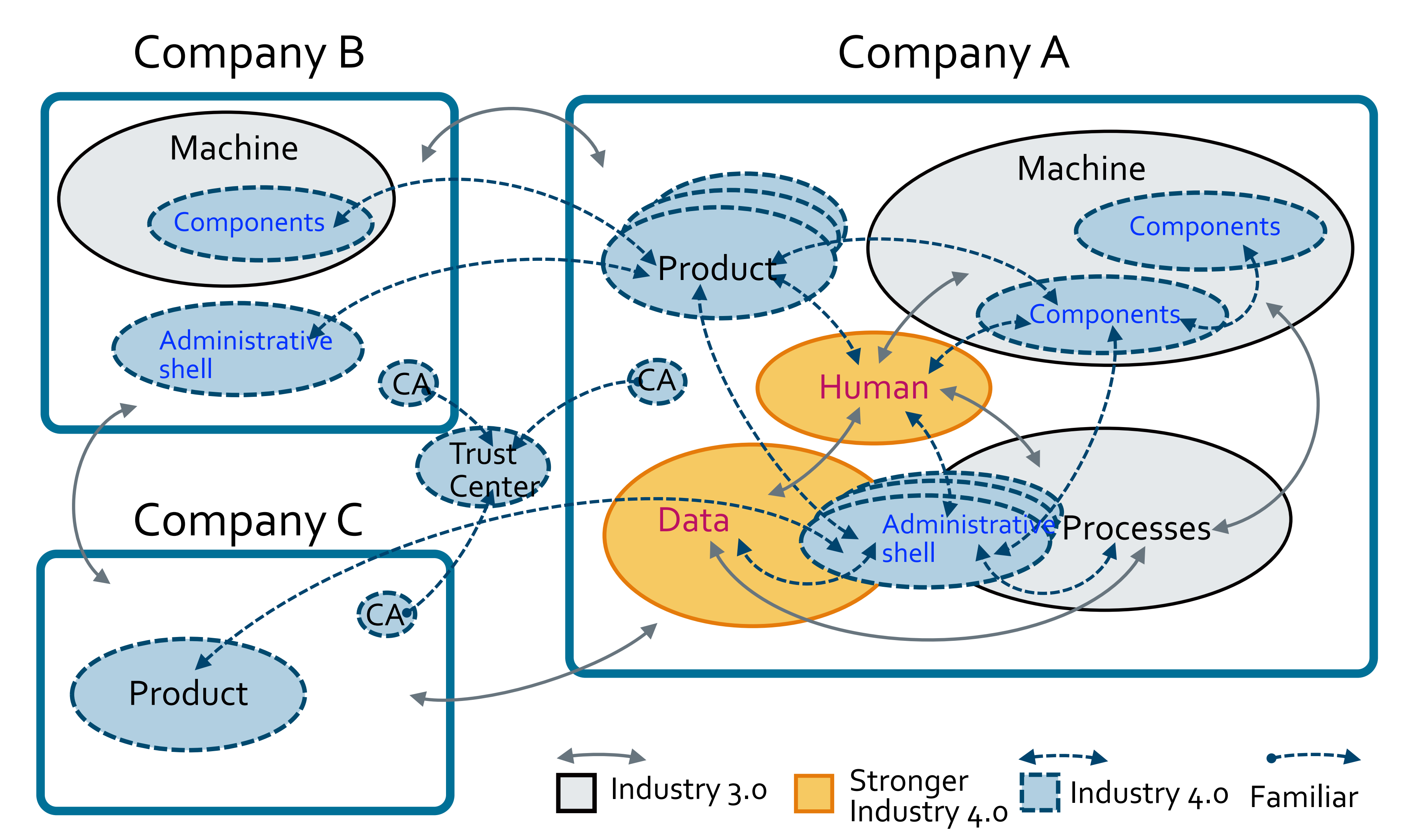


IT-Security in Industrie 4.0

https://www.plattform-i40.de/I40/Redaktion/EN/Downloads/Publikation/it-security-in-i40.html

Industry 3.0

Industry 4.0

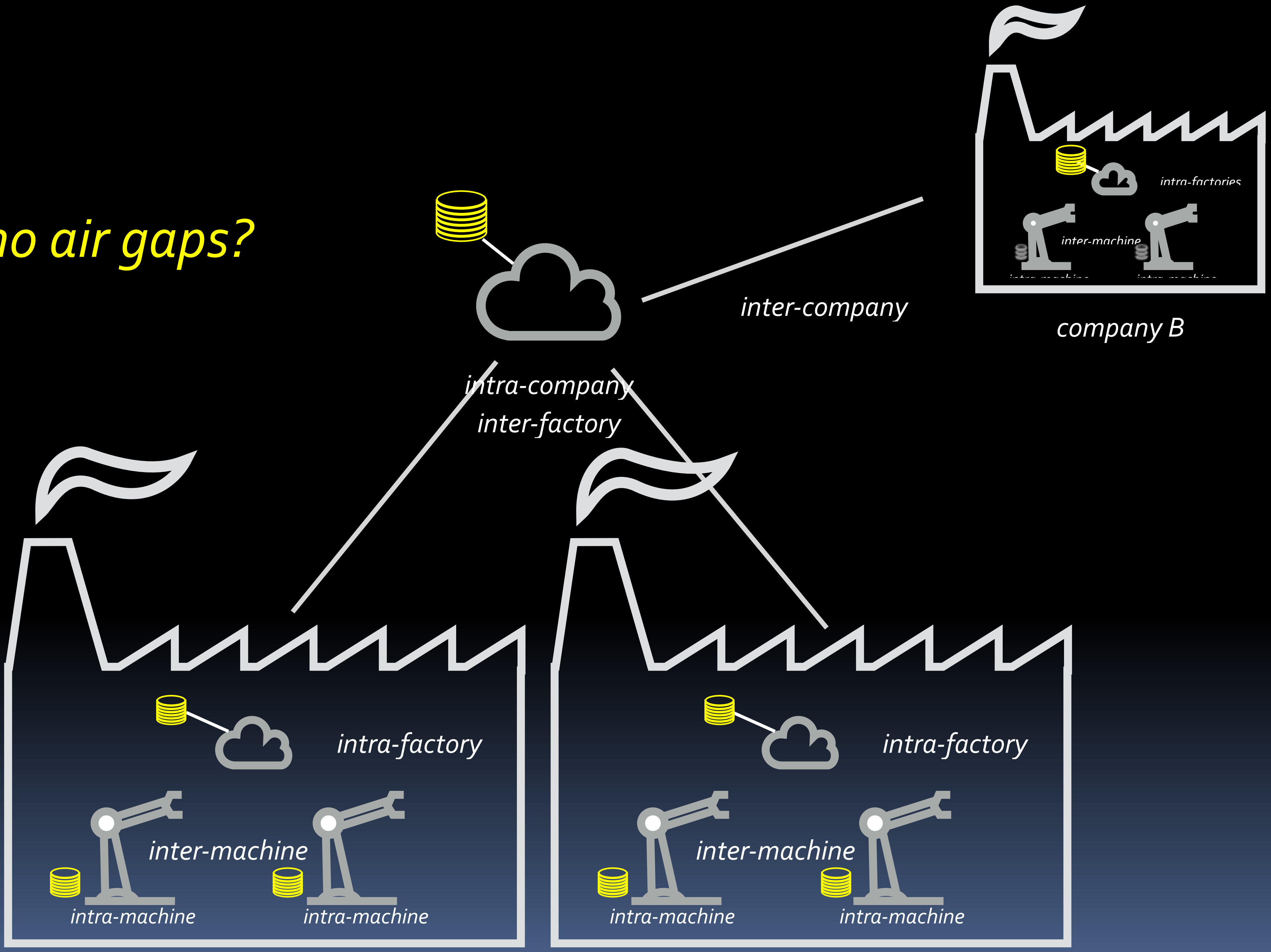


It says,

> *The essential prerequisite for a successful implementation of Industrie 4.0 is a secure and trustworthy treatment of data and a reliable protection of inter-company communication from external attacks.*

Industry 4.0

no air gaps?



inter-company

company B

intra-factories

inter-machine

intra-machine

intra-machine

intra-company
inter-factory

intra-factory

inter-machine

intra-machine

intra-machine

intra-factory

inter-machine

intra-machine

intra-machine

company A

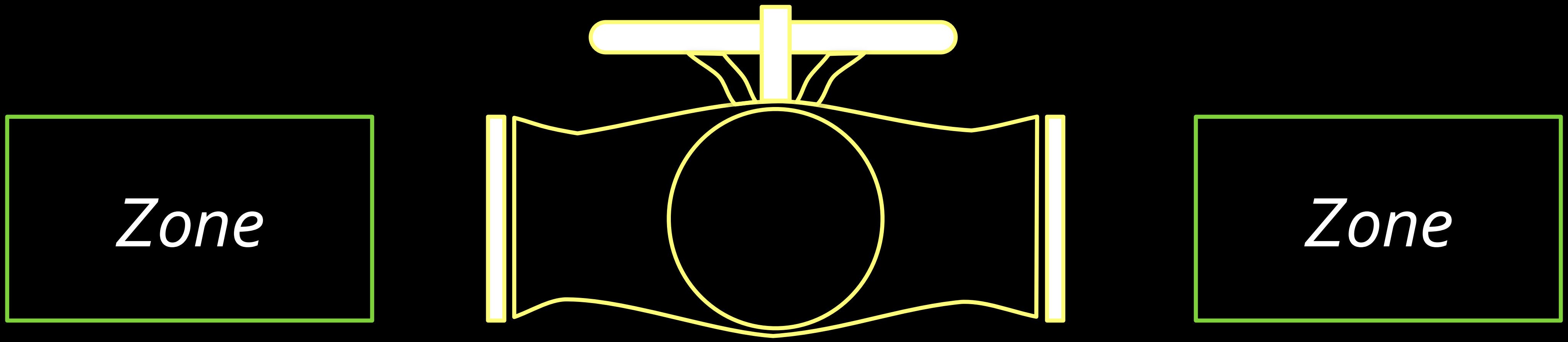
Comparison of Standards @ concpt phase

Security	ISA/IEC 62443
Safety	ISO 26262

Comparison of security and safety standards

- Security
  - ISA/IEC 62443 (ISA99) is the comprehensive standards for security of the industrial automation and control system (IACS). It aims to prevent:
    - endangerment of public or employee safety
    - loss of public confidence
    - violation of regulatory requirements
    - loss of proprietary or confidential information
    - economic loss
    - impact on national security
- Safety
  - ISO 26262
    - *ISO 26262 is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production passenger cars with a maximum gross vehicle mass up to 3 500 kg.*

ISA/IEC 62443 uses zone & conduit model



Zone

Zone

Conduit

Zone and Conduit of IACS

- Data Center

  inter-factory or -company

- Network

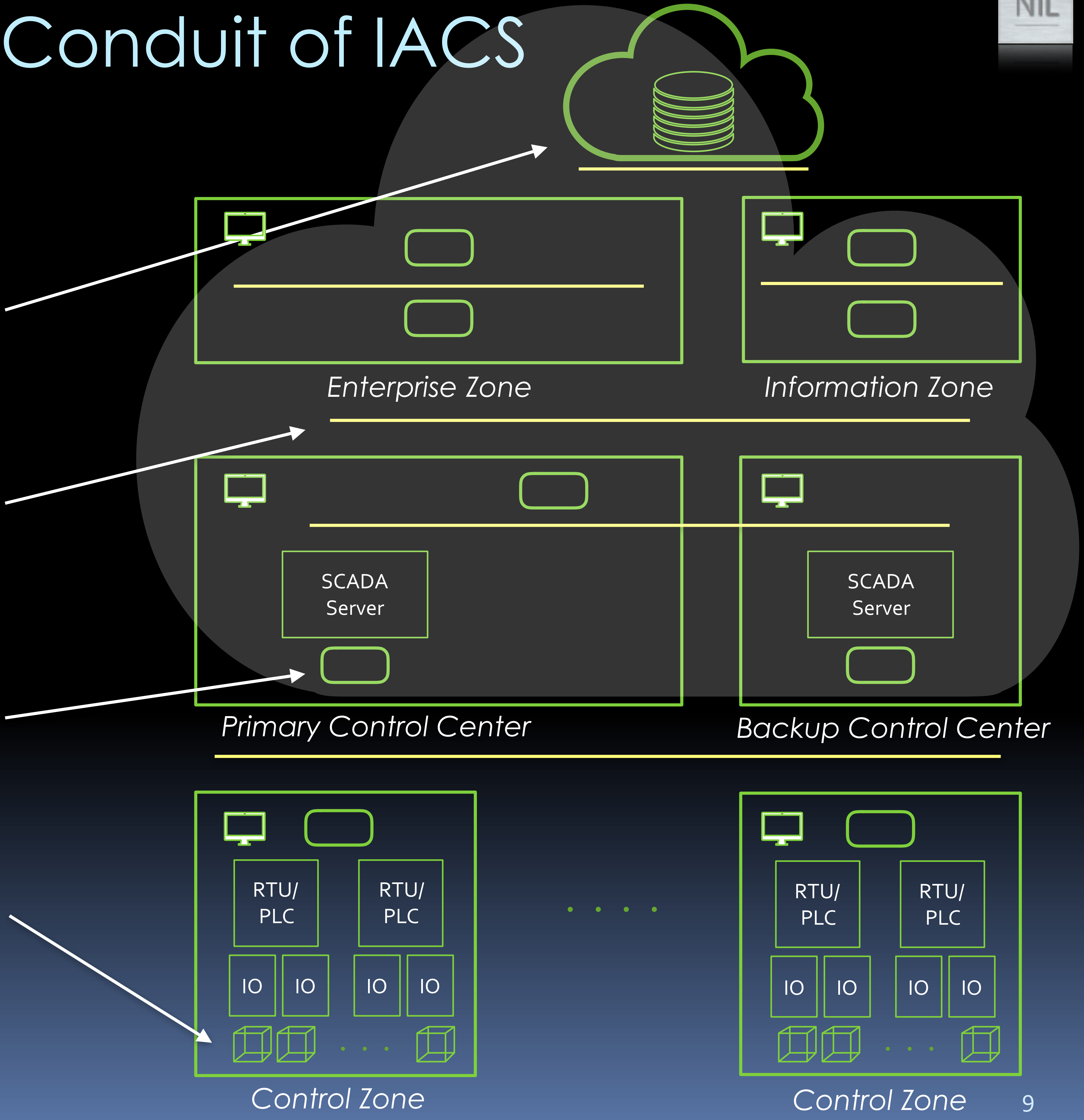
  intra-factory

- Gateway

  intra-factory inter-machine

- End-Point

  intra-machine



SCADA: Supervisory Control And Data Acquisition
RTU: Remote Terminal Unit
PLC: Programmable Logic Controller

ISA/IEC 62443 Standards

Reference	IEC Reference	Title
ISA-TR62443-0-3	N/A	Gap assessment of ANSI/ISA-99.02.01-2009
ISA-62443-1-1	IEC/TS 62443-1-1	Models and concepts
ISA-TR62443-1-2	IEC/TR 62443-1-2	Master glossary of terms and abbreviations
ISA-62443-1-3	IEC 62443-1-3	System security compliance metrics
ISA-TR62443-1-4	IEC/TR 62443-1-4	Security life cycle and use cases
ISA-62443-2-1	IEC 62443-2-1	Requirements for an IACS security management system
ISA-TR62443-2-2	IEC/TR 62443-2-2	Implementation guidance for an IACS security management system
ISA-TR62443-2-3	IEC/TR 62443-2-3	Patch management in the IACS environment
ISA-62443-2-4	IEC 62443-2-4	Requirements for IACS solution suppliers
ISA-TR62443-3-1	IEC/TR 62443-3-1	Security technologies for IACS
ISA-62443-3-2	IEC 62443-3-2	Security risk assessment and system design
ISA-62443-3-3	IEC 62443-3-3	System security requirements and security levels
ISA-62443-4-1	IEC 62443-4-1	Product development requirements
ISA-62443-4-2	IEC 62443-4-2	Technical security requirements for IACS components

The Early Stage of Process

Table 1. Comparisson of the early stage between IEC 62443 with ISO 26262

IEC 62443-1-1	ISO 26262 Part 3 (Concept Phase)
Concept Phase (Identification step, Concept step)	3-5: Item Definition 3-6: Initiation of the Safety Lifecyle
Analysis Phase (Definition step)	3-7: Hazard Analysis and Risk Assessment
	3-8: Functional Safety Concept

- Continue developing the security program
- Establish security functional requirements for industrial automation and control systems and equipment, production systems, information systems, and personnel
- Perform vulnerability assessment of facilities and associated services against the list of potential threats
- Discover and determine legal requirements for industrial automation and control systems
- Perform a risk analysis of potential vulnerabilities and threats
- Categorize risks, potential impacts to the enterprise, and potential mitigations
- Segment security work into controllable tasks and modules for development of functional designs
- Establish network functional definitions for security portions of industrial automation and control systems

Security Level

3.2.107 security level
level corresponding to the required effectiveness of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit [13].

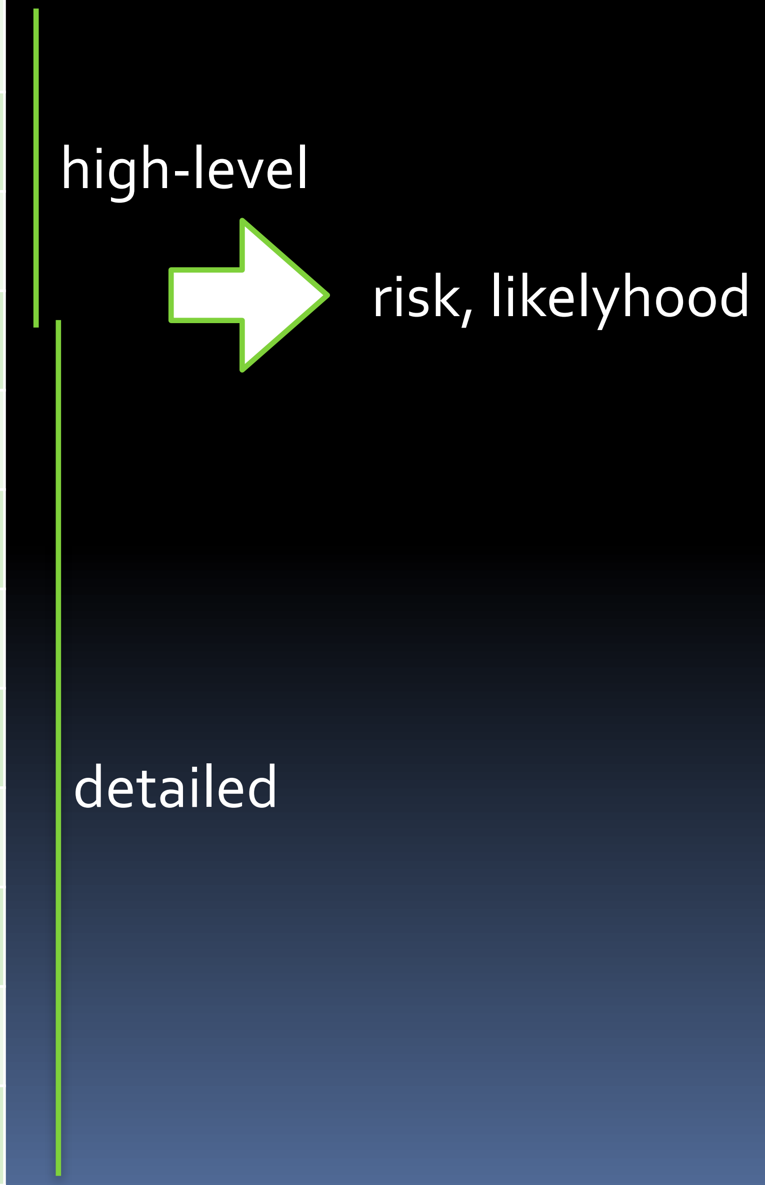
Security Level	Qualitative Description
1	LOW
2	Medium
3	High

• Target SL	User
• Capability SL	User and Vendor
• Achived SL	User

IEC 62443 Risk analysis requirements

The target SL(Security Level) does NOT identified here

4.2.2.1	Develop a business rational
4.2.3.1	Select a risk assessment methodology
4.2.3.2	Provide risk asssessment background information
4.2.3.3	Conduct a high-level risk assessment
4.2.3.4	Identify the industrial automation and control systems
4.2.3.5	Develop simple network diagrams
4.2.3.6	Prioritize sytems
4.2.3.7	Perform a detailed vulnerability assessment
4.2.3.8	Identify a detailed risk assessment methodology
4.2.3.9	Conduct a detailed risk assessment
4.2.3.10	Identify the reassessment frequency and triggering criteria
4.2.3.11	Integrate physical, HSE and cyber security risk assessment reuslts
4.2.3.12	Conduct risk assessments throughout the lifecycle of the IACS
4.2.3.13	Document the risk assessment
4.2.3.14	Maintain vulnerability assessment records

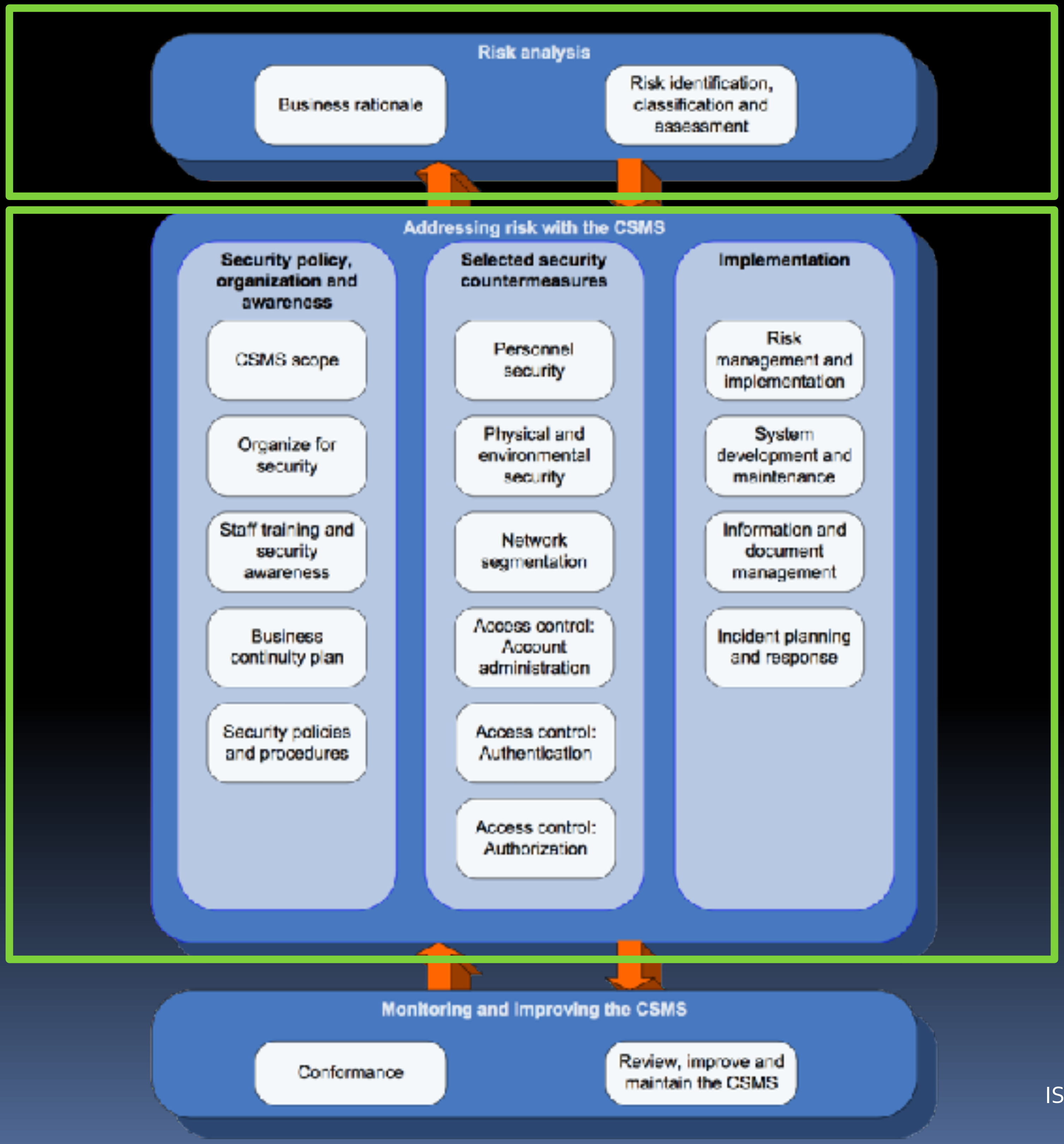


high-level

risk, likelyhood

detailed

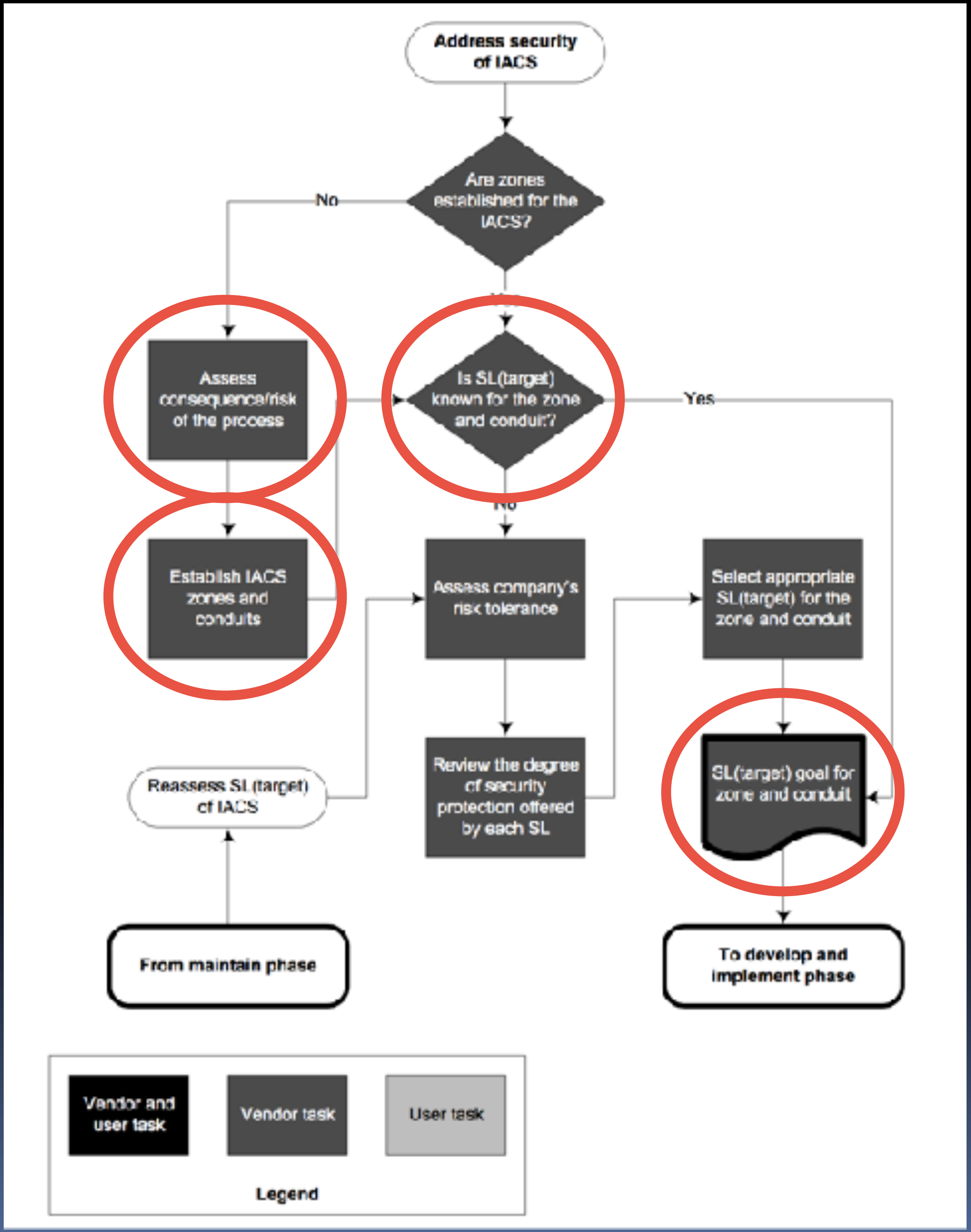
Risk Analysis


Risk analysis
Business rationale
Risk identification, classification and assessment
Addressing risk with the CSMS
Security policy, organization and awareness
CSMS scope
Organize for security
Staff training and security awareness
Business continuity plan
Security policies and procedures
Selected security countermeasures
Personnel security
Physical and environmental security
Network segmentation
Access control: Account administration
Access control: Authentication
Access control: Authorization
Implementation
Risk management and implementation
System development and maintenance
Information and document management
Incident planning and response
Monitoring and improving the CSMS
Conformance
Review, improve and maintain the CSMS

Security Level (SL) can be determined after established the zone and conduit model

ISA/IEC 62334-2-1 p.48

Security Level Lifecyle Model: Assess Phase


Address security of IACS
Are zones established for the IACS?
No
Yes
Assess consequence/risk of the process
Establish IACS zones and conduits
Is SL(target) known for the zone and conduit?
Yes
No
Assess company's risk tolerance
Select appropriate SL(target) for the zone and conduit
Review the degree of security protection offered by each SL
Reassess SL(target) of IACS
SL(target) goal for zone and conduit
From maintain phase
To develop and implement phase
Vendor and user task
Vendor task
User task
Legend

ISA/IEC 62334-2-1 p.122

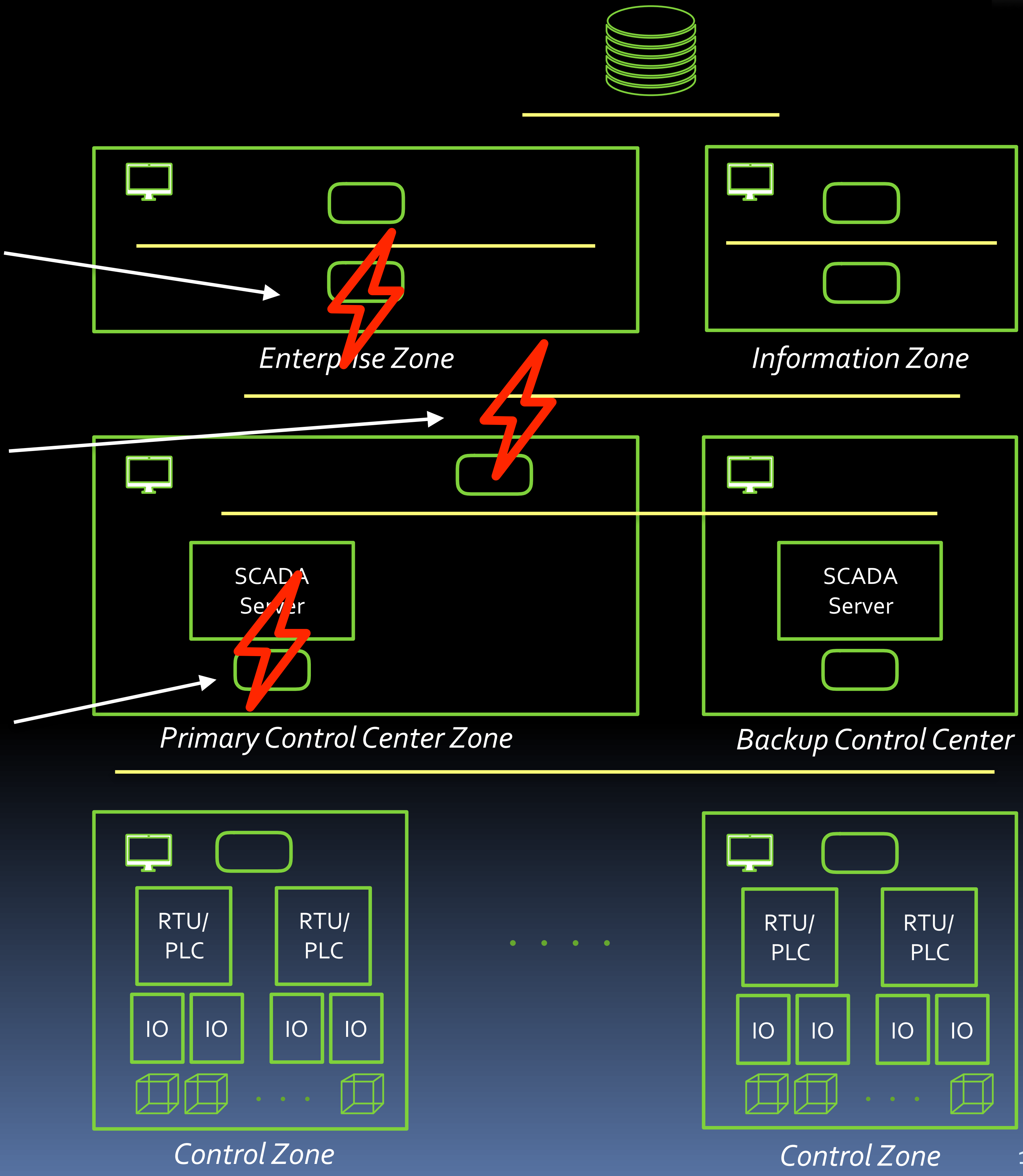
ISA/IEC 62443 vs. ISO 2626 standard

- The both standards define required (security/safety) level in the early stage: target SL (62443), ASIL (26262).
- But, in 26262, we give the ASIL only to the item (abstract system), and later apply them to parts (c.f. ASIL decomposition).
- In 62443, we give the target SL to each zone (or conduit) after designing the zone-conduit model.

Detection of Anomality of Data

Catch the threats in the conduit

- Virus entered and it emitted the wrong information
- The access control was violated because of poor mechanism
- Infected USB memory was inserted



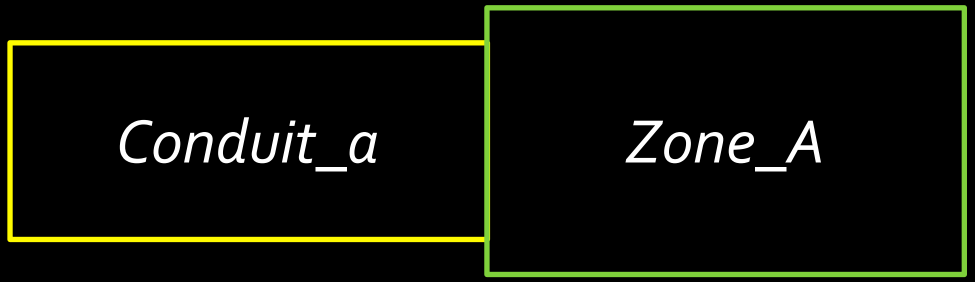
SCADA: Supervisory Control And Data Acquisition
RTU: Remote Terminal Unit
PLC: Programmable Logic Controller

W32.Stuxnet

It attacks systems (centrifuge separator) that spin between 807hz to 1210hz, once it found them, it manipulated the operation of the motors by changing their rotational speed.

it modified the frequency anywhere from 1410hz to 2hz, all while sending false data back to the operators.

Verification function



<u>Conduit: Flow data</u>

ValidityOfFlowData(Direction, Contents, Timing)

Direction: toZone_A / fromZone_A

<u>Zone: Saved data</u>

ValidityOfStoredData(Action, Contents, Timing)

Action: Create/Read/Update/Delete to the Data

Possibility of security violation

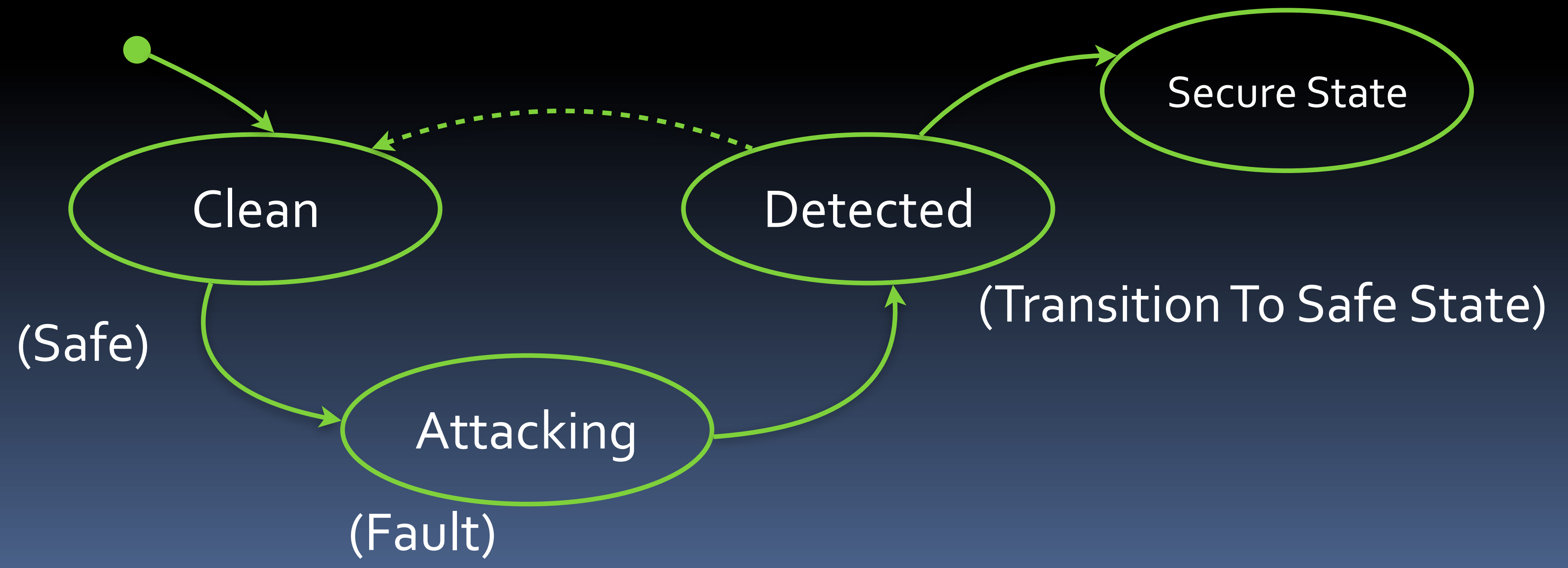
It returns false;
The contents and the timing of data is valid, but the data wrongly go out throuth the conduit.

It returns false;
The data was updated timely, but the contents of it is wrong.

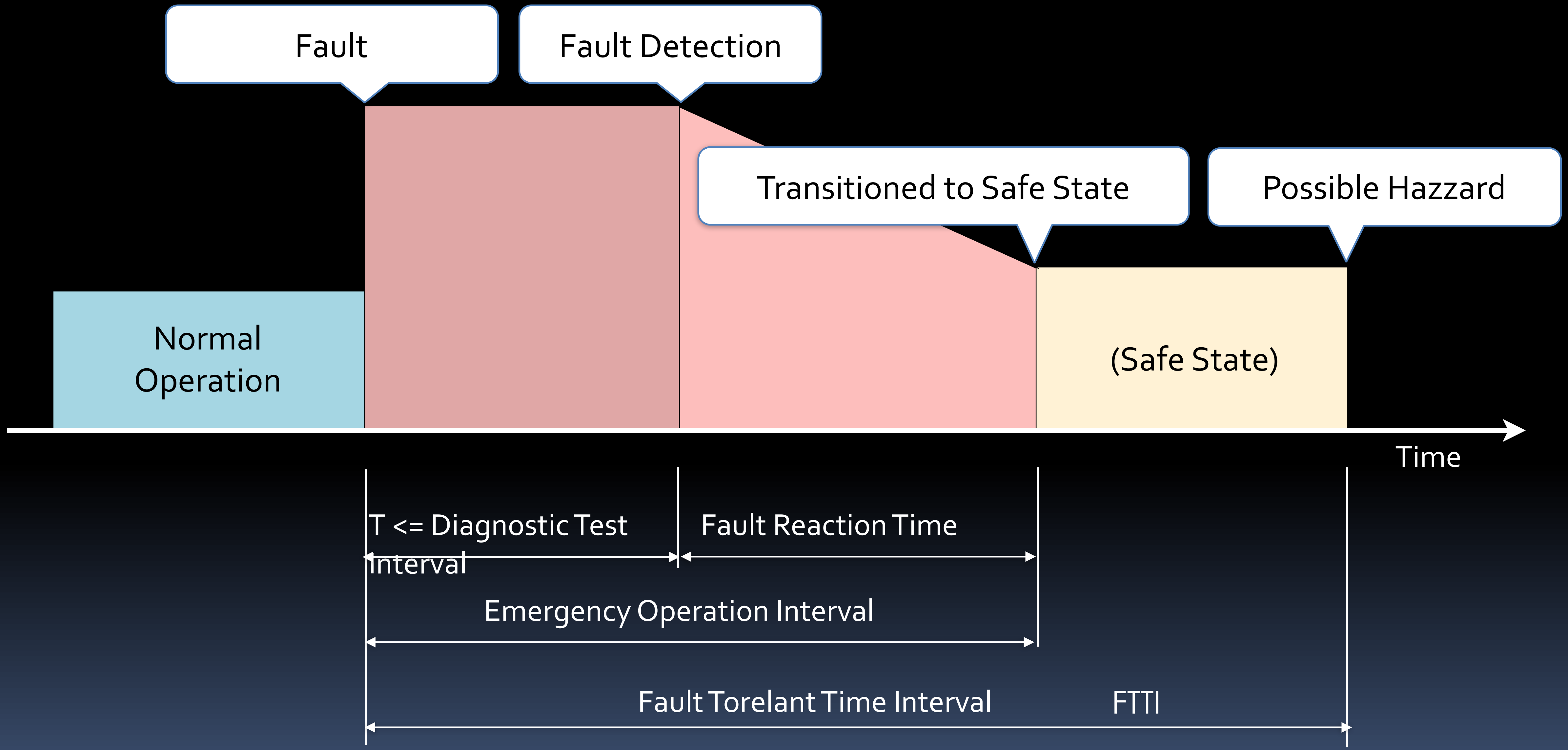
Detection in ISO 26262

- In 26262, fault detection is important, such as Fault Tolerant Interval Time (FTTI).

> *The safety goal can include features such as the fault tolerant time interval, or physical characteristics (e.g. a maximum level of unwanted steering-wheel torque, maximum level of unwanted acceleration) if they were relevant to the ASIL determination. (ISO 26262 3-7.4.4.6)*

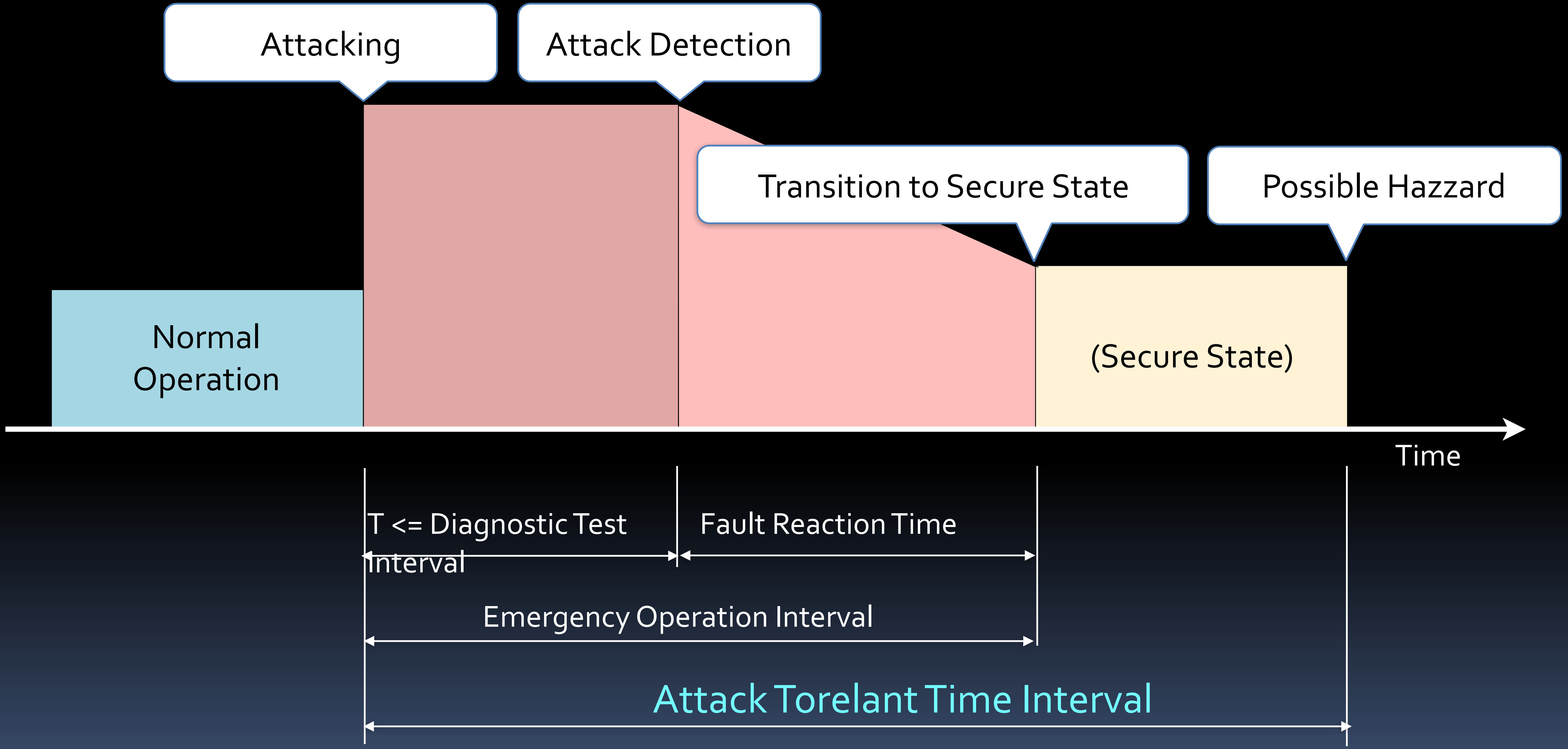


FTTI & Emergency Operation Interval


Fault
Fault Detection
Transitioned to Safe State
Possible Hazzard
Normal Operation
(Safe State)
Time
T <= Diagnostic Test Interval
Fault Reaction Time
Emergency Operation Interval
Fault Torelant Time Interval
FTTI

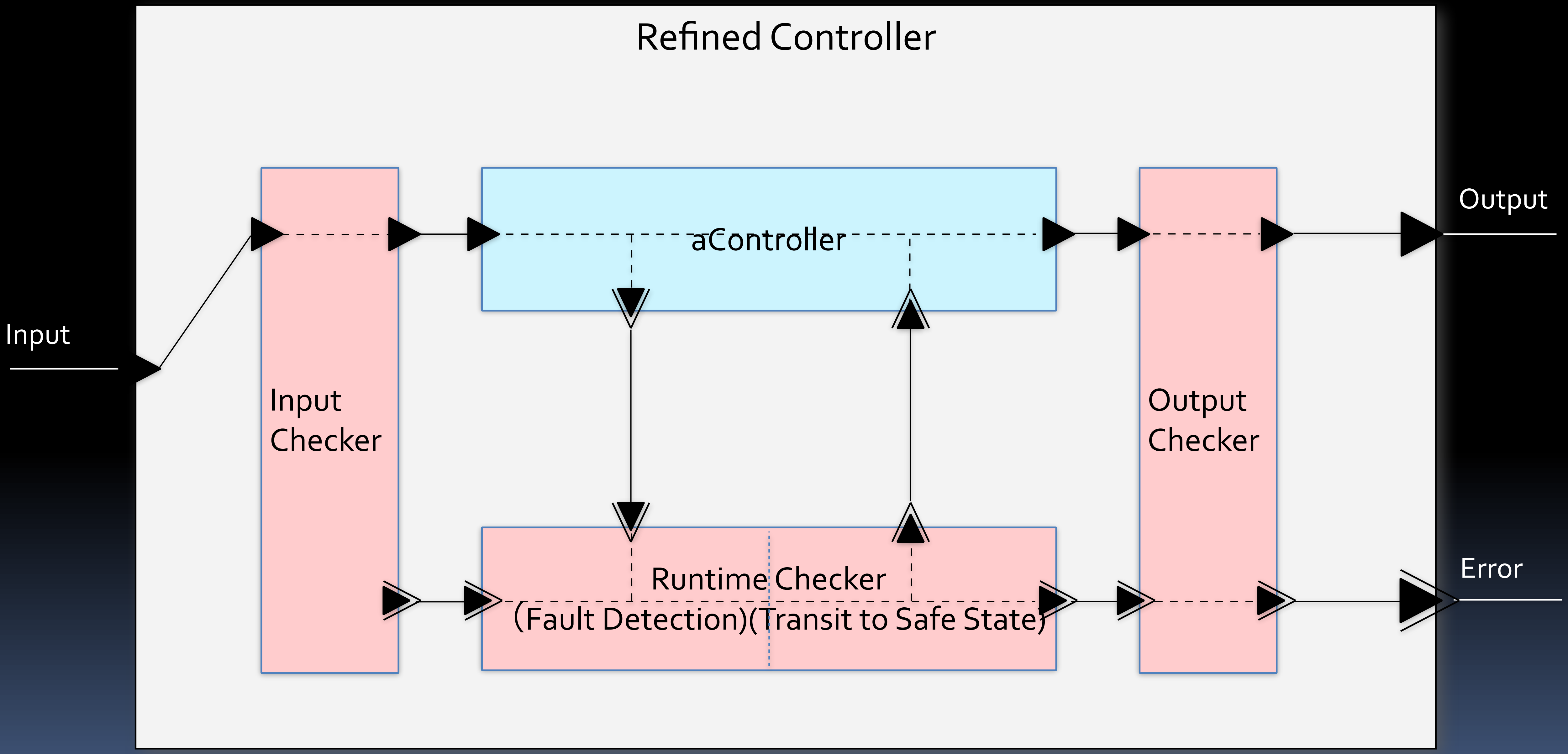
Fault reaction time and fault tolerant time interval (ISO26262-1 Fig.4)

ATTI: Attack Torelant Time Interval


Attacking
Attack Detection
Transition to Secure State
Possible Hazzard
Normal Operation
(Secure State)
Time
T <= Diagnostic Test Interval
Fault Reaction Time
Emergency Operation Interval
Attack Torelant Time Interval

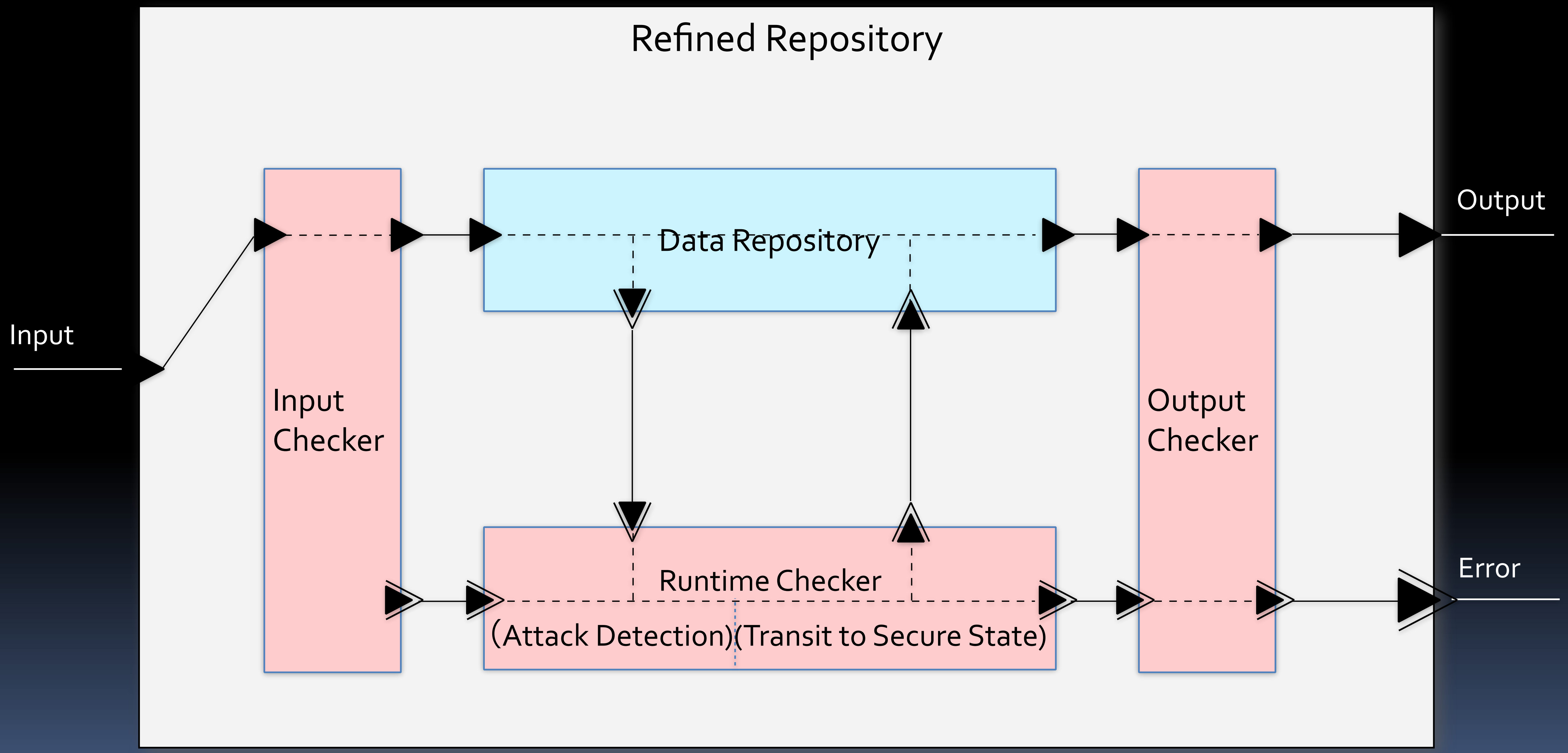
Generic mechanism to calculate FTTI

- To calculate FTTI, we need the various flow paths



Generic mechanism to calculate ATTI

- Detection mechanism and calculation of ATTI



Conclusion

- In industry 4.0 era, the network of a company will be opened to other company to communicate each other. So, we have to focus on the security and data that is transferred between companies and stored in those companies.
- The IACS uses the zone and conduit model to keep them secure. The zone is in a layer according to its security level. The conduit is the communication channel between the zones. We have to think the security of zone (and the data in it) and conduit.
- As for concept model, there are some differences between security standard (IEC 62443) and the safety standard (ISO 26262). In ISO 26262, we give the ASIL to an item, that is the abstraction of the system. On the other hand, in IEC 62443, we just assess the requirement and context in the context phase. In the next step, we give the SL to each zone (and conduit). We need the zones and conduits after first design.

Conclusion

- The zone and conduit model has the rationale. However, if anything breaks it, it is hard to detect the intruder and to protect a system. In this presentation, we provide the model for detection based on the ISO 26262 definition and our approach for FTTI calculation. The ATTI is the attack tolerant time interval, and to assure this ATTI we can use the mechanism for attack detection.