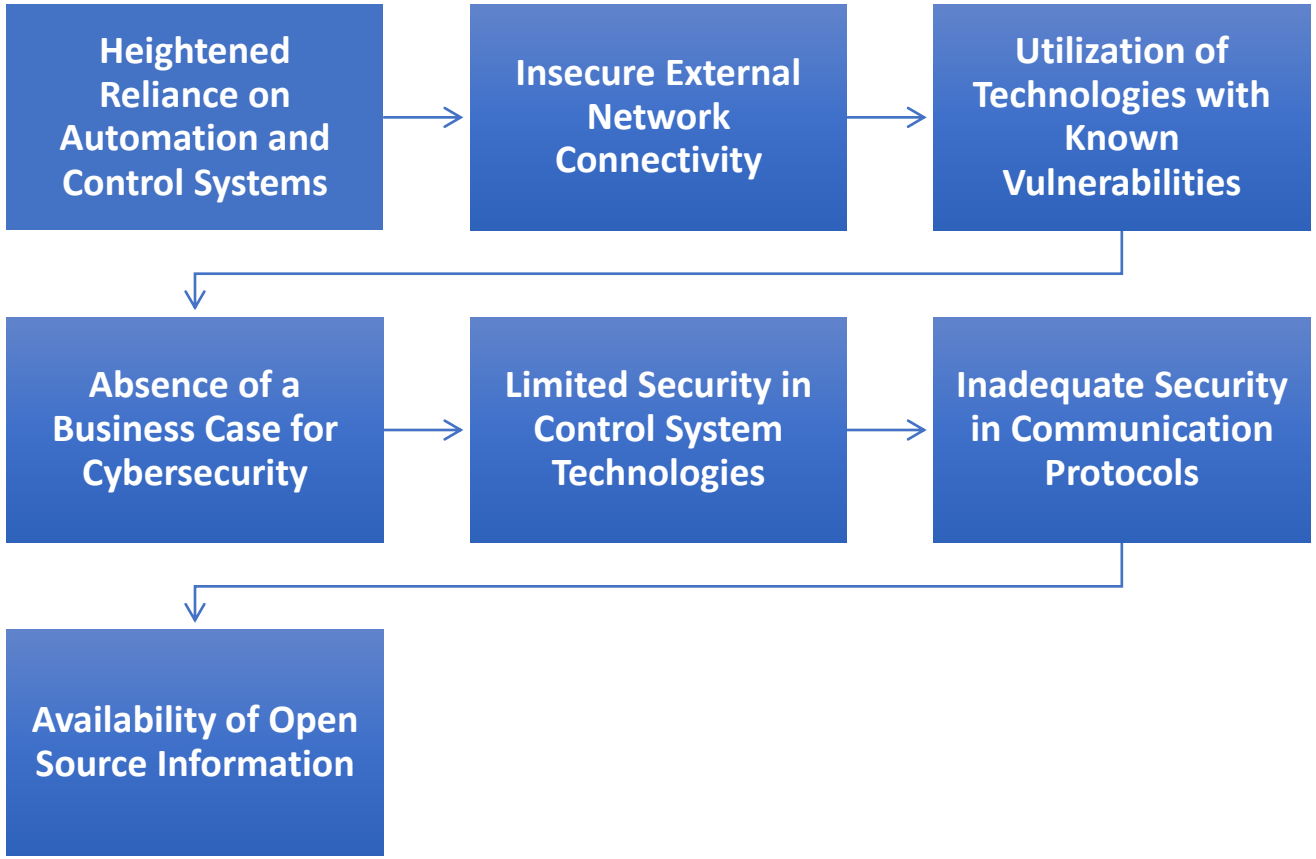
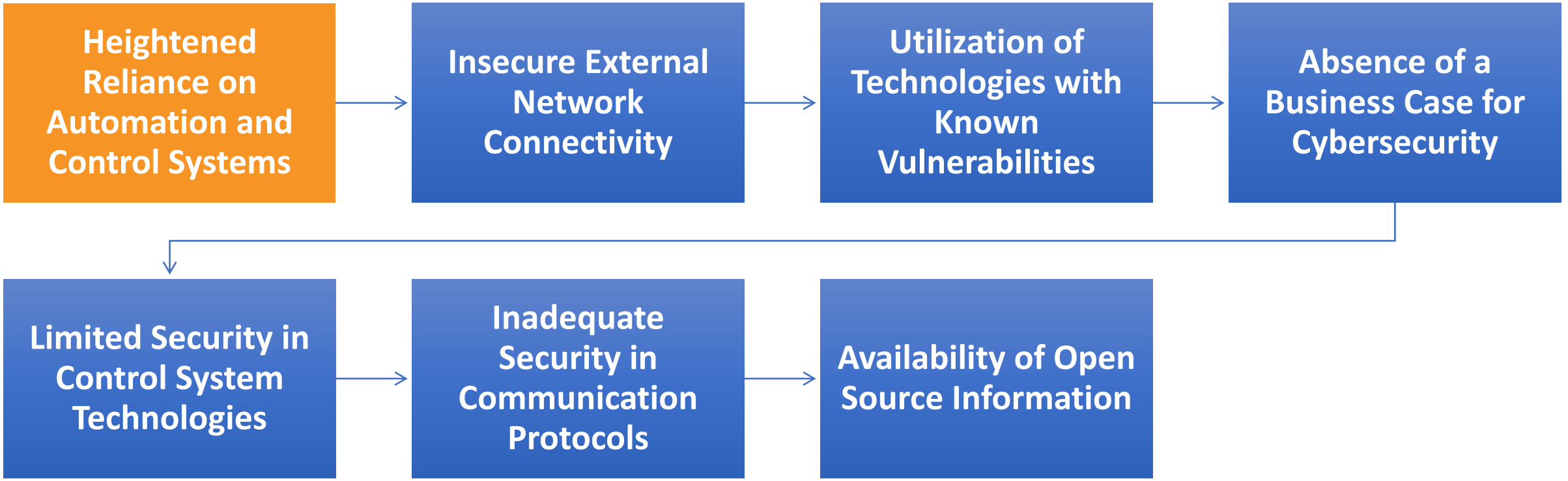
PROJECT
ENG
PRO

CYBER SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

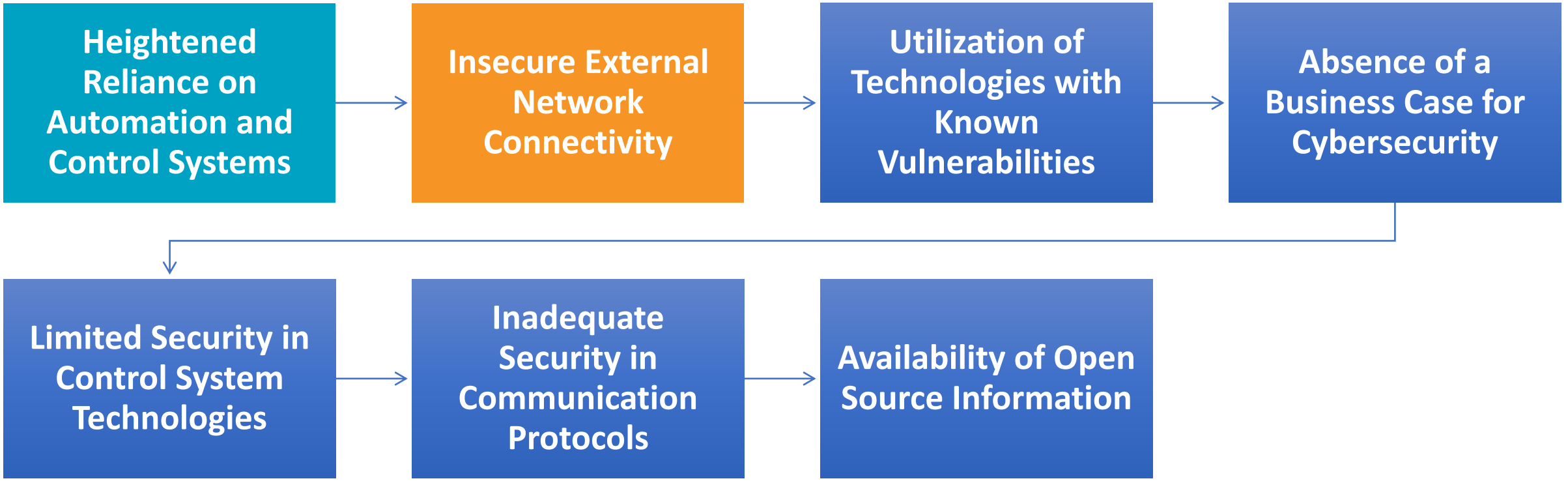
By Project ENG PRO

Contemporary Control System Architectures

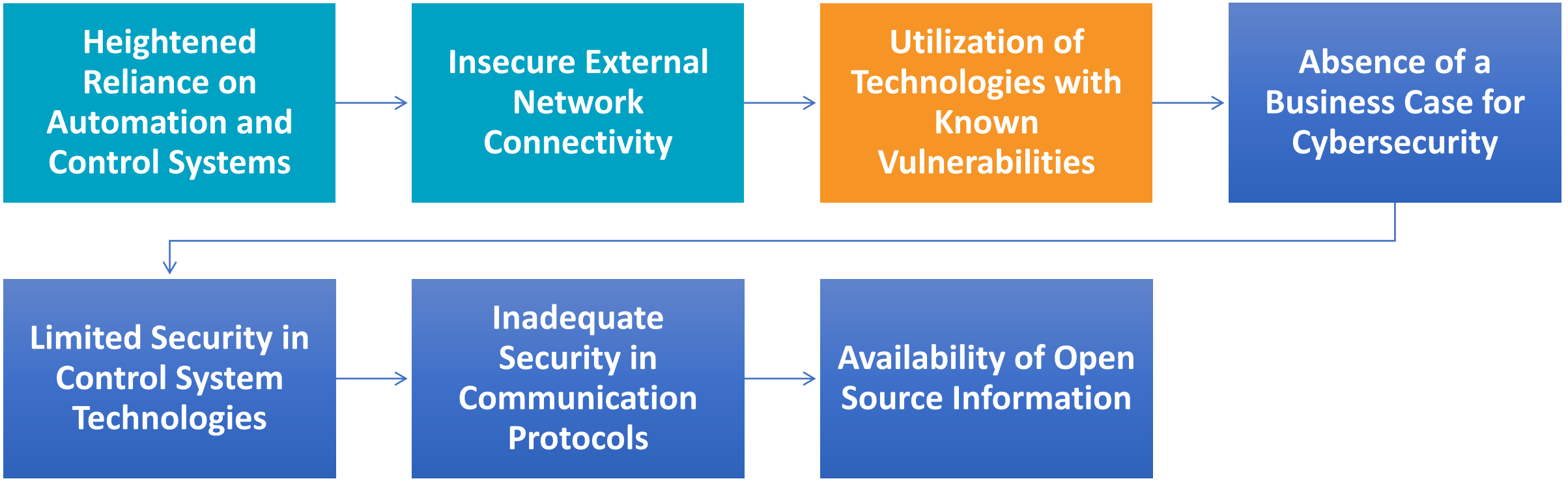




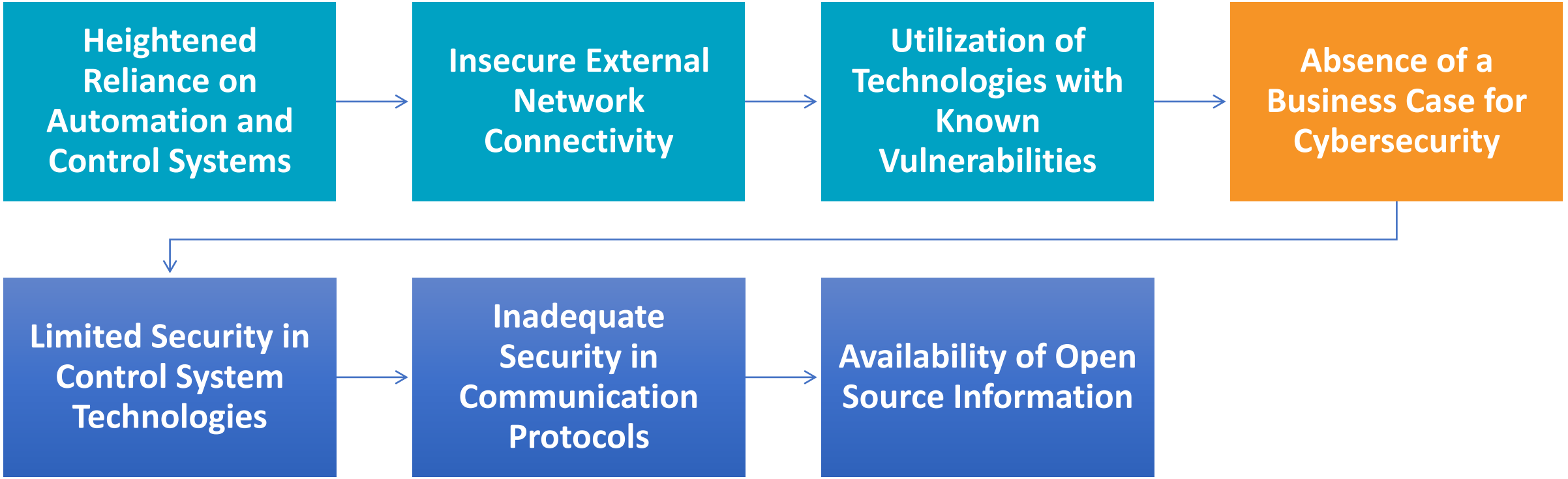
Several driving factors contribute to the increase in security lapses or problems within control systems. One of the primary factors is the growing dependency on automation and control systems.



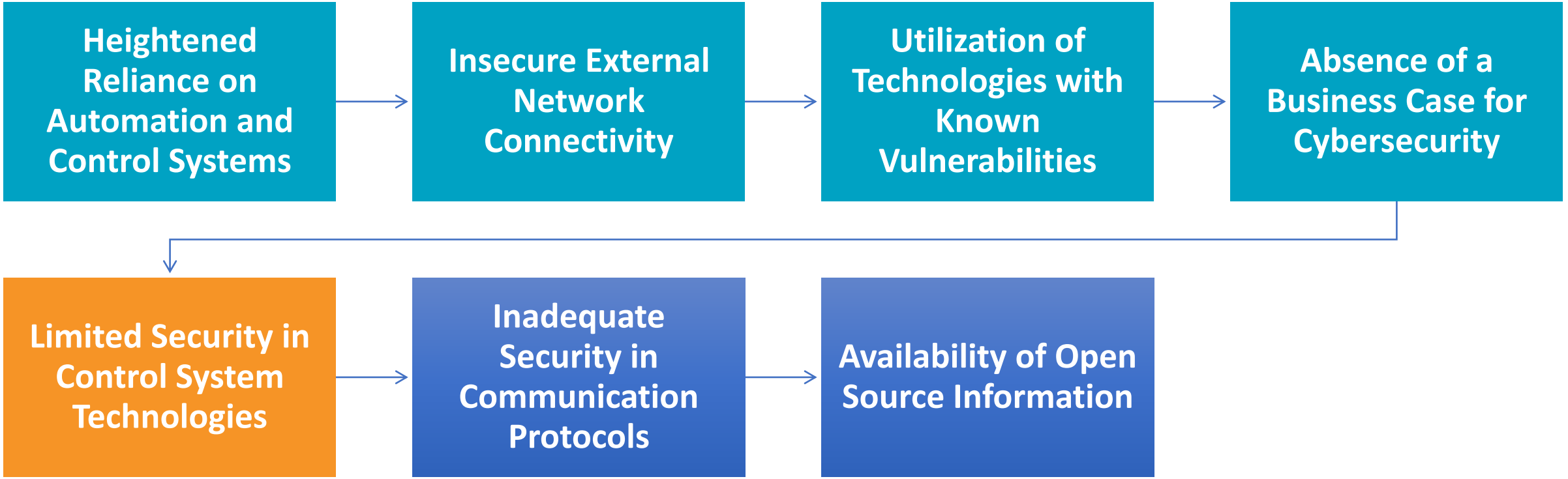
As control systems generate vast amounts of data, there is a desire to connect these systems with external networks to facilitate easier data access and derive valuable insights.



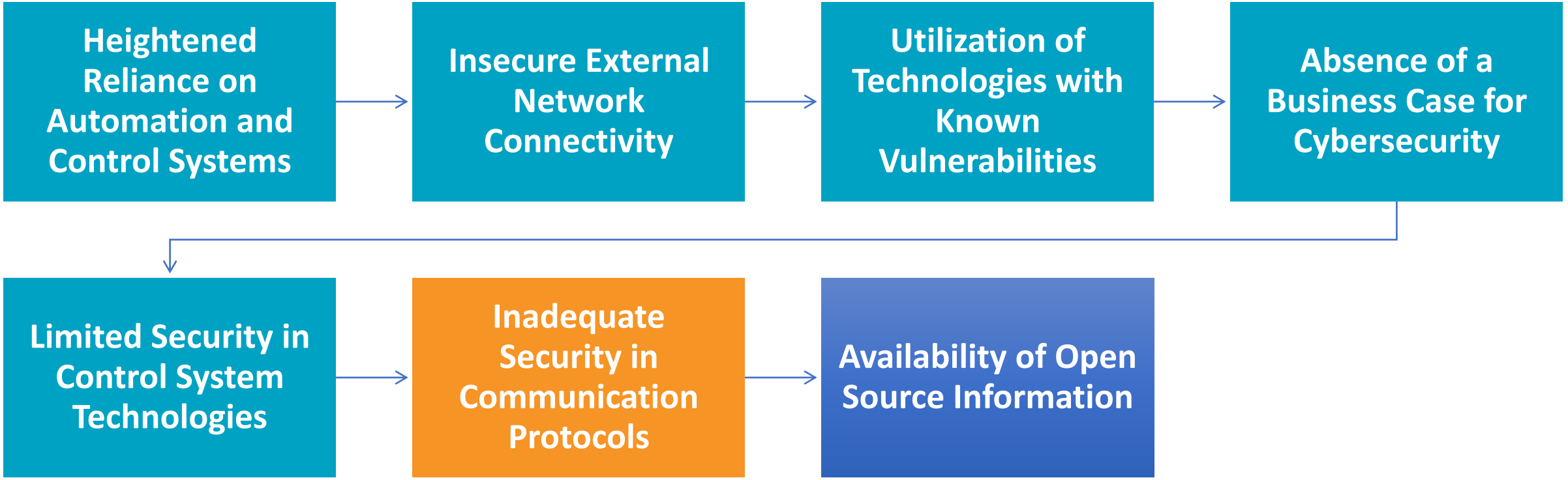
Control systems often become highly dependent on specific technologies, and even if vulnerabilities are discovered, it may be impractical to upgrade or replace these technologies.



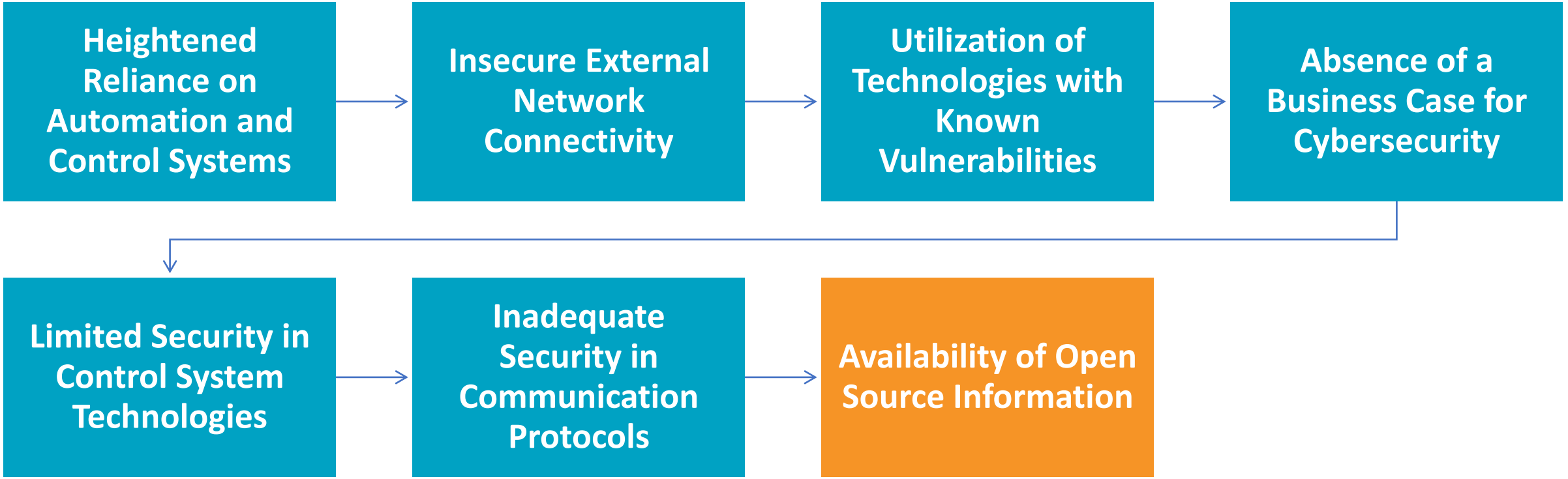
Quantifying the tangible return on investment for cybersecurity measures can be challenging, which can discourage organizations from prioritizing security in control system implementations.



Control system technologies themselves may have limited built-in security capabilities. In some cases, the security capabilities provided by vendors are only enabled if the administrator is aware of their existence.



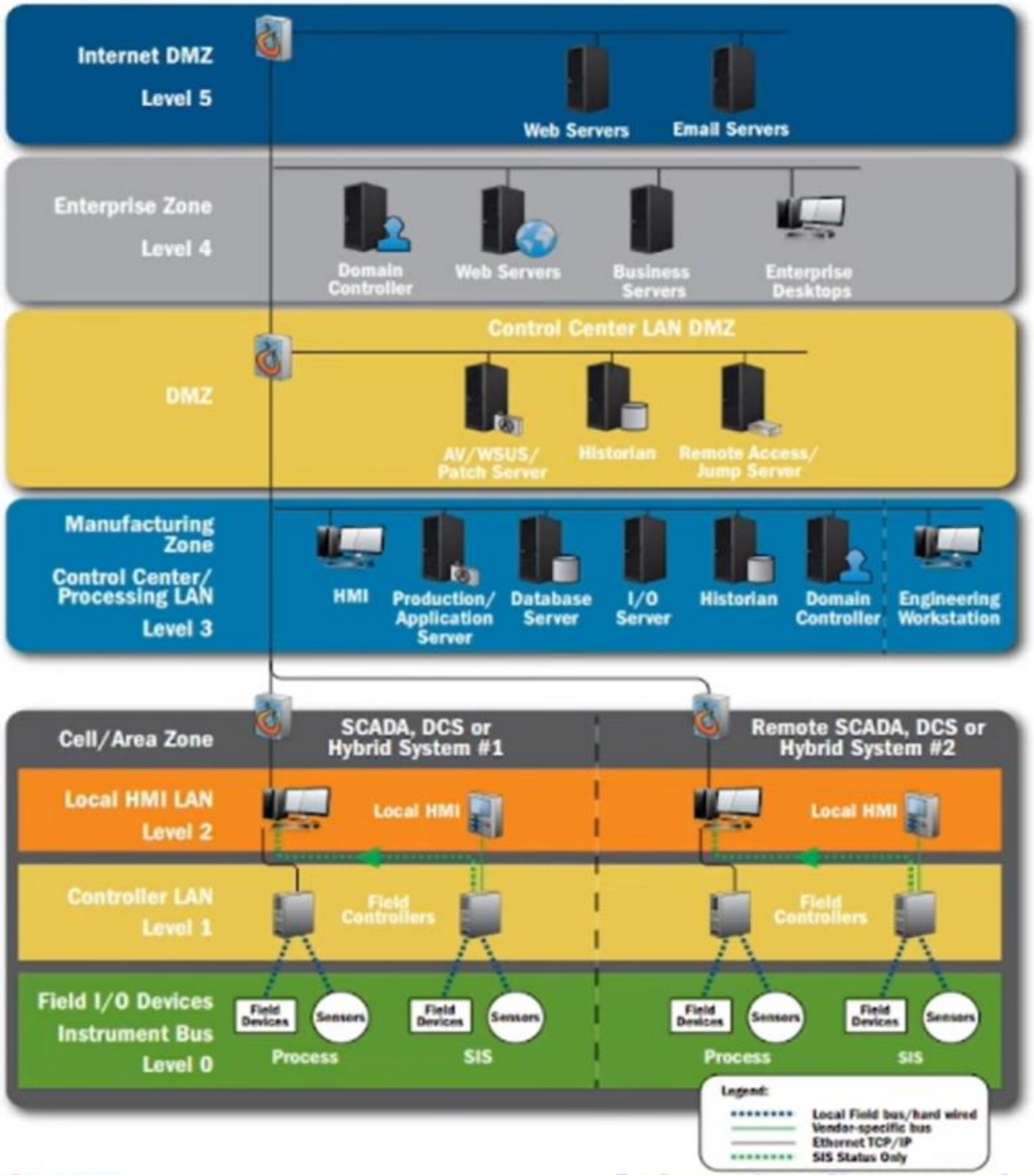
Many control system communication protocols lack built-in security functionality. For example, protocols like RS232 serial communication or OPCDA often do not support encryption or secure communication methods, making it challenging to add robust cybersecurity measures.



Another vulnerability stems from the considerable availability of open-source information regarding control system configuration and operation.

ICS Network Architectures

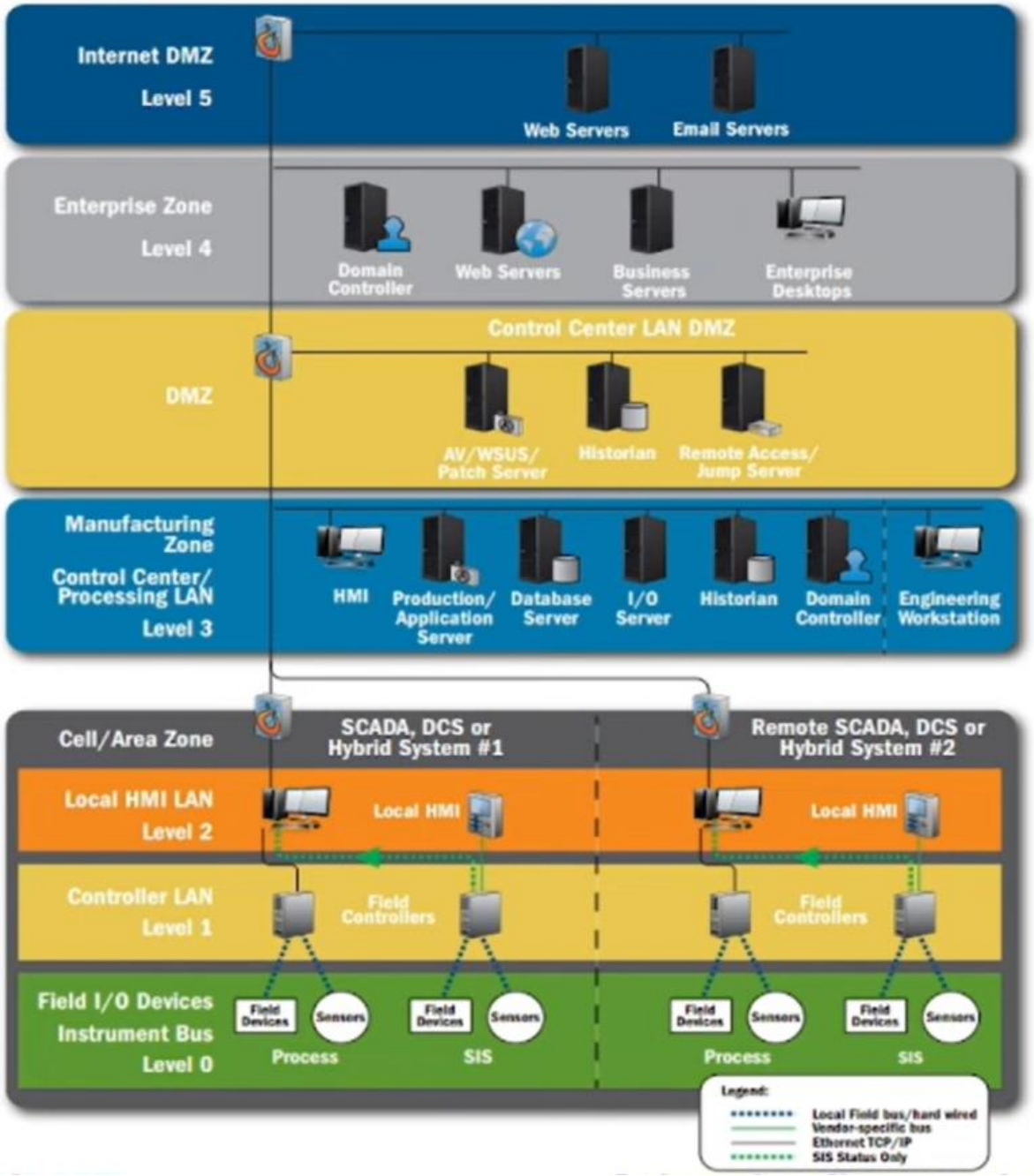
This architecture is referred to as the integrated architecture, and it adheres to the Purdue model. This model provides insight into the widely accepted hierarchy of control systems.



ICS Network Architectures

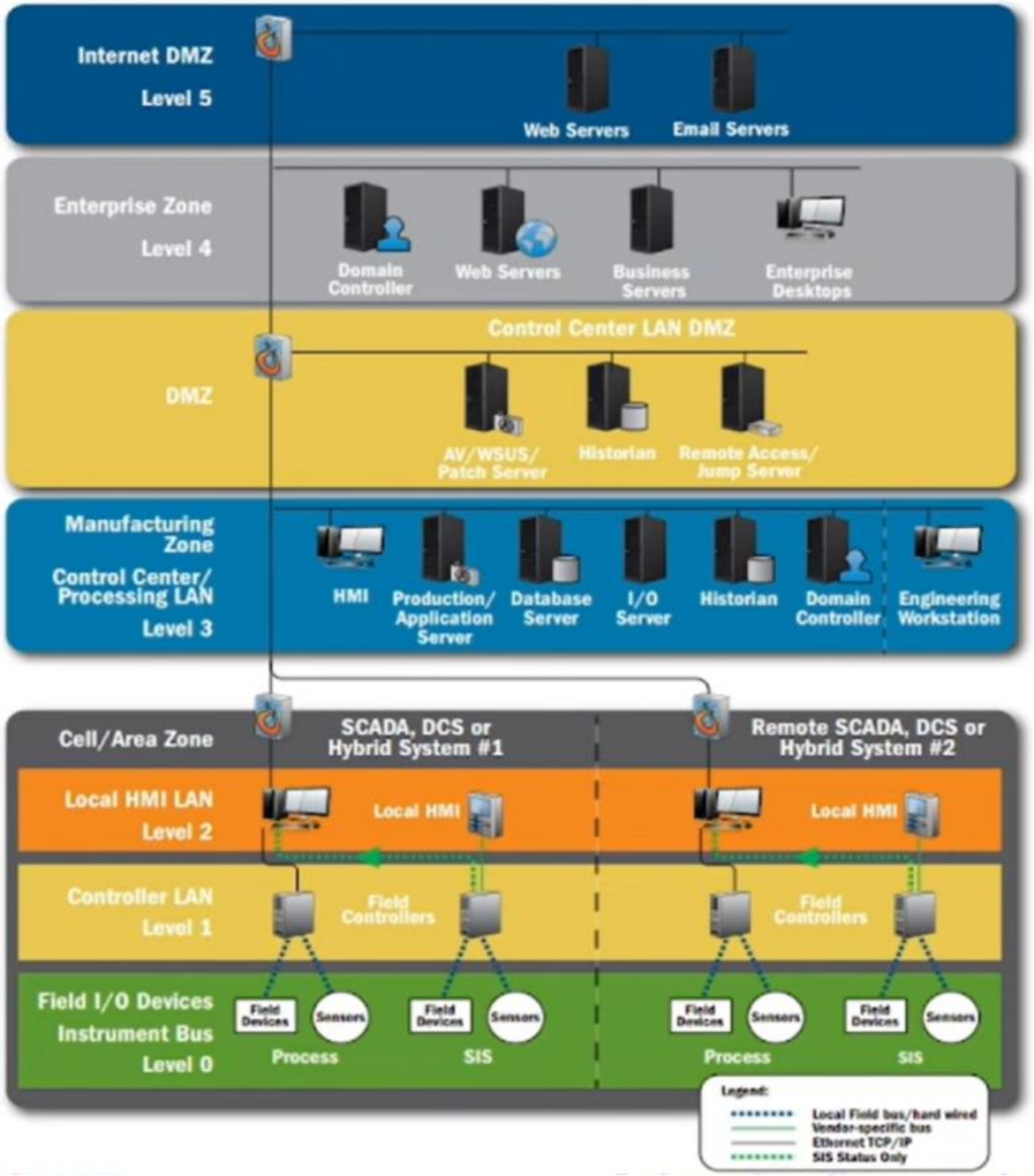
The network comprises various levels, each designed to accommodate specific functionalities and security controls:

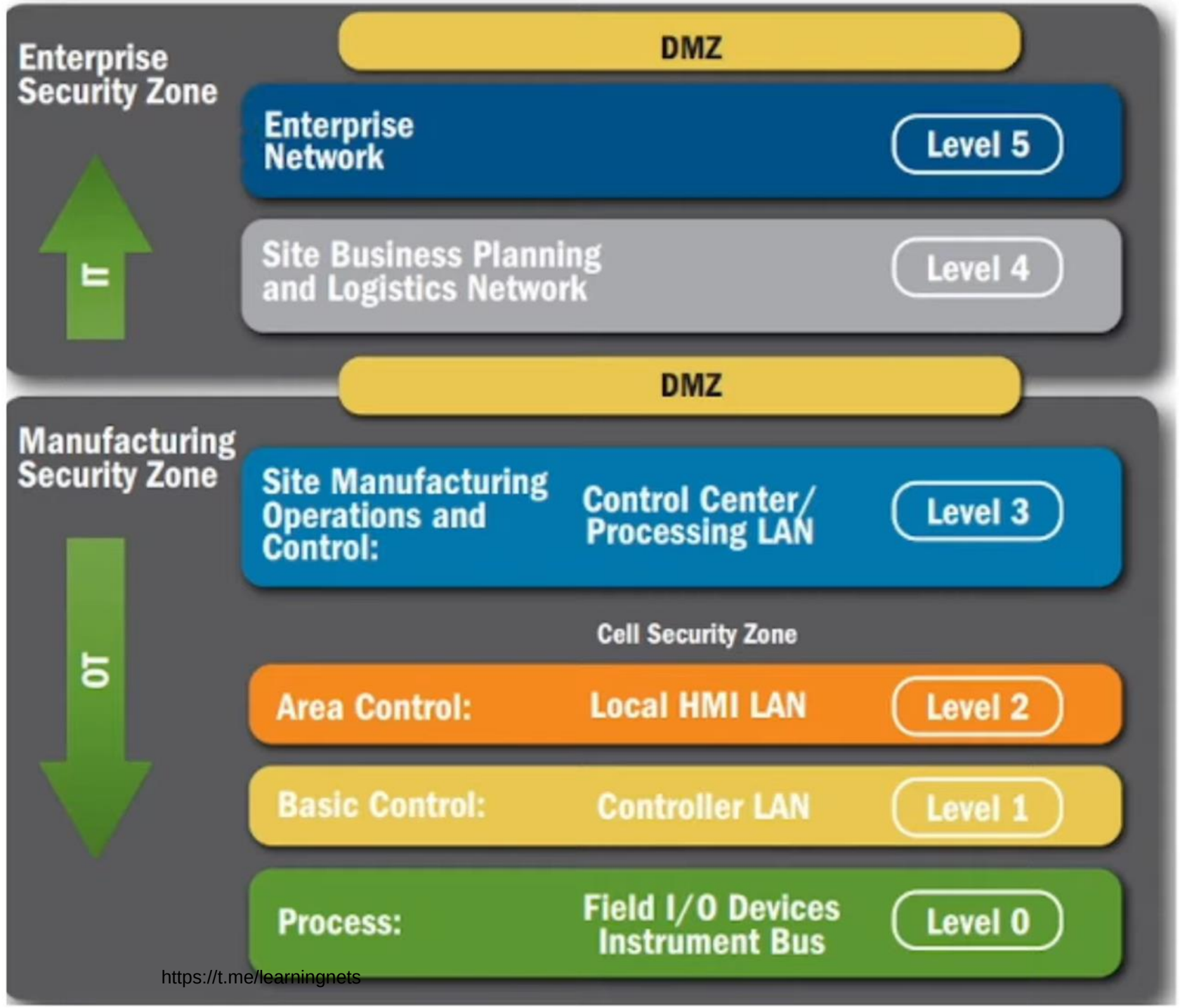
1. Field Devices and Sensors (Level 0)
2. Controllers and Local HMI (Level 1)
3. Cell/Area/Zone (Level 2)
4. Manufacturing Control Center (Level 3)
5. DMZ (Demilitarized Zone
6. Enterprise Zone



ICS Network Architectures

This standardized architecture enhances security through segmentation and controlled access. Understanding the architectural zones and aligning servers accordingly empowers organizations to design a robust and tailored cybersecurity strategy, safeguarding their ICS environment effectively

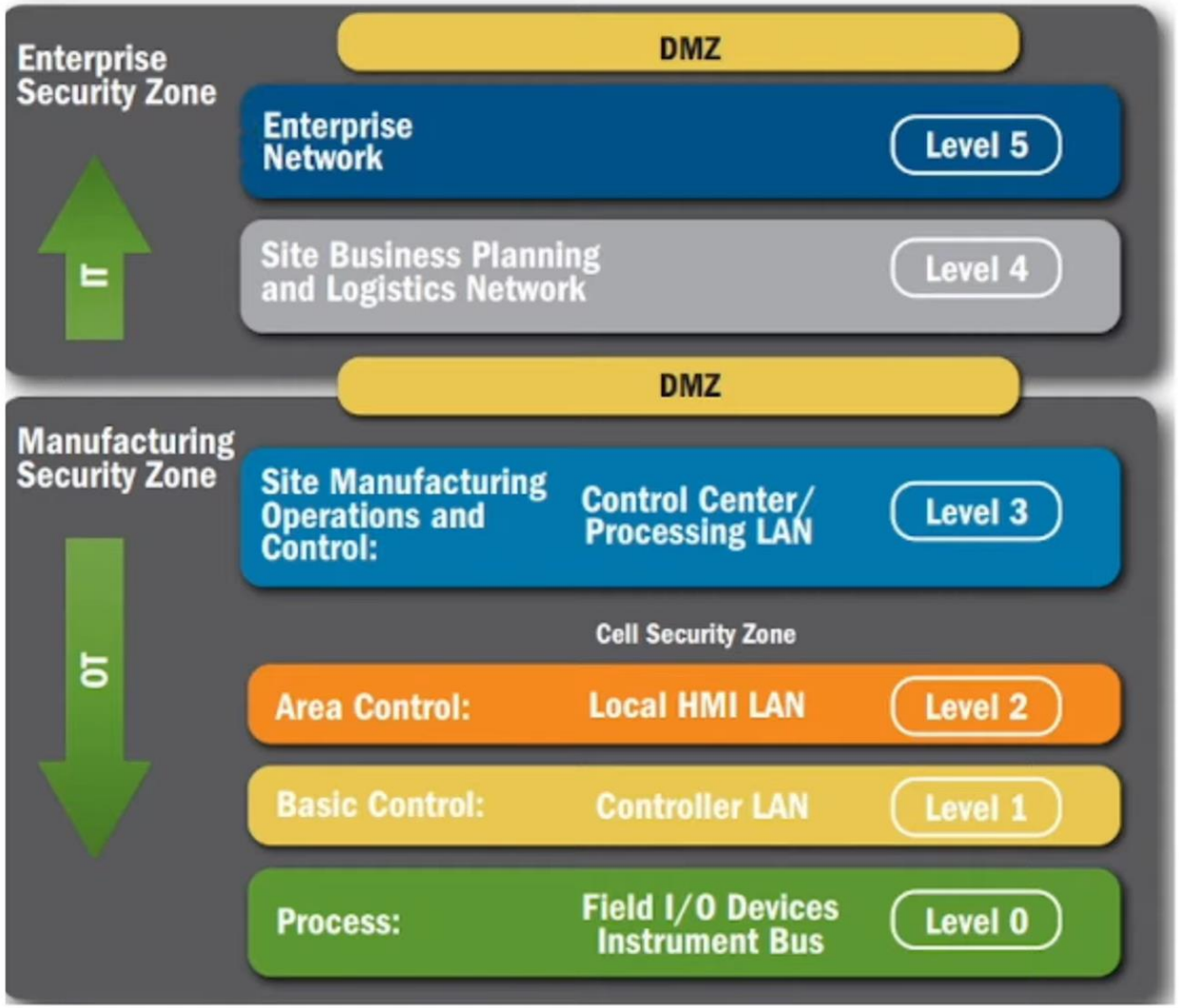


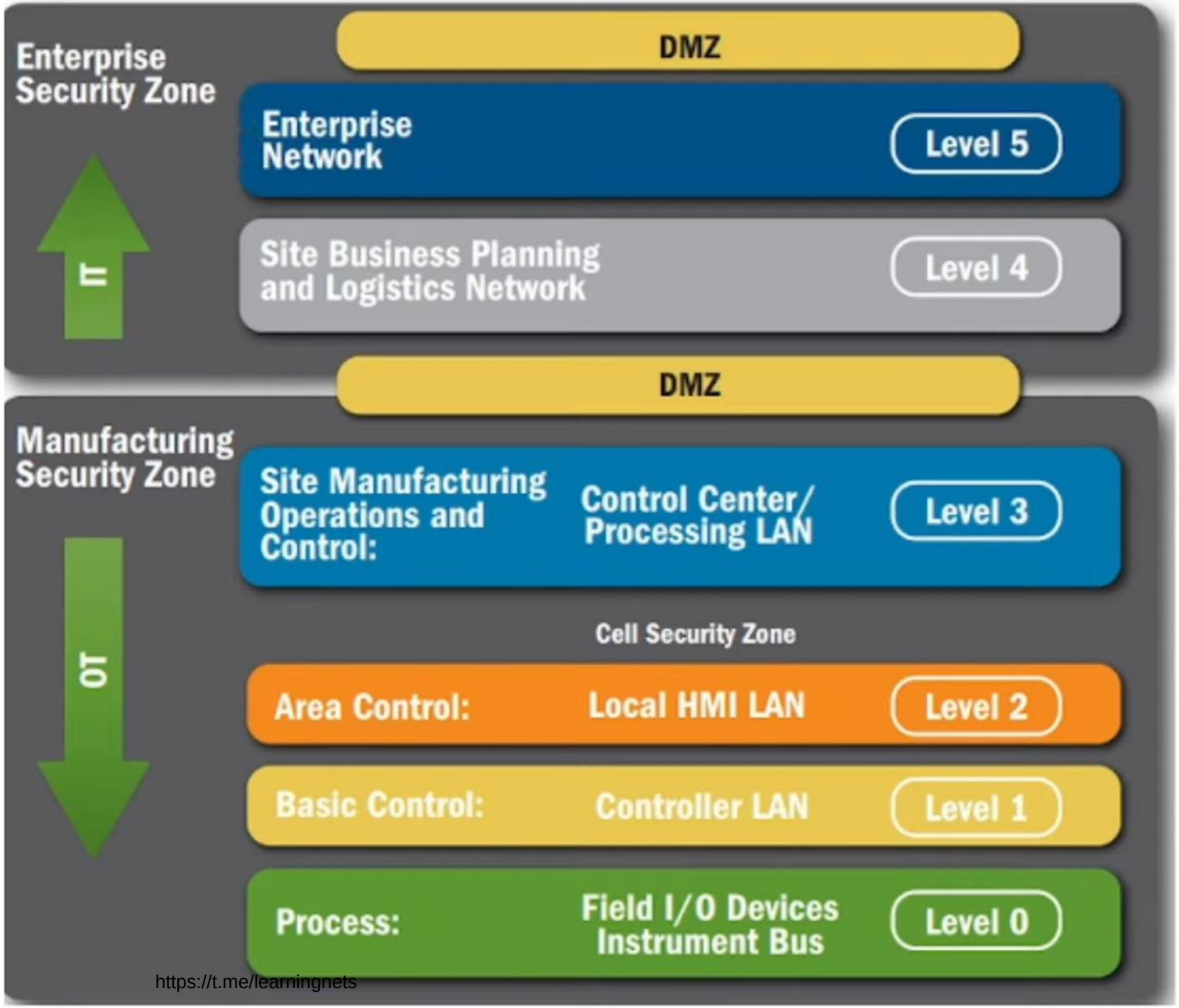


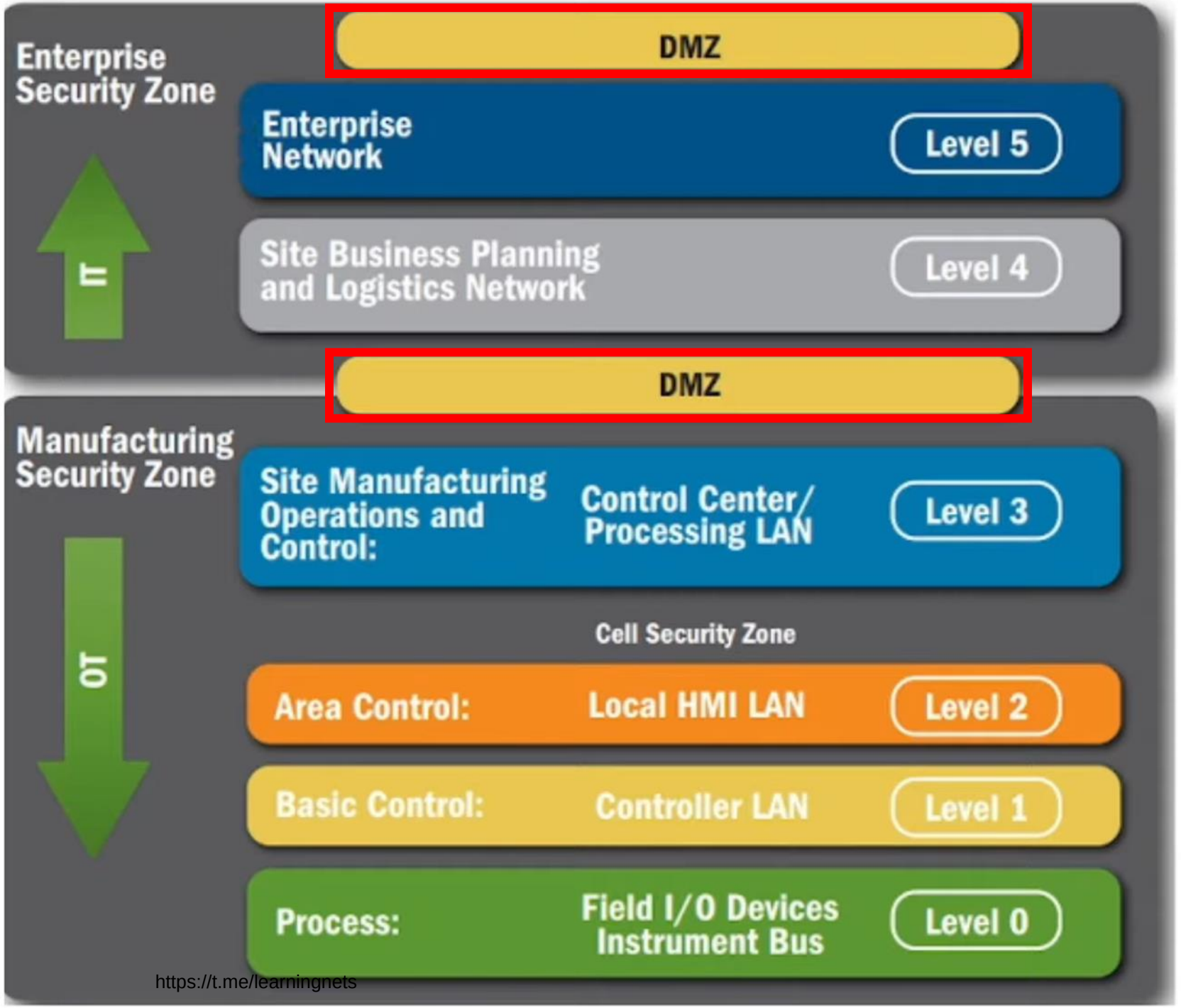
ICS Network Architectures

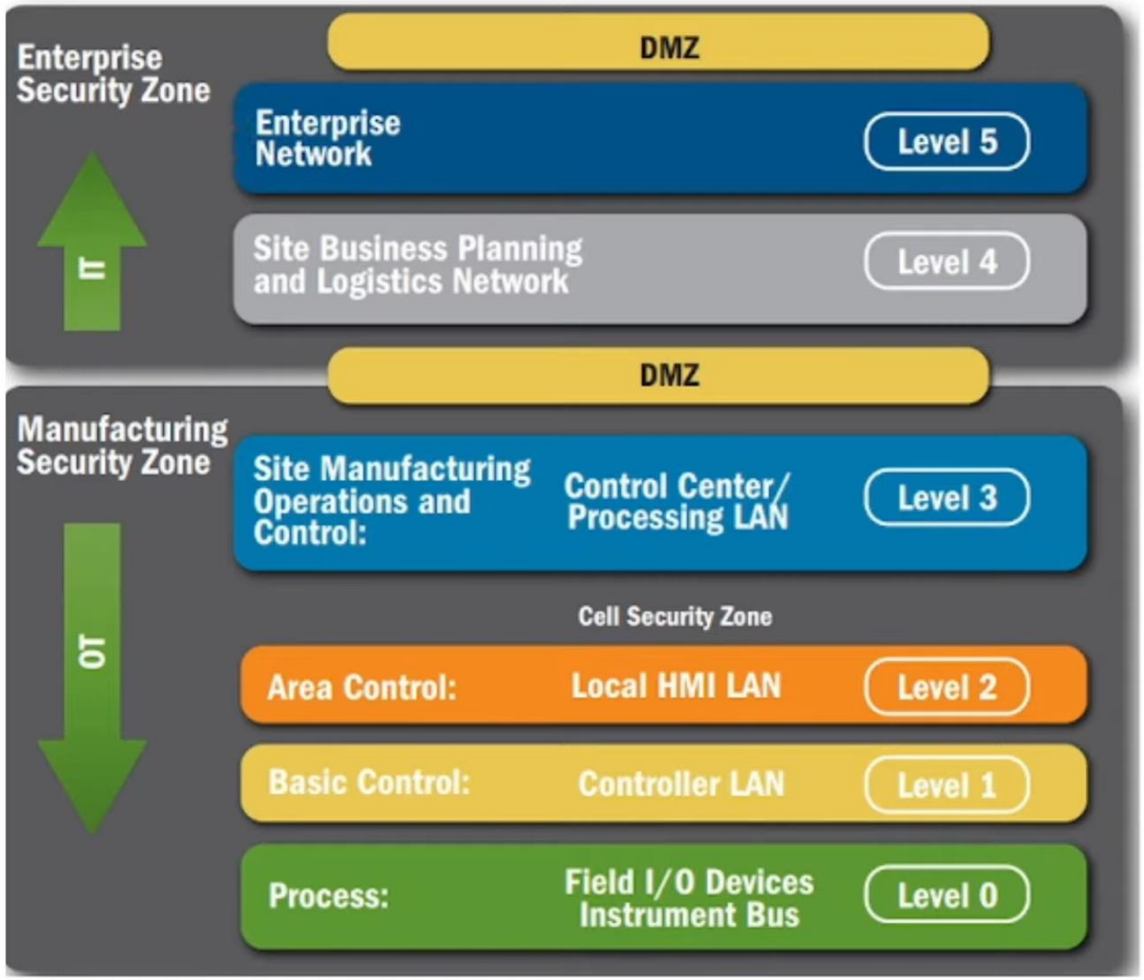
Achieving network segmentation is a critical step in defining these architectural zones. Let's explore the specific zones within this model:

1. Enterprise Security Zone (Level 4 and 5)
2. Manufacturing Zone (Level 3)
3. Cell Security Zone (Level 2)









ICS Network Architectures

Adopting this recommended architecture design provides heightened security and a clear visual representation for both designers and engineers. It facilitates the implementation of multiple layers of cybersecurity, ensuring robust protection while accommodating various technology components and interconnections.

Wrap Up

- IT integration into control systems brings security challenges and increased attack surface.
- Factors like automation reliance, connectivity, vulnerable tech, and control system limitations contribute to issues.
- Solutions: recommended architectures, clear zones, network segmentation, and DMZs.
- Enhancing control system security requires staying informed, implementing robust measures, and constant improvement.