PROJECT
ENG
PRO

CYBER SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

By Project ENG PRO

FR 3 – System Integrity

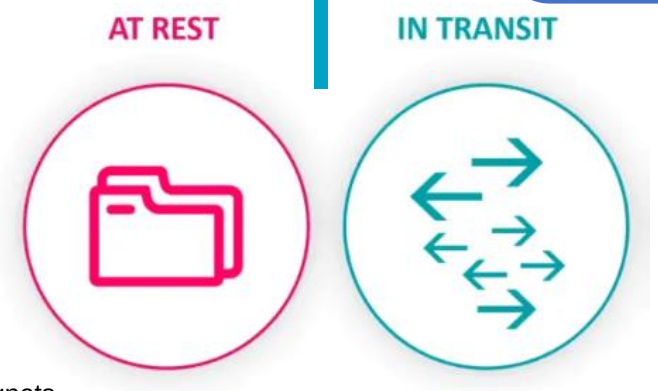
- FR1 – Identification, authentication and access control
- FR2 – Use Control
- FR3 – System Integrity
- FR4 – Data Confidentiality
- FR5 – Restrict Data Flow
- FR6 – Timely response to event
- FR7 – Resource Availability

Data Security

Data security encompasses safeguarding data confidentiality, integrity, and availability, both at rest and in transit.

Data at Rest

Data in Transit



Data at Rest

To fulfill FR 3, organizations should use encryption, access controls, monitoring, and backup processes to safeguard data at rest from unauthorized access or modifications, ensuring its integrity and availability.

Data at Rest

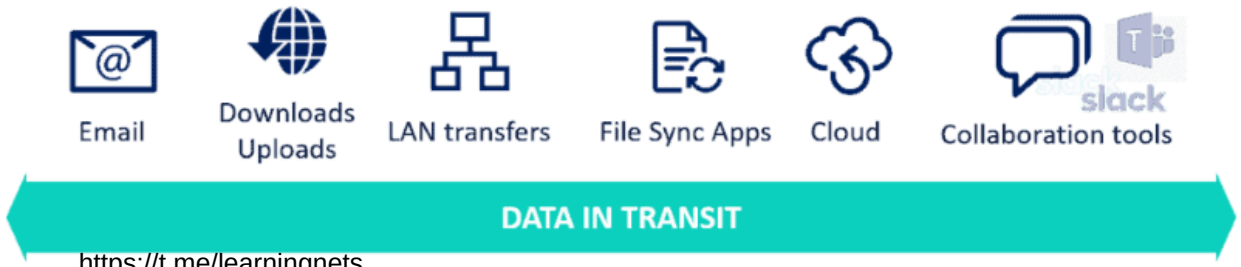
Data in Transit

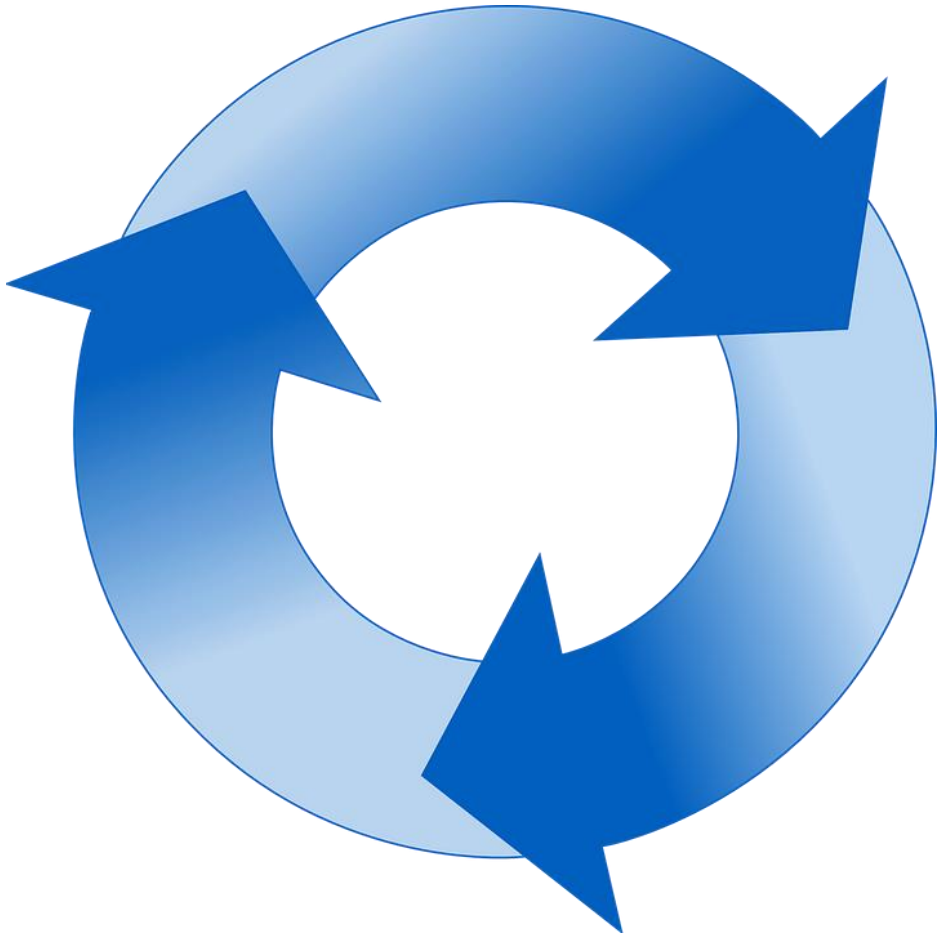
Data in Transit

To address FR 3, organizations should use encryption, secure protocols, and authentication to safeguard data in transit, while continuous network monitoring detects threats and upholds data integrity.

Data at Rest

Data in Transit





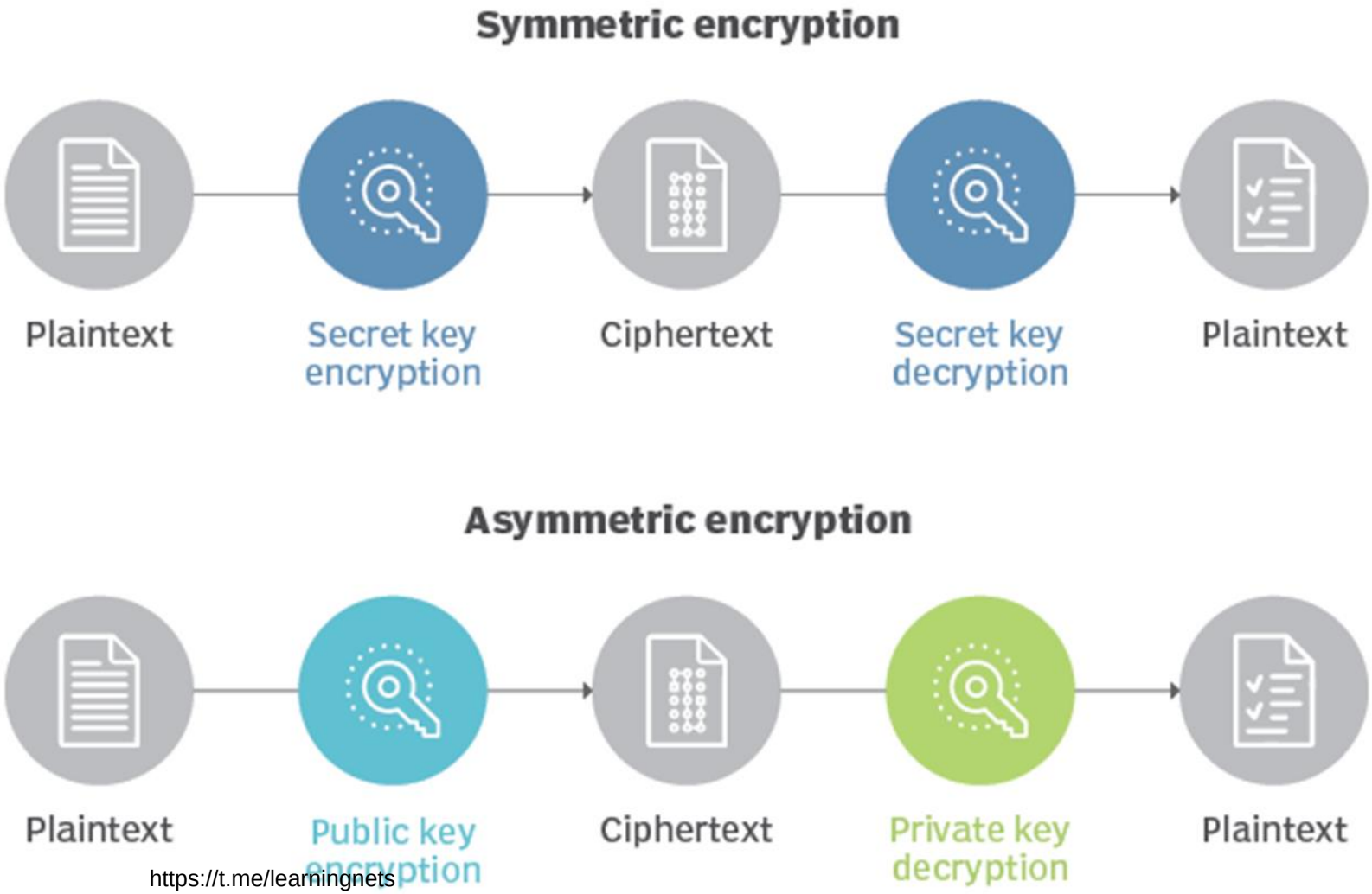
Beyond securing data at rest and in transit, it's crucial to extend protection to assets post-removal and prevent leaks, necessitating robust security measures across the data lifecycle.

Data Life Cycle

Cryptography

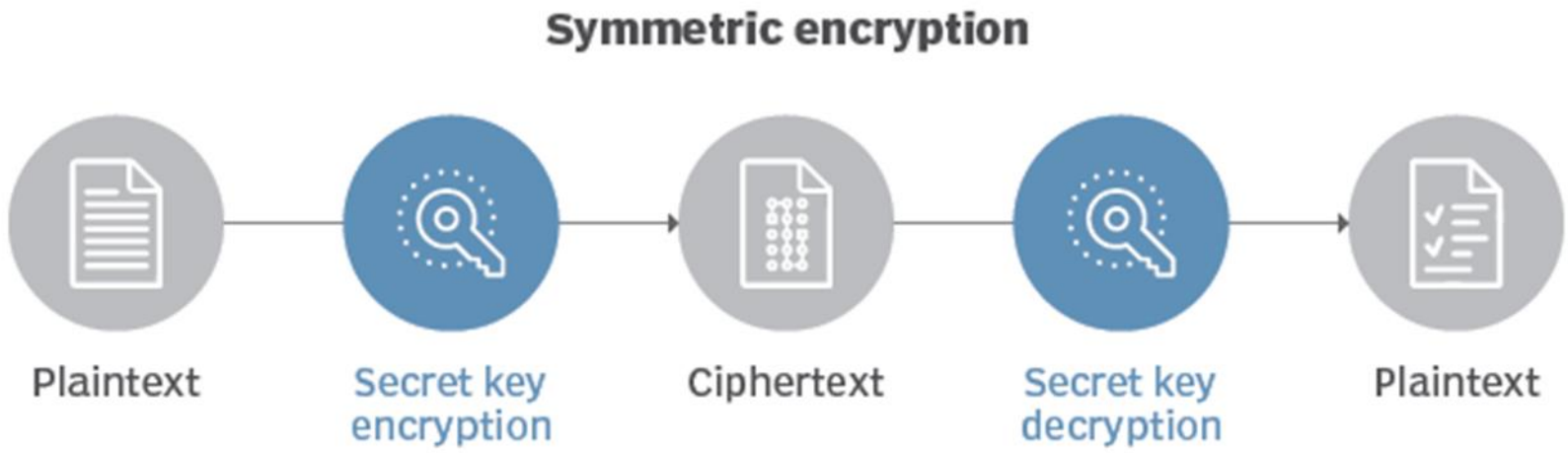
Cryptography secures industrial control systems with encryption, digital signatures, and hashing, protecting data confidentiality and integrity.

Encryption



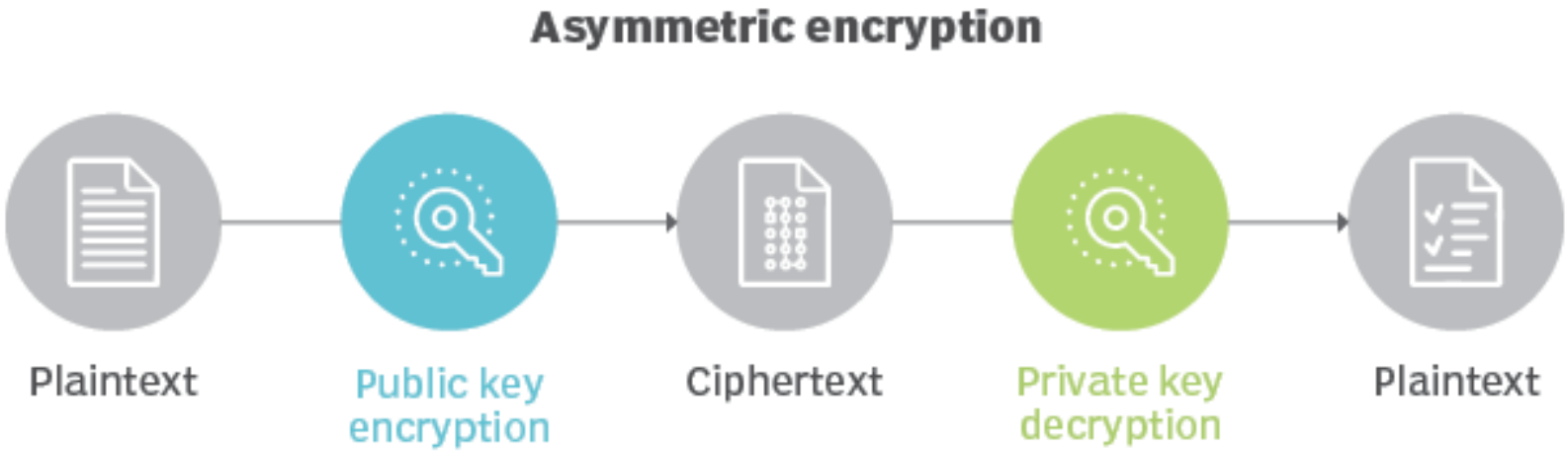
Encryption

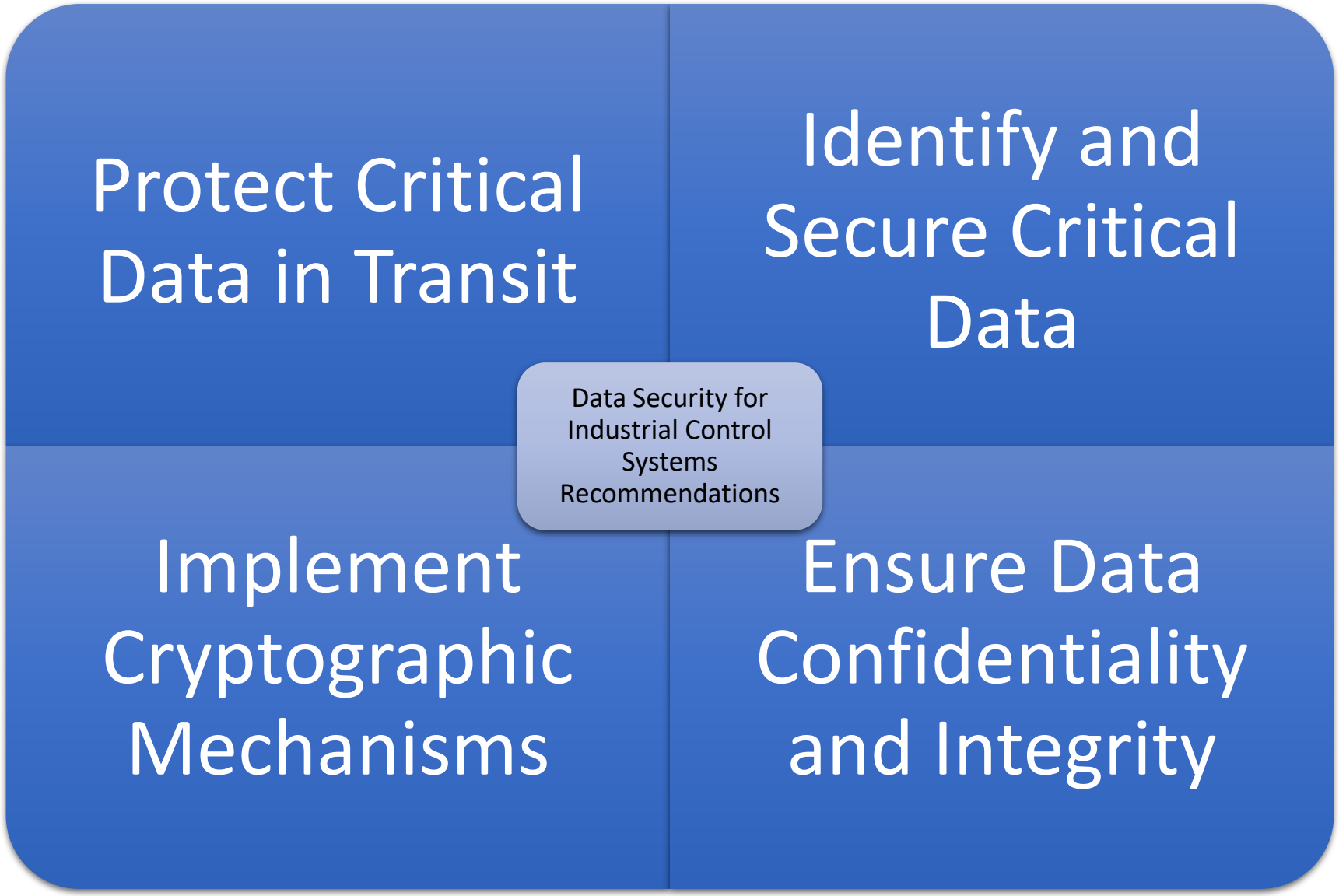
Symmetric encryption uses a single secret key to both encrypt and decrypt data, ensuring its confidentiality and integrity during transmission and storage.



Encryption

Asymmetric encryption involves a pair of keys: a public key for encryption and a private key for decryption, enhancing security and enabling secure communication and authentication.





Wrap Up

- Focus on the third foundational requirement: safeguarding ICS integrity to prevent unauthorized manipulation.
- Explores data security for data at rest and in transit, emphasizing the role of cryptography.
- Covers encryption, digital signatures, hashing, and more as cryptographic techniques.
- Recommendations include protecting critical data during transit, implementing encryption, and ensuring confidentiality and integrity.