Kry10 OT Network Guard

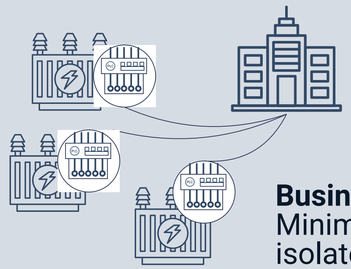
Inline, formally verified protocol defence for legacy OT

1.Vulnerability Evolution

How the OT vulnerability environment has evolved over the last 30 years

Mid 90s - 2000s

PLCs connected over isolated or private OT network

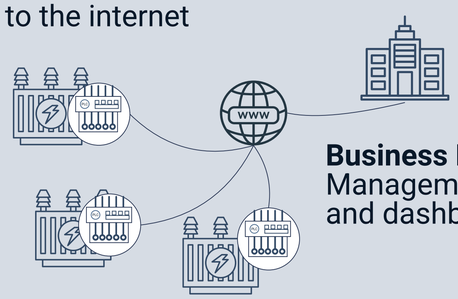


Business Priority:
Safety not security

Business Challenge:
Minimal metrics available from isolated networks

2000s - 2010s

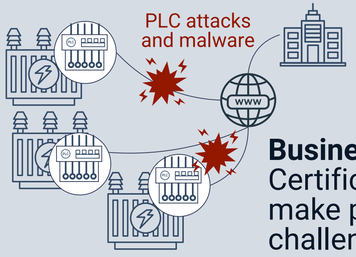
OT Networks become networks become connected to the internet



Business Priority:
Management data, metrics and dashboards

2010s - Present Day

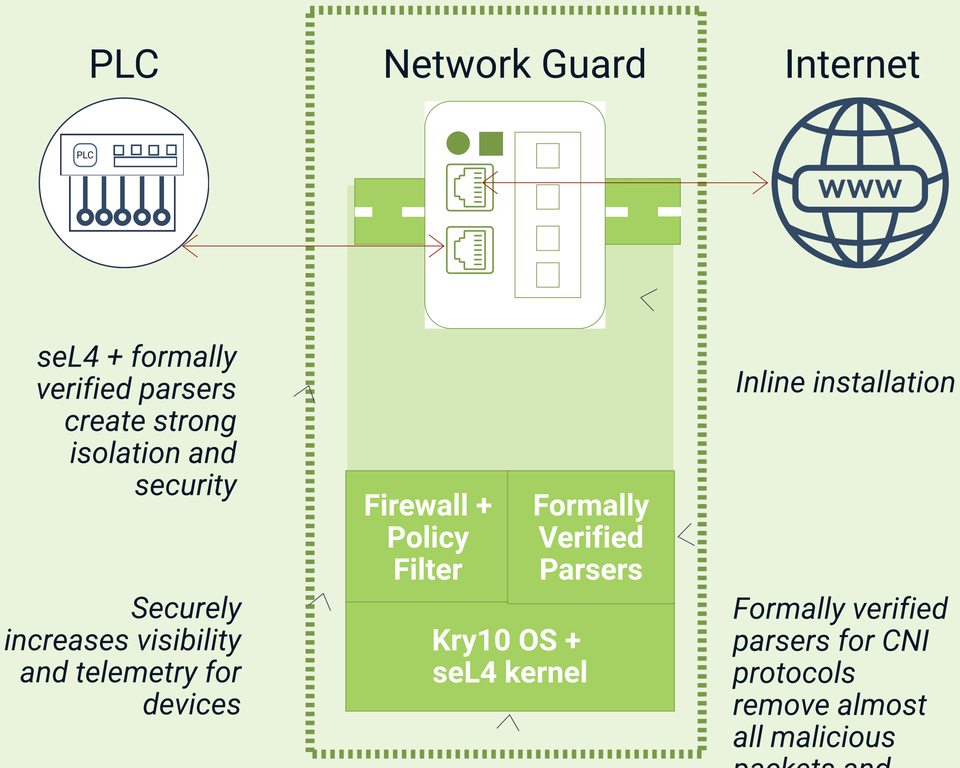
Threat actors access OT networks via the internet



Business Priority:
Maintaining service levels while under attack.

Business Challenge:
Certification and safety requirements make patching and cyber security challenging

2.Network Guard resolves the challenges



seL4 + formally verified parsers create strong isolation and security

Inline installation

Securely increases visibility and telemetry for devices

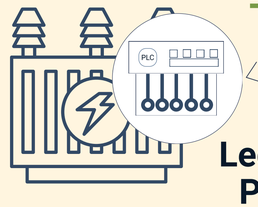
Formally verified parsers for CNI protocols remove almost all malicious packets and ensure standards compliance

Kry10 OS, backed by seL4, prevents Network Guard from becoming a target or an access vector

3.Threat Scenario

Attacker sends a malicious packet targeting a PLC vulnerability

Malicious packet is dropped at the Network Guard boundary



Legacy PLC

Checked and compliant commands pass through

- ✓ No network re-configuration
- ✓ No PLC recertification
- ✓ Legacy PLC remains unchanged

KRY10