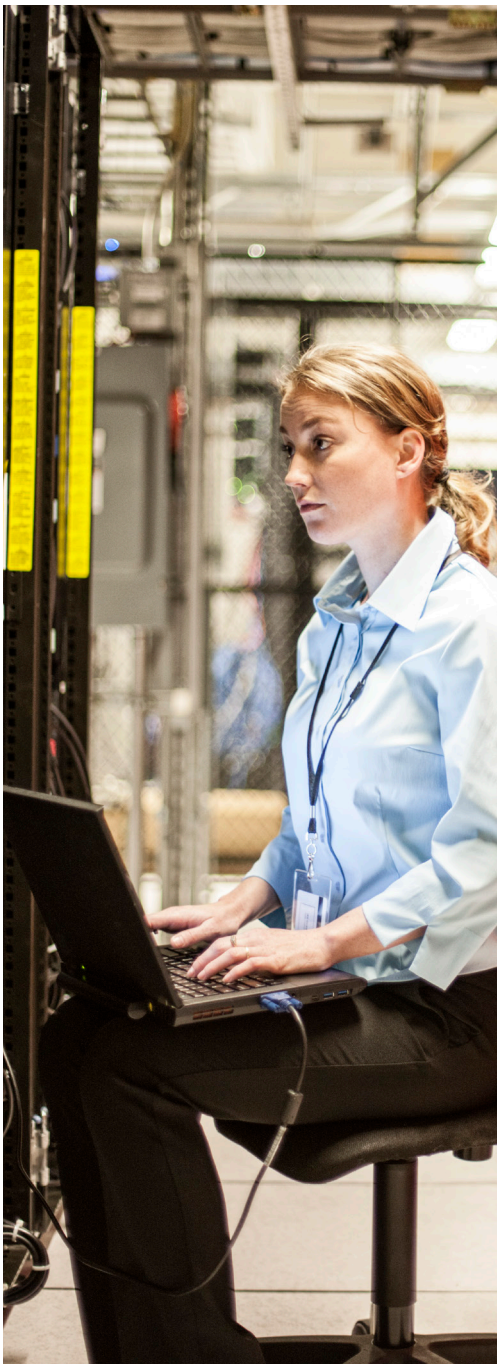
TuxCare
We Take Care of Linux

WHITEPAPER

Live Patching within the Purdue and ENISA Models for ICS/OT/IIoT

www.tuxcare.com

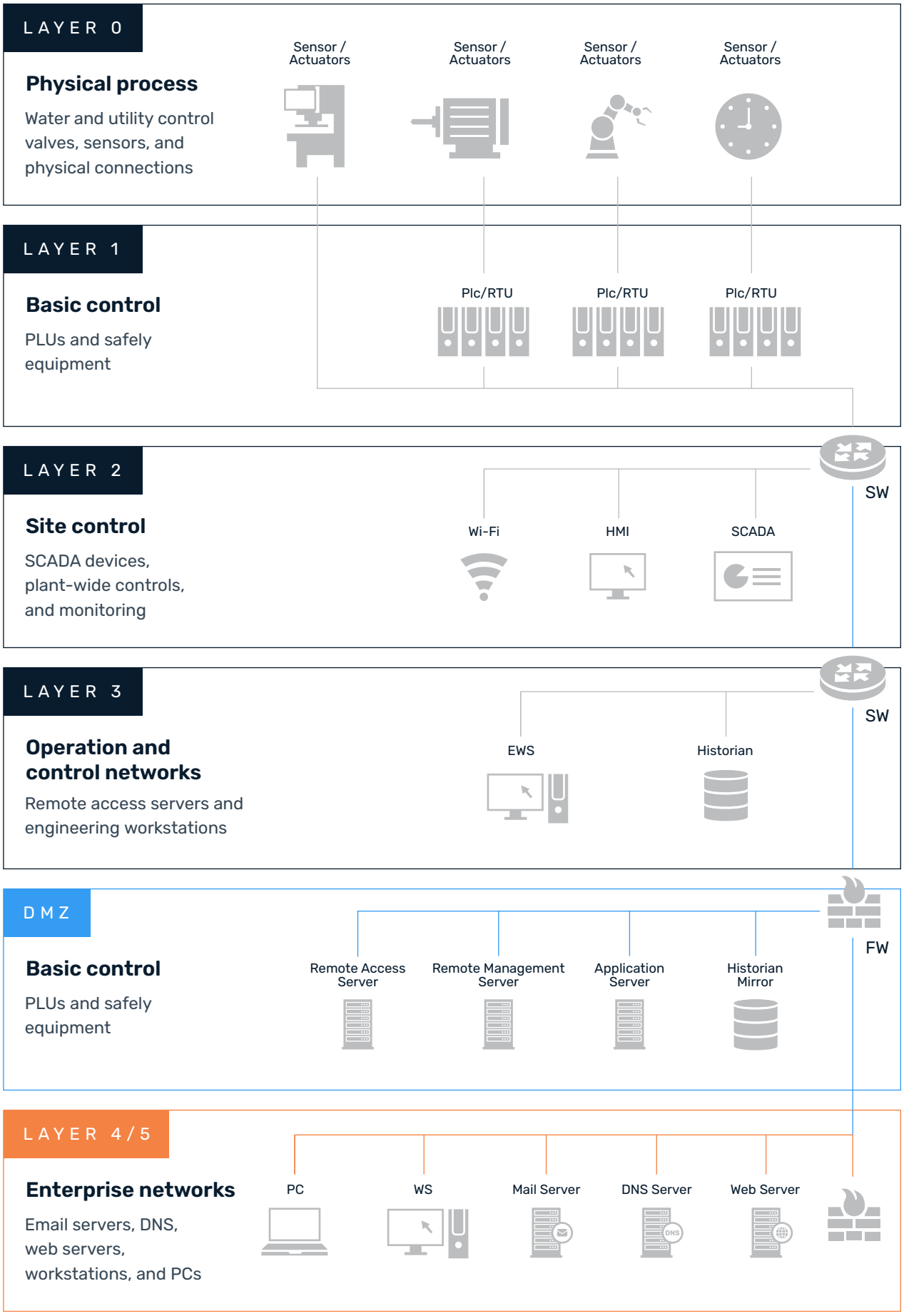
Billions of internet-connected sensors and other Internet of Things (IoT) devices span the world's manufacturing plants and logistics infrastructure. They enable remarkable efficiency and unprecedented data collection. A tiny unpatched IoT device can expose a business to as much risk as a large-scale server in a data center. Once compromised, it can wreak havoc on information systems or serve as a gateway for malicious actors. Cybersecurity countermeasures are available with KernelCare IoT for ARM64-based embedded devices, Linux hosts, and critical applications, including Python and PHP.



Migrating from the Purdue Model to the ENISA Frameworks

Continuous operational and production efficiency are the mandates for operational technology (OT), industrial control systems (ICS), and industrial internet of things (IIoT) networks, along with comprehensive visibility across the entire operation. Cybersecurity has taken a pivotal role in protecting these legacy frameworks. With OT/ICS devices migrating into next-generation IIoT component devices and expanding 5G networks with external connectivity to various cloud analytics platforms, the need to revisit cybersecurity posture is critical to all manufacturing and utility organizations.

Most legacy OT/ICS/IIoT systems leveraged the Purdue Enterprise Reference Architecture (PERA) model. This industrial infrastructure model is designed to help create necessary air gap separation between the OT network control and enterprise IT layers. The PERA broke the layers into five sections:


LAYER 0
Physical process
Water and utility control valves, sensors, and physical connections
Sensor / Actuators
Sensor / Actuators
Sensor / Actuators
Sensor / Actuators
LAYER 1
Basic control
PLUs and safely equipment
Plc/RTU
Plc/RTU
Plc/RTU
LAYER 2
Site control
SCADA devices, plant-wide controls, and monitoring
SW
Wi-Fi
HMI
SCADA
LAYER 3
Operation and control networks
Remote access servers and engineering workstations
SW
EWS
Historian
DMZ
Basic control
PLUs and safely equipment
FW
Remote Access Server
Remote Management Server
Application Server
Historian Mirror
LAYER 4/5
Enterprise networks
Email servers, DNS, web servers, workstations, and PCs
PC
WS
Mail Server
DNS Server
Web Server

IIoT Cybersecurity Challenges

Most OT/ICS architectures are flat networks with exposed areas from a security standpoint. The attack space covers the entire range of potential attacks against an IoT solution. These include both internal and external attacks. Internal attacks may come from insiders who have access to the technology, such as employees, contractors, partners, and customers. External attacks may come from outside sources, including hackers, criminals, terrorists, and nation-states. In addition to these two categories, there are also physical attacks, which involve damage to equipment or facilities.

Physical attacks can occur anywhere within the industrial network, including inside buildings, vehicles, and on the ground. They can also happen through natural disasters like floods, earthquakes, hurricanes, tornadoes, and tsunamis. Finally, there are social engineering attacks, where attackers attempt to trick users into giving them information they shouldn't have access to.

Greenfield and Brownfield OT to IIoT Migrations

Organizations considering moving their legacy OT infrastructure systems into a more modern IIoT design should think that this migration strategy aligns best with their business and technical objectives.

- ## Greenfield

  For most utility companies, a greenfield deployment would be a complete construction of a new services network and critical infrastructure delivery layer. This new deployment would have no dependencies on legacy OT/ICS systems or management console layers. Wind and solar panel farms would be ideal examples of a greenfield IIoT model. The utility would consider utilizing the European Union Agency for Cybersecurity (ENISA) baseline security framework for IoT.

- ## Brownfield

  Organizations, including utility and manufacturing, are considering adopting IIoT technology into an existing OT/ICS environment; this architecture is commonly referred to as a brownfield environment. Though complicated and complex to manage, organizations with current OT/ICS investments with the business requirement to add additional service layers that require IIoT capabilities need a way to coexist in both environments. In many cases, creating a brownfield environment is both costly and operationally challenging. Operations teams and cybersecurity groups will need to maintain two separate security and technology systems until the legacy OT/ICS solutions can be sunsetted and replaced with IIoT capabilities. During the interim, this dual coexistence will expose the organization to new attack surfaces and attack vectors

Managing Risk with Greenfield and Brownfield Deployments

Risk management is perceived differently by an organization's business IT team and the operations technology (OT) team. Balanced considerations between these two groups are essential to ensuring the reliability of IIoT systems. In the case of IIoT, the controls and flow of information may cross multiple intermediaries. Trust must also permeate the entire system production process lifecycle, including various actors and functional entities. From hardware and software component manufacturers as well as system and platforms developers to the end user, trust should direct visibility to every aspect of the IIoT physical equipment systems.

From a technical perspective, the IIoT industrial systems view focuses on analyzing and evaluating technical aspects of an IIoT system, including its benefits, risks, and costs. It then maps these technical considerations to the underlying system capabilities.

Managing Risk through Threat Modeling

Threat modeling focuses on three core factors:

Threats

The expected or unexpected future cybersecurity event resulting from a vulnerability exploit

Risk

A calculated value of the expected impact of cybersecurity threats against the organization

Vulnerability

Potential vulnerabilities remain a weakness within the internal and external IT digital resources supporting the organization's business operations

Threat modeling provides the context for managing these elements. Each of them has a level of influence on the other. Modeling focuses on the risk to the IIoT infrastructure and aligns with several critical security concerns already identified by the organization.

Strategic risk is measured by determining which vulnerabilities pose the most significant threat to the organization. Choosing the proper threat analysis modeling methodology is essential for the organization. Aligning to the correct method requires the organization to face the grim reality that each strategy requires qualified personnel.

Leveraging DREAD Threat Modeling for IIoT

To assess the security posture of an IIoT device, one needs to identify the vulnerabilities and then rank them according to their severity. The DREAD methodology was initially developed for software systems, but it can be applied to any plan.

DREAD is an acronym that represents five criteria for threat assessment:

D	**Damage**	Critical damage from the cybersecurity breach or event from cyber threats
R	**Reproducibility**	Ability of the organization to readdress how the attack occurred
E	**Exploitability**	What vulnerabilities within the IIoT are exploitable by threat actors?
A	**Affected User**	What users are affected by the destructive actor's attacks?
D	**Discoverability**	Are the threats and security gaps easy to detect?

Once these vulnerabilities have been ranked, they should be prioritized based on their potential impact.

Adoption of an IIoT Edge, Platform, and Enterprise Architecture – Gartner IoT Reference Architecture

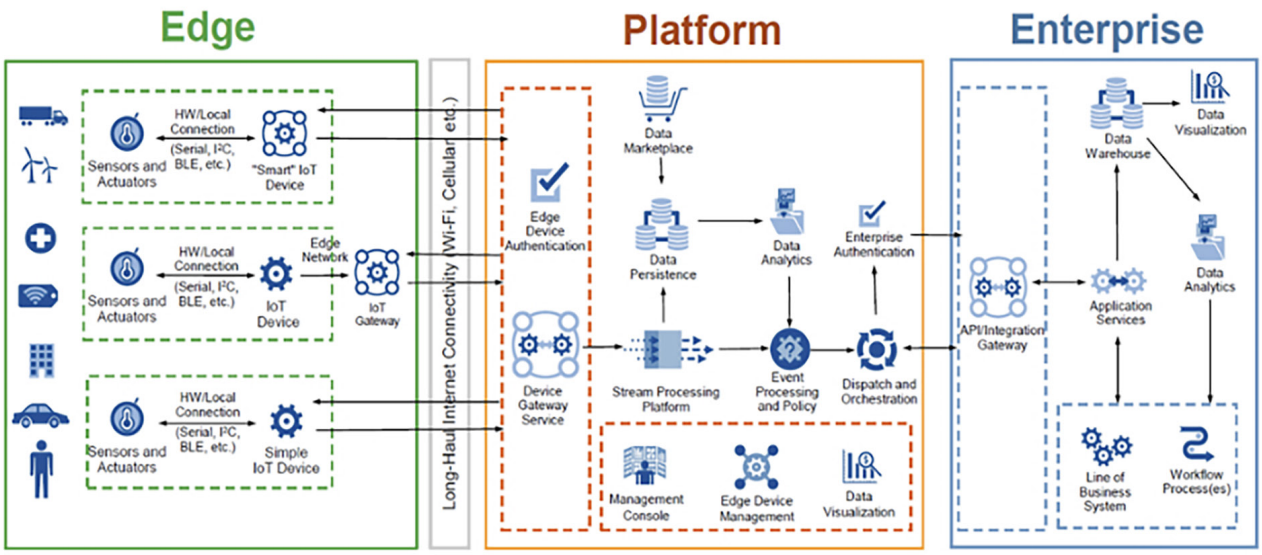


Figure 1: Gartner IT Reference Architecture

The legacy Purdue model no longer provides adequate levels of security projection, as newer IIoT devices become additions to the model. IIoT gateways, connections to external cloud analytics platforms, and 5G network connectivity extend more unique capabilities while possibly more exposure to cyber criminals and hackers. The newer IIoT model incorporates several integrated security controls built into each layer.

- **Edge**

  The edge continues the location of the IIoT devices, sensors, cars, and windmills. The IoT gateway will execute connectivity between the edge layer and the platform.

- **Platform**

  The platform layer accepts connections from the edge layer through a series of edge device authentication security functions. The platform includes patch management, edge device management, orchestration, automation, and data analytics within the platform layer. Data, device, and host security is critical in this layer.

- **Enterprise**

  The platform layer communicates through the API gateway into the enterprise segment. Within the enterprise layer, classic and next-generation IT applications, data warehousing, data lakes, and business automation exist.

Enabling the Various Domains within the IIoT Security Architecture

With the establishment of the edge, platform, and enterprise layers, the next critical component to complete the IIoT architecture is the enablement of the five domains. These domains include:

- **Business domain**

  This domain is part of the enterprise layer that provides for BI analytics, CRM, and other enterprise applications relevant to support IIoT objectives.

- **Application domain**

  Also part of the enterprise layer, this domain provides API proxy services from the business domain to the various business units.

- **Operations domain**

  Spans all three layers with various operational services, including patch management, security updates, API portal access, monitoring, diagnostics, provisioning services, and automation.

- **Control domain**

  This domain operates at the edge layer that connects the sensors, IIoT devices, and the application gateway.

- **Information domain**

  This domain exists in the platform layer. However, this critical business object has interconnections between the enterprise-tier business and application domains, along with a connection to the operations domain for provisioning.

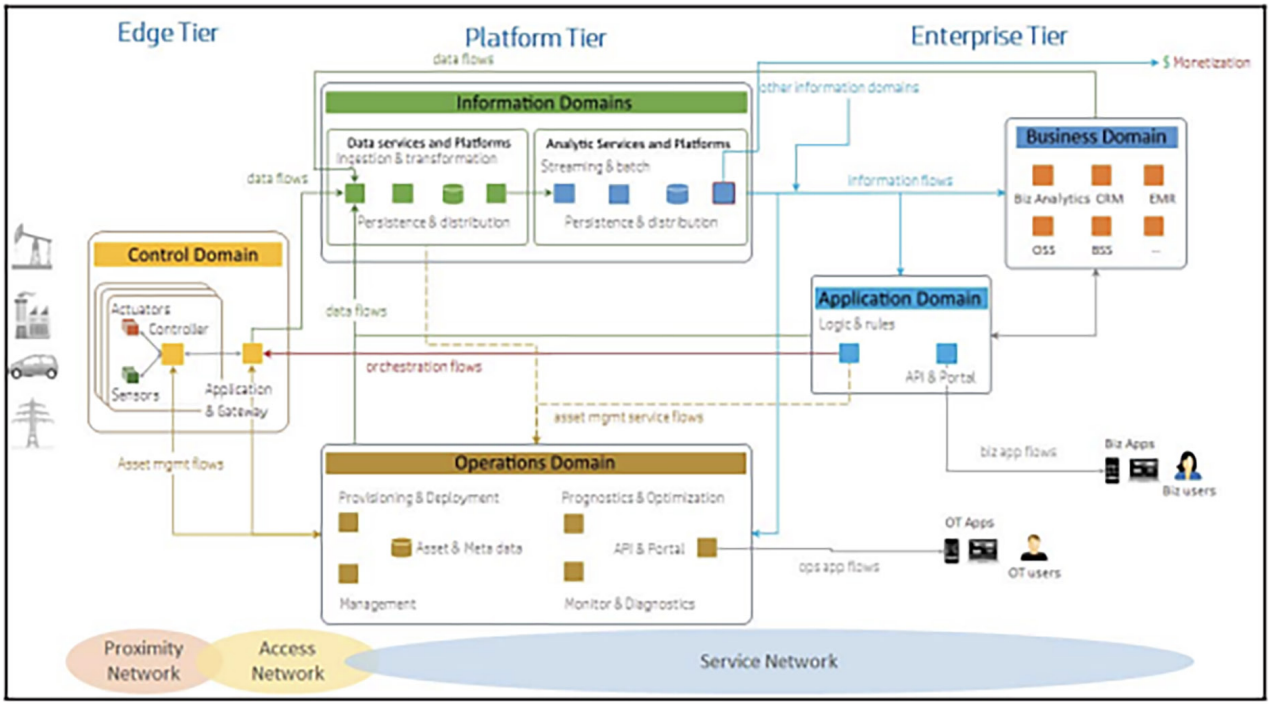


Figure 2: Functional domain representation in a three-tier IoT architectural pattern. Source: IIC-IIRA

Importance of Security Governance and Automation for Risk Reduction

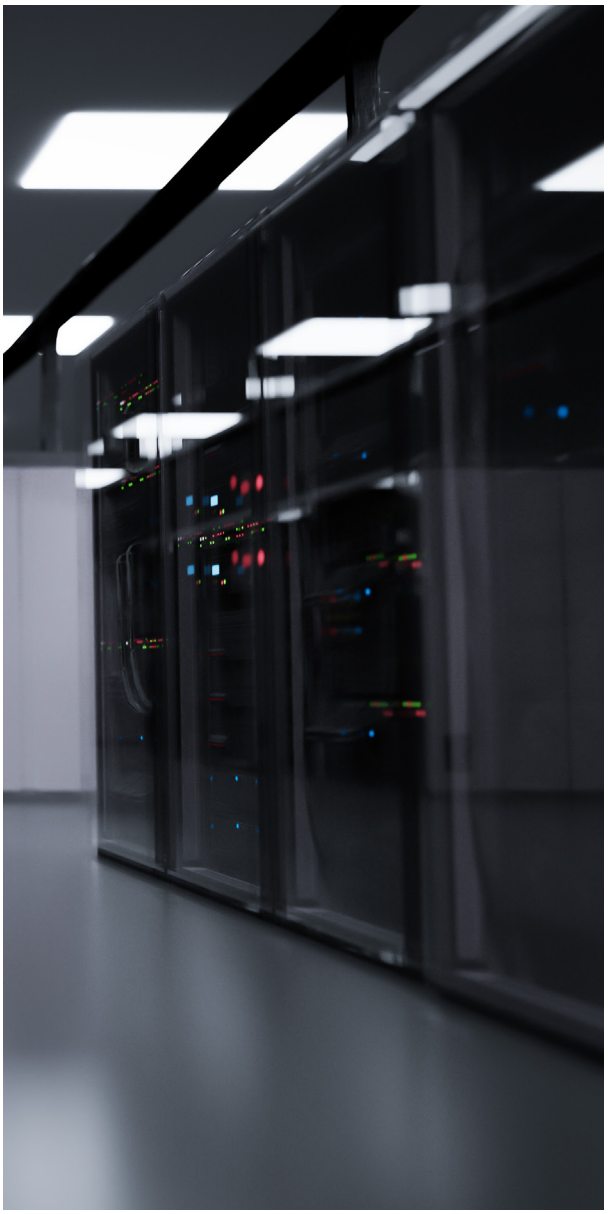
While the IIoT framework is a comprehensive model for better security for IIoT deployments, the model does introduce the criticality of continuous monitoring, patching, and remediating the various systems to maintain the highest state of readiness, security, and availability.

Patching live systems is essential to maintaining the continuous uptime of these components with the IIoT framework. While the framework promotes resilience, each element's reliability is critical to maintaining the expected security posture.

Along with live system patching, updating essential and critical software libraries, and having a strategy for extended software security support for applications reaching end of life, organizations need to incorporate these automation tool functions within the operations domain.

TuxCare's Live Patching, ELS, and Library Updates Align with the IIoT Security Framework

TuxCare, a global leader in live patching critical components and overall security patching for end-of-life distributions and languages, aligns with several of the domains within the IIoT security model:



Operations domain

TuxCare live patches Linux OS kernels, libraries, and other critical components across all three layers.

Application domain

TuxCare live patching extends into this domain by offering live patching of several Linux distros and ongoing security updates for end-of-life versions of Python and PHP applications.

Business domain

TuxCare live patching extends into any Linux hosts, along with application support for open support databases (mySQL, Maria, PostgreSQL, etc), and Python and PHP based applications deployed within this domain.

Control domain

KernelCare for IoT is a solution for updating critical hosts and IoT devices with the edge, platform, and enterprise layers, as well as the control domain. TuxCare live patching also extends to IIoT-specific devices supporting RaspberryPi, Yocto, Ubuntu Core, AlmaLinux, and others on ARM64.

TuxCare Patching Automation Capabilities for Risk Reduction

Waiting to apply security patches until you're ready to restart systems and devices is leaving your organization vulnerable and putting your compliance posture at risk. TuxCare's live patching solutions protect your Linux systems by rapidly eliminating vulnerabilities with no need to wait for maintenance windows or downtime. With TuxCare, IT teams can automate the process of taking new patches through staging, testing, and production on all popular Linux distributions.

TuxCare features flawless interoperability with vulnerability scanners, security sensors, and automation and reporting tools, as well as our ePortal management platform – a dedicated private patch server that runs inside your firewall on premise or in the cloud.

TuxCare is the only provider that can live patch virtually all vulnerabilities in kernels, shared libraries, virtualization platforms, and open-source databases across all popular distributions.

CONTACT A TUXCARE EXPERT