

Securing Power Grid Operations with ArrowLinux

ArrowLinux 5000 Series • powered by ST Engineering data diode technology

AT A GLANCE

SECTOR

Power utilities: generation, transmission and distribution

NEED

Live operational data for analytics, security monitoring and reporting, with no inbound path to the control network

SOLUTION

ArrowLinux 5000 Series (powered by ST Engineering) used together with Kepware+ industrial connectivity

MODELS

5280, 5282 and 5283

ASSURANCE

Common Criteria EAL 4+ certified by CSA Singapore (models 5282 and 5283)

RESULT

Operational insight for the utility while the control network stays isolated

OVERVIEW

Power utilities depend on operational technology (OT) networks to run generation, transmission and distribution. These include SCADA systems, substation automation and plant control systems. Utilities also need the data from those networks for monitoring, analytics, regulatory reporting and enterprise planning, which live on IT networks and increasingly in the cloud.

Connecting the two with a conventional firewall creates a two-way path. If that path is compromised, an attacker on the IT side can reach systems that control physical infrastructure. ArrowLinux replaces that path with a hardware-enforced one-way link, so operational data flows out and nothing can flow back in.

THE CHALLENGE

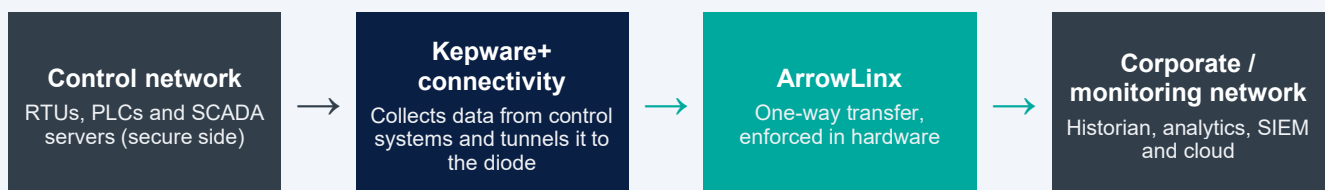
- **Growing attack surface.** Grid digitalisation, remote monitoring and IT/OT convergence expose control systems that were designed to be isolated.
- **Consequences of compromise.** A successful attack on control systems can lead to outages, equipment damage and safety risks, as well as regulatory and reputational fallout.
- **Data still has to move.** Control room operators, asset managers, analysts and regulators all need timely operational data, so a fully air-gapped network isn't practical.
- **Legacy and multi-vendor protocols.** Utility environments run a mix of industrial protocols, so the solution has to work with what is already deployed.

THE SOLUTION

ArrowLinux sits between the control network (the secure side) and the corporate or monitoring network (the lower-trust side). The one-way direction is enforced in hardware, so software misconfiguration or a network-borne attack cannot reverse it.

Built on ST Engineering's patented SFP+ technology, the diode transfers data at up to 10 Gbps. It also includes real-time file loss detection, which matters when operational records must arrive complete.

HOW THE DATA FLOWS



✗ No path back into the control network

Data moves from the control network out to the IT side only. Nothing can flow back.

HOW IT WORKS IN A POWER ENVIRONMENT

Data flow	Source (secure OT side)	Destination (IT / monitoring side)	Relevant protocols
Telemetry and SCADA data	RTUs, PLCs, SCADA servers	Historian, analytics platform, enterprise dashboards	OPC UA, MODBUS (RS232/TCP), IEC 104
Legacy and proprietary device data	PLCs, RTUs and other devices on proprietary protocols	Historian, analytics platform, enterprise dashboards	Converted by Kepware, tunnelled over OPC
Sensor and IoT streams	Substation and field sensors	Monitoring platforms and cloud analytics	MQTT, Kafka
Logs and alarms	Control system and network devices	Security operations centre (SOC) / SIEM	SYSLOG, SNMP traps
Reports and records	Plant and substation systems	Regulatory reporting, asset management	SFTP, FTP, folder mirroring (SMB/SAMBA)
Video surveillance	Substation and plant cameras	Remote security operations	RTSP
Time synchronisation	Trusted time source	OT devices	NTP over the data diode

A TYPICAL DEPLOYMENT IN THREE STEPS

1 Collect

Kepware, acting as the protocol agent on the secure side, collects data from control systems, including devices on legacy protocols, and tunnels it to the diode.

2 Transfer

The diode transfers it one way, with file loss detection confirming that records arrive intact.

3 Republish

The receiving side republishes the data to historians, dashboards, SIEM tools or cloud analytics, with no return path into the control network.

KEY BENEFITS FOR UTILITIES

Zero data leakage in the reverse direction

Malware, remote commands and ransomware cannot travel back into the control network through the diode.

Real-time visibility without added risk

Operators and analysts get live operational data while the control network stays isolated.

Reliable data delivery

The maximum file loss rate is 1 in 5 million files, and the diode handles more than 200 small files per second.

Independently certified

Models 5282 and 5283 are Common Criteria EAL 4+ certified by the Cyber Security Agency of Singapore (CSA), giving security teams and auditors an assurance benchmark.

Built for critical infrastructure

Redundant power supplies and a 0 to 40°C operating range suit control rooms and substations. Health alerts go out via SYSLOG, email, SNMP traps and file export.

Simple to run

An integrated management portal covers configuration, monitoring and maintenance.

Works with legacy equipment

Used together with Kepware+, whose drivers convert data from many PLC and RTU protocols, the diode can carry data from older and multi-vendor equipment.

Supports compliance efforts

One-way segmentation between OT and IT helps utilities enforce the zone-and-conduit separation that industrial security frameworks such as IEC 62443 call for.

ABOUT KEPWARE+

Kepware+ is Kepware's solution for standardising and managing industrial connectivity across an enterprise. It standardises the secure movement of OT data between industrial devices and both OT and IT systems, and brings together device connectivity, cloud and enterprise integrations, flexible deployment methods and enterprise management.

25+ years

of industrial connectivity experience, as stated by PTC

150+

drivers and plug-ins in Kepware Server

IT + OT

system agnostic, built for interoperability between them

WHAT KEPWARE+ INCLUDES

Device connectivity

Kepware Server converts proprietary device data into standardised, application-ready information, with 150+ drivers and plug-ins for PLC and industrial protocols.

Cloud and enterprise integrations

Connects OT data to cloud and enterprise systems. Built on OPC, with IT-centric protocols including SNMP, ODBC and web services.

Flexible deployment

Kepware Server runs on Windows. Kepware Edge offers a Linux-based option for edge and containerised deployments.

Enterprise management

Kepware+ Manager gives one central point to manage Kepware Server and Edge instances across sites, including remote configuration of connected servers.

WHY ORGANISATIONS ADOPT IT

Enhanced transparency

A unified view of every Kepware deployment, with configuration and visibility for installations company-wide from a central point.

Reduced operational time

Faster configuration and simpler scaling of replicated setups across large footprints.

Efficiency in workflow

Hybrid SaaS functions for essential tasks let teams work from any location, with less need for on-site access.

Robust security

Modernise, standardise and secure the movement of data from operations to the wider enterprise.

Design note for isolated networks. Kepware+ enterprise management uses an agent that must be reachable by both the cloud components and the on-premises servers. For Kepware servers on the secure side of ArrowLinux, plan management access so that it does not create a path into the control network.

Kepware+ includes access to the latest upgrades, ongoing maintenance for supported versions and security updates through a support contract. Kepware is now part of Velotix (formerly PTC).

BETTER TOGETHER: KEPWARE+ AND ARROWLINX

Kepware+ handles connectivity

Many devices, many protocols

- Sits on the secure side and collects data from PLCs, RTUs and other devices, including those on legacy or proprietary protocols
- Converts that data into standardised formats that IT systems can use
- Tunnels it over OPC through the diode

ArrowLinx handles isolation

One direction only

- Enforces one-way transfer in hardware, so nothing can flow back
- File loss detection confirms that records arrive intact
- The receiving side republishes the data to historians, dashboards, SIEM tools or cloud analytics

Proven together. Kepware used with ST Engineering's data diode technology has been validated through rigorous testing and deployed at a data centre in Singapore to move OT and IoT data securely while keeping networks strictly separate.

MODEL SELECTION

Model 5280

500 Mbps file transfer

Suited for

Smaller sites or single-flow deployments, such as a substation or a single plant, where 500 Mbps file transfer throughput is enough.

Model 5282

1 Gbps file transfer • CC EAL 4+

Suited for

Regional control centres and larger generation sites needing 1 Gbps file transfer throughput and CC EAL 4+ certification.

Model 5283

1 + 1 Gbps file transfer • CC EAL 4+

Suited for

Central control centres and critical hubs consolidating multiple flows, with 1 + 1 Gbps file transfer throughput over 10 + 10 Gbps media links, the highest capacity in the series.

EXAMPLE SCENARIO

A regional utility operates several substations and a central control room. It wants to give its analytics team and security operations centre live visibility of grid performance, without opening any inbound path to the control network.

ArrowLinx is deployed at the boundary of the control network, with Kepware collecting data from substation devices, including any on older proprietary protocols. MODBUS and IEC 104 telemetry, OPC UA data, alarms and system logs flow one way to the enterprise side. Any attempt to send data back toward the control network has no physical path to succeed. The utility keeps its operational insight, and the control network stays isolated.

In summary

ArrowLinx, powered by ST Engineering technology, lets power utilities share operational data without creating a route for attackers to reach the systems that keep the grid running.

Talk to ArrowLinx

www.arrowlinx.com

sales@arrowlinx.com