

WHITE PAPER
Securing Factory
Automation
Networks



Manufacturing facilities and extended supply chains rely on a wide array of plant floor instruments and control systems that must communicate reliably via wired or wireless networks. Particularly in defense, aerospace, electronics, and other high-tech plants, critical control systems need end-to-end traffic protection that is simple to install in each device and simple to scale throughout the factory infrastructure.

In manufacturing automation networks and related just-in-time supply chain and asset tracking networks, KoolSpan reduces security costs and complexity with device-based network traffic security that integrates advanced crypto hardware and software directly into network devices, controllers and I/O devices, so that

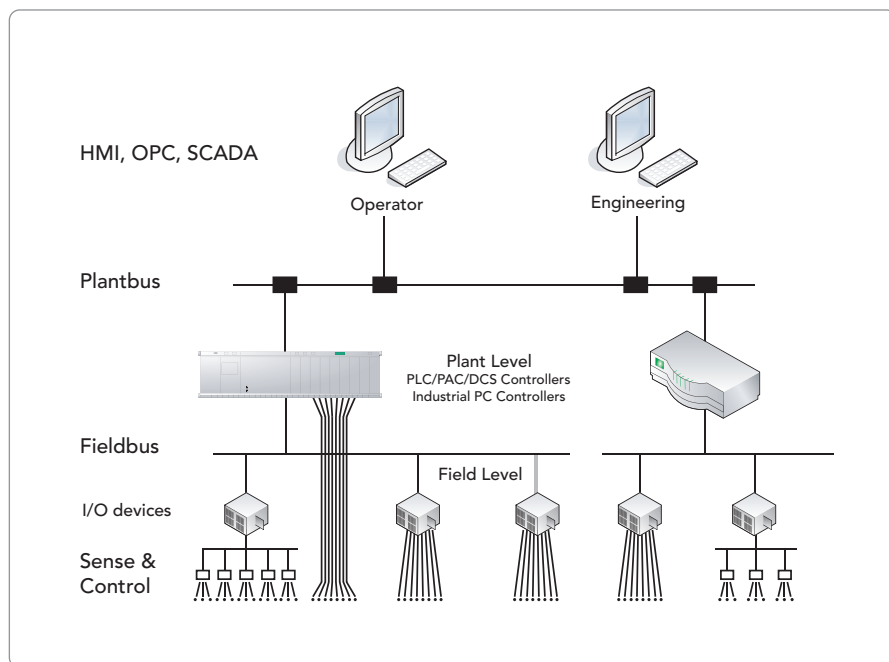
plant-bus and field bus traffic can be cost-effectively encrypted and authenticated end-to-end.

Securing Industrial Ethernet

Manufacturing and supply chain automation have benefited greatly from mainstream IT and network technologies such as UNIX,

TCP/IP and Ethernet. IP networks are allowing manufacturing plants to gradually replace various legacy and proprietary data links with open IT infrastructure that supports heterogeneous plant-and field-bus traffic running across standards-based routers, switches, hubs, fiber optics and wireless access points.

Figure 1. *Manufacturing automation networks at plantbus and fieldbus levels*



Factory automation abbreviations:

- DCS** - Distributed Control System
- HMI** - Human Machine Interface
- OPC** - Object Linking and Embedding for Process Control
- PAC** - Programmable Automation Controller
- PLC** - Programmable Logic Controller
- RTU** - Remote Terminal Unit
- SCADA** - Supervisory Control and Data Acquisition

EtherCAT, Ethernet Powerlink, EtherNet/IP, SERCOS III, and related Industrial Ethernet products have their benefits, but along with the interoperability and performance gains, open network protocols and open platforms introduce some substantial security challenges. Security software and encryption routines running on open platforms are largely defenseless and vulnerable to a vast number of hacker exploits and viral threats. In addition to threats at the application and operating system level, factory systems can also be attacked at the network transport level by hackers who monitor plant traffic, inject packets, and masquerade as end systems for purposes of stealing data, corrupting data, and controlling or destroying factory capabilities.

In the current era of escalating cyber threats, manufacturing networks need highly reliable end-to-end encryption and authentication that works at a granular level to protect specific devices and their communications inside fieldbus and plant-bus infrastructure. Endpoint-to-endpoint protection is the only way to address the growing list of security threats that manufacturing automation networks face.

KoolSpan for simple, end-to-end secure connections

KoolSpan's end-to-end secure connectivity solution protects traffic from the originating device, through the network, to the destination system. In this context, the endpoints can be PLC, DCS, RTU, PAC or PC-based controllers, and various related I/O devices, application servers, management consoles or user PCs. Both intelligent and slave (dumb) devices are supported. The KoolSpan solution is a two-way secure tunnel that encrypts and mutually authenticates traffic end to end, regardless of vulnerabilities in underlying cellular, WiFi or wireline networks.

KoolSpan's award-winning enhanced 256-bit AES cryptographic algorithms run on hardened TrustChip hardware that is installed in endpoints in the form of industry-standard Smart Cards, SD Cards, USB tokens or embedded hardware. With on-board crypto processing and secure memory operations, the KoolSpan TrustChip platform creates an ideal tamper-proof, tamper-evident environment for running advanced encryption routines, and storing keys and other security data.

KoolSpan's Solution is a great improvement over conventional security software approaches that store secret keys on end-user or server hard disks that are vulnerable to human and malware attacks, including a wide range of Trojan Horses, backdoors, rootkits, etc. The memory and processing resources on TrustChip cards and embedded silicon are hardened to defend against digital and physical attacks. By running encryption processing on specialized hardware, KoolSpan TrustChips off-load computationally intensive CPU demands and storage overhead from the security device. This approach ensures minimal device footprint and high performance, even on resource-constrained, dedicated or legacy platforms.

KoolSpan encryption software sets up an AES 256-bit secure tunnel between endpoints without the need for public keys or certificate management (PKI, IKE, Keberos, RSA, etc). KoolSpan authentication is conducted bidirectionally at three levels: 1) at the device level, 2) at the session level, and 3) on a per-packet basis, which ensures that hackers cannot conduct man-in-the-middle attacks, dictionary attacks, replay, and cloning or spoofing exploits.

Creating trusted plant floor device communities

In operation, KoolSpan's integrated TrustChip crypto hardware and software

together provide a hardened and dedicated "security engine" in each device, enabling a very wide range of simple, secure network interactions. With its own processor and memory, KoolSpan's high-performance, host-independent security engine supports encryption, authentication, identification and key management services that allow a device to create 256-bit, AES-based TrustedConnections with other devices and upstream hosts or controllers. The KoolSpan engine grants membership into a virtually limitless number of different, independently managed security groups—referred to as TrustGroups. In peer-to-peer device communities, TrustGroups do not require central administration after initial installation. In centralized configurations, security groupings and associations within TrustGroups can be managed from a central KoolSpan console.

For device software running at the network layers, the KoolSpan security engine API can be called on to encrypt and authenticate network and transport layer traffic. Application level software can also make direct calls to the KoolSpan security engine to protect data before it is handed off to the network layers. KoolSpan's streamlined service API also makes it easy for developers and OEMs to set up TrustedConnections, which work like a virtual secure LAN between any two devices. This connection looks like a standard Ethernet link to a device's applications, ensuring full interoperability with virtually all enterprise and industrial software.

Any end device or server application can use the KoolSpan TrustChip to protect traffic across wired and wireless infrastructure in a completely seamless and transparent manner. All KoolSpan traffic is routable and manageable by the IT department, yet the traffic is fully encrypted at all times as it passes through routers, switches and firewalls.

Security engine services running internal to hardened TrustChips are available to OEMs and developers through a complete yet simple set of APIs and reference device drivers. In cases where devices don't have a standard SD card interface for a TrustChip, the KoolSpan Lock appliance and USB Key (token) products use the same TrustChip security engine to provide turnkey Layer 2 tunneled protection to all higher layer protocols and applications running.

A 360 degree security strategy

KoolSpan's powerful encryption technology is necessary for protection of critical infrastructure, but many attack vectors aren't directed exclusively at the encrypted data in transit. Hackers and blackhats will also hack into end devices and servers via internal backdoors, rootkits, bots, or through VPN tunnels. Badly implemented IT security infrastructure and misconfigured security settings are of great assistance to hackers and many types of malware. With KoolSpan, encrypted and authenticated connectivity is, by design, a plug-and-play, out-of-the-box security solution. KoolSpan requires little or no setup, and completely isolates critical device traffic and operator console traffic from outside attack, end to end. Most importantly, KoolSpan allows the critical device data to fully utilize IP networks while maintaining total isolation within public and private IT infrastructure.

The five secure connectivity scenarios below highlight how KoolSpan integrates into manufacturing, supply chain and asset tracking networks:

- 1) Embedded in plant floor controllers and intelligent I/O devices
- 2) Embedded in network routers, switches and wireless APs
- 3) In wireless smartphones, PDAs and VoIP devices

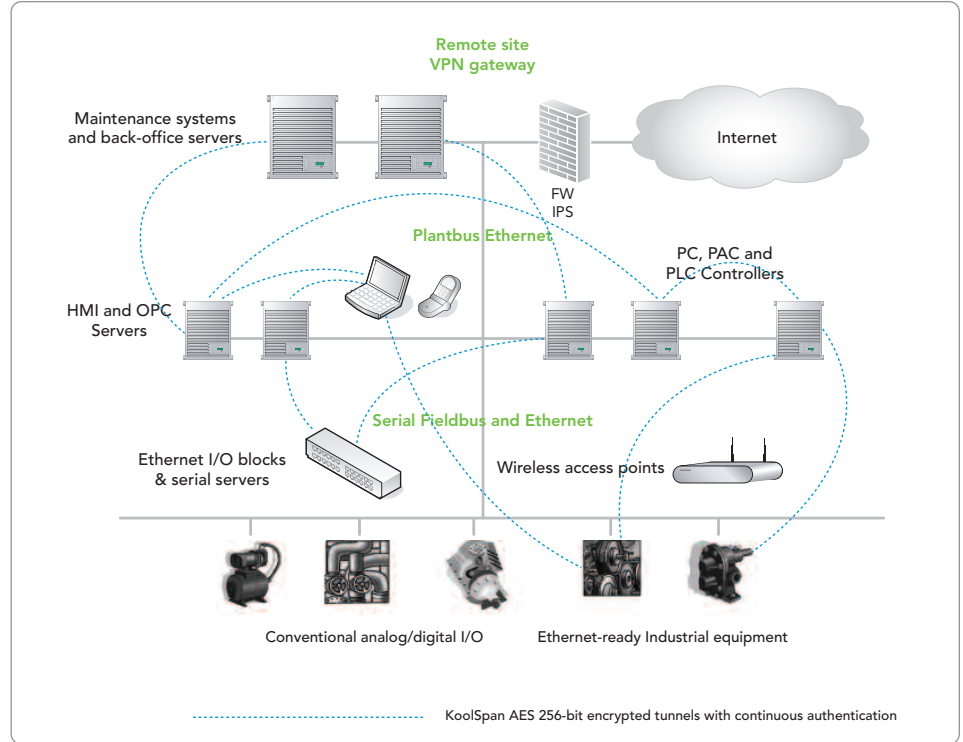


Figure 2. *KoolSpan secure tunnels in fieldbus and plantbus networks*

- 4) In stand-alone secure tunnel adaptors for dumb/legacy devices
- 5) In control room servers and operator consoles and PCs

Scenario 1. Embedded in PLCs and other intelligent field controllers

In process automation, machinery automation and motion control environments, most organizations have some mix of Ethernet and fieldbus connectivity on the plant floor and in control rooms. Serial fieldbus networks are still widely used, particularly in downstream sensors, controls and instrumentation. Ethernet is more widespread in high-bandwidth upstream areas of the network as a control system backbone, connecting PC/PLC/PAC/DSC controllers, HMI stations, OPC servers, and

various back-office IT resources. Whether at the plantbus or the fieldbus level, most automated industrial facilities have Ethernet integrated into the production infrastructure, which introduces a large universe of cyber threat vectors from malware and human attackers.

With the KoolSpan solution, Industrial Ethernet connections are uniquely protected with strong encryption and continuous authentication running on hardened cryptographic hardware that is embedded in intelligent field controllers, I/O devices, and specialized plant floor computers (see Figure 2). KoolSpan secure connectivity is a uniquely simplified security solution that relieves automation engineers of the complexities and cost of conventional VPN, firewall and PKI security methods.

To deploy KoolSpan, Crypto processing hardware in the form of the KoolSpan TrustChip is embedded through a custom ASIC/FPGA, or integrated via industry-standard Smart Card, SD Card or USB form factors. To complement the TrustChip silicon, KoolSpan crypto software is available in quickly deployable API libraries that can be added to controller, I/O and management platforms in the form of a driver that is loaded during boot up. A KoolSpan management console software is also available for integration and OEM product development.

Other embedded security solutions rob horsepower and code space from control and I/O devices with processing in software, which contributes to latency. With the TrustChip SD Card and other embedded formats, KoolSpan minimizes the footprint, latency and resource demands on plant floor systems.

Peer-to-peer or centralized

Security associations between field controllers, intelligent I/O devices and control room systems can be either peer to peer or centrally administered. In the central KoolSpan model, a management console function allows network administrators to dynamically create security groups and permit/deny security associations for participating users and devices. Security groups can include any mix of controllers, slave instruments, data acquisition points, servers, consoles, wireless devices and end-user PCs.

All necessary authentication keys, identity codes and crypto algorithms are pre-loaded into the KoolSpan TrustChip hardware during installation. From that point on, end devices are able to authenticate sessions, and then set up secure end-to-end

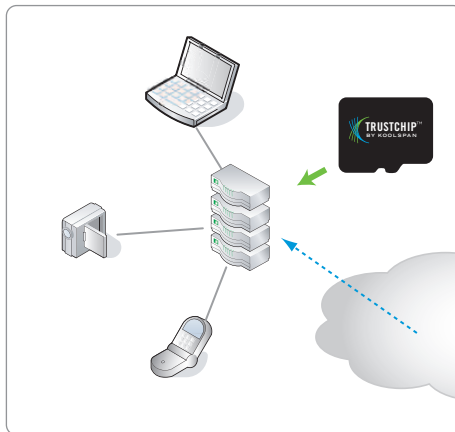
tunnels automatically. Once peer-to-peer devices are installed and operational, they can continue to dynamically form secure connections within their TrustGroups or security groups for an indefinite amount of time without operator intervention.

Embedding KoolSpan in control room and plant floor systems presents opportunities to create a granular set of privileges for each operator or engineer. Access rights for secure KoolSpan connections can be defined for each operator and each downstream device. Operators have connectivity only to instruments and controls for which they have explicit rights.

In both the peer-to-peer and centralized versions, KoolSpan secure field/plantbus connectivity is essentially plug-and-play, requiring none of the complex configuration, administration and network architecture modifications that are associated with conventional IP firewalls, VPNs and PKI.

Scenario 2. Embedded in network routers, switches and wireless access points

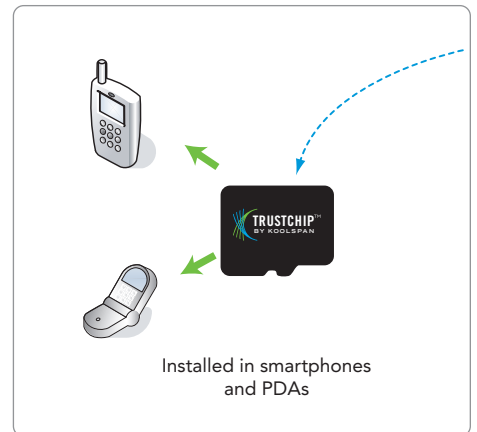
In some manufacturing network applications, a group of controllers, I/O devices or



special-purpose systems need secure upstream connectivity to a control room or data center. This scenario is found in large manufacturing campuses and extended processing plants with multiple sites or product areas that are part of hub-and-spoke, mesh or daisy chain topologies. In these cases, KoolSpan TrustChip technology and crypto algorithms are integrated into a network device (router, hub, or switch) in each remote site. This is similar to the remote VPN gateway model, but without the complexities of IPsec, SSL, IKE and PKI configuration and network management. In the upstream site (i.e., control room or administrative center) KoolSpan-based network devices or plant systems complete the end-to-end secure tunnels. In this environment, KoolSpan simplified security connections will work equally well across Ethernet or wireless transmission with plug-and-play connectivity.

Scenario 3. Wireless smartphones, PDAs and VoIP devices

In an environment where KoolSpan is creating encrypted and authenticated connectivity for plantbus and fieldbus



devices, there is also the opportunity to use the secure connections for wireless productivity devices, including smart-phones, PDAs and various ruggedized mobile voice/data platforms (e.g., Symbol Technologies and Motorola). KoolSpan can be easily installed in wireless devices using standard Smart Cards, SD Cards or USB flash memory add-ins. Once the add-in and a software driver are loaded, mobile devices can:

- Participate in peer-to-peer secure voice communications
- Conduct remote monitoring and control plant instruments
- Access business systems and other data center resources

One example of this application is a central VoIP server that gives wireless devices secure encrypted voice communications throughout the plant. Peer-to-peer secure voice sessions without a VoIP server are also supported. KoolSpan mobile device connections can run on cellular, WiFi, or wired IP LANs. KoolSpan secure tunnels are high performance and low latency, which make them suitable for the full range of voice and multimedia traffic, including streaming video and interactive multimedia exchanges.

Scenario 4. Stand-alone secure tunnel adaptor for dumb/legacy devices

In the above examples, KoolSpan either is embedded directly in network or plant devices, or installed via SD Card in a mobile device. These approaches assume either OEM embedding or a device with a Smart/SD Card header or a USB interface. When devices don't have embedded support or standard Smart Card/SD/USB interfaces, OEMs of general-purpose serial device connectors can incorporate

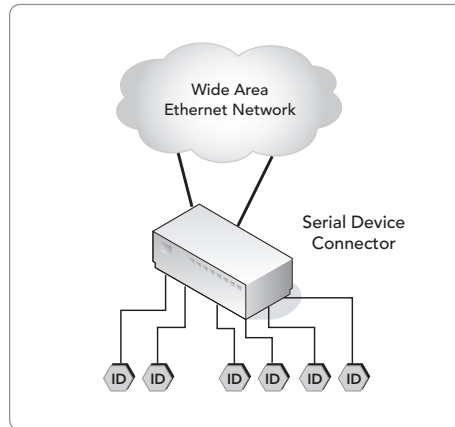


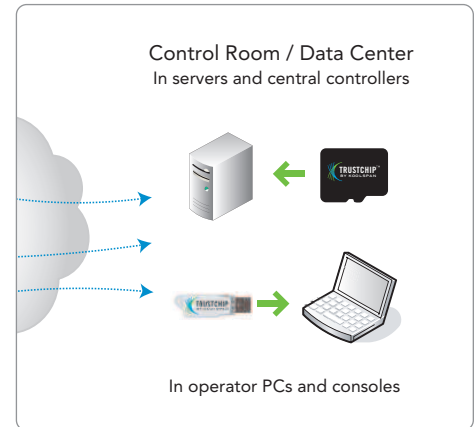
Figure 3. *General-purpose serial device server with KoolSpan technology for secure upstream connections to PLC, SCADA, and control room systems*

KoolSpan to deliver secure tunnel connections (see Figure 3). Legacy and “dumb” devices that need this sort of support include slave RTUs, dumb terminals, intercom systems, scanners, card readers, and many other industrial instruments and legacy IT peripherals.

For legacy and proprietary devices with Ethernet interfaces, the KoolSpan Lock and Key solution is particularly useful for protecting the traffic of devices that don't have the processing power, memory or open interfaces, which are necessary for internal crypto software support. Please see the [Product section](#) of KoolSpan Web site for more information on the Lock and Key units.

Scenario 5. Control room servers operator consoles and PCs

In the upstream realm of the manufacturing network, KoolSpan can be integrated easily into a wide range of HMI and SCADA



systems, OPC servers, management consoles and operator PCs in data centers and control rooms. KoolSpan crypto software can be easily installed on any server or client platform that supports industry-standard Smart Card, SD Card, or USB interfaces.

For Example, when an operator sitting in a control room with a laptop computer plugs in a KoolSpan flash card or USB token, the laptop will automatically form security associations with any other KoolSpan-based computers, controllers and downstream process devices that it is authorized to access. Once a security association is initialized between the operator's laptop and a control room or plant floor device, the connection looks like a standard link to any applications running on the laptop. Operators can use KoolSpan plug-and-play AES 256-bit encrypted and authenticated tunnels to connect to any field-or plant-level device, without the need for complex and expensive IPsec or SSL products that don't protect end-to-end traffic streams.

Conclusion

Given the current security climate, manufacturing automation networks and related supply chain and asset tracking systems must have secure network communications that are cost effective and simple to install. KoolSpan has responded to this need by providing advanced crypto software and hardware that is specially designed to easily integrate into existing fieldbus and Industrial Ethernet environments. The KoolSpan solution provides servers, controllers and I/O devices end-to-end encryption and authentication that runs in a secure, tamper-resistant crypto hardware environment that is hardened to attacks from external hackers

and platform-based malware. Whether you are an OEM, systems integrator, consultant or enterprise end-user, please contact KoolSpan for detailed information on how your specific manufacturing or process control application can benefit from simplified, secure connectivity today.

For more details on the underlying security technologies, please see [KoolSpan's Foundation Technology white paper](#)

For More Information

Please call 240.880.4400, or go to www.koolspan.com