WHITE PAPER

Securing Process Control Networks

KOOLSPAN®

Securing Process Control Networks

Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Programmable Logic Controller (PLC) networks and other industrial systems are widely used by utilities, energy companies and other "critical infrastructure" providers that deliver vital utility services and key manufacturing processes. Industrial process control systems are in the midst of a long transition from closed, proprietary platforms to open systems and network protocols based on mainstream IT standards, TCP/IP, Windows, Linux, Ethernet, etc.

As industrial controls (e.g., PLC, RTU, DCS) have migrated to open IT platforms and open protocol networks, they have acquired better performance, interoperability and connectivity, but the security implications remain increasingly problematic.

Security software and encryption routines running on open platforms are largely defenseless and vulnerable to a host of hacker exploits and viral threats. In addition to threats at the application and operating system level, process networks 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 corrupting or controlling process communications.

In the current era of escalating cyber threats, process networks need highly reliable end-to-end encryption and authentication that works at a granular level to protect specific devices and controls inside SCADA and DCS infrastructure. Endpoint-to-endpoint protection is the only way to address the growing list of security threats that process networks face, including:

1. **Malware** – Like any IT system, industrial systems are potentially vulnerable to viruses, worms, Trojans and spyware. Even if malware threats have no special interest in industrial systems, they are nevertheless very effective at compromising data through open IP, Ethernet, Windows, and Linux ports and protocols. Malware can impact critical industrial systems by corrupting data, overwhelming communications, or installing backdoors or key stroke loggers.

2. **Insiders** – Disgruntled workers who know the system can be a significant threat to industrial networks. The insider may be motivated to damage or disrupt the industrial system due to malice, or an insider may attempt to illicitly gain higher privileges for convenience sake. Bored or inquisitive operators may inadvertently create problems, as is the case when engineers make errors that bring down the system.

3. **Hackers** – This threat vector includes individuals who are outsiders who may be interested in probing, intruding or controlling a system because of the challenge, or for financial gain (e.g., theft of service, modifying data related to rate generation, etc).

4. **Terrorists** – This threat distinguishes critical infrastructure systems from most IT systems. A terrorist is likely to want to disable the industrial system to disrupt monitoring and control capability, take control of the system to feed false values to the operators, or use the control system to degrade service or possibly damage the physical critical infrastructure system.

SCOPE OF THE KOOLSPAN SOLUTION:
SCADA systems are often linked to related enterprise systems, such as Energy Management Systems (EMS), Distribution Management Systems (DMS), Manufacturing Execution Systems (MES) and Substation Automation (SA). This paper focuses on SCADA systems, but the discussion of security issues is applicable to DCS systems and other varieties of control systems.

The KoolSpan simple and secure connectivity solution

KoolSpan secure connections offer critical infrastructure devices a simplified plug-and-play approach to end-to-end network encryption and authentication. The KoolSpan solution delivers enhanced 256-bit AES encryption with per-packet keying and mutual authentication that is deployed in hardened, tamper-proof crypto acceleration hardware. KoolSpan secure connections have minimal configuration and administration requirements, which means easy and cost-effective installation and maintenance, regardless of the vulnerabilities or limitations of the underlying IP network infrastructure.

KoolSpan's award-winning enhanced 256-bit AES cryptographic algorithms run on hardened silicon hardware with on-board crypto processing and secure memory operations. The crypto card platform creates an ideal tamper-proof, tamper-evident environment for running advanced encryption routines, and storing keys and other security data. This 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 crypto cards and embedded silicon are hardened to the point where they are virtually impenetrable. By running encryption processing on specialized hardware, KoolSpan off-loads 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, Kerberos, 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 process 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 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 devices membership in 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 that work like a virtual secure LAN between any two devices. This connection looks likes 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.

The KoolSpan Lock and Key solution is particularly useful for protecting the traffic of legacy or proprietary devices that don't have the processing power, memory or open interfaces, which are necessary for internal crypto software support.

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. 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. In contrast, KoolSpan encrypted and authenticated connectivity is, by design, an out-of-thebox 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.

KoolSpan for industrial process and control environments: five scenarios
The five secure connectivity scenarios below highlight how KoolSpan can integrate into industrial settings:

1) Embedded in PLCs, smart RTUs and DCS controllers
2) Embedded in network routers, switches and wireless access points
3) Wireless smartphones, PDAs and VoIP devices
4) Stand-alone secure tunnel adaptor for dumb/legacy devices
5) Control room servers and operator consoles and PCs

Scenario 1.
Embedded in PLCs, smart RTUs and DCS controllers

PLCs, RTUs and other data collection and control devices feature increasing intelligence levels, and the ability to manage a wide range of industrial control points, instruments and sensors. Increasingly, programmable controllers are given Ethernet interfaces and folded into IT infrastructure and IP networks. Unfortunately, VPNs, firewalls and other IT protections do not provide end-to-end encryption and authentication, which leaves PLCs, RTUs and other controllers open to malware.

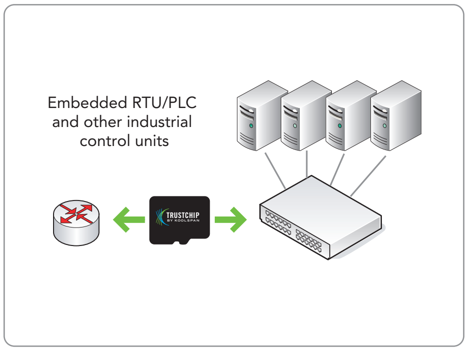
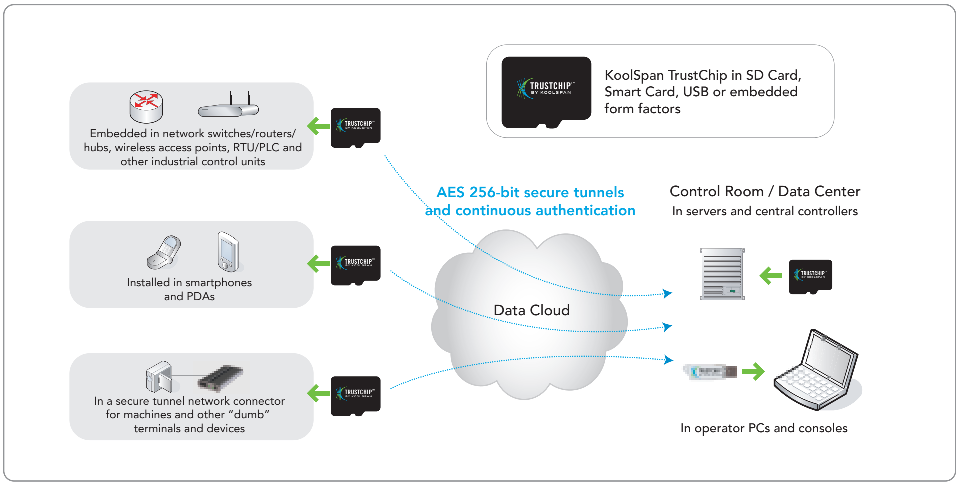


Figure 1. *KoolSpan simple, secure connectivity for industrial control environments*


KoolSpan TrustChip in SD Card, Smart Card, USB or embedded form factors
TRUSTCHIP BY KOOLSPAN
Embedded in network switches/routers/hubs, wireless access points, RTU/PLC and other industrial control units
Installed in smartphones and PDAs
In a secure tunnel network connector for machines and other "dumb" terminals and devices
AES 256-bit secure tunnels and continuous authentication
Data Cloud
Control Room / Data Center
In servers and central controllers
In operator PCs and consoles

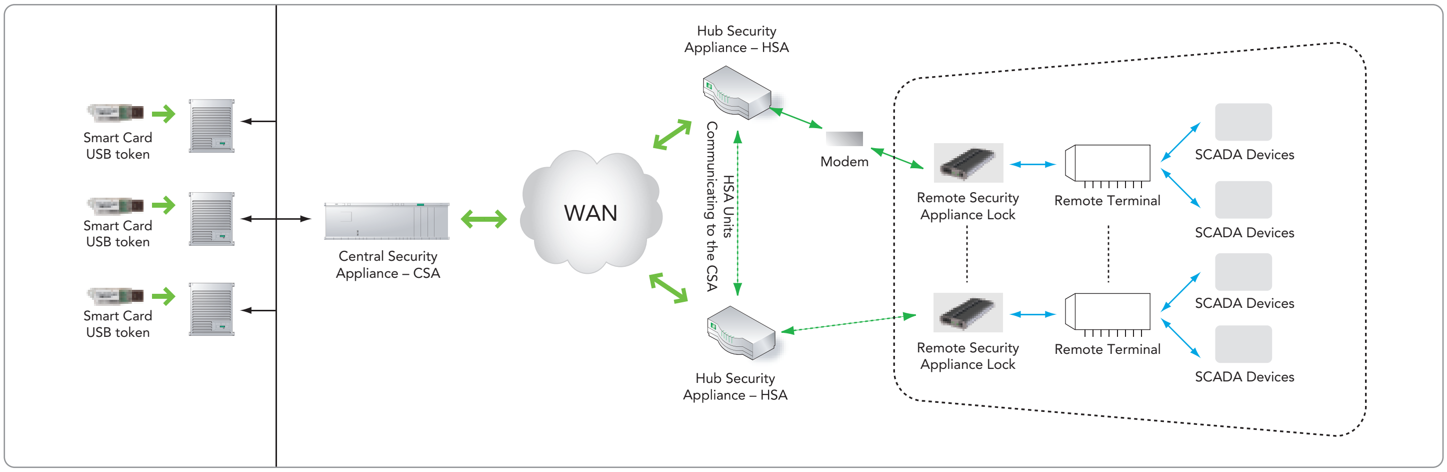
With the KoolSpan solution, strong encryption and mutual authentication is deployed on hardened cryptographic hardware that is embedded in the controller itself. Crypto processing hardware in the form of the KoolSpan TrustChip™ is embedded through a custom ASIC/FPGA or integrated via an industry-standard Smart Card, SD Card or USB form factor. To complement the TrustChip silicon, KoolSpan crypto software is available in quickly deployable API libraries that can be added to controller platforms. Management console software is also available for integration and OEM product development.

KoolSpan software sets up standard secure connections between programmable controllers, control points and other specialized devices. 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 relationships between data collection/control points and a PLC/RTU/DCS controller can be either peer to peer or centrally administered. In the centralized KoolSpan model, a management console function allows operators to dynamically create security communities (TrustGroups) and permit/deny security associations for participating devices. TrustGroups can include any mix of PLC/RTU/DCS controllers, slave instruments, data acquisition points, servers, consoles, wireless devices and end-user PCs.

In the peer-to-peer version, all the necessary authentication keys, identity codes and crypto algorithms are loaded into the KoolSpan TrustChip hardware during installation. From that point on, control/sensor devices are able to, authenticate sessions, and then set up secure end-to-end tunnels automatically. Once peer-to-peer devices are operational, they can continue to dynamically form secure connections within their security groups for an indefinite amount of time without operator intervention.

Figure 2. *Using KoolSpan secure connectivity, operators have access to a specific set of downstream controllers and control points with granular security associations.*

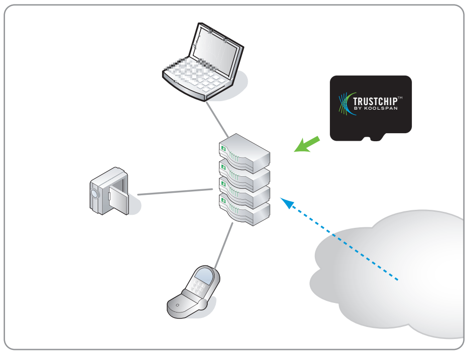

Smart Card USB token
Smart Card USB token
Smart Card USB token
Central Security Appliance – CSA
WAN
Hub Security Appliance – HSA
HSA Units Communicating to the CSA
Hub Security Appliance – HSA
Modem
Remote Security Appliance Lock
Remote Terminal
Remote Security Appliance Lock
Remote Terminal
SCADA Devices
SCADA Devices
SCADA Devices
SCADA Devices

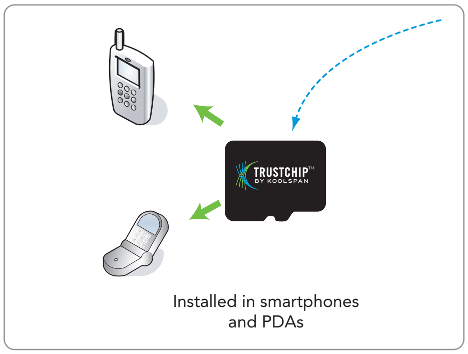
In the peer-to-peer or centralized versions, KoolSpan end-to-end security for embedded systems is essentially plug and play, requiring none of the complex configuration, administration and network architecture modifications that are associated with conventional IP firewalls, VPNs and PKI.

Embedding KoolSpan in PLC/RTU/DCS control devices presents an opportunity 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. This means that operators have connectivity only to RTUs and other instruments for which they have explicit rights (see Figure 2 for embedded KoolSpan application with fine-grained operator access rights management).

Scenario 2.
Embedded in network routers, switches and wireless access points
In some industrial network applications, a group of controllers, control points, I/O devices and other systems all need secure upstream connectivity to the control room or data center. This scenario is found in remote branch offices, pumping stations or transmission substation facilities that are part of a hub-and-spoke, mesh or daisy chain topology. For this application, KoolSpan TrustChip technology and crypto algorithms are integrated into network routers, hubs or switches 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 control room devices and consoles complete the end-to-end secure tunnels. In this environment, KoolSpan simple secure 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 programmable controllers, RTUs and other industrial devices, there is also the opportunity to create plug-and-play secure connections for wireless productivity devices, including smartphones, PDAs, and various ruggedized mobile





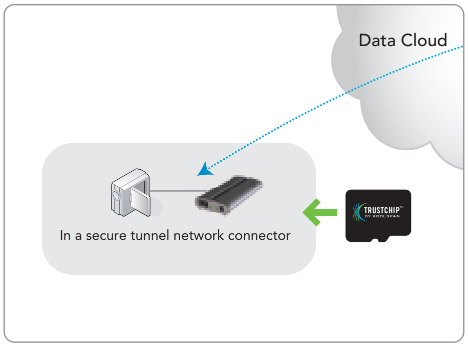
voice/data platforms (e.g., Symbol Technologies, and Motorola). KoolSpan can be easily installed in wireless devices using standard Smart Cards, SD Cards or USB flash memory add-ins. Once the add-in and a software driver are loaded, mobile devices can:

- Participate in peer-to-peer secure voice communications
- Conduct remote system monitoring and control
- 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. KoolSpan connections can be set up with either cellular WiFi or IP LAN. KoolSpan secure tunnels support voice and multimedia data, including streaming video and interactive multimedia exchanges.

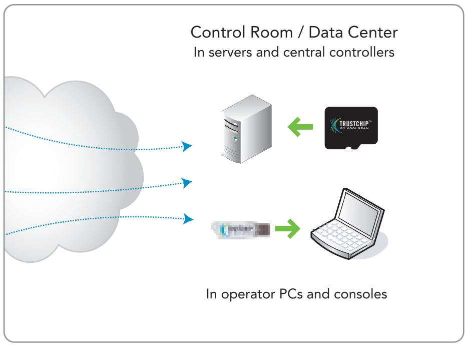
Scenario 4.
Stand alone secure tunnel adaptor for dumb/legacy devices

In the above examples, KoolSpan either is embedded directly in a network device or a programmable controller, or installed via flash card or USB into a mobile device. But in the case of legacy and dumb devices, KoolSpan secure connectivity is provided in the form of a stand alone, Ethernet-based security connector—the KoolSpan Lock appliance. The Lock can operate as a standalone secure network adaptor. Alternatively, this functionality can be integrated into OEM equipment. In this model, the KoolSpan Lock appliance conducts authentication and initializes secure connections on behalf of any downstream devices, including slave RTUs, CCTV video cameras, intercom systems, fax machines, identity card readers, and many other industrial and office systems.



Scenario 5.
Control room servers and operator consoles and PCs

KoolSpan plug-and-play secure connections can be integrated easily into a wide range of servers, HMI consoles and PC stations in data center and control room environments. KoolSpan crypto software will run immediately 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 the KoolSpan SD Card or USB stick, the laptop will automatically form security associations with any other computers, controllers and downstream process devices that it is authorized to access. Once a security association is initialized between the laptop and a downstream control device, the connection looks like a standard link to any applications running on the laptop. This means that operators can use plug-and-play AES 256-bit encrypted tunnels to any downstream KoolSpan devices, without the need for complex and expensive VPN and firewall protections that don't protect end-to-end traffic streams.


Control Room / Data Center
In servers and central controllers
TRUSTCHIP
In operator PCs and consoles

Conclusion

Utilities, manufacturers and other users of distributed control systems have a mandate to create secure network communications proactively and comprehensively. KoolSpan has responded to this need by providing plug-and-play crypto software and hardware that is specially designed to easily integrate into existing RTU, PLC and DCS devices, industrial network routers and the many related industrial/office systems that need end-to-end encryption and authentication that is not typically available from conventional VPN and firewall solutions. Whether you are an OEM, systems integrator, consultant or enterprise end-user, please contact KoolSpan for detailed information on how your specific application can benefit from simplify, 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