INDUSTRIAL CONTROL SYSTEM REMOTE ACCESS OPTIONS

Security for remote access is the most important aspect of preserving production assets. The industrial hardened access solutions listed below are designed to:

- Provide secure layers of protection to prevent unwanted access and maintain data integrity
- Work with existing corporate policies and provide additional layers of security
- Deliver a cost effective solution to support production goals

Corporate IT security policies vary greatly, and our options below provide a robust technology designed to work seamlessly within corporate security standards.

CTI	**Cross Team Interface** The CTI solution utilizes TeamViewer® software and allows the end-user IT department to deploy and manage the firewall and VPN encryption settings based on corporate policy. The TeamViewer® software provides a secure remote connection utilizing AES 256-bit encryption for data transit and two-factor authentication as an additional layer of protection. This solution allows an end-user to fully manage the external connection security functions to ensure data integrity.
CVI	**Cross Virtual Interface** This solution utilizes a Siemens® Scalance firewall module that provides IPsec Virtual Private Network (VPN) tunnelling with stateful packet inspection, NAT/NAPT routing coupled with data encryption using SOFTNET security client to manage authentications. The hardware and setup services are provided and the end-user IT department shall deploy this between the IT and OT networks. The end-user is responsible for providing an external firewall and/or VPN based on corporate security policies.
CCI	**Cross Cellular Interface** The cellular solution offers a hardware enclosure with the Siemens® Scalance firewall listed in the above option but coupled with a cellular connection. This option provides access without using the IT network but uses all of the best security functions available. This option adds an additional layer of protection by requiring the remote connection to locally be enabled and it will physically disconnect after time-out. This enhancement removes the human error from a possibility to preserve the data integrity.

REMOTE ACCESS OPTIONS	CTI	CVI	CCI	
Access Authentication	✔	✔	✔	Encoded Base64 access controls
Data Encryption	✔	✔	✔	Process of encoding data using a proprietary algorithm
Software Provided	✔	✔	✔	Software used to encrypt and manage security functions
Hardware Provided		✔	✔	Firewall with VPN functionality built-in
Firewall Provided		✔	✔	Blocking unauthorized access while permitting outward communications
Security Token		✔	✔	Physical device with electronic key for access
VPN Provided		✔	✔	Established point-to-point connection through virtual tunnelling
Automatic Disconnect Timeout			✔	External connection physically removed automatically
IT Network Access Required	✔	✔		Physical connection from business network to internet

*Hardware,VPN, and procedural security provided by end user for CT option I.
**End user must allow for data access of into IT network for both CTI & CVI options.