District of Barriere

REPORT TO COUNCIL

Date: July 13, 2020	**File:** 530.20/Rpts
To: Council	**From: Ian Crosson, Utilities Manager**
Re: Water Department Update	

Discussion: Wells Update

The utilities department would like to welcome Mr. Bob Payette, our new CAO. Bob has had a chance to make his way around to our facilities and meet our staff in the past week. We look forward to a bright and prosperous future with him as our leader.

The utilities department has been making progress since our last council meeting with the start up and "commissioning' of Bradford Park PW1. After a lengthy discussion with IHA, we deemed it safe to allow water from that well into the system. As of day 1, the programming and alarm testing of PW1 satisfied the department to the point where we felt comfortable that we could run it throughout the day while still meeting the requirements of BCGW and giving a break to DW2. Pending discussions around PW3 are still ongoing with all our consultants and CAO.

The LCIP system is in its final stage of deficiencies with almost all being completed. A final walk-through with TRUE Engineering is being scheduled for the very near future. The reservoir is being monitored for leakage, which will be on going, and signs are showing that the initial loss of water after primary filling was due to absorption into the concrete. Levels are only currently fluctuating +/- 5 mm daily, to every other day, which is highly likely to it being open to the atmosphere.

Discussion: Communications Upgrade

The utilities department would like to present for Council's review and consideration, a communications upgrade proposal and capital cost estimate, put forth by Exceed Electrical (attached). This proposal includes new 4G cellular networking that would replace the existing communications towers. The current communications system is proven to be extremely vulnerable and unreliable with respect to the operations and security of the District's highly sensitive wells.

Recommendation: Pending TRUE Engineering review and approval, THAT Council approve moving forward with Exceed Electrical and the communications upgrade at a cost of $25,534 and that the funds come from Water Reserve.

Prepared by: Ian Crosson, Utilities Manger
Reviewed by: Bob Payette, CAO

EXCEED
ELECTRICAL ENGINEERING

DISTRICT OF BARRIERE

SCADA Communications Upgrade

Prepared by:

EXCEED
ELECTRICAL ENGINEERING

Prepared for:

BARRIERE

Author	Date	Document	Revision	Comment
Christan Beharrell / Malkolm Alburquenque	2020-06-16	Cost Estimate	0	Initial Submittal

OVERVIEW

This document serves as a class 'B' cost estimate for a SCADA communications upgrade for the various water and waste water facilities throughout the District. The North Thompson Valley is known to be prone to lightning surges and thus the existing network has experienced frequent strikes resulting in downtime and an abundance of replacement work required to maintain the system. Exceed proposes a new communications network across all sites utilizing 2020 communications technology to optimize performance and reliability in the District's geological topography.

The Objective

Exceed is proposing a 4G cellular network that aggregates to a central point of management and control at the District of Barriere's office.

Included in the options is some additional engineering for network and cybersecurity configuration as SCADA networks can be vulnerable to attacks including ransomware, viruses, and bad actors. Since remote access will be a priority for remote management and operator control, we want to ensure that access is controlled to authorized personnel only. Exceed employs an IT Cybersecurity professional that can discuss some options with the District.

As cellular coverage has improved in many communities around BC, cellular has become a viable option to connected facilities for SCADA purposes as its high in bandwidth and does not require line of site to operate. As the valley is subject to frequent lightning strikes, 4G communication has a distinct advantage over traditional radio communication systems due to the lack of elevated antennas. Also, the challenging line of site paths between facilities makes for a poor quality radio signal.

In order for the cellular system to function, the District will need to provision a SIM card for each site with 5GB of available data. A server will also need to be configured to in the District's office to manage the VPN network and monitor its health. This configuration will ensure the SCADA and the IT/Enterprise networks are segregated from each other as we do not want vulnerabilities in the regular IT office network to affect the SCADA system.

4G cellular routers and antennas will be installed in all sites (including the District's office).

EXCEED
ELECTRICAL ENGINEERING

Capital Cost Estimate

All district sites will receive the same network hardware, to allow communication over the 4G 3rd party network. The District of Barriere office will additionally be configured as a central hub receiving communication from all sites.

The cellular product that we have chosen is a robust, industrial grade product that is hot swappable in the event of a failure. To change units, an operator can plug the configuration dongle, replace the unit, and plugin the configuration dongle into the new unit. When it is powered back up, it will read the configuration from the dongle and start working as previously in under a minute.

Cellular system pros:

- Installation is quick and effort is minimal
- No external equipment from building (no penetrations)
- Surge protection not required
- No line of site required for a good connection
- Seamless transfer between the 4G network and 3G network to provide optimal uptime in the event of a network outage.

Cellular system cons:

- Requires a data plan for each site
- Dependent on a 3rd party to operate (Telus, Rogers, etc) Cost ?
- Data must be managed to avoid overage charges how ?
- Configuring the network is more involved

Item	Description	Qty	Unit Cost	Total Cost
1	New virtualized server hardware to manage network • Windows Server 2016 License • Physical hardware and configuration	1	$6,000	$6,000
2	Siemens M876-4 4G Cellular Router	5	$1,578	$7,890
3	Siemens 4G Cellular Antenna	5	$110	$550
4	Siemens Key Plug (Device Backup Key)	5	$190	$950
5	Siemens Sinema Remote Connect VPN Software	1	$440	$440
6	Siemens Sinema RC Software Upgrade 64 VPN Connection	1	$1,634	$1,634
7	Electrical Engineering & Configuration (See Note 1) • Onsite for 5 days with 2 people • 4G router configuration • IP subnet changes for every PLC device. • Includes PLC Network Improvements to manage traffic	1	$6,790	$6,790
8	Network Firewall and Cyber Security Services (optional)	1	$1,280	$1,280
			Total	$25,534

The prices listed in the preceding table are an estimate for the services discussed. This summary is not a warranty of final price. Estimates are subject to change if project requirements are changed or costs for materials change before a contract is executed.

Note 1: All fixed price costs include incidentals and employee expenses including personal vehicle mileage at the government prevailing rate of $0.55 per kilometer. Includes food, and rate for two engineers for two a total time of 5 days (including travel).

The success of this cellular option is contingent on the leasing of a public static IP address to the District of Barriere. This can arranged through the District's ISP, typically for a minimal charge of $15/month.

CONCLUSION

It is Exceed's professional opinion that the District would best be served with a 4G communication network across their various site locations. No markup has been added to these prices as we expect the District to order directly from the vendor. The hardware is also budget prices, so costs may decrease once an official quote is obtained.

If you have any questions regarding this fee estimate, please feel free to contact myself via email or phone.

Regards,

Christan Beharrell, P.Eng.
Control Systems Engineer

C: 778-538-4676

E: chris@exceedeng.com

APPENDIX – 4G CELLULAR BROCHURE

SIEMENS

Industrial Remote Communication

Remote networks

Easy remote access to machines and plants

Brochure

Edition 04/2019

siemens.com/remote-networks

Many ways of connecting to remote networks

Increasing bandwidths, higher speeds and performance levels, as well as falling communication costs are all opening up new possibilities in both public and industrial environments.
It's now easier than ever to connect your widely distributed plants, remote machines or mobile applications via remote networks. Siemens offers a wide range of modems and routers for establishing the ideal connection to remote networks over dedicated lines, public switched or cellular telephone networks, or Internet – regardless of whether wired or wireless, IP-based or analog.

The IP-based network components of SCALANCE M and SCALANCE S can be used widely in the fields of telecontrol, teleservice and any other application for industrial remote communication. These devices protect remote networks and the communication between them against unauthorized access and data espionage by means of integrated security functions like Firewall and VPN encryption.
In addition, SINEMA Remote Connect, a management platform, facilitates secure and straightforward administration of communication connections.

The remote networks portfolio for IP-based networks is suitable for use in many different industries, such as:

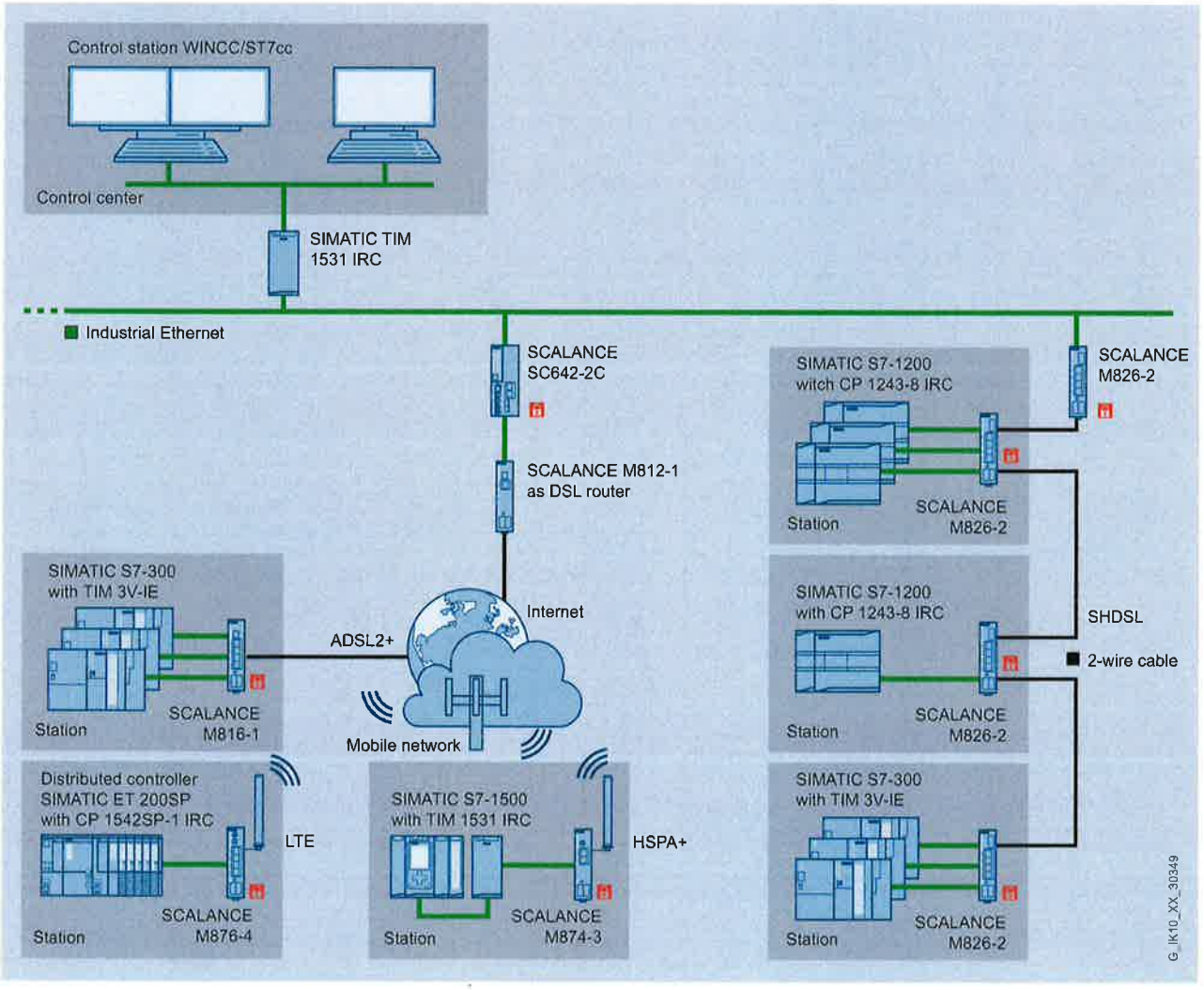
- Power distribution
- Transportation systems
- Plant and machine building
- Water/wastewater treatment plants
- Oil and gas supply
- District heating networks
- Pumping stations

In the field of wind energy and photovoltaic plants, this portfolio also enables a global network to be set up for condition monitoring.

For more information, visit:
siemens.com/remote-networks

Your benefits with the Siemens remote networks portfolio:

- Low investment and operating costs for operator control and monitoring of remotely connected substations
- Reduction in travel and personnel costs thanks to remote programming and diagnostics
- IP-based and analog routers for any application
- Higher standard of data communication security thanks to integrated encryption and access protection mechanisms
- Commissioning and diagnostics via user-friendly web interface
- Easy and secure administration of virtual private network (VPN) connections
- Greater clarity in the control cabinet thanks to space-saving SIMATIC module design
- Integrated into TIA (Totally Integrated Automation)
- 5 years warranty for all SCALANCE products



Application example – telecontrol: Various options for connecting substations

SCALANCE M

The SCALANCE M portfolio consists of industrial routers for wireless or wired access. The products facilitate efficient connection of stationary and mobile stations to a control center. Extensive security functions, such as firewalls and VPN encryption, offer protection during transmission of data.

Wired routers

Wired SCALANCE M routers enable the connection of Ethernet-based subnets and automation devices via existing cable infrastructures. The connection of devices in PROFIBUS networks is also possible.This portfolio includes devices for connection to two-wire cables or wired telephone and DSL networks.

Your benefits:

- Simple connection of local networks using IP communication via WAN
- Low transmission costs, thanks to economical high-volume tariffs
- High process availability due to redundant transmission paths

				
	SCALANCE M804PB	**SCALANCE M812-1**	**SCALANCE M816-1**	**SCALANCE M826-2**
Standard	PROFIBUS/ MPI	ADSL2+	ADSL2+	SHDSL
Frequency bands	Private (existing infrastructure)	Public networks	Public networks	Private (existing infrastructure)
Bandwidth	Up to 12 Mbit/s (at the PROFIBUS/MPI interface)	Downlink: up to 25 Mbit/s Uplink: up to 1.4 Mbit/s	Downlink: up to 25 Mbit/s Uplink: up to 1.4 Mbit/s	Up to 15.3 Mbit/s
DI/DO	1/1			
DSL connection system	–	1 x ADSL2+ (RJ45)	1 x ADSL2+ (RJ45)	2 x SHDSL
LAN interfaces	2 x RJ45	1 x RJ45	4 x RJ45	4 x RJ45
Temperature range	-20 °C ... +60°C	0 °C ... +60 °C	0 °C ... +60 °C	-40 °C ... +70 °C
Safety class	IP20			
Security	VPN (IPsec/ OpenVPN*)/ Firewall			
Special characteristics	Redundant power supply; Network management via SNMP; NAT; connection to SINEMA Remote Connect; PROFIBUS/ MPI interface	Redundant power supply; Network management via SNMP; NAT	Redundant power supply; Network management via SNMP; NAT; connection to SINEMA Remote Connect	Redundant power supply; Network management via SNMP; NAT; connection to SINEMA Remote Connect; certified for rail applications
Advantages				
	■ Convenient and cost-efficient connection of existing systems with PROFIBUS/MPI to SINEMA Remote Connect for secured remote access ■ Standardized remote maintenance concept for new and existing plants	■ Cost-effective connection to DSL provider networks thanks to ADSL2+ support ■ Flexible use as router or modem without need for configuration	■ Cost-effective connection to DSL provider networks thanks to ADSL2+ support ■ Secure direct connection of multiple stations via integrated 4-port switch	■ Connection to existing two-wire infrastructure thanks to SHDSL support ■ Wide range of possible network topologies – e.g. point-to-point, line, link aggregation (4-wire) ■ Low investment and operating costs for operator control and monitoring of remotely connected substations

* For connection to SINEMA Remote Connect as a client

Wireless routers

The wireless SCALANCE M routers use the globally available, public cellular telephone networks (2G, 3G, 4G) for data transmission. This makes them a cost-effective alternative to the set-up of corporate wireless networks.

Your benefits:

- High data rates allow the transmission of mass data or images in real time
- Provider independent
- Connection of extremely remote substations is possible

				
	SCALANCE M876-4 (LTE)	**SCALANCE M876-3 (UMTS)** (EV-DO & CDMA2000)	**SCALANCE M874-3 (UMTS)**	**SCALANCE M874-2 (GSM)**
Standard	4G	3G	3G	2 – 2.5G
Frequency bands	GSM 900/1800 MHz UMTS 900/1800/ 2100 MHz LTE 800/900/1800/ 2100/2600 MHz	GSM 850/900/1800/ 1900 MHz UMTS 800/850/900/ 1900/ 2100 MHz EV-DO: 800/1900 MHz	GSM 850/900/1800/ 1900 MHz UMTS 800/850/900/1900/ 2100 MHz	GSM 850/900/1800/ 1900 MHz
Bandwidth	Downlink: up to 100 Mbit/s (LTE) Uplink: up to 50 Mbit/s (LTE)	Downlink: up to 14.4 Mbit/s (HSDPA) Uplink: up to 5.76 Mbit/s (HSUPA) Forward Link: 3.1 Mbit/s Reverse Link: 1.8 Mbit/s	Downlink: up to 14.4 Mbit/s (HSDPA) Uplink: up to 5.76 Mbit/s (HSUPA)	Downlink: up to 237 kbit/s Uplink: up to 237 kbit/s
DI/DO	1/1			
Antenna connectors	2x SMA	2x SMA	1x SMA	1x SMA
LAN interfaces	4x RJ45	4x RJ45	2x RJ45	2x RJ45
Temperature range	-20 °C ... +60 °C			
Safety class	IP20			
Security	VPN (IPsec/ OpenVPN*)/ Firewall			
Special characteristics	Redundant power supply; network management via SNMP; text message alerts; managed 4-port switch; NAT; connection to SINEMA Remote Connect; certified for rail applications	Redundant power supply; network management via SNMP; text message alerts; managed 4-port switch; NAT; connection to SINEMA Remote Connect	Redundant power supply; Network management via SNMP; text message alerts; managed 2-port switch; NAT; connection to SINEMA Remote Connect	
Advantages				
	High security standards by means of a firewalls (stateful packet inspection) and VPN connections (IPsec) as an integral component of the Industrial Security concept			

* For connection to SINEMA Remote Connect as a client

SCALANCE S

SCALANCE S Industrial Security Appliances ensure secured access to globally distributed plants, machines and applications. They protect automation cells and all devices without their own protection functions from unauthorized access, such as espionage and manipulation.

SCALANCE S components secure communication with stateful inspection firewall and virtual private networks (VPN). All variants enable configuration via Web-based Management (WBM), Command Line Interface (CLI), Simple Network Management Protocol (SNMP), Network Management SINEC NMS and TIA Portal. A digital input enables the controlled establishment of a VPN connection, e.g. for remote maintenance.

Your benefits:

- High firewall and encryption performance
- Management of up to 200 VPN connections
- Network Address Translation (NAT/NAPT) for communication with serial machines with identical IP addresses

					
	SCALANCE SC632-2C	**SCALANCE SC636-2C**	**SCALANCE S615**	**SCALANCE SC642-2C**	**SCALANCE SC646-2C**
Firewall data throughput	600 Mbit/s	600 Mbit/s	100 Mbit/s	600 Mbit/s	600 Mbit/s
IPsec-VPN data throughput	-	-	35 Mbit/s	120 Mbit/s	120 Mbit/s
DI/DO	1/1				
Electrical connection	2x RJ45 ports	6x RJ45-ports	5x RJ45-ports	2x RJ45-ports	6x RJ45-ports
Optical connection	2x combo ports with SFP		–	2x combo ports with SFP	
Temperature range	-40 °C ... +70 °C				
Protection class	IP20				
Bridge firewall	Yes	Yes	No	Yes	Yes
User-specific firewall	Yes	Yes	Yes	Yes	Yes
Password protection	Yes	Yes	Yes	Yes	Yes
Product function with VPN connection	OpenVPN*		IPsec, OpenVPN*		
Number of VPN tunnels	-	-	20	200	200
Number of firewall rules	1000	1000	128	1000	1000
MRP-Client / HRP-Client	No	Yes	No	No	Yes
Special characteristics	Configurable security zones, VRRPv3 coupling, connection to SINEMA Remote Connect				

* For connection to SINEMA Remote Connect as a client

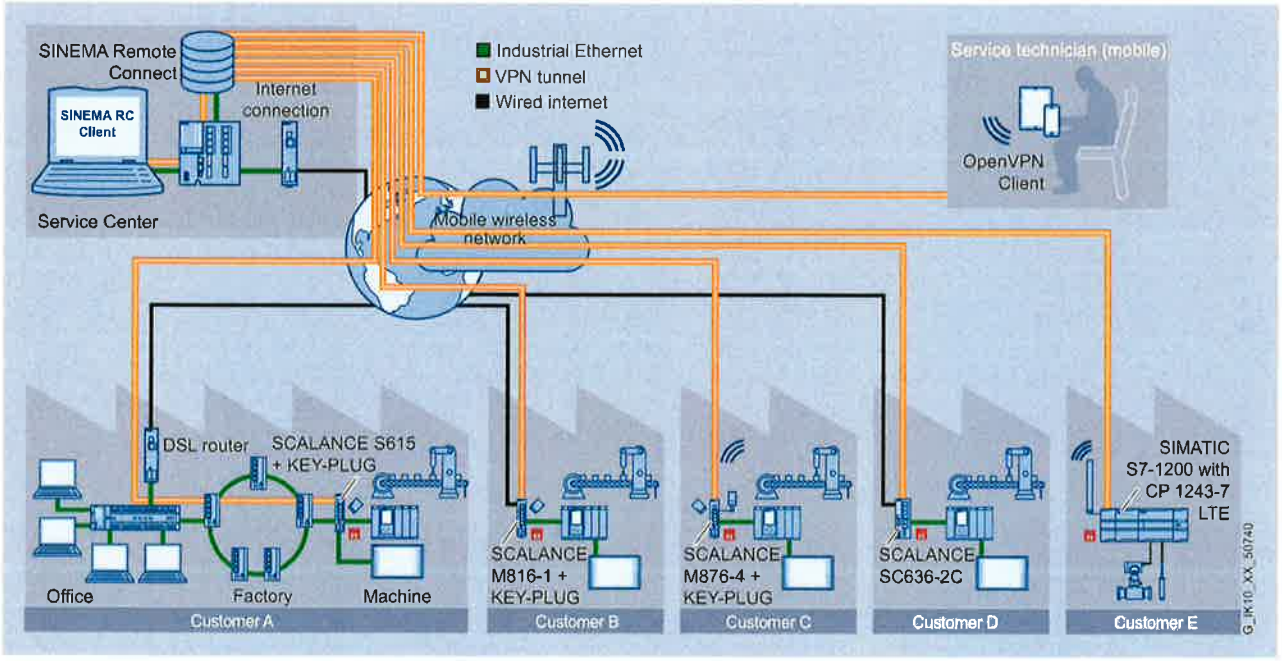
SINEMA Remote Connect – the management platform for remote networks

The management platform for remote networks – SINEMA Remote Connect – is a server application. It allows users to easily maintain widely distributed plants or machines by secured remote access.
SINEMA Remote Connect ensures the secured administration of VPN connections between the control centers, the service engineers and the installed plants. Direct access to the corporate network, in which the plant or machine is integrated, is avoided. The service engineer and the machine to be maintained each establish an independent connection to SINEMA Remote Connect server. The identity of the partners is verified by an exchange of certificates, before any access to the machine is granted. The connection to SINEMA Remote Connect can be set up over diverse media such as cellular phone networks, DSL or existing private network infrastructures.

Your benefits with SINEMA Remote Connect:

- Central administration of all VPN connections
- Simple management of different users including user-specific access rights – even to unique IP addresses in the subnet (Dedicated Device Access)
- Adress book function for fast connection
- Protocol independent, IP-based communication
- Easy integration of the Siemens routers, Industrial Security Appliances, compact RTUs and communications processors by auto-configuration
- Special IT knowledge regarding remote access is not necessary
- Easy selection and connection to identical serial machines for original equipment manufacturers (OEM)
- Operation also in virtualized environment
- Multi-factor authentication

For more information, visit:
siemens.com/sinema-remote-connect



Secured remote service of serial machines and remote stations by means of SINEMA Remote Connect

Siemens AG
Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

Article number 6ZB5530-0CB02-0BA4
IC-FPN9Z-DIPAP-XXXX-32 / Dispo 26000
BR 0319 3. ROT 8 En
Printed in Germany

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit **https://www.siemens.com/industrialsecurity**.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under **https://www.siemens.com/industrialsecurity**.