STARCONTROLS

YOUR GLOBAL IIOT, SCADA & TELECOMMUNICATIONS PARTNER

WE DELIVER SCADA

CYBER SECURITY SOLUTIONS

offering you end-to-end protection

www.star-controls.com

sales@star-controls.com

954.603.0491

THREATS & VULNERABILITIES

With numerous threats and vulnerabilities that could affect critical services, securing SCADA systems must be a top priority.

- Lack of Network Segmentation
- Lack of Encryption
- Ransomware
- Remote Access Policies
- DDoS Attacks
- Malware
- Legacy Software
- Default Configuration
- Policies and Procedures
- Command Injection and Parameters Manipulation damage.

Attacks on SCADA systems are on the rise. The frightening truth is that many infiltrated systems have gone undetected. All too often, cyber criminals “infect” systems and silently monitor traffic, observe activity, and wait for months or even years before taking any action allowing them to strike when they can cause the most damage.

GLOBAL ATTACKS

"We recognize the enemy will use the Internet to recruit, to take down SCADA systems. In short, we expect a cyberattack as a prelude to war." - LTG Alan Lynn, DISA (Defense Information Systems Agency) Director

IN THE PAST FEW YEARS WE HAVE SEEN:

- July 2017 - "We never anticipated that our critical infrastructure control systems would be facing advanced levels of malware," Mr. Wellinghoff said. "Hackers Are Targeting Nuclear Plants, U.S. Says" *New York Times*
- June 2017 - Greenberg, a senior reporter at *Wired*, reports that many cybersecurity experts believe Russia is using Ukraine as a cyber-war testing ground.
- December 2016 - Incident occurred amid a flurry of 6,500 cyber attacks over two months, according to Ukraine's President Petro Poroshenko. Poroshenko said the attacks indicated Russian "cyberwar."
- September 2016 - Largest DDoS attack ever delivered by botnet of hijacked IoT devices, according to Network World.
- October 2015 - Chatham House, a UK think-tank, reported that the risk of a cyber attack on nuclear infrastructure is growing. The trend towards the digitization of SCADA systems is increasing the vulnerability of nuclear facilities, and many are inadequately prepared. Even where facilities are air-gapped, this safeguard can be breached with nothing more than a flash drive.
- April 2015 - According to the 2015 Dell Security Annual Threat Report, SCADA attacks are on the rise. The report found that in 2014, the number of attacks on SCADA systems doubled compared to the previous year. Most of these attacks occurred in Finland, the United Kingdom, and the United States.
- March 2015 - A report by the US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) found that it received 245 cyber incident reports from asset owners and industry partners in the fiscal year of 2014.
- December 2014 – An unnamed German Steel Mill suffered extensive damage from a cyber-attack. The attackers were able to disrupt the control system and prevent a blast furnace from being shut down, resulting in 'massive' damage.

Star Controls offers end-to-end, holistic approach, that integrate technologies, products and protocols that were designed for the ICS/SCADA security, and leverages technical Star Controls' know how.

At a granular level, all products and solutions that Star Controls work with offer the highest level of security at every critical stage of operation. The solutions covers the OT (Operational Technology, the traditional ICS/SCADA), as well as the IT (traditional IT security). Star Controls provides a complete Cyber Security solution for the ICS/SCADA systems, which detect and protect any potential entry point into the system. It's integrated and holistic approach stitches the Cyber Security for all components that are part of the SCADA system:

- Data Center - SCADA Servers and Front End Processors (or Gateways)
- Networks - Devices, such as Wireless Radios and Gateways
- Remote Sites - RTUs/PLCs and Smart Devices and Site Security

Star Controls offers end-to-end, holistic approach, that integrate technologies, products and protocols that were designed for the ICS/SCADA security, and leverages technical Star Controls' know how.

SCADA SOFTWARE

For Cyber Security Star Controls offers different SCADA software products, while the VTScada is among the best fit for Cyber Security.

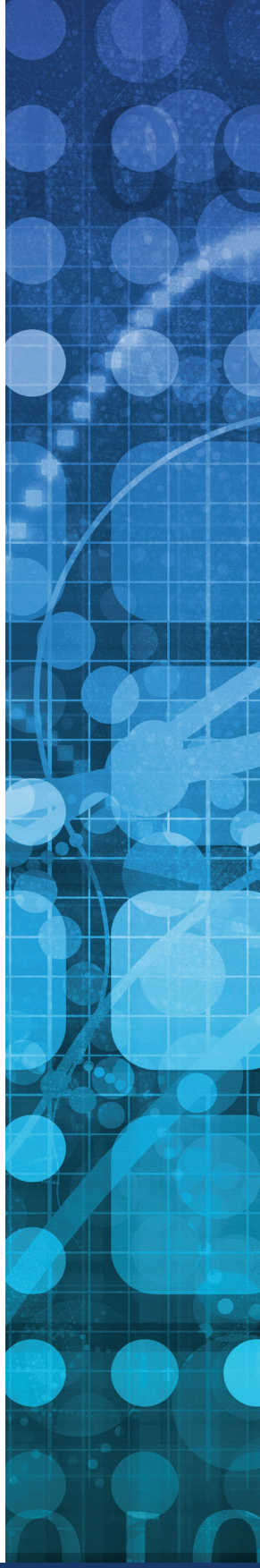
VTSCADA SCADA SOFTWARE

Each application includes its own security accounts and settings which control access to all parts of the application including workstations, thin clients, mobile clients, and alarm notifications. Deployed security changes are immediate and application wide. Accounts are easily copied, modified, and deleted. You can now even share accounts across multiple applications.

- Military-grade encryption
- Security protocols
- Password protection
- Group management
- Share security accounts applications

FIREWALLS FOR ICS/SCADA

Star Controls includes products from Check Point, the industry leader in IT Security, to provide a complete To-Down IT Security to the ICS/SCADA systems.



Star Controls has partnered with the top vendors to include best of breed products in the SCADA Cyber Security Field

CHECK POINT GATEWAY AND ANALYTIC MANAGER

Check Point offers the most advanced cyber security. Aligning Operational Technology (OT) with Information Technology (IT) security, Check Point provides an end-to-end multi-layer threat defense, allowing real-time protection and monitoring against threats with full visibility along with granular control of SCADA traffic. Paired with ruggedized appliance options and comprehensive protocol support, Check Point ensures critical assets are never compromised. With our best in class management platform all IT and OT environments are supported with a single, unified and robust management; the most advanced existing today.

Check Point's SandBlast is a complete solution for IT security, including Firewall, Anti-Malware, Anti-Bot, Anti-Ransomware, Forensics and more. The following information on the SandBlast Zero Day Protection and Anti-Ransomware includes more details on its capabilities in these areas.

SANDBLAST ZERO DAY PROTECTIONS

All enterprises are at risk of targeted attacks such as spear phishing and Advanced Persistent Threats. Check Point SandBlast Zero-Day Protection, with its unique exploit-level detection and threat extraction, provides an additional layer of security from even the most sophisticated hackers and dangerous attacks. Unlike traditional sandboxing solutions that are subject to evasion techniques and either introduce unacceptable delays or let potential threats through while under evaluation, Check Point catches more malware, with minimal impact on delivery times. SandBlast is offered at the Network level, in the Cloud, and at the EndPoint.

ANTI-RANSOMWARE

Check Point SandBlast Agent with Anti-Ransomware and zero phishing technology, extends zero-day protections to web-browsers and end-user devices to defend against advanced attacks, keeping users safe no matter where they go. With continuous data collection and automated incident analysis, SandBlast Agent provides actionable forensics, which accelerates the process of understanding the complete attack lifecycle, damage & attack vectors, to maximize response team productivity and minimize resolution times. Anti-Ransomware keeps businesses one step ahead of attacks by automatically detecting, blocking and removing the most sophisticated ransomware infections and restoring any encrypted data as part of its automated remediation capability.

WIRELESS GATEWAYS

Star Controls offers a variety of wireless Gateways, such as cell modems or data radios, for private and public networks. Star Controls engineers will add all necessary authentication and encryption to the units, so secure this segment of the SCADA system.

PRIVATE NETWORKS

Star Controls offers products from leading vendors, such as CalAmp, 4RF and GE-MDS.

PUBLIC NETWORK

Star Controls offers products from leading vendors such as Sierra Wireless and Red-Lion. Our IT security experts will facilitate the dialogue with the cellular service provider, to define and implement all necessary IT security, e.g. VPN, while the data is going through the SP's networks.

The AirLink Raven RV50 from Sierra Wireless is an example for Cellular Gateway that meets the OT and IT requirements. The Raven RV50 is loaded with features to secure critical data. It supports secure communications to multiple back-end systems by providing up to five concurrent VPN sessions. Remote authentication management allows enterprise-grade systems to manage access

RTU, PLCS AND SMART DEVICES

This area in the system is vulnerable and has been ignored by almost all vendors. Star Controls is addressing existing systems by adding layer of IT Security to sites with PLCs and Smart Devices that are used by the different vertical market. Star Controls is also promoting the Motorola ACE3600 RTU, which is the first RTU in the industry that provides a complete end-to-end IT Security to the remote monitor and controls.

SECURED ACE3600

Secured ACE3600 RTUs, FEP (ACE IP Gateway or ACE3600 FIU) with enabled security features such as access/interface control, secured communication, secured files, and security-related logs. ACE3600 Security Policy is a set of configurable system-wide security parameters for enforcing the organization's security policy in the ACE3600 system management tools (STS), front-end units and field units.

ACE SECURED SYSTEM – SECURITY LAYERS

- Secure Access Control
  - –User access control to all system parts
  - –Roles and permissions
  - –M2M access control
  - –Central access management & control
- Audit
  - –Integrated security log
  - –Logging security events
  - –Sending security alerts
- Stored Data Encryption
  - –File encryption
- Communications Security
  - –Data payload encryption
  - –Encryption key management
  - – Integrated IP Firewall
  - –Unused port disabling
  - –Suppressing vulnerable protocols
  - –Message Life Time
- White listing
  - –Run-file white listing in the RTUs
  - –Management tools white listing & configuration change control
- Secured programming
  - –Implementing secured programming methodology
  - –Avoiding "backdoors"
  - –Using protocols / port scanners
  - –.NET Code obfuscation

STARTU SOFTWARE APPLICATION

Star Controls' flagship software product, for the Motorola RTUs, is a game changer in the RTU/PLC market, providing the SCADA and the O&M team unparalleled capabilities and ease of use to configure, change and maintain every aspect of the RTU. The StaRTU has been upgraded to work on the Motorola Secured ACE600 RTU. Star Controls is also planning to incorporate logs from the StaRTU loggers (i.e. Communications and I/Os) into the Cyber Security Analytic at Check Point Manager. This will cover non-IP, legacy, SCADA systems.

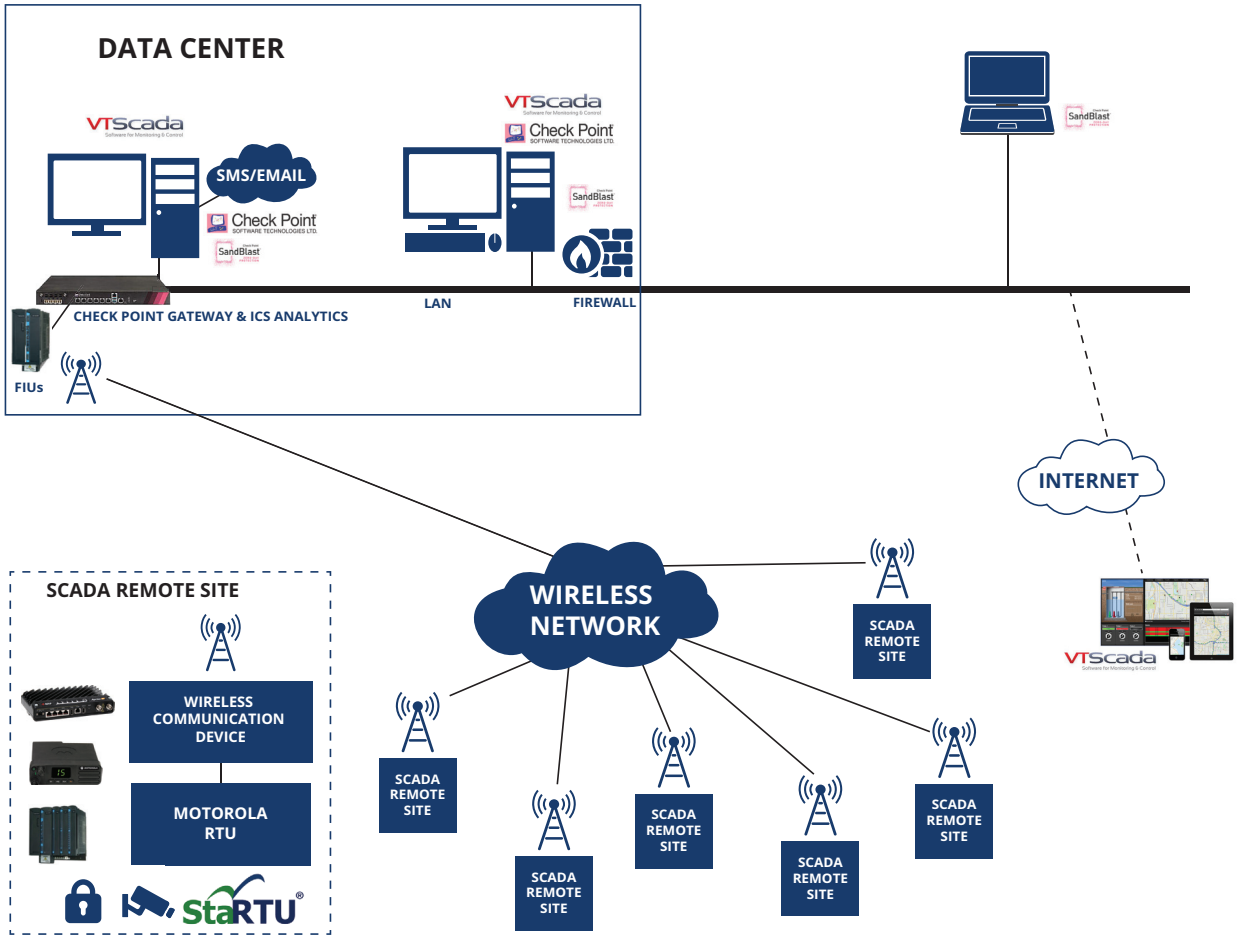
SITE SECURITY

The site security is an important part of the overall security of the ICS/SCADA system. The integration of the two systems allows the correlation between alerts from IT security with the site security. The site security includes access management and advanced video surveillance, including video analytics.

CYBER-SECURED SCADA SYSTEM

CONCEPTUAL BLOCK DIAGRAM

with Cyber Security Solution Partners



Check Point SOFTWARE TECHNOLOGIES LTD.

MOTOROLA SOLUTIONS

SIERRA WIRELESS™ Solution Partner

VTScada Software for Monitoring & Control

STARCONTROLS

YOUR GLOBAL IIOT, SCADA &
TELECOMMUNICATIONS PARTNER

11555 Heron Bay Blvd, Suite #200
Coral Springs, FL 33076

+1-954-603-0491

sales@star-controls.com

star-controls.com