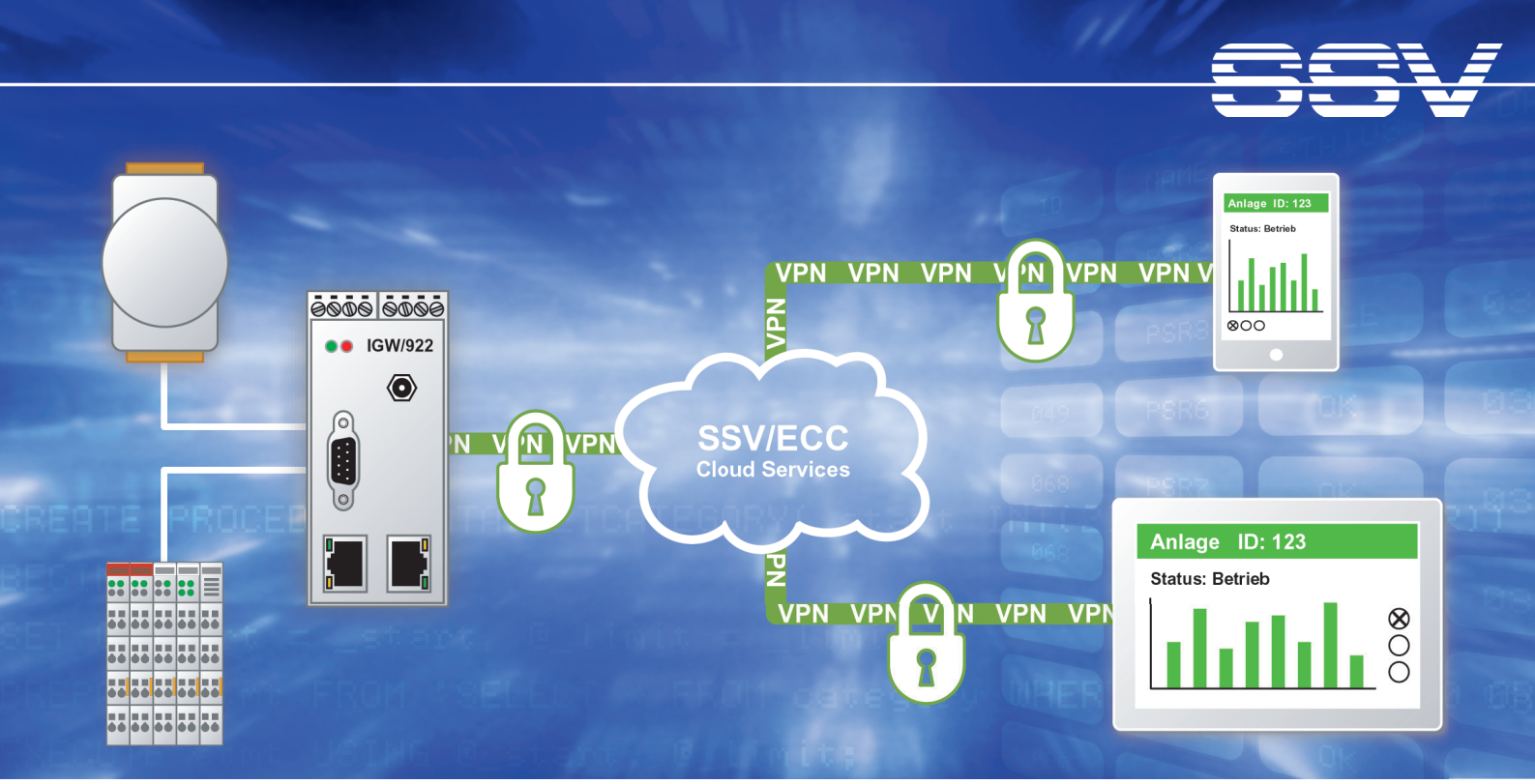


Safety ohne Security geht nicht!

Das Thema „Safety und die funktionale Sicherheit“ haben im deutschen Maschinen- und Anlagenbau inzwischen einen sehr hohen Stellenwert. Dieser Sachverhalt ist sicherlich auch mitverantwortlich für den beachtlichen Exporterfolg deutscher Produkte und deren guten Ruf.

Etwas anders sieht es offensichtlich mit der Security aus – also dem Schutz gegen Cyberangriffe und deren Folgen. Da werden komplette Anlagen mit dem Internet verbunden und die Fernzugriffsschnittstelle lediglich mit einer Benutzername-Passwort-Kombination geschützt. Dass man damit heute keine Angreifer fernhalten kann, musste Anfang dieses Jahres auch ein führender deutscher Hersteller von Hightech-Heizungen erfahren, der die Steuerungen eines namhaften Schweizer Anbieters einsetzt. Da viele betroffene Anlagen sogar über die Angriffsziel-Suchmaschine Shodan zu finden waren, wurde in diesem Fall sogar das BSI (Bundesamt für Sicherheit in der Informationstechnik) eingeschaltet. Über diesen Vorfall wurde in den Medien ausgiebig berichtet.

Eigentlich haben wir in Deutschland das Potenzial, auch bei der Security für Maschinen und Anlagen ganz vorne mitzuspielen. Wir müssen nur dafür sorgen, dass die erforderlichen Security-Baugruppen und Funktionen – ähnlich wie Kfz-Sicherheitsgurte in den 70er Jahren – nicht erst vom Betreiber nachträglich selbst beschafft und hinzugefügt werden müssen, sondern gleich zur Standardausstattung gehören.

Wir haben inzwischen eine hochentwickelte und praxiserprobte Security-Plattform mit zahlreichen Bausteinen für Maschinen- und Anlagenbauer zu bieten, mit der nicht nur der betroffene Hightech-Heizungshersteller die aktuellen Fernzugriffsprobleme lösen konnte und die auch erfolgreich einem umfangreichen Sicherheitscheck durch einen Prüfdienstleister unterzogen wurde.

Ich würde mich freuen, wenn meine Mitarbeiter und ich Ihnen diese Plattform einmal vorstellen dürften, um mit Ihnen über Ihre konkreten Anforderungen zu sprechen!

Ihr Klaus-Dieter Walter

Geschäftsführung
SSV Software Systems GmbH

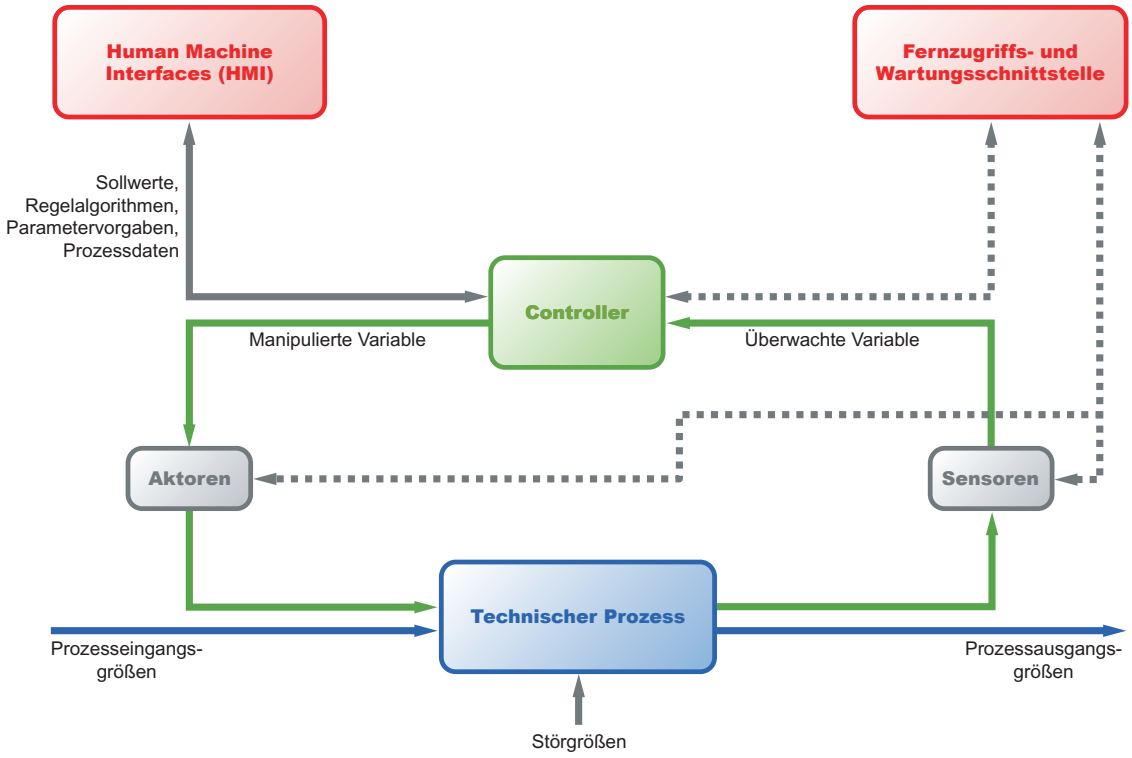
© 2014 SSV Software Systems GmbH · Dünenweg 5 · D-30419 Hannover · Fon: 0511/40 000-0 · Fax: 0511/40 000-40 · info@ssv-embedded.de · www.ssv-embedded.de

Architekturbedingte Schwachstellen

Eigentlich ist es schon mehr als verwunderlich, dass unzählige Steuerungen und MSR-Baugruppen heute zwar überwiegend mit IP-fähigen Schnittstellen und entsprechenden Softwarefunktionen (z. B. Webserver) ausgestattet sind, aber meistens ohne spezielle bzw. geeignete Schutzmaßnahmen gegen externe und interne Angriffe betrieben werden. Dabei zeigt schon ein Blick auf die typische Regelschleife einer MSR-Anwendung, dass es aus Sicht der IT-Security mit der HMI- und Fernzugriffs- bzw. Wartungsschnittstelle zwei architekturbedingte Schwachstellen für Angreifer gibt. Über diese Schnittstellen lassen sich MSR-Systeme mit überschaubarem Aufwand manipulieren und nachhaltig stören.

Dieser Sachverhalt ist vielen MSR-Technikern und Anlagenverantwortlichen häufig noch nicht einmal bekannt – sie meinen nach wie vor, ihre Anlage bzw. MSR-Lösung hat überhaupt keine Verbindung zum Internet.

Fernzugriffs- und Wartungsschnittstelle: Um die Verfügbarkeit einer Lösung zu steigern und im Störungsfall möglichst schnell reagieren zu können, haben viele Hersteller ihre Produkte und Lösungen mit einer internetbasierten Fernwartungsschnittstelle ausgestattet. Welches Gefahrenpotenzial sich hinter einem solchen Zugang verbirgt, kann man dem BSI-Dokument *Industrial Control System Security – Top 10 Bedrohungen und Gegenmaßnahmen* entnehmen. Die „Unberechtigte Nutzung von Fernwartungszugängen“ findet man dort auf dem ersten Platz der Top 10.



Human Machine Interface (HMI): Die meisten Steuerungen und Regelungen benötigen eine Bedienerschnittstelle, um zum Beispiel Sollwerte einzustellen und aktuelle Prozessdaten zu visualisieren. Solche HMI-Lösungen werden entweder als dedizierte Systeme oder aber als Baustein auf einer PC-Plattform realisiert, die häufig in andere Netzwerke, zum Beispiel ein Corporate-LAN, eingebunden ist. Durch eine solche Office-IT-Verbindung besteht aber oftmals ein risikobehafteter (indirekter) Link zum weltweiten Internet.

Durch zukünftige Industrie 4.0-Anwendungen wird noch mindestens eine weitere „unsichere“ Schnittstelle hinzukommen. Neben dem Fernwartungs-Interface wird dann auch eine spezielle Interoperabilitätsschnittstelle existieren, um die einzelnen Steuerungs- und IT-Anwendungen verschiedener Standorte miteinander zu verbinden. Ohne entsprechende Sicherheitsvorkehrungen können Angreifer dann nicht nur die IT- und Automatisierungssysteme eines einzelnen Unternehmens, sondern sogar einer vollständigen Lieferkette attackieren.

© 2014 SSV Software Systems GmbH · Dünenweg 5 · D-30419 Hannover · Fon: 0511/40 000-0 · Fax: 0511/40 000-40 · info@ssv-embedded.de · www.ssv-embedded.de

Firewalls und VPNs nutzen

HMI-Schnittstellen sind in der Regel völlig ungeschützte Zugänge, um einer Visualisierungsbaugruppe oder Software den Schreib-/Lesezugriff auf die Daten einer Steuerung zu ermöglichen. Ein typisches Beispiel wäre der Zugriff einer SCADA-Software auf die Modbus-Schnittstelle einer SPS, um Parametervorgaben zu schreiben und Prozessdaten zu lesen. Zwischen der IP-Schnittstelle einer Steuerung und einem HMI-System sollte aus Sicherheitsgründen ein geeigneter Paketfilter als Firewall betrieben werden.

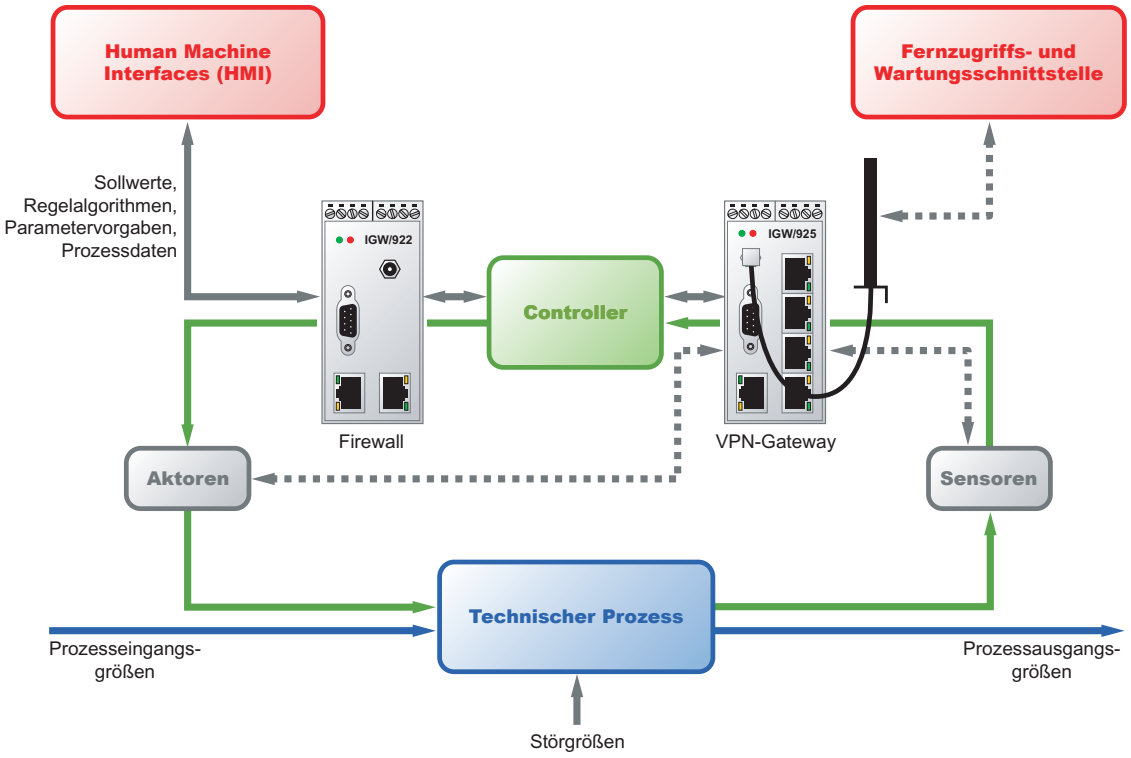
Viele Wartungszugänge besitzen lediglich einen einfachen Passwortschutz. Das reicht auf keinen Fall aus. Zur wirkungsvollen Absicherung einer Fernzugriffs- und Wartungsschnittstelle empfiehlt sich der Einsatz eines Virtual Private Networks (VPNs).

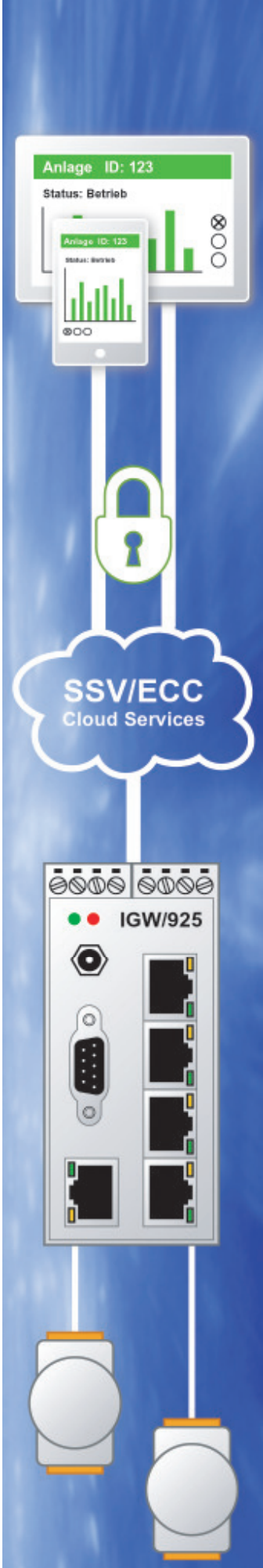
Dafür wird zwischen Steuerung bzw. MSR-Baugruppe und Internet ein VPN-Gateway geschaltet, das den Endpunkt eines speziellen Sicherheitstunnels bildet. Am anderen Tunnelende befindet sich in der Regel ein Servicerechner für den Fernzugriff mit einer entsprechenden VPN-Software. Die Tunnelverbindung durch das Internet wird mit Hilfe einer aufwändigen Datenverschlüsselung und Signierung abgesichert. Um die Sicherheit zu optimieren, wird der Schlüssel (Session Key) für den Tunnel alle paar Stunden automatisch geändert. Vor dem Aufbau des VPN-Tunnels müssen sich die Kommunikationspartner beidseitig mit Hilfe sogenannter X.509-Zertifikate authentifizieren. Da der Verbindungsaufbau zwischen VPN-Gateway und Servicerechner nicht direkt, sondern über einen Fernwartungs-Infrastrukturserver (z. B. Security Server SSR/525) erfolgt, lässt sich durch das Ausstellen und Sperren einzelner Zertifikate die Zugriffsberechtigung für alle Systeme verwalten.

Gesamtlösung prüfen und testen

Hinsichtlich der Security ist jede Lösung ein individuelles System mit unterschiedlichen Anforderungen und Gegebenheiten. Insofern kann es für eine bestimmte MSR-Anwendung auch keine Security-Lösung „von der Stange“ geben, die einmal eingebaut und dann vergessen wird. Die Sicherheit einer Anwendung muss als Prozess behandelt werden.

Insofern ist das Ergebnis auch immer wieder durch Audits zu überprüfen. Dazu gehören auch Penetrationstests nach den jeweils neuesten Gesichtspunkten, um einen optimalen Schutz für die HMI- und Fernzugriffsschnittstellen zu gewährleisten.





© 2014 SSV Software Systems GmbH · Dünenweg 5 · D-30419 Hannover · Fon: 0511/40 000-0 · Fax: 0511/40 000-40 · info@ssv-embedded.de · www.ssv-embedded.de

Security-Plattform

für den Maschinen- und Anlagenbau

SSR/525
Security Server

1 HE Server-Hardware für 19“ Racks (Abbildung ähnlich). Intel Atom D525 CPU (2 Cores mit 1.8 GHz), 4 GByte DRAM, 1.000 GByte HDD, 2x 10 / 100 / 1000 Mbps LAN. Linux O/S und SSV OpenVPN-Server-Software für bis zu 500 Clients vorinstalliert. Die gesamte Software eines SSR/525 können Sie auch auf einem eigenen Server hosten, der direkt in Ihrer IT oder bei einem Service-Provider betrieben wird.

IGW/922
VPN Remote Access Gateway

VPN Client Gateway mit Embedded Linux und SSV Firmware mit OpenVPN, SSL, SSH, Firewall, verschiedenen Proxy-Funktionen, COM-Port-Redirector und webbasierter Konfigurationsoberfläche.

2x 10 / 100 Mbps LAN
1x RS232
1x RS232 / RS485
1x GSM / GPRS oder
1x UMTS / HSPA Wireless Modem
1x interner SIM-Kartenhalter
12 - 24 VDC

IGW/925
VPN Remote Access Gateway mit 4x Switch

VPN Client Gateway mit Embedded Linux und SSV Firmware mit webbasierter Konfigurationsoberfläche wie IGW/922.

1x 10 / 100 Mbps LAN (MAC1)
4x 10 / 100 Mbps LAN (MAC2)
(über internen Switch)
1x RS232
1x RS232 / RS485
1x GSM / GPRS oder
1x UMTS / HSPA Wireless Modem
1x interner SIM-Kartenhalter
12 - 24 VDC

IGW/935
VPN Micro Server / Web Application Gateway

Multifunktionales Industrial Gateway für den Einsatz als Web Application Plattform oder VPN Micro Server. Embedded Linux mit Webserver und Webbrowser, SSV FDE, Python, Java, PHP, OpenVPN, SSL, SSH und mit webbasierter Konfigurationsoberfläche.

1x 10 / 100 Mbps LAN
1x USB 2.0 Host Port
1x DVI / HDMI Interface
1x RS485
12 - 24 VDC

IGW/936-L
LTE Router / Application Gateway

Hochperformanter 4G Industrial Router mit LTE-Mobilfunkmodem (unterstützt GSM, UMTS, HSPA und LTE). Embedded Linux und SSV Firmware mit webbasierter Konfigurationsoberfläche wie IGW/935 plus Erweiterungen.

1x 10 / 100 Mbps LAN
1x 10 / 100/1000 Mbps LAN
1x USB 2.0 Host Port
1x DVI / HDMI Interface
1x RS485
1x RS232 / RS485
12 - 24 VDC

© 2014 SSV Software Systems GmbH · Dünenweg 5 · D-30419 Hannover · Fon: 0511/40 000-0 · Fax: 0511/40 000-40 · info@ssv-embedded.de · www.ssv-embedded.de