Industrial Security

- **Introduction** 2
- **The Siemens Solution** 10
- **Application Examples** 50
- **Benefits of Working with Siemens** 70
Security Trends
Globally we are seeing more network connections than ever before

Trends Impacting Security

- Cloud Computing approaches
- Increased use of Mobile Devices
- Wireless Technology
- Reduced Personnel Requirements
- Smart Grid
- The worldwide and remote access to remote plants, remote machines and mobile applications
- The “Internet of Things”

Figure 4: Top 5 in terms of Likelihood

- Severe income disparity
- Chronic fiscal imbalances
- Rising greenhouse gas emissions
- Cyber attacks
- Water supply crises

Source: World Economic Forum
Source: World Economic Forum, 50 Global Risks
Industrial Security
The corporate security chain is only as strong as its weakest link

Security Can Fail at Any of these Points

- Employee
- Smartphone
- Laptops
- PC workstations
- Network infrastructure
- Mobile storage devices
- Tablet PC
- Computer center
- Policies and guidelines
- Printer
- Production systems
Industrial Security
Why has industrial security become so important?

Main Trends Impacting the Vulnerability of Automation Plants

- Horizontal and vertical Integration at all network levels
- Connection of automation networks with IT-Networks and Internet for remote maintenance
- Increased use of open standards and PC-based systems
- Possible Threats increased due to these trends:
  - Access violation through unauthorized persons
  - Espionage and manipulation of data
  - Damages and data loss caused by malware
- Several security incidents reveal the vulnerability of automation plants.
Industrial Security
The Defense in Depth Concept

Plant security
- Physical prevention of access to critical areas
- Establishing a Security Management Process

Network security
- Controlled interfaces between office and plant network e.g. via firewalls
- Further segmentation of plant network

System integrity
- Antivirus and whitelisting software
- System hardening
- Maintenance and update processes
- User authentication for plant or machine operators
- Integrated access protection mechanisms in automation components

Security solutions in an industrial context must take account of all protection levels
Industrial Security
The Siemens Approach

- Implementation of **Security Management**
- The **interfaces** are subject to regulations - and are monitored accordingly.
- **PC-based systems** must be protected.
- The **control level** must be protected.
- **Communication** must be monitored and can be segmented.

The Siemens approach is based on five key points
## Industrial Security
### Security Integrated – Overview

<table>
<thead>
<tr>
<th></th>
<th>SCALANCE S Family</th>
<th>SCALANCE M Family</th>
<th>CP 343-1 Adv</th>
<th>CP 443-1 Adv</th>
<th>S7-1200 CPU 1)</th>
<th>S7-1500 CPU</th>
<th>CP 1243-1 1)</th>
<th>CP 1543-1 1)</th>
<th>CP 1628</th>
<th>SOFNET Security Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configurable copy protection</td>
<td>•</td>
<td></td>
<td></td>
<td></td>
<td>•</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access protection (authentication)</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extended access protection (Firewall)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual Private Network with IPSec</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manipulation protection (communication, configuration)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1) applies 1) from CPU firmware V4.0 from STEP 7 Professional V13 (TIA Portal)
Defense in Depth on the Plant Floor

Adapted measures for production

**Network Access Control**
- Interface to IT networks: Secure architecture with DMZ (SCALANCE S623)
- Secure Remote Access via Internet
- Local network access (port security) via device and user authentication (SCALANCE S)

**Redundancy**
- Protection of redundant network topologies and secure redundant connection of underlaid networks or rings with S627-2M

**Cell Protection**
- Risk mitigation through network segmentation
- Cell protection concept with Security Appliances or S7-Security CPs.
- Use of secure communication protocols (e.g. https) prevent espionage and manipulation
Industrial Security

- Introduction
- The Siemens Solution
- Application Examples
- Benefits of Working with Siemens
DMZ at the enterprise interface
Secure redundant rings with firewall & standby
Cell Protection

PC/IPC with SOFTNET Security client software

Security Module SCALANCE S

Industrial Ethernet

VPN tunnel

Access Point SCALANCE W788-1 RJ45

PC/PG/Notebook with SOFTNET Security Client software

Automation cell 1

Automation cell 2

Automation cell 3
Access control & Network separation

TIA Portal

Industrial Ethernet

Automation Cell

SIMATIC S7-1500 with CP 1543-1

S7-1200 with CM 1242-5

ET 200SP

S7-300 with CP 343-1 Lean

SINAMICS

PROFIBUS DP

PROFINET

Industrial Ethernet

Automation Cell

SIMATIC S7-1500 with CP 1543-1

S7-1200 with CM 1242-5

ET 200SP

S7-300 with CP 343-1 Lean

SINAMICS

PROFIBUS DP

PROFINET

Industrial Ethernet

Control center

Products with firewall or VPN functions
Protection of Industrial PCs
Software management

Antivirus and Whitelisting solutions provide different security functions:
- Protection against Viruses, Worms and Trojans
- Stop unauthorized applications and malware

Patch Management & software updates
- Necessary reality of modern manufacturing
Combining security elements
Industrial Security
Security Integrated: SCALANCE S Security Modules

Customer Requirement
Network protection and segmentation
Protection against:
- Espionage
- Data manipulation
- Accidental access
Enabling of secure remote access for:
- Telecontrol
- Teleservice

Our Solution
SCALANCE S security modules with Security Integrated provide:
- Stateful Inspection Firewall
- VPN (data encryption and authentication)
- NAT/NAPT (address translation)
- Router functionality (PPPoE, DynDNS) for broadband internet access (DSL, cable)
- S623 with an additional VPN port (DMZ), allowing the possibility of securely connecting an additional network for service or remote maintenance purposes.
- S623 for secure, redundant connection of underlying networks via router and firewall redundancy
Customer Requirement
- More flexibility by creating and establishing of security concepts
- Securing of redundant network structures
- High availability due to redundant coupling
- Use in industrial environments

Our Solution
SCALANCE S627-2M security module with Security Integrated provides:
- All functionalities of SCALANCE S623
And additionally:
- Two additional slots for 2-port media modules for direct integration into ring or line topologies
- Direct interface to FO networks with FO media modules
- Securing of redundant ring topologies (MRP, HRP)
- Secure, redundant connection of underlying networks with stand-by-coupling
- Secure, redundant connection of underlying networks and rings via router and firewall redundancy
### Customer Requirement

Network protection

**Protection** against:
- Espionage
- Data manipulation
- Accidental access

Enabling of **secure remote access** for:
- Telecontrol
- Teleservice

### Our Solution

**UMTS Router SCALANCE M874-3** (UMTS) and **M874-2** (GSM) with **Security Integrated** provide:

- Stateful Inspection Firewall
- VPN (data encryption and authentication)
- NAT/NAPT (address translation)
- Router functionality for mobile broadband Internet access (GPRS, UMTS)
- Greater field of applications due to high bandwidth, performance and speed
- Application dependent use of mobile radio services of 2nd und 3rd generation
Customer Requirement

Network protection and separation without separate security appliance

Protection against:

- Espionage
- Data manipulation
- Accidental access

Our Solution

CP 1543-1 with Security Integrated provides:

- Stateful Inspection Firewall
- VPN (data encryption and authentication)
- NAT/NAPT (address translation)
- HTTPs (access to Websites with encrypted transfer via SSL)
- FTPs (Secure file transfers)
- NTP secure (Secure transfer with time synchronisation and authentication)
- SNMP V3 (Tap-proof transfer of network analysis information)
Industrial Security
Security Integrated: CP 1243-1

Customer Requirement
Network protection and separation without separate security appliance

Protection against:
- Espionage
- Data manipulation
- Accidental access

Our Solution
CP 1243-1 with Security Integrated provides:
- Stateful Inspection Firewall
- VPN (data encryption and authentication)
- HTTPs (access to Websites with encrypted transfer via SSL)
- Engineering with Step 7 Professional in TIA Portal V13
Industrial Security
Security Integrated: CP 343-1 Advanced / CP 443-1 Advanced

Customer Requirement

Network protection and segmentation without separate security appliance

Protection against:
- Espionage
- Data manipulation
- Accidental access

Our Solution

CP 343-1/ CP 443-1 Advanced with Security Integrated provide:
- Stateful Inspection Firewall
- VPN (data encryption and authentication)
- NAT/NAPT (address translation)
- HTTPS (access to Websites with encrypted transfer via SSL)
- FTPs (Secure file transfers)
- NTP secure (Secure transfer with time synchronisation and authentication)
- SNMP V3 (Tap-proof transfer of network analysis information)
Industrial Security
Security Integrated: CP 1628

Customer Requirement
Protection of engineering and operator station PCs

Protection against:
- Espionage
- Data manipulation
- Accidental access

Our Solution
CP 1628 with Security Integrated provides:
- Stateful Inspection Firewall
- VPN (data encryption and authentication)
- NTP(secure) (secure transfer with time synchronisation and authentication)
- SNMP V3 (Tap-proof transfer of network analysis information)
Industrial Security

- Introduction 3
- The Siemens Solution 10
- Application Examples 49
- Benefits of Working with Siemens 70
Industrial Security
Overview: Application Examples Network Security

Adapted measures for production

Network Access Control
- Interface to IT networks: Secure architecture with DMZ (SCALANCE S623)
- Secure Remote Access via Internet
- Local network access (port security) via device and user authentication (SCALANCE S)

Redundancy
- Protection of redundant network topologies and secure redundant connection of underlying networks or rings with S627-2M

Cell Protection
- Risk mitigation through network segmentation
- Extension of the cell protection concept with Security PC- and S7-CPs (CP1628, CP343-1 Adv., CP443-1 Adv., CP1543-1)
- Use of secure communication protocols (e.g. https) prevent espionage and manipulation
Protection and segmenting through firewalls with SCALANCE S

**Task**

Parts of the system, which represent a logical unit and sometimes even come from different suppliers, should have only as many connections to one another as are absolutely necessary.

**Solution**

SCALANCE S is placed before an automation cell, thereby segmenting the network and reducing communication through firewall rules on the permitted connections.
VPN for secure remote maintenance with SCALANCE S623

Task
System access via the Internet using an encrypted VPN tunnel.

Solution
Starting point (e.g. system integrator): e.g. SSC, CP1628 or SCALANCE M as VPN client
End point (e.g. end client system): SCALANCE S623 as VPN server
- Red port: Connection to plant network
- Yellow port: Connection of modem / router
- Green port: Connection of secure cells
Secure and redundant connection of redundant rings with SCALANCE S627-2M

Task

Two rings are to be connected in a secure and redundant way.

Solution

Ring A is connected via the ports of the first media module (red ports) and ring B is connected via the ports of the second media module (green ports) with SCALANCE S627-2M. S627-2M works as router and firewall. A second redundant SCALANCE S627-2M is connected in the same way and is in a stand-by-linking. The state comparison is done via the yellow ports.

*) alternatively to MRP the ring A or ring B could be also an HRP ring
VPN for secure remote maintenance with SCALANCE M874

**Task**
Classical applications such as remote programming, parameterization and diagnosis, but also monitoring of machines and plants installed worldwide can be performed from a service center that is connected over the Internet.

**Solution**
Any IP-based devices, particularly automation devices that are downstream of the SCALANCE M874 in the local network, can be accessed. Multimedia applications like video streaming can be implemented thanks to the increased bandwidth in the uplink. The VPN functionality allows the secure transfer of data around the world.
Access control and network separation through firewalls with CP1543-1

**Task**
The communication between automation network and separated automation cell with a S7-1500 controller should be controlled and secured.

**Solution**
The CP1543-1 secures the S7-1500 controller with integrated security functions (firewall and VPN) against unauthorized access, espionage and manipulation. Via the network separation it is possible to use identical networks respectively machines with the same IP addresses.
Access control and network separation through firewalls with CP1243-1

Task
The communication between automation network and separated automation cell with a S7-1200 controller should be controlled and secured.

Solution
The CP1243-1 secures the S7-1200 Controller with integrated security functions (firewall and VPN) against unauthorized access, espionage and manipulation. Via the network separation it is possible to use identical networks respectively machines with the same IP addresses.
Protection and segmenting through firewalls with CP 343-1 Advanced or CP 443-1 Advanced

**Task**

The communication between automation network and separated automation cell with a S7-300 or S7-400 controller should be controlled and secured.

**Solution**

The CP343-1 Advanced or CP443-1 Advanced secures the S7-300 or S7-400 controller with integrated security functions (firewall and VPN) against unauthorized access, espionage and manipulation. Via network segmentation it is possible to use identical networks respectively machines with the same IP addresses.
Protection and segmenting through firewalls with CP 1628

**Task**

The communication from and to PC systems (e.g. operator stations) should be controlled and secured.

**Solution**

The CP1628 is an ethernet card for PCs and can be used to protect them with integrated security functions (firewall and VPN) against unauthorized access, espionage and manipulation.
Secure Redundancy with CP1628 and CP443-1 Advanced

**Task**

Protection for the redundant connections between a PC system and the S7-400H controllers in a high-availability plant.

**Solution**

VPN tunnels are set up between the security communications processors CP 1628 and CP 443-1 Advanced, which allow the secure transmission of the H-communication. In addition, the CP 1628 protects the PC system from unauthorized access by means of its integrated firewall.
Task

Configuration of the User Management für Security Integrated products (Firewalls) and assignment of roles and rights in TIA Portal

Solution

Step 1: Navigate to global security settings and open the User Management Folder.

Step 2: Click the flag „user“ to assign user names and passwords for the predefined system roles Administrator, Standard und Diagnosis. Optionally, additional roles can be added.

Step 3: Click the flag „roles“ to assign the engineering and device rights to the different roles via a specific list of rights.
Industrial Security
SIMATIC S7-1500 and TIA Portal: Setup of Security features including protection level

**Task**

Setup Security features including protection level for a SIMATIC S7-1500 connected to an HMI device.

**Solution**

STEP 1: Select the SIMATIC S7-1500 in the device view or network view and select the properties view of the SIMATIC S7-1500.

STEP 2: Navigate to the Display properties and set the password for the display.

STEP 3: Navigate to the Web server properties, enable the Web server and activate https. Afterwards add an user and assign access rights to the new user.

STEP 4: Navigate to the Protection properties and set the protection level.

   Note: “Complete protection” means protection level 4.

STEP 5: Enter password for the HMI communication.
### Example 1
The maintenance for an operating system on a computer important for production requires:
- Reboot after the installation of security patches.
- During this update process the production needs to be stopped.

### Solution
The time interval for maintenance can be extended by setting up whitelisting on this computer:
- Since only predefined software runs on this computer, security patches need to be installed less frequently.
- Accordingly, the production process needs to be stopped less frequently.

### Example 2
The Microsoft support for Windows XP ends 2014. For current versions of mEC controllers this means:
- mEC controllers do not support a 64 bit operating system.
- An mEC controller supporting a 64 bit operating system is excepted after 2014.

### Solution
The lifetime of an mEC controller can be extended by setting up whitelisting on such a controller:
- Since only predefined software runs on this controller it may still be used for a certain period of time even after 2014 without further security patches.
Industrial Security

- Introduction 3
- The Siemens Solution 10
- Application Examples 50
- Benefits of Working with Siemens 69
## Industrial Security

### Siemens Vertical Expertise: Automotive

### Automotive Environment

- High Grade of Automation
- Horizontal and Vertical Integration
- Different Machine Suppliers
- Real-time Communication

### Industrial Security provides

- Secured Plant Uptime
- Segmented and Monitored Communication
- Secure Remote Access
- Real-time Communication in Secure Cell Concept

### Industrial Security to keep your plant running securely
Industrial Security

Customer benefits...

- Security is at the Core of TIA
- Increased Protection
- Increased Plant Availability
- Reduced Risk
- Intellectual Property Protection
- Complete Security Life-Cycle Support
Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit [http://www.siemens.com/industrialsecurity](http://www.siemens.com/industrialsecurity).

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit [http://support.automation.siemens.com](http://support.automation.siemens.com).
**Backup: Industrial Security**
The Defense in Depth Concept in Detail

---

**Potential Attack**

---

**Plant Security**

- **Physical Security**
  - Physical access to facilities and equipment

- **Policies & procedures**
  - Security management processes
  - Operational Guidelines
  - Business Continuity Management & Disaster Recovery

---

**Network Security**

- **Security cells & DMZ**
  - Secure architecture based on network segmentation

- **Firewalls and VPN**
  - Implementation of Firewalls as the only access point to a security cell

---

**System Integrity**

- **System hardening**
  - Adapting system to be secure by default

- **User Account Management**
  - Access control based on user rights and privileges

- **Patch Management**
  - Regular implementation of patches and updates

- **Malware detection and prevention**
  - Anti Virus and Whitelisting

---

*DCS: Distributed Control System
SCADA: Supervisory Control and Data Acquisition*
What is Remote Connectivity?

- Remote Maintenance
- Remote Monitoring
  - Streaming Video
  - SCADA Systems
  - Water/Wastewater
  - Oil & Gas
Benefits

- Reduce Downtime
- Rapid response to breakdowns
- Worldwide remote maintenance
- Preventative maintenance
- Short, easy commissioning
- Minimization of travel costs
- Minimization of waiting times for on-site service engineer
- Solutions tailored to industrial automation are available

Reacting faster, reducing costs
Remote Connectivity – Then and Now

Machine X:

HMI

S7 PLC

Remote maintenance

Remote maintenance

Dial-up modems
Limited bandwidth
Limited functionality
Physical restriction

DSL, cellular, cable, dial-up
Higher bandwidth
Webservers, Email, SMS, VPN
Scalable secure connections
Remote Connectivity concepts

Point-to-Point Connection

Rendezvous Server
Networked Power Supplies

UPS1600

PSU8600
IP67 Power Supply 5A and 8A

IP67 & NEC
Class 2 Coming
Soon!
Power Supply System SITOP PSU8600

Highlights

- **Integrated Ethernet/Profinet-communication** for the optimal integration in the machine or plant automation
- **Support of energy management** by capturing energy data and on/off switching of outputs
- **Modular extension** without wiring effort for selective monitoring of the outputs and buffering of short-term power failures
- **Multiple individually configurable outputs** with high efficiency and an extremely narrow width
- **Integration in TIA portal** saves time and costs during engineering and in operation
- **Complete monitoring and diagnosis in operation** for preventive maintenance

…with SITOP PSU8600, the power supply becomes an integral part of automation solutions
PSU 8600: A True Power Supply System

Traditional Three Phase Power Supply + SITOP Electronic Diagnostic Module + SITOP Buffer Module
Overview of specifications

- **UPS modules:** 24 V DC / 10 A and 20 A
- **Energy storage:** Battery modules (lead-acid) 1.2 to 7 Ah (switchable to parallel)
- **Backup time:** e.g. 22 min at 10 A and 7 Ah
- **Signaling:** LED, signal contacts and via USB or Ethernet/PROFINET
- **Battery management:** Automatic battery detection, temperature-controlled charging, charge detection, service life and wire break
- **Temperature range:** -10 …+50 °C (battery)

Highlights/Benefits

- Bridges up to hours, depending on the power requirements
- Flexible integration in the automation via inputs and outputs, USB or Ethernet/PROFINET interface (2 ports)
- Intelligent battery management for optimal charging and continuous monitoring
- Remote monitoring with integrated web server
- Simple configuration and monitoring via SITOP UPS Manager (free PC software)
- Full integration in TIA saves time and money
PSU8600 & UPS1600 - fully integrated into the TIA Portal

Actual project for PSU8600 demo
PSU8600 & UPS1600 - fully integrated into the TIA Portal

Actual project for PSU8600 demo
PSU8600 & UPS1600 - fully integrated into the TIA Portal

This is the actual project on the demo.
PSU8600 & UPS1600 - fully integrated into the TIA Portal

This is the actual project on the demo.
Web Server for PSU8600 & UPS1600

Web server integrated in the UPS enables remote access
- Can be opened with standard Web browser
- Accessible with IP address of the UPS
- Password protected

Functions
- Display of hardware configuration data
- Display of operating data:
  - Alarm messages
  - Diagnostics data
Web Server, WinCC Faceplates & UPS Manager for UPS1600

SITOP UPS1600
- Status (normal, buffer mode)
- Input voltage
- Load current
- Achievable buffer time

SITOP UPS1100 battery module
- Battery capacity
- Charge status
- End-of-charge voltage
- Charge current
- State of health
- Battery temperature

Display of historical values

Overview of all relevant UPS data (WinCC faceplate)

Trend diagram for displaying the historical values (UPS Manager)
UPS Manager

Monitor
Pending alarms
Alarm history
Operational data
Trend chart
DC-UPS base unit
Energy storage
Online functions
Firmware update

Name
Communication with battery fault (battery index: 1)
Communication with formerly known battery is no longer possible - check communication

Time stamp
31.01.2016 00:39:11

Help

Monitor
Pending alarms
Alarm history
Operational data
Trend chart
DC-UPS base unit
Energy storage
Online functions
Firmware update

Name
Insufficient charge level
The battery charge level is too low to guarantee the configured buffer capacity

Time stamp
31.01.2016 00:40:06
UPS Manager

Monitor
- ENERGY STORAGE
  - Battery charge
    - Battery charge - 31.01.2016 00:00
    - Remaining buffer time - 31.01.2016 00:00

Monitor
- Operational data
  - DC-UPS base unit
    - Energy storage
  - Trend chart
    - DC-UPS base unit
      - Energy storage
      - online functions
      - Firmware update

Monitor
- Pending alarms
- Alarm history
- Operational data
  - DC-UPS base unit
  - Energy storage
  - Trend chart
  - DC-UPS base unit
    - Energy storage
    - online functions
    - Firmware update
UPS Manager

Hardware configuration

Base unit

Location-ID

Connection threshold 21.5 V
Buffer time 20 s

Additional buffer time after PC shutdown 10 s
Switch off time after shutdown 5 s
Enable reset after buffering

Downtime alarm 125 ms
Input voltage OK time 0.5 s

Monitor

DC-UPS base unit

Input voltage - 31.01.2016 00:00

Graph showing input voltage over time.
UPS Manager
• Intro & Portfolio Overview
**SITOP Portfolio overview**

**FUNCTIONALITY + PRICE**
- Overload characteristics
- Energy efficiency
- Switchable parallel
- Signalling contact
- Temperature Range
- Redundancy
- Durability
- Ethernet

**SITOP modular**
- PSU600
- PSU8200
- PSU400M
- PSU300M
- PSU200M
- PSU100M

**SITOP smart**
- LOGO!Power
- PSU300S
- PSU100S

**SITOP compact**
- PSU100C

**SITOP direct mount**
- PSU100D
- PSU100L

**SITOP lite**
- PSU100S

**COMPARED TO BMW**

**BMW 5 Series**
- BMW 520d: 47,700,- €
- 140 kW

**BMW 3 Series**
- BMW 320d: 37,250,- €
- 140 kW

**BMW 1 Series**
- BMW 120d: 30,100,- €
- 140 kW

**Look & Feel**
- Same power - 140 kW -
- BUT different kind of customers

**Room / Space**

**Assistance systems**

**SITOP modular**
- PSU600
- PSU8200
- PSU400M
- PSU300M
- PSU200M
- PSU100M

**SITOP smart**
- LOGO!Power
- PSU300S
- PSU100S

**SITOP compact**
- PSU100C

**SITOP direct mount**
- PSU100D
- PSU100L

**SITOP lite**
- PSU100S
# SITOP

## Portfolio overview

<table>
<thead>
<tr>
<th>Output</th>
<th>Rated voltages (V DC)</th>
<th>12</th>
<th>24</th>
<th>5</th>
<th>12</th>
<th>15</th>
<th>24</th>
<th>24</th>
<th>12</th>
<th>24</th>
<th>24</th>
<th>24</th>
<th>24</th>
<th>36</th>
<th>48</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rated currents (A)</td>
<td>2/6.5</td>
<td>0.6/1.3/2.5/4</td>
<td>3/6.3</td>
<td>1.9/4.5</td>
<td>1.9/4</td>
<td>1.3/2.5/4</td>
<td>2.5/5/10/20</td>
<td>7/14</td>
<td>2.5/5/10/20</td>
<td>5/10/20/40</td>
<td>5/10/20/40</td>
<td>13</td>
<td>10/20</td>
<td></td>
</tr>
<tr>
<td>Input</td>
<td>DC input</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3-phase</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Overload characteristics</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Energy efficiency</td>
<td>++</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>General</td>
<td>Switchable parallel</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Signaling contact &quot;Output voltage OK&quot;</td>
<td>++</td>
<td>++</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ambient temperature range</td>
<td>++</td>
<td>++</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Safety</td>
<td>Explosion protection: ATEX, IECEx, or FM</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Approved for shipbuilding: GL or ABS</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Expandable</td>
<td>- Redundancy module</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Selectivity/diagnostic module</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Buffer module</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- DC UPS</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
</tbody>
</table>
Totally Integrated Automation – Including Power Supplies!

Select device series

- Controls
  - Industrial controls
- Software
  - Software
- Communication
  - Industrial Communication
- Power supply
  - SITOP power supply
- Industrial identification systems
  - SIMATIC Ident
- Other devices
  - Other devices
Totally Integrated Automation – Including Power Supplies!

The stabilized SITOP power supplies are characterized by high quality, reliability and functionality. They provide a high level of safety in the direct voltage supply of industrial applications and building management systems.
Totally Integrated Automation – Including Power Supplies!

Power Supply library with logic similar to SITOP Selection tool
Accessories also suggested
Totally Integrated Automation – Including Power Supplies!

- Configure a complete system with Power Supplies & Accessories
- Export system to iMall with Power Supplies included
SITOP Tools

- SITOP selection tool
- SITOP interactive iPad presentation
- SITOP videos
- SITOP cross-reference tool
- Web-based training

Learn more about the unique features and the simple engineering of SITOP PSU6600 power supply system as well as DC-UPS SITOP UPS1600 in TIA Portal.
Thank you for your attention

Paul Nuss
SITOP Product Marketing Manager
RC-US PD PA CI IND
469.763.2597
5300 Triangle Parkway
Norcross, GA 30092

E-mail:
paul.nuss@siemens.com

usa.siemens.com/sitop