Security Guideline

Securing an IGSS SCADA-installation

by IGSS Development Team

Executive summary

This document provides recommendations on how to secure an IGSS SCADA installation.

The descriptions are recommendations rather than requirements and aimed for System Integrators who are setting up and configuring IGSS systems.

The recommendations should be considered to improve the general security in accordance with the end-user's organizational policies and objectives.

Introduction

This document is intended to provide recommendations on how to secure an IGSS SCADA installation.

The following sections are aimed at System Administrators who are setting up and configuring IGSS systems and are recommendations that should be considered to improve the general security.

The steps provided are recommendations rather than requirements and should be considered in accordance with the end-user's organizational policies and objectives.

Defending OT Systems

When securing OT systems it is recommended that System Administrators follow the "Purdue Enterprise Reference Architecture" as it contains important guidance on how to isolate and defend OT systems.

Purdue Enterprise Reference Architecture

The current Purdue architecture models OT and IT into six functional levels that run from Level 5 to Level 0 and span three functional zones.

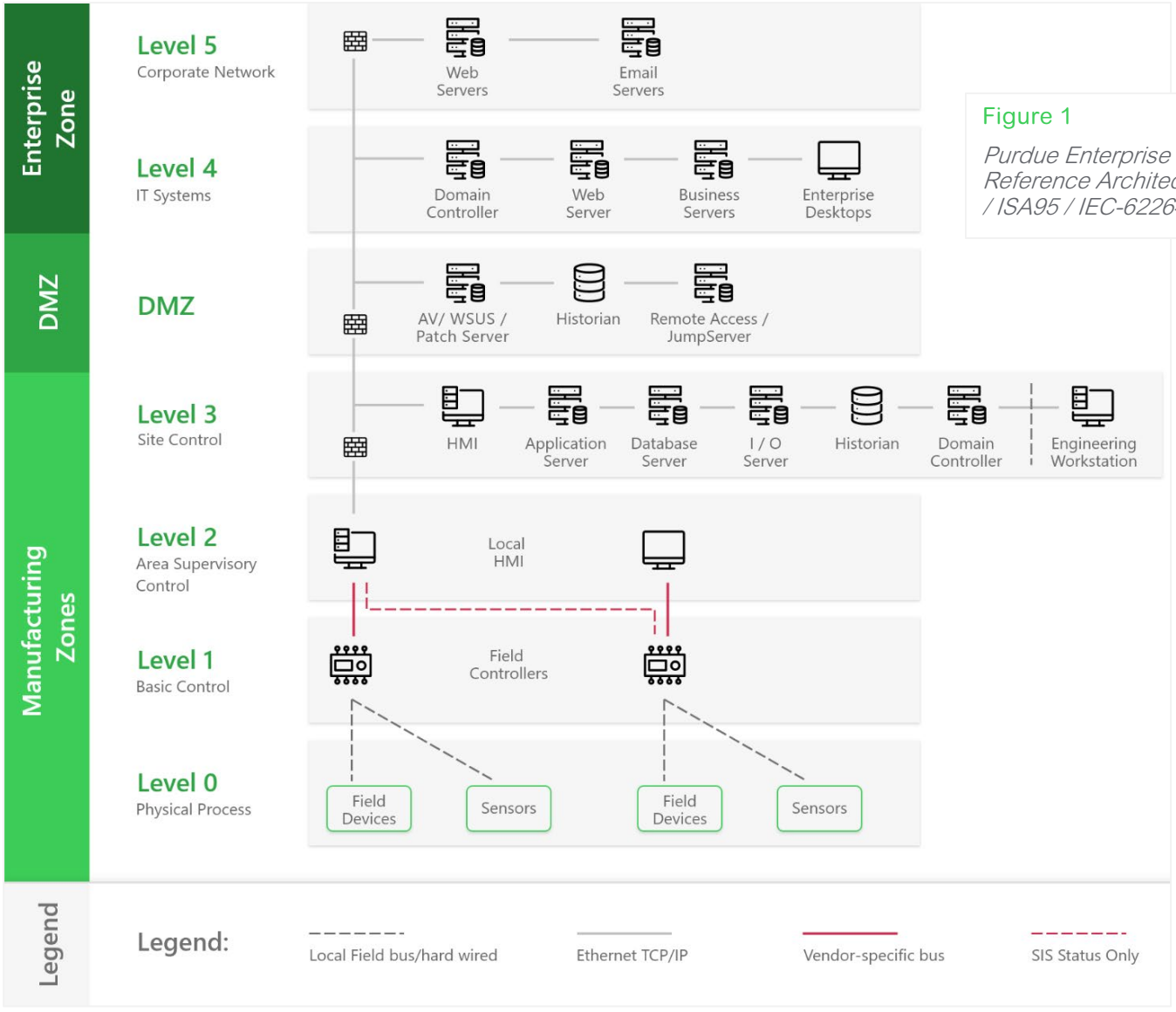

Figure 1

Purdue Enterprise Reference Architecture / ISA95 / IEC-62264

Each zone should be installed on separate networks and only connected via firewalls with whitelist configuration.

Level 5 — Corporate Network: A broader set of enterprise IT systems, including connections to the public Internet.

Level 4 — IT Systems: Business logistics systems can include database servers, application servers, and file servers.

Level 3 — Site Control: This level includes systems that support plant-wide control and monitoring functions. Level 3 systems also aggregate lower-level data that needs to be pushed up to higher-level business systems.

Level 2 — Area Supervisory Control: Control logic for analyzing and acting on Level 1 data. Systems include human-machine interface (HMI); supervisory and data acquisition (SCADA) software.

Level 1 — Basic Control: These are the control devices such as PLCs that monitor and control Level 0 equipment and safety instrumented systems.

Level 0 — Physical process: This is the physical equipment that does the work and is known as the equipment under control. This consists of valves, pumps, sensors, actuators, compressors, etc.

PLC's and Field Controllers

Many PLCs and field controllers are running protocols that do not implement any, or only sparse, security features. It is therefore very important that these devices are installed on completely separated subnets, that are only connected to the IGSS servers running the appropriate drivers.

Also consider using VLAN's to segment the sub-nets even further or use dedicated point-to-point tunneling hardware (VPN) if it is a requirement that the communication with the PLC is encrypted. Make sure that you follow the security recommendations available from the supplier of the PLCs or field devices.

For devices that are connected remotely (for example pump stations), we recommend connecting through a private MPLS cloud. Contact your telecom provider for more options on creating your own private MPLS cloud.

Many PLCs are starting to support the OPC-UA protocol and from a security point of view, this is the preferred option. Make sure that you configure the PLC with at least a transport security policy and client certificate validation. Many PLCs will support anonymous unencrypted connections out of the box – make sure this is disabled. Configure the PLCs only to allow connections from the appropriate IGSS OPC-UA driver.

Server and Client Hardware

The following are common security recommendations relating to the configuration of the BIOS for IGSS server and client machines. These recommendations are aimed at reducing the ability of unauthorized users compromising the physical systems. You should refer to the manufacturer's system manuals of each machine for detailed information about the available BIOS settings as they may vary for each machine.

To reduce the risk of unauthorized access to a server or workstation using various forms of bootable media (for example USB devices and CD/DVD's), we recommended that you change the permitted boot devices to only enable the internal local disk. We recommended that you disable one-time boot options from the startup menu. This provides an additional level of security to prevent users from bypassing any defined boot sequences within the BIOS.

Most PC systems provide an option to configure a password to restrict access to the BIOS configuration. We recommended that you define a setup password that is suitably complex, to prevent any system changes to the BIOS configuration.

Server OS Configuration

When the SCADA network is using Windows Active Directory, we recommend the use of Group Policies to apply global security settings for all server and client machines on the domain. This method provides you a much easier way to maintain the PC network and for further enhancement without having to perform the changes manually on each individual machine.

Most, but not all, of the settings applied are available via local security policy, which could also be used for standalone machines that are not part of a domain. However, Group Policy provides the most manageable deployment solution for multiple machines across a network.

There will be various requirements and considerations that need to be included when introducing or applying changes to a Workstation Group Policy. Some considerations are below.

- Restricted desktop by means of:
  - Start menu options
  - Shutdown prevention
  - Restricted task manager options
  - Registry access denial
  - File execution prevention (for example, disable Command Prompt, Explorer.exe)
- Web Browsing restrictions
  - Fixed default browser
  - Internet options
  - Security zone settings

We recommend that you consult local system administrators for the guidance needed to set this up. There are various other options common to the Server Group Policies, which will need to be considered depending on the customer requirements.

Installing IGSS on both servers and workstations require administrative privileges, but we recommend that the IGSS user accounts do not have administrative privileges as it is not required for the normal day-to-day operation of IGSS.

The user running IGSS must have write access to the IGSS configuration folder (depends on configuration) and %AppData%\Roaming\Schneider Electric\IGSS32\V<n>.0 (where <n> is the IGSS version number).

Anti-virus Software

We recommend that you install antivirus or anti malware software on IGSS servers and clients. Please note that this may affect system performance, as IGSS servers write a lot of data to the hard drives during runtime operation, which again will trigger the antivirus software (depending on the antivirus software configuration). We recommend the use of fast SSD M.2 NVMe drives on IGSS servers if you enable the antivirus scanner in the IGSS data folder.

Install Security Updates

Microsoft, Schneider Electric and other suppliers release security updates to their products on a regular basis. Make sure that you have a policy in place for installing such updates on servers, workstations, PLCs, and other equipment.

Network Security

One of the most important areas when it comes to securing an IGSS installation is securing the network. We strongly recommend that you follow the Perdue Architecture described earlier, with a clear network separation between the different zones. To allow communication between the zones, network firewalls should be applied.

Where possible, use fixed IP-addressing with private address ranges such as 10.0.0.0/8 or 172.16.0.0/12 or 192.168.0.0/16.

We recommend the use of an endpoint firewall in addition to the firewall built into Windows. The firewalls should be configured as whitelist only, according to the required services in IGSS as shown in the following table.

Component	Description	Port
IGSS Operator Connection	Basic connection between operator stations and the IGSS server. Required for all stations.	TCP:12397
IGSS Data Server	Data exchange between operator stations and the IGSS server. Required for all stations.	TCP:12401
IGSS Distributed Drivers	Connection between IGSS server and a driver running on a station (distributed driver). Only used when running distributed drivers. Enable firewall between IGSS server and the station running the distributed driver.	TCP:12396
IGSS A-B Servers	Connection to A/B switch between two IGSS servers in an A/B server configuration. Only used when A/B server has been configured. Enable firewall between the two IGSS servers.	TCP:12400
IGSS Super Alarm	External access to the IGSS alarm list from distributed alarm viewers *or* the IGSS Notifier application. Required when IGSS Notifier is used. Enable firewall between station running IGSS Notifier and the IGSS server.	TCP:12399
IGSS Software Update	Used when downloading software updates from the IGSS update server to IGSS. Updates are downloaded from Dropbox to the IGSS station. Port should be opened during update operation only.	HTTPS:443
IGSS Update to Operator	Used when pushing software updates from an IGSS station to the other stations. Last two digits of the port number is the IGSS version number, so for IGSS version 17 the port will be 12417. Enable firewall between the source station and IGSS stations only.	TCP:12416
IGSS ODBC Server	Creates a database interface to the IGSS configuration. Can be used for everything from changing object configuration to querying live object values. Enable firewall on private network only and only to specific stations that do require ODBC access.	TCP:20202
IGSS Mobile Server	Used when giving users of the IGSS Mobile App access to the site. Firewall must support DNS and enable access to igssmobile.servicebus.windows.net and igsspush.servicebus.windows.net Use of fixed IP address whitelisting is not feasible, as the IP addresses of Azure services tend to change frequently. Enable firewall between the IGSS server running the IGSS mobile server and the 2 DNS mentioned above only.	TCP:9350 to 9354 HTTPS:443

IGSS OPC-UA Server	OPC-UA interface to live and historical object values in IGSS. For external access always configure enhanced security with client- and server certificate validation. Enable between the station running the IGSS OPC-UA server and OPC-UA client PCs only.	TCP:12403 HTTP:12402
IGSS MQTT Gateway	Used to exchange values of IGSS objects with a MQTT broker. Always configure to use encrypted communication via TLS with client- and server certificate validation.	TCP: 1883 TCP: 8883 (TLS)

Apart from this list, you will also need to open the ports required by the various PLC communication drivers that have been installed in IGSS. Consult the PLC documentation to find out exactly which ports to enable.

The IGSS server can be configured only to accept an operator station connection from a specific IP-address (introduced in IGSS version 15). It is recommended that you enable this option in IGSS System Configuration.

Audit Trail

IGSS provides an option to log all user activity to an audit trail located on an SQL server. We recommend that you enable this option and monitor any unusual activity such as failed logins and changes to the user account system on a regular basis.

External Interfaces

Although the Purdue model recommends that the OT network is kept completely isolated, this is not always possible as external access to SCADA data is sometimes required. Precautions should be made to maximize the security around such external interfaces.

IGSS ODBC Server

The IGSS ODBC Server exposes a database interface to the IGSS configuration that can be used to perform both configuration and runtime operations on the site.

Please note that ODBC is not encrypted and does not have any authorization model, so the IGSS ODBC Server should NEVER be made accessible on an open network. Even on a private network, we recommend that you only give specific applications on specific stations access in the firewall configuration.

IGSS Mobile Server

The IGSS mobile server is used in conjunction with the IGSS Mobile App. The IGSS mobile server creates a connection to a Microsoft Azure service bus where the IGSS Mobile App connects via the Internet and gives the user of the app access to the site. All communication between the IGSS Mobile App and the site is based on HTTPS and is thus encrypted.
Although the communication is encrypted, the IGSS mobile server creates an endpoint that is accessible providing you have

a) the mobile access key for the site and
b) matching username/password for an IGSS user with mobile access enabled.

We recommend that you keep the mobile access key secret and only enable mobile access for selected users. Users with mobile access should use a strong password that is changed on a regular basis.

IGSS OPC-UA Server

The IGSS OPC-UA server gives access to live and historical object values using the OPC-UA protocol. Please note that the default configuration of the IGSS OPC-UA server includes an anonymous unencrypted access point which should not be used on an open network. We recommend that you only use endpoints with encryption and client/server certificates. Please contact IGSS Support for instructions on how to configure this.

IGSS MQTT Gateway

The IGSS MQTT Gateway is used to exchange IGSS object values via a MQTT broker. We recommend that you always configure the IGSS MQTT Gateway to use secure connections on TLS 1.2 with client- and server certificate validation. Please contact IGSS Support for instructions on how to configure this.

Contact us

For feedback and comments about the content of this white paper:

IGSS Technical Support
DK-IGSS-support@se.com