GE
Grid Solutions

DS Agile Cyber Security

Defense In-depth Applied to Substation Automation

To mitigate the impact of deliberate or inadvertent cyber security events, utilities need to deploy an in-depth, multi-layer defensive strategy. GE's DS Agile digital substation control system provides this cyber security, working as an integrated component of a utility's IT system and infrastructure.

In line with the latest in industry cyber security standards such as NERC, IEC and IEEE, the DS Agile system employs the same type of multi-layer strategy to mitigate risks or unplanned downtime associted with a cyber attacks.

DS Agile Perimeter to be Protected

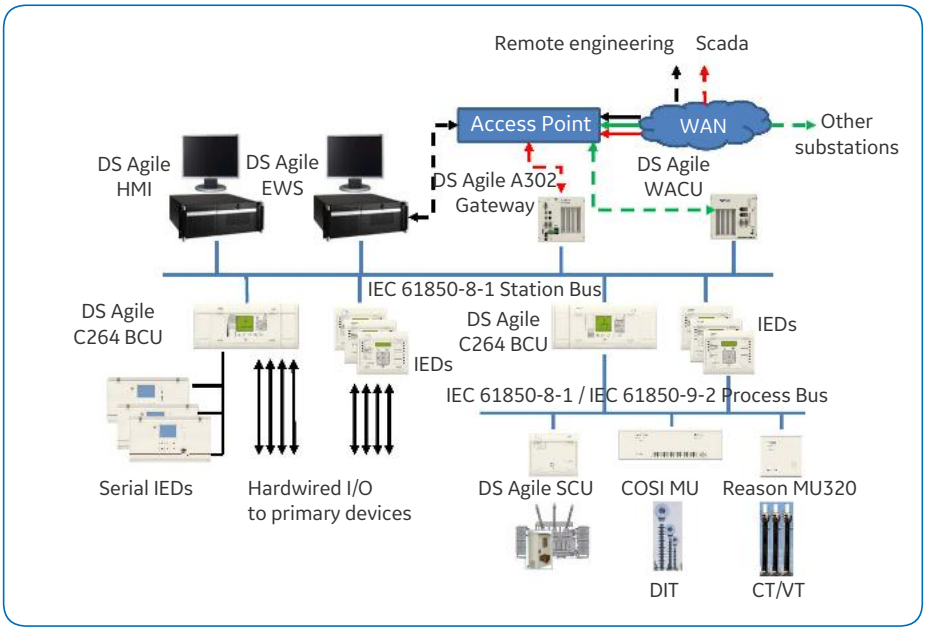


Figure 1: DS Agile Digital Control System Architecture Example

The NERC defines the Electronic Security Perimeter (ESP) as “the logical border surrounding a network to which critical cyber assets are connected and for which access is controlled”. In DS Agile, the ESP is the DCS LAN, the network to protect.

Multiple Layers of Security

- Network segregation
- Host hardening
- Malware prevention
- Authentication, RBAC
- Security event logging
- Software integrity

System Level Security

- Firewalls
- Switches
- VPN
- VLAN
- IEC 61850-8-1 station bus
- IEC 61850-8-1 / IEC 61850-9-2LE Process Bus

Component Level Security

- Operator and engineering workstations
- Bay controllers BCU, IEDs
- Gateways and wide area control units
- Switchgear controllers and merging units

Imagination at work

DS Agile Cyber Security Strategy

The different technical countermeasures used to ensure cyber threat detection, prevention and protection in DS Agile are highlighted hereafter. On top of these different security layers, operational and emergency procedures combined with user training are also needed to achieve proper security implementation.

DS Agile Network Protection

Access Point to DS Agile

To optimize DS Agile LAN protection against external threats, the DS Agile architecture must limit the number of its access points (one if possible). The access point is generally a router combining VPN, firewall and authentication proxy functions.

Virtual Private Network

Communication between the substation and other remote systems (remote centers or other substations) are tunnelled in a virtual private network (VPN) - a secure encrypted point-to-point communication channel.

LAN Firewall and IDPS

Global protection of the ESP is ensured by a firewall to control communications to-or-from the substation. The firewall denies all communications by default, and is configured to allow only specific protocols communication between specific devices and zones, the latter being:

- Public zone: anything outside the ESP.
- Private zone: the substation LAN. There is no direct communication between the public and private zones.
- DMZ: where all outside traffic is redirected by default.

The firewall acts also as an authentication proxy to the ESP by requiring user authentication before allowing traffic to go through. Logins are recorded and audited.

The IDPS (Intrusion Detection and Prevention System) is configured to detect, report or block malicious traffic. Threat detection relies on rules and a signature database allowing an authorised operator or group of operators to react efficiently upon threat detection by using a panel of predefined actions.

Jump Box

Remote maintenance is done by connecting to a “jump box” (a standard Windows-based PC with Ethernet access) in the DMZ zone, and from there accessing a restricted list of devices and applications on the private zone. This allows controlling the traffic to the substation IEDs.

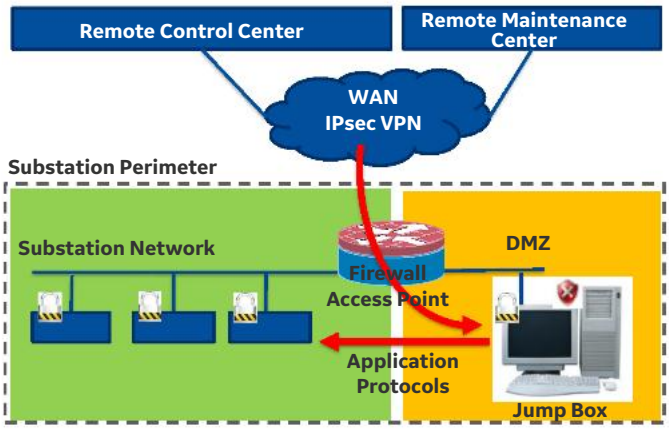


Figure 2: Router/firewall securing communication with remote centers and bringing single mandatory path to DCS LAN

Switches

Switches are configured to reduce threat impact on the network by organizing the LAN traffic (broadcast storm limitation, QoS to prioritize IEC-61850 traffic, VLANs to segregate traffic, MAC address filtering, etc.).

Host Security

System Hardening

Hardening aims at improving security by reducing the number of possibilities a threat has to disrupt or take control of the operating system on which DS Agile software is installed.

DS Agile provides the hardening scripts which vary according to the computer type.

- Where possible, USB ports are disabled in the BIOS or from Windows. Some PCs may require the USB port be enabled for keyboard and mouse.
- Unnecessary user accounts (including “guest” and “administrator”) and daemons/services are disabled.
- A vast number of registry keys are setup to increase security and the audit and password policies are set.
- There are no backdoors or hardcoded user accounts.
- A user session is automatically terminated after a configurable time out.

Host Firewall

As a complement to the LAN firewall, software firewalls on Windows PC are configured to allow only the required communication flows between authorized PCs.

OS Upgrade

The Windows PC in DS Agile are updated to the latest patch set provided by OS vendors before FAT.

Software Integrity

All GE software is free of malware and digitally signed to guarantee authenticity and integrity at installation time.

Malware Prevention

DS Agile uses two techniques in each of its Windows PC to improve malware prevention: anti-virus and whitelisting. There is no known anti-virus software for protection relays at the time of writing.

- Application Control (Whitelist)

  Application whitelist is the preferred malware prevention approach. Contrary to anti-viruses that work with a "allow by default" policy, whitelisting software have a "deny by default" policy. Only software that is present in the white list is allowed to be executed.

  This approach is particularly adapted to the substation automation system where the system being stable, the whitelist seldom changes. The result is that malware, which are processes, cannot execute on the protected system. All Windows PC in the DS Agile system come with whitelisting software installed and configured. Following whitelist activation, only software digitally signed by GE can be installed or updated on the PC. This guarantees the binary file integrity and authenticity on the PC.

- Anti-virus

  In addition to the software whitelist, an anti-virus can be installed on Windows PCs. The malware signature database update is pulled by each end point from a single location or pushed by a central management server in the substation. To limit the effect of false positives (legitimate software could be suddenly quarantined after a signature database update), DS Agile software directories can be excluded from the scan.

  In order to limit CPU and memory consumption, GE recommendations are:

  - For "non-real-time" PC (such as EWS): anti-viruses to be configured for real-time monitoring.
  - For "real-time" PC (such as HMI, GTW and WACU), the anti-virus to be configured only for on-demand scans with malware prevention completed by whitelisting software.

- Host Intrusion Prevention System (IPS)

  The host IPS consists in the combination of host-based firewall and whitelist software.

Application Security

Authentication

All users are required to authenticate to interact with any IED. Users have individual accounts and passwords (no shared accounts).

It is possible to enable a password policy to configure the minimum password length and character content which provides the complexity looked for. All passwords are securely stored using a one way secure hash algorithm with a unique salt.

Authorization

DS Agile implements Role Based Access Control (RBAC) to tightly manage the authorized users. Each user account is assigned one or more roles and associated non-overlapping rights.

The main roles are:

- Observer
- System Engineer
- System Administrator
- Security Administrator

Security Event Logging (Non-repudiation)

All basic security events are logged on each device:

- Successful and failed login attempts
- User management actions including password changes and role assignment
- Configuration database changes

The log includes the user name, originating IP, timestamp and action description. No sensitive information (such as passwords) is logged.

In addition to these roles, it is possible to configure additional custom roles for the operator interface in order to meet the "least privilege" concept.

Remote Access

Authentication can be required to access the substation LAN remotely by configuring the firewall as a proxy authentication, as mentioned into previous LAN Firewall section.

Threat Monitoring and Patches

As a service contract, GE can propose to monitor the threat landscape and inform its customers of new vulnerabilities discovered in third party software included in the DS Agile solution. In addition, GE can test and recommend or discourage the application of a software update published to fix such vulnerability.

The following software can be monitored:

- Microsoft Windows Seven operating system
- VxWorks operating system
- McAfee Viruscan
- McAfee Embedded Control

Patch deployment depends on the customer's infrastructure and can be done manually on site, manually remotely or automatically through a deployment server.

Network and System Security Guide

DS Agile is delivered with its Network and System Security Guide which documents all system's cyber security related information:

- Installation sequential steps, including hardening, application control, default password changes
- List of protocols and ports that are used in the installed system
- Deviations from the standard installation (to accommodate customer specific requests)
- Good practices for a secure system

This guide allows the engineering teams to properly configure the cyber security of the system and is a baseline for future audit.

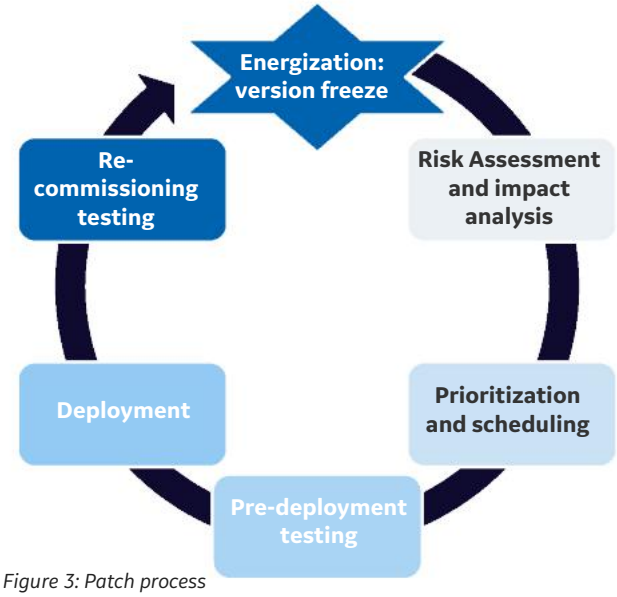
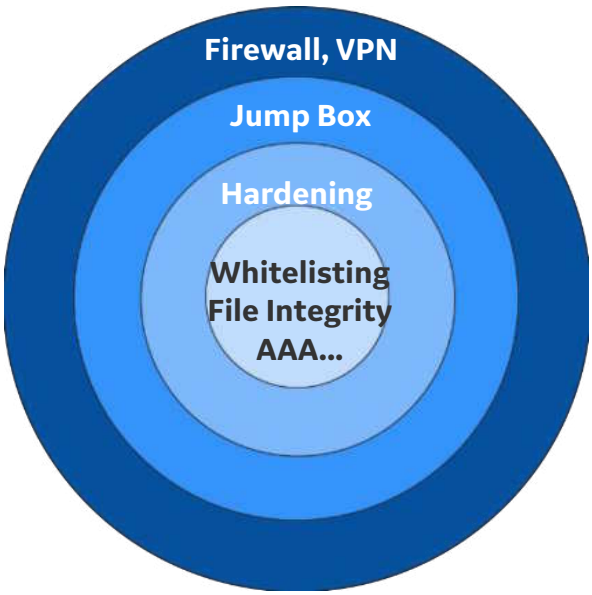


Figure 3: Patch process

Conclusion

GE has strongly reinforced the substation cyber security by implementing in DS Agile this differentiated defence in-depth strategy with emphasis on prevention and detection at each level in DS Agile architecture.



For more information please contact
GE Power
Grid Solutions

Worldwide Contact Center

Web: www.GEGridSolutions.com/contact
Phone: +44 (0) 1785 250 070

Imagination at work

GEGridSolutions.com