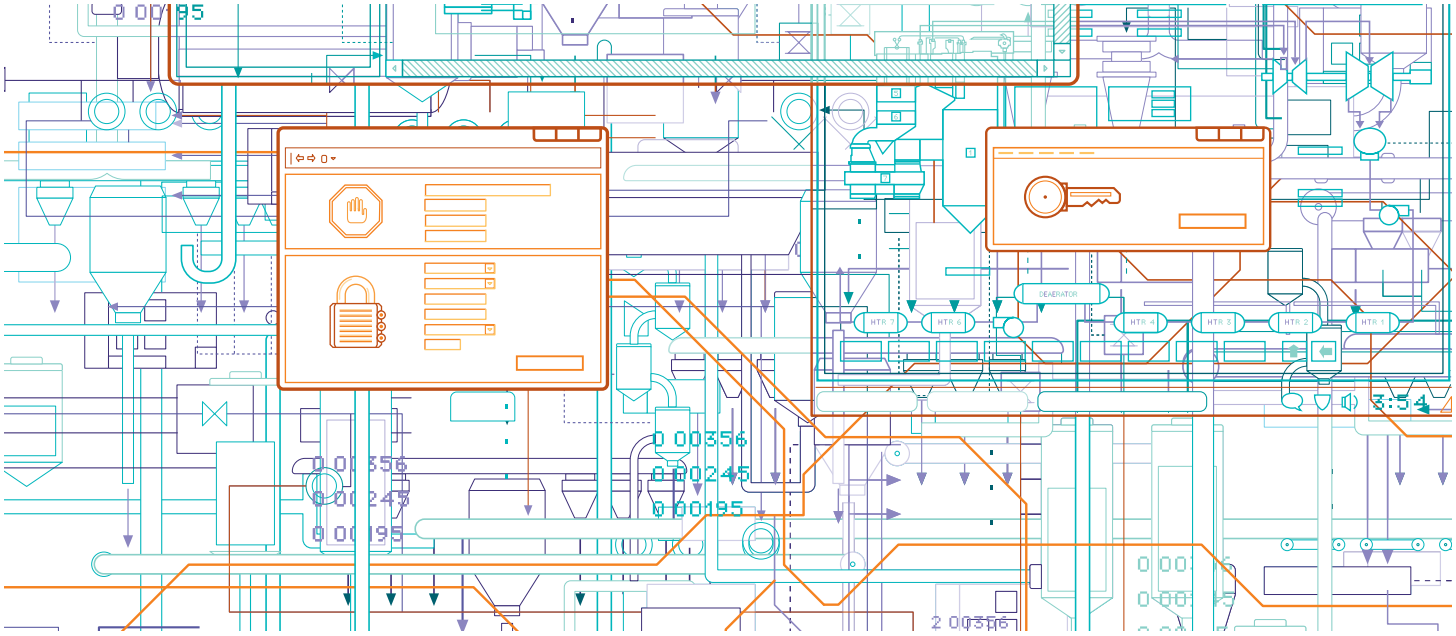
Power Generation

Security Workplace: MAINTAIN
Reliability – Security – Compliance



The reliable operation of your ABB Distributed Control System (DCS) depends on your abiliity to MAINTAIN the ABB recommended security baseline for the networking and computing platforms that comprise the system. Un-patched servers and clients with outdated A/V are very soft targets, easily compromised by a virus or malware which can adversely affect the reliable operation of the DCS.

To achieve and maintain the OEM recommended security baseline, ABB delivers the **Security Workplace MAINTAIN** solution. These applications and services have been validated for your ABB DCS, providing the automation required to reduce human error and time required to implement these security best practices.

Security Workplace MAINTAIN includes:

- System and Network Hardening
- Security Patch Delivery Disk
- Centralized Microsoft Patch Management
- Centralized Anti-Virus Management
- Automated Back-up and Recovery

System and Network Hardening

Server and Workstation hardening is the process of securing a system by reducing its surface of vulnerability. A system has a larger vulnerability surface the more functions it fulfills. To reduce vulnerability ABB limits the amount of functions and communications as much as practical for the control system to operate as intended. ABB applies basic server and workstation hardening profiles based on the operating system, DCS system, and third party software of the machines. ABB's standard server and workstation hardening elements include:

- Validate Microsoft operating system is at current approved patch level and McAfee DAT are current
- Configure the local security policies to audit Windows Security Incidents and Events
- Disable unnecessary Operating System services
- Configure Windows Firewall to block unnecessary. TCP/UDP ports.
  - Rules for ABB Inc. DCS software
  - Rules for approved 3rd party software
  - Customer must provide rules for any non-standard software requested
- Define Local Security or Group Policies
  - Implement Operator protected login profile as applicable
  - Account Policies/Password Policy
  - Enable and define audit policy
  - Disable and/or rename local machine accounts
  - Deny all removable media storage classes to non-admin

Security Patch Delivery Disk

ABB's worldwide testing facilities download, install and qualify Microsoft patches every month. Once the new patches have been qualified they are published in validation documents available to ServiceGrid members with access to SolutionsBank. Once the validation documents are published, a DVD is created that includes all the patches sorted by each product and platform required for that month. This disk can be imported into the ABB Security Workplace Patch Management Utility (PMU) which will centrally manage and distribute patches to ABB machines.

Centralized Microsoft Patching Management

The deployment of tested, validated Microsoft patches for your ABB DCS is greatly simplified using the PMU:

- The time required to manually deploy Microsoft patches to your systems is reduced by up to 75%
- The PMU works directly with the ServiceGrid Cyber Patch Delivery DVD to allow an air-gap functionality within the DCS network (no Internet connection required)

The PMU software is installed on a designated server within the DCS that has connectivity to all the endpoints desired to be patched. The PMU scans DCS nodes and reports on a machine basis an inventory of patches to be installed or removed. Once the scan is complete, the PMU creates an installation package for approved patches for each node The operator is able to drill down on the GUI for specific patch and knowledge bank information. The installation package is then pushed to the endpoint and an automated install can be initiated remotely or at each workstation to allow supervision.

Centralized Anti-Virus Management

The ABB Centralized Anti-Virus Deployment Utility greatly simplifies the deployment of validated McAfee A/V signatures for your ABB DCS. Based on McAfee ePolicy Orchestrator (ePO), the utility works directly with the ServiceGrid Cyber Patch Delivery DVD to scan nodes, report on definition status and push approved DAT files. MAINTAIN provides enhanced end point protection for your ABB DCS, which includes:

- Configurable On-Access System and Device Scans
- Central management via ePolicy Orchestrator (ePO)
- End point protection with VirusScan Enterprise + AntiSpyware Enterprise

Automated Back-up and Recovery

ABB provides an Automated Backup and Recovery solution that is validated and tested to maximize DCS and plant availability. The backup software is configured to capture full disk images and critical files to cover the full range of restoration requirements such as restoring an entire server or a simple restoration of a deleted file such as a graphic.

The backup process is designed around network bandwidth and device processing constraints to insure availability and reliability are not affected.

The default backup plan for each machine is as follows:
- Full backups once a month
- Differential backups once a week
- Incremental backups every day
- Images will be retained for 90 days

Additionally, ABB configures a quarterly plan for Server machines in which a full backup is taken and then converted to a Virtual Machine. This virtual machine can be loaded on VMware Workstation and tested for functionality.

Contact us

ABB Inc.
Power Generation
Wickliffe, Ohio, USA
Phone +1 440 585 3087
E-Mail: pspmarketing@us.abb.com

www.abb.com/powergeneration

3VAC000087 Power Generation 1214