Depending on your needs, ABB Ability™ System Hardening includes various services:
- System Hardening
- Secure Datatransfer
- Network Security
- OPC Secure Gateway
- Awareness Training

The following protective measures make it difficult to access your system without authorization. Technical solutions as well as awareness measures are offered for your employees.

**System Hardening**
System Hardening is a basic measure for meeting fundamental security standards. It includes:
- Locking unused ports
- Removing or deactivating unnecessary software and services
- User/password management
- Testing and adjustment of group policies

**Secure Datatransfer**
Data can only be exchanged with the automation system via the plant security server. All USB ports and external drives of the control system are locked. The data are checked and prepared for transfer at the plant security server. This quarantine computer function also increases data security during remote sessions and remote maintenance accesses. User-friendly access to these data is still ensured from every computer, despite the high security measures.
Network Security
Protect the data traffic in your system. As a central component of the control system, the network should provide basic functions to protect the system from unauthorized external access. ABB provides custom solutions that match the state of technology in cyber security.

Protection of gateways is a decisive factor in establishing an effective defense against attacks via the Internet or Intranet. All external interfaces with the automation system are identified, inspected for security, and verified to ensure they are necessary. Data traffic can be regulated and monitored through data flow control, e.g. using a firewall, to the extent that is operationally necessary.

Standardized network structure to improve security. The automation system network should consist of several network segments, for instance, operating and process station levels with different individual protection needs. Networks are effectively separated by establishing a demilitarized zone (DMZ).

Basic measures in the network area:
- Network segmentation through VLANs:
- Extended network segmentation using firewalls
- Implementation of a demilitarized zone (DMZ)
- Compliance with the ABB password guidelines for network devices
- Limitation of access
- Shutting down unused network ports
- Improvements in physical security
- Securing switch configurations
Secure OPC Gateway
Secure OPC Server/client communication. IT networks are subdivided according to security levels, to protect highly sensitive or critical data against unauthorized access. The interfaces and clear separation of such security levels need special attention, because these points can present opportunities for access to intruders.

In classic OPC DA/AE communication, segmentation via firewalls, and therefore, separation into security levels, is very difficult. A Secure OPC Gateway eliminates these historical deficiencies. Communication between different security levels takes place in a controlled way, and obtaining access from a lower security level to a higher one is made significantly more difficult.

Optimize your processes with modern manufacturing execution systems (MES) and carry out controlled transportation of this information from the control system to the MES network.

Awareness Training
Raising awareness among all the employees working within a facility is an easy and very effective way of highlighting the most dangerous weaknesses, threats and hazards. A general understanding of the field of cyber security helps prevent attacks.

Cyber Security Awareness Training is intended for operators, maintenance staff, technical and facility managers. In order to meet the different needs of these groups, the one-day training can be divided into two training units, according to the target group. The ABB University offers awareness training at D467 and on-site.