Version 1.0 - Published 19.01.2017

Guideline for the ABB Cyber Security Requirements for Suppliers

Disclaimer

The purpose of this guideline is to help ABB suppliers to understand the "ABB Cyber Security Requirements for Suppliers", which are available under www.abb.com/supplying/cybersecurity.

This guideline contains information and clarifications for each of the listed requirements. Unless specified otherwise, the listed practices, guidelines, and standards are not meant to be exhaustive nor mandatory for the compliance with the "ABB Cyber Security Requirements for Suppliers", but are examples of practices, guidelines, and standards that may be applied.

The information, suggestions, and recommendations in this guideline are provided as is without any representation or warranty of any kind, including but not limited to accuracy or completeness of its content, either express or implied including but not limited to implied warranties for merchantability, fitness for a particular purpose or non-infringement.

In addition, this guideline does not attempt to provide legal advice or any kind of consulting or advisory services. It is up to the supplier to assess the impact and requirements of any applicable legislation or regulation on its business and the use of its products.

This guideline may be modified or amended at any time with our without notice. To get the latest version of this guideline, visit: www.abb.com/supplying/cybersecurity.

Introduction

The security of our products, systems, and services, as well as our customer’s and ABB’s data is of great importance to ABB.

Our suppliers play a crucial role in ABB‘s cyber security program and therefore, our suppliers are requested to support and complement ABB’s efforts to cyber security. More specifically, we demand our suppliers to comply with the “ABB Cyber Security Requirements for Suppliers” available under www.abb.com/supplying/cybersecurity.

The “ABB Cyber Security Requirements for Suppliers” are a set of minimum cyber security requirements that constitute the minimum baseline of cyber security measures that ABB expects its suppliers to comply with.

This guideline contains information and clarifications for each of the requirements listed in the “ABB Cyber Security Requirements for Suppliers”.

Applicability of the “ABB Cyber Security Requirements for Suppliers”

The requirements and clauses stated in the “ABB Cyber Security Requirements for Suppliers” shall be fulfilled for any software-related product that is supplied to ABB.

A supplied product is a product that is supplied to an ABB entity from a non-ABB party, i.e., an entity outside the ABB group. Here, *product* is used as a blanket term to describe a product, good, component, or system and includes software.

A software-related product is defined as a product that:

1. uses any type of software,
2. is partly based on any type of software, or
3. is in itself a type of software.

Here, *software* shall be considered in its broadest sense and includes for instance firmware, drivers, applications, etc.

Without limiting the generality of the foregoing, examples of such software-related products are:

- Supplied products that are integrated or embedded into ABB products and systems, such as software libraries, communication stacks, middleware, software interfaces, frameworks, user interfaces, and firmware, as well as embedded systems such as input/output modules and boards.
- Supplied products that are developed, manufactured, and assembled by the ABB supplier on which ABB products and systems (e.g., automation systems and service infrastructures) rely or are based, such as operating systems, IT and network components (e.g., application software, user interfaces, databases, historians, routers, and switches), as well as industrial control systems (e.g., controllers, sensors, actuators, and supervisory systems).

Requirement 1: Secure development lifecycle

Requirement

The supplier shall establish, document, and implement initiatives in line with commonly accepted industry standards and practices to build security into the software development process. Such initiatives shall build security within all phases of the development lifecycle, e.g., training, requirement, design, implementation, verification, release, and response.

Clarification on the requirement

The supplier is required to embed security throughout its software development lifecycle and to cover all the development phases. Specifically, solid security requirements as well as secure design and implementation best practices shall be considered. In addition, it is necessary to be able to properly react to, and deal with, found vulnerabilities (no software can be 100% bug or vulnerability free). Furthermore, members of software development teams and in general any individual that is directly involved in the development of software shall be adequately trained (with respect to his/her role) in security matters.

Requirement 2: Security quality

Requirement

The supplier shall proactively take measures to improve the security quality of the product. These measures shall follow commonly accepted industry standards and practices and shall include, where technically feasible:

- Robustness testing, including fuzzing and flooding.
- Vulnerability scanning for known vulnerabilities and exploits.
- Security testing, including static code analysis or binary code analysis.

Clarification on the requirement

The supplier is required to take measures to improve the security quality of its product. That is, to perform security verification activities such as security review, analysis, and testing.

Several activities with different scope, targets, approaches, techniques, and results can be performed; in order to guarantee a minimum, but fundamental, level of security verification, the supplier is required where technically feasible to perform at least:

- Robustness testing: fuzzing and flooding
- Vulnerability scanning
- Security testing: either static code analysis or binary code analysis

Requirement 3: Backdoor accounts and hardcoded credentials

Requirement

The product shall not have any accounts, passwords, or private/secret keys that cannot be changed, disabled, or removed by the authorized end user of the product.

The product shall not have any accounts (individual, shared, debug, etc.) that are not documented (this does not imply that the associated access credentials have to be disclosed).

Clarification on the requirement

The supplier is required to avoid hardcoded passwords and cryptographic keys, as well as to enable the possibility to change any password or key in its product.

The supplier is not required to avoid default passwords as long as they can be changed and their presence, together with the recommendation to change them, is properly communicated (e.g., in the product documentation).

Similarly, the supplier is required to document all accounts in its product and to provide the possibility to change, disable, or remove any of such accounts.

For accounts that are used by the supplier (e.g., for maintenance or support purposes), i.e., for which the supplier is the "authorized end user", access credentials do not necessarily have to be disclosed by the supplier. Similarly, the possibility to change those access credentials shall still exist, but not necessary made available to anyone else but the supplier. However, the presence of such accounts has to be clearly documented and the product must provide the capability to disable or remove such accounts.

Requirement 4: Cryptographic tools and security functionalities

Requirement

Any cryptographic tool and security functionality implemented or used in the product shall follow commonly accepted security industry recommendations and guidelines (e.g., as recommended by NIST or defined in international standards). This includes, for example:

- Cryptographic algorithms to hash, encrypt, or sign data for storage or transmission.
- Protocols and procedures to support cryptographic algorithms (e.g., to exchange certificates, to establish keys, or to generate random numbers).
- Functionality to authenticate end users or for access control.

Any cryptographic tool or security functionality implemented or used in the product that does not follow commonly accepted security industry recommendations and guidelines shall be documented and communicated to ABB. Such documentation shall include, at least, its origin (e.g., proprietary tool), its reference documentation (e.g., academic publication), its functionality (e.g., encryption), its main security-related features, characteristics, and parameters (e.g., used ECC curve), as well as in which context or part of the product it is used (e.g., user authentication).

Clarification on the requirement

The supplier is required to rely on commonly accepted security industry recommendations and guidelines when using, implementing, or updating any cryptographic tool and security functionality in its product.

In certain specific cases, purposely-designed, customized, non-recommended, or non-standard cryptographic tools and security functionalities may be necessary, or even not possible to avoid or replace. In such cases, the supplier is required to document and communicate to ABB such cryptographic tools and security functionalities. In order for ABB to be able to assess the potential resulting risk, the supplier is required to provide ABB with information regarding the origin, functionality, use, and security-related features, characteristics, and parameters of such cryptographic tools and security functionalities.

Requirement 5: Protection from malware propagation

Requirement

The supplier shall proactively take measures to prevent malware from being propagated. These measures shall follow commonly accepted industry standards and practices and shall include successfully scanning software deliverables (including their storage media, e.g., CDs, hard disks, or flash cards) with different suitable and up-to-date antivirus solutions before delivery.

Clarification on the requirement

The successfully scanning of any software deliverable – including its delivery storage (e.g., CDs, hard disks, or flash cards) – with different, suitable, and up-to-date antivirus solutions before delivery is considered as a fundamental and minimal first-line-of-defense activity that the supplier is specifically required to perform.

Not all antivirus solutions detect all types of malware. Therefore, using more than one solution increases the detection probability. Although not specified, using three different, suitable, and up-to-date antivirus solutions is considered an acceptable compromise between security and complexity.

In addition, different and complementary initiatives and activities, including security policy, security awareness, vulnerability mitigation, threat mitigation, and defensive architectures, should be followed.

Requirement 6: Handling of digital certificates

Requirement

If digital certificates are used in the development of the product (e.g., to sign code or as a root to derive product-specific certificates), they shall be protected and handled according to commonly accepted industry standards and practices.

Clarification on the requirement

The supplier is required to protect digital certificates that are used in the development of its product. Measures to protect digital certificates shall cover how to generate, store, access, and use private keys, as well as how to issue certificates. Such measures shall address both technological and process related aspects.

Requirement 7: Product documentation

Requirement

The documentation provided with the product shall include:

- All user and system accounts in the product with a recommendation to change at least the access credentials.
- Description of all ports, services, and software needed to support any functionality in the product, as well as how these ports, services, and software can be configured and, when applicable, how these can be disabled, blocked, or uninstalled.
- Information on proper configuration and usage of cyber security related functionalities in the product.
- Specific instructions on how to configure the security controls provided by the product (e.g., RBAC, security logging, or secure communication), as well as security controls provided in addition to the product (e.g., antivirus, whitelisting, or security monitoring).
- A recommendation for at least one malware prevention solution to be used during the operation of the product, if such a solution exists. The recommendation shall include the specific version of the malware prevention solution, as well as a description of the performed testing and validation by the supplier.

Clarification on the requirement

In order for end users to minimize cyber security risks, it is necessary that they are able to properly deploy, configure, and harden any product. It is imperative to provide end users with the necessary information to enable them to do this efficiently and effectively.

The product users shall be aware of any account in the product (no secret accounts are allowed as defined in requirement 3). Also, hardcoded credentials such as hardcoded passwords are not permitted (as defined in requirement 3). The presence of default, non-hardcoded credentials (i.e., that can be changed), together with the recommendation to change them, has to be properly communicated to the users.

Hardening means reducing the attack surface, i.e., to remove/disable any inessential point from where an attacker could get into a system and could get data out of a system. Such points are usually ports, services, and software.
To allow users to harden the product accordingly to their needs (e.g., with respect to the actual used product functionalities), it is necessary to provide description of such points and on how to disable, block, or uninstall them (where applicable). In addition, information on ports, services, and software can be used by the users to correctly configure their systems around the product (e.g., firewall settings).

To fully benefit from the cyber security functionalities in the product, users have to know how to properly configure and use them. In addition, to effectively leverage the security controls provided by the product, as well as any provided additional security control such as antivirus or security monitoring solutions, users have to know how to properly deploy them.

The supplier is required to complement the product documentation with the listed items.

Requirement 8: Vulnerability handling

Requirement

The supplier shall establish, document, and implement a process to react to vulnerabilities and security issues associated with the product. The process shall follow commonly accepted industry standards and practices and shall include procedures and interfaces to:

1. Enable ABB to submit vulnerability reports.
   - The supplier shall provide ABB with all necessary information on how ABB can report found vulnerabilities.
2. Acknowledge the receipt of a vulnerability report submitted by ABB within 2 business days or such shorter term as reasonably requested by ABB from the report submission.
3. For vulnerabilities where ABB is the original finder, submit information to ABB on the result of the vulnerability verification within 7 business days or such shorter term as reasonably requested by ABB from the acknowledgment of a vulnerability submission by ABB.
   - The supplier shall provide information on the vulnerability validity and severity, the list of potentially affected products and their versions, as available at that time, and whenever possible information on how to verify the existence of the vulnerability in its products.
   - The supplier shall also provide an estimate regarding the timeframe for the remediation release, as well as possible workarounds while the remediation solution is defined and implemented.
4. Share vulnerability remediation and advisory reports.
   - The supplier shall provide ABB with information on how vulnerability remediation and advisory reports related to any submitted vulnerability by ABB or any other entity are shared with ABB.
   - The advisory report shall include the description of the vulnerability, information about the remediation and workarounds, the list of affected systems and products, the vulnerability impact (threats, exploits, and severity rating), and related references (e.g., to related vulnerabilities).
   - If the product is included in the build or installation package of any ABB product (e.g., such as libraries or an embedded OS), the supplier shall have a means to release the vulnerability remediation and the advisory report to ABB prior to public disclosure.

In addition, the supplier shall take all actions as reasonably requested by ABB in case of a vulnerability or other security issue associated with the product.

Clarification on the requirement

The supplier is required to implement a process to react to vulnerabilities and security issues associated with its product and found after product release. Within that process, the supplier is required to perform specific actions that are considered fundamental to enable a proper vulnerability handling. Such actions can be mapped into the four common stages of the vulnerability handling process. Starting from the discovery of a vulnerability by a finder:

1. Reception and acknowledgement of vulnerability reports
   - To enable the finder to report potential vulnerabilities, it is fundamental to provide all the necessary information on how to report found potential vulnerabilities.
   - Timely acknowledgement of a vulnerability report assures the vulnerability finder that the report has been received and that the vulnerability handling process has started.
2. Verification of received reports and vulnerabilities
   - Timely information on the result of the vulnerability verification – which should include vulnerability validity and severity, list of potentially affected products and their versions, and information on how to verify the existence of the vulnerability – provides the finder and other informed parties with an initial tool to assess the impact of the vulnerability within their domains.

     Complementing this information with an estimate regarding the timeframe for the remediation release and on possible workarounds gives the finder and other informed parties a first indication on the time window over which alternative/temporal mitigations shall be deployed while waiting for a proper fix.
3. Resolution development
4. Advisory dissemination
   - To enable an effective advisory dissemination, it is fundamental to provide all the necessary information on how vulnerability remediation and advisory reports are shared.

     Advisory reports shall include all necessary information to provide a clear description of the vulnerability and its impact, which products are affected by it, and how to mitigate and fix it.

     It is recommended to publish advisories in commonly accepted dissemination channels such as, e.g., the supplier's website, US-CERT, ICS-CERT, and national CERTs.

- There may be situations in which a vulnerability in the supplier's software will trigger a security patch or update of an ABB product. For example, if this vulnerability is within the supplier's software included in the build of an ABB product (e.g., a software library).
  In such cases, in order to allow ABB to timely analyze the issue and define or develop an appropriate resolution (e.g., patch or update), the supplier is required to release the vulnerability remediation and the advisory report to ABB prior to public disclosure.

ABB's approach to vulnerability handling can be found here: ABB's approach to Software Vulnerability Handling.

Requirement 9: Patch management

Requirement

The supplier shall establish, document, and implement a strategy and process to deal with 3rd-party software security updates and patches relevant to the product.

Relevant 3rd-party software shall at least include:

A Any 3rd-party software that is included in the build or installation package of the product (e.g., 3rd-party libraries or embedded OS).

B Any 3rd-party software on which the product depends or that is typically used in the deployment of the product without being an integrated part of it (e.g., MS Windows, MS Office, Java Runtime Environment, or Acrobat Reader).

The strategy and process for 3rd-party software of type A (as specified above) shall at least include:

- Monitoring for security updates and patches to all relevant 3rd-party software.
- Execution of the vulnerability handling process (as defined in requirement 8) for security updates and patches deemed applicable and where the patch or update addresses vulnerabilities or security issues.

The strategy and process for 3rd-party software of type B (as specified above) shall at least include:

- Maintaining a list of all relevant 3rd-party software dependencies.
- Recommended general approach for application of security updates and patches for each of the listed 3rd-party software dependencies.
- As reasonably requested by ABB, for security updates and patches deemed applicable:
    - Validation of 3rd-party software updates and patches.
    - Communication to ABB of the validation results and the taken/planned actions to resolve validation issues.
    - At ABB’s discretion, ABB can perform the validation of the product’s 3rd-party software updates and patches. In such circumstances, the supplier shall first inform ABB of any product’s 3rd-party software update or patch and then support ABB during the validation and to resolve validation issues.

Clarification on the requirement

Security patches and updates allow to fix bugs and code/design flaws as well as to update security mechanisms in a way of resolving associated security issues.

Relevant 3rd-party software includes both software components that are part of the build or installation package of the supplier’s product (type A), as well as software on which the supplier’s product depends or that is typically used in the deployment of the supplier’s product (type B).

The requirement does not detail the overall strategy to choose or processes to implement; the supplier should define, e.g., if, when, and how software components inside its product are updated or patched, or if and how to test that 3rd-party security updates and patches do not negatively impact its product.

However, the supplier is required to take some actions that are considered fundamental for a proper 3rd-party patch management.

For 3rd-party software of type A, the supplier shall first monitor for security updates and patches to all relevant type-A 3rd-party software. Then, the supplier shall start its vulnerability handling process if an applicable security update or patch addresses a vulnerability or a security issue. Such security update or patch indicates that the affected 3rd-party software presents a vulnerability or a security issue. Consequently, since the affected 3rd-party software is part of the supplier’s product, this latter may also present a vulnerability or a security issue that has to be investigated.

For 3rd-party software of type B, the supplier shall first maintain a list of relevant type-B 3rd-party software on which its product depends. Then, the supplier shall recommend general approaches and procedures for the application of security updates and patches of those dependencies. This means, for example, to indicate whether security updates and patches of a certain dependency can be applied with no restrictions or particular procedures. Or, for example, to provide specific procedures to follow when applying security updates and patches of a certain dependency.

Additionally, the supplier shall take the following actions if requested by ABB and when these requests are reasonable under the circumstances: for updates and patches of relevant type-B 3rd-party software that are considered applicable, the supplier is required to perform patch/update validation and communicate the validation results to ABB, together with taken/planned actions to resolve possible validation issues.

There may be cases in which ABB would potentially want to perform patch/update validation itself. For example, as in the following scenario:

- An ABB application running on a general-purpose OS, e.g., MS Windows, depends on a non-standalone communication stack running in the same OS environment.
- The communication stack is not part of the ABB build or package.
- A security patch for the general-purpose OS is available (and applicable).

Such OS patch is relevant to both the ABB application and the communication stack. However, in this case, ABB may prefer to perform the validation of the OS patch for the combined ABB application and communication stack. This, due to the fact that the validation on the communication stack alone may not be feasible (non-standalone) or that the validation of the communication stack combined with a “test application“ would not provide useful/reliable results.

Requirement 10: Software integrity and authenticity

Requirement

The supplier shall provide ABB with the capability to verify the integrity and authenticity, e.g., through digital signatures, of software deliverables associated with the product, at least, by packaging any software delivered to ABB in a way to allow ABB to verify the integrity and authenticity of such package.

Where technically feasible, all relevant files of the software deliverable shall be digitally signed.

Clarification on the requirement

The supplier is required to provide ABB with the capability to verify the integrity and authenticity of delivered software.

The supplier is required to enable software integrity and authenticity verification at least for the overall software deliverable. That is, to pack all files and data of its software deliverable and enable ABB to verify the integrity and authenticity of that package.

Digitally signing may not always be technically feasible. As an alternative, for example, a hash of the software package can be created and published separately on a trusted and legitimate repository or web site for user verification.

Nevertheless, where technically feasible, it is required to rely on digital signatures to enable software integrity and authenticity verification, as well as to digitally sign all relevant files in the software deliverable.

Requirement 11: Data collection

Requirement

While the supplier's rights, if any, with regard to collection, processing, and use of data are covered in separate documents, the supplier shall in any case document, and make available to ABB such documentation, any data collection activity performed by the product, detailing which data are collected and the related functionality and/or purpose, as well as if, where, and how these data are stored, used, processed, and transmitted.

Clarification on the requirement

The knowledge of which data are supposed to be collected and where and how those data are stored, used, processed, and transmitted provides a fundamental baseline upon which measures to prevent unauthorized (intentional or inadvertent) disclosure of potentially sensitive information can be based.

The supplier is required to document and communicate to ABB any data collection activity performed by its product, detailing which data are collected and the related functionality and/or purpose, as well as if, where, and how these data are stored, used, processed, and transmitted.

This requirement is not meant to define which data the supplier/product can collect, process, and use. This requirement is meant to provide ABB and ABB's end users with transparency and a means to assess potential risks associated with data collection activities by the product.

Requirement 12: Sub-suppliers and sub-contractors

Requirement

The supplier shall ensure that all sub-suppliers and sub-contractors that supply software-related products that are part of the product or provide services related to the development of the product (e.g., code implementation or testing) comply with the requirements listed in this document (requirements 1 to 12) or with equivalent requirements to the ones listed in this document.

The supplier shall take adequate measures to mitigate the risks associated to sub-suppliers and sub-contractors that do not meet the listed or equivalent requirements.

Notwithstanding the foregoing, the supplier shall be fully responsible for all acts and omissions of its sub-suppliers and/or sub-contractors as if they were its own acts or omissions and as if a 3rd-party software-related product which is part of the product was its own product.

Clarification on the requirement

It is important that each component of a solution or product, disregarding if developed by the supplier, supplied to the supplier by its sub-suppliers, or developed for the supplier by its sub-contractors, presents the same or a similar security level. This means that each component shall meet the listed cyber security requirements or equivalent ones, i.e., requirements that address the same security risks and provide risk mitigations equivalent to the listed requirements. In case this is not possible, it is still necessary to address and mitigate the risks related to unmet requirements.

The supplier is required to take responsibility and accountability for its sub-suppliers and sub-contractors and to ensure that they comply with the cyber security requirements listed in the “ABB Cyber Security Requirements for Suppliers”.

Sub-suppliers and sub-contractors in scope are those that supply software-related products that are part of the supplier’s product or that provide services related to, or for the development of the supplier’s product (e.g., code implementation or testing).

Such sub-suppliers and sub-contractors shall comply with the listed cyber security requirements or with equivalent requirements. Alternatively, if sub-suppliers and sub-contractors are not able to meet the listed cyber security requirements (or their equivalent ones), the supplier is required to take actions to mitigate the risks associated with such non-compliances.