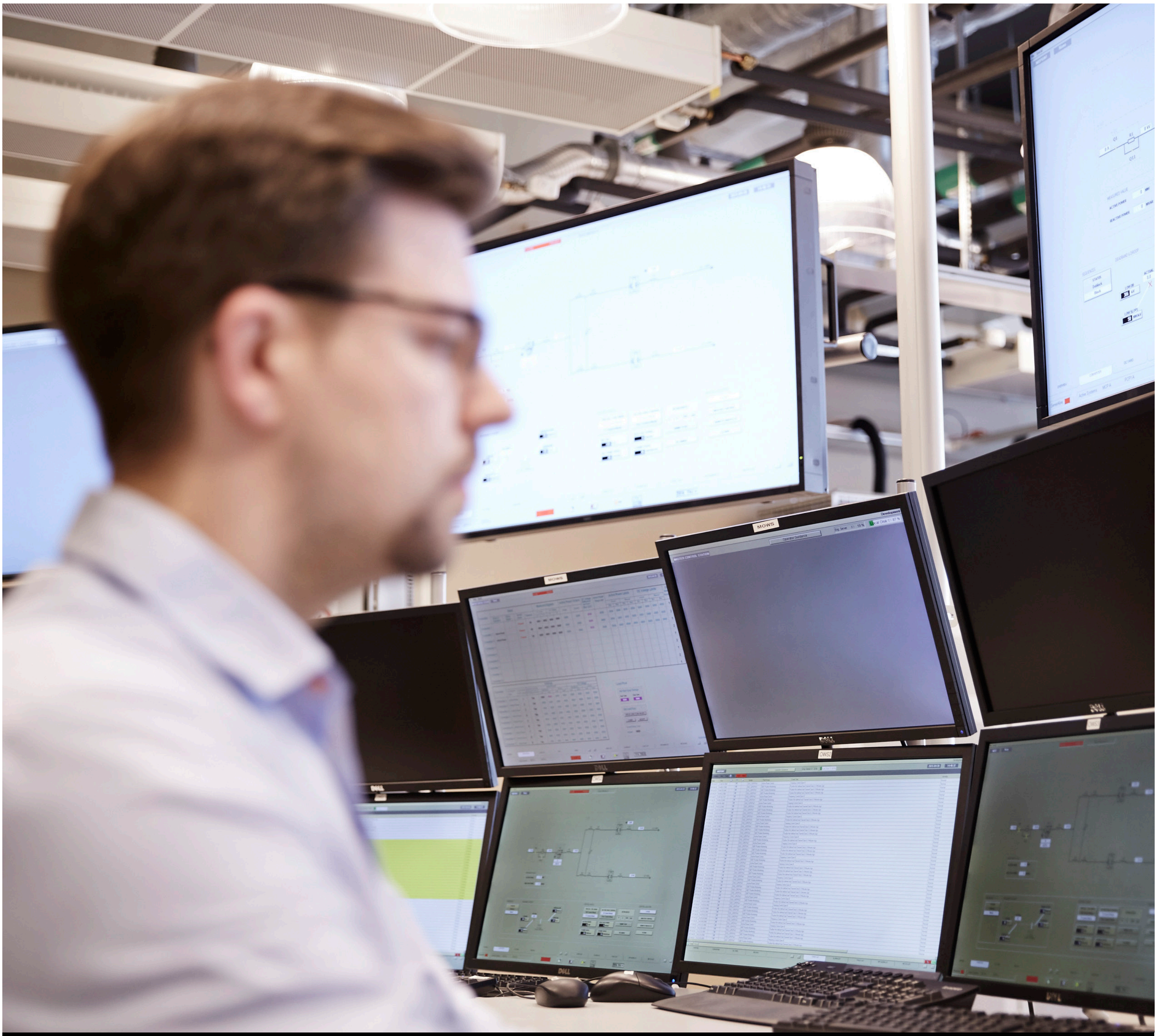

Version 1.0 - Published 18.01.2017

ABB Cyber Security Requirements for Suppliers

Applicability and compliance requirements

This document states minimum cyber security requirements that shall be fulfilled for any software-related product[1] that is supplied to ABB pursuant to the respective contract referencing this document (hereinafter referred to as "Product").

The supplier of the Product (hereinafter referred to as "Supplier") is responsible to take all the necessary measures and steps to comply with the requirements listed in this document.

ABB reserves the right to ask for documentation and evidence, as well as to perform or order a compliance audit, in order to determine whether the listed requirements are fulfilled.

ABB reserves the right to perform an assessment on the security of the Product to identify potential vulnerabilities.

This document contains the terms "including", "include", "in particular", "such as", or similar expressions. They shall be construed as illustrative and shall not limit the sense of the words preceding those terms.

1. Secure development lifecycle

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.

2. Security quality

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.

3. Backdoor accounts and hardcoded credentials

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).

4. Cryptographic tools and security functionalities

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).

[1] A software-related product is defined as a product or system, including all versions and updates, that (i) uses any type of software, (ii) is partly based on any type of software, or (iii) is in itself a type of software. Here, software shall be considered in its broadest sense and includes for instance firmware, drivers, applications, etc.

5. Protection from malware propagation

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.

6. Handling of digital certificates

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.

7. Product documentation

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.

8. Vulnerability handling

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.

9. Patch management

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.

10. Software integrity and authenticity

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.

11. Data collection

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.

12. Sub-suppliers and sub-contractors

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.

Changes to these Cyber Security Requirements for Suppliers

This document may be modified or amended from time to time. Any such modification or amendment will be applicable from the date of the respective modification or amendment as indicated in the new release of this document which shall, however, not be earlier than the actual release date.