Automation Security 2020 –
Design, Implementierung und Betrieb industrieller Automatisierungssysteme

Automation Security 2020 –
Design, Implementation and Operation of Industrial Automation Systems

NE 153

Vorbemerkung

Bei den NAMUR-Empfehlungen („NE“) und -Arbeitsblättern („NA“) handelt es sich um Erfahrungsberichte und Arbeitsunterlagen, die die NAMUR-Mitglieder erarbeitet haben.

NAMUR übernimmt keine Gewähr für die Vollständigkeit oder Richtigkeit der NE und NA. Jede Verwendung durch Mitglieder oder sonstige Dritte erfolgt in eigener Verantwortung und auf das eigene Risiko des Verwenders. Schadensersatzansprüche sind ausgeschlossen, soweit diese nicht auf zwingenden gesetzlichen Haftungsvorschriften beruhen. Einzelheiten regelt die Satzung und die Vereinsordnung bzw. die zwischen NAMUR und Dritten getroffene Vereinbarung.

NE und NA haben nicht den Grad des Konsenses von technischen Normen (z. B. DIN-Normen) oder Richtlinien (z. B. VDI-Richtlinien). Sie stellen lediglich Empfehlungen der NAMUR dar.

Der englische Text ist eine Übersetzung. Im Zweifelsfall ist der deutsche Originaltext anzuwenden.

Preliminary note

The NAMUR recommendations („NE“) and worksheets („NA“) are working documents and practical reports prepared by the NAMUR members.

NAMUR does not warrant that the NE and the NA are complete or accurate. Any use of the NE and the NA by the NAMUR members or by third parties is at the responsibility and the risk of the user. All claims for damages are excluded, except as stipulated by mandatory liability laws. Details are established in the Articles of NAMUR and NAMUR Regulations or in the agreement between NAMUR and a third party.

NE and NA do not enjoy the same level of consensus as normative standards (e.g. DIN standards) or guidelines (e.g. VDI standards). They merely represent recommendations from NAMUR.

The English text is a translation. In case of doubt you should follow the original German text.

Frühere Ausgaben

-

(Dies ist die Erstausgabe)

Previous editions

-

(This is the first edition)

Diese Ausgabe ist freigegeben zur freien Verwendung durch/This edition is authorized for free use by

ZVEI, BSI und KIT

Änderungen	**Amendments**
-	-

Erstellt durch/Prepared by

NAMUR-Arbeitskreis AK 4.18 Automation Security/

NAMUR Working Group WG 4.18 Automation Security

Beteiligte Mitglieder/ Members involved

Martin Schwibach, BASF SE (Arbeitskreisleiter/Working Group Manager)

Als externe Experten waren die folgenden Gäste des AK an der Erarbeitung der NE/NA beteiligt/The following guests of the Working Group participated as external experts in the compilation of the NE/NA:

ZVEI Fachverband Automation

Carolin Theobald. ZVEI
Heiko Adamczyk, Knick
Pierre Kobes, Siemens
Ragnar Schierholz, ABB
Peter Sieber, HIMA
Gerd Wartmann, Endress+Hauser

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Federal Office for Information Security

Holger Junker, BSI

Karlsruher Institut für Technologie (KIT)

Hubert Keller, KIT

Befürwortet durch/Supported by

WIB

Herausgabe der Empfehlung erfolgt durch die NAMUR-Geschäftsstelle/ Distribution by the NAMUR Office

NAMUR- Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V.
c/o Bayer Technology Services GmbH
Gebäude K 9
51368 Leverkusen
Germany

Phone: +49 214/30-71034
Telefax:+49 214/30-9671034
E-Mail: office@namur.de
Internet:www.namur.net

Inhaltsverzeichnis

Contents

1 Einleitung

Moderne Automatisierungslösungen setzen im zunehmenden Maße offene und vernetzte Systemarchitekturen sowie Komponenten der Standard IT ein, häufig mit direkter oder indirekter Verbindung zum Internet.

Solche Automatisierungslösungen sind erhöhten Risiken und Bedrohungen ausgesetzt, denn die für die Standard IT bekannten Angriffe, Fehler etc. wirken sich damit auch in der industriellen Automatisierungstechnik aus.

Zum Zeitpunkt dieser Veröffentlichung werden technische IT-Security Maßnahmen in der Regel zusätzlich zu den eigentlichen automatisierungstechnischen Komponenten[1] in Lösungen eingebaut, um offensichtliche IT Bedrohungen zu vermindern. Dies führt zur Erhöhung der Komplexität von Automatisierungssystemen und Anwendungen, die immer schwerer beherrschbar wird. Eine weitere Problematik stellt die Tatsache dar, dass diese zusätzlichen IT-Security Komponenten weitere unbekannte IT-Security Schwachstellen in das Gesamtsystem einbringen können. Die unterschiedlichen Lebensdauern der Komponenten einer industriellen Automatisierung auf der einen Seite und der Standard IT auf der anderen Seite erhöhen darüber hinaus weiter die IT Risiken und Bedrohungen.

Um dem langfristig zu begegnen, werden in dem vorliegenden Papier für zukünftige Automatisierungslösungen einige grundsätzliche Anforderungen definiert und in der vorliegenden NAMUR Empfehlung NE 153 *Automation Security 2020 – Design, Implementierung und Betrieb künftiger industrieller Automatisierungssysteme* zusammengefasst.

Diese Empfehlung richtet sich in erster Linie an die Lieferanten[2] und Betreiber von Systemen und Komponenten moderner Automation. Es handelt sich hierbei nicht um ein vollständiges Kompendium von IT-Security Anforderungen, sondern um einige, aus Sicht der Autoren wichtige und prinzipielle, branchenunabhängige Anforderungen an zukünftige Automatisierungslösungen.

Im Kern lassen sich diese Anforderungen darauf

1 Introduction

Open and networked system architectures and standard IT components are increasingly used in modern automation solutions, frequently with a direct or indirect link to the internet.

Automation solutions of this nature are exposed to an increased level of risks and threats, as those attacks, faults, etc. which are familiar in standard IT also have an effect on industrial automation technology.

At the time of publication, technical IT security measures are usually integrated in solutions to supplement actual automation technology components and reduce clear IT threats. This increases the complexity of automation systems and applications which are becoming difficult to master. A further problem is the fact that these additional IT security components[1] can introduce additional IT security vulnerabilities to the overall system. Moreover, the differing lifespan of industrial automation components on the one hand and, on the other, that of components in standard IT further increases the level of IT risks and threats.

To address this in the long term, a few fundamental requirements are defined in this paper for future automation solutions and summarised in this NAMUR recommendation NE 153 *Automation Security 2020 – Design, implementation and operating of future industrial automation systems*.

This recommendation primarily addresses suppliers[2] and operators of modern automation systems and components. This does not involve a complete compendium of IT security requirements, but rather a few sector-independent requirements for future automation solutions which, from the point of view of the authors, are significant and fundamental in nature.

In essence, it is possible to summarise these re-

[1] *Anmerkung 1*: Unter dem Begriff *Komponenten von Automatisierungslösungen* werden Geräte und Anwendungen für Automatisierungslösungen zusammengefasst.

Note 1: Equipment and applications for automation solutions are pooled under the term *automation solution components*.

[2] *Anmerkung 2*: die Rolle des Lieferanten soll in Anlehnung an die Richtlinie VDI/VDE 2182 sowohl den eigentlichen Hersteller von Geräten, Systemen und Anwendungen umfassen als auch den Integrator, der Lösungen entsprechend den Vorgaben der Betreiber erstellt. Abweichungen von dieser Festlegung werden explizit erwähnt.

Note 2: in line with VDI/VDE 2182, the role of the supplier should encompass both actual manufacturers of equipment, systems and applications and the integrator who create solutions pursuant to the specifications of the operator. Deviations from this definition are explicitly mentioned.

zusammenfassen, dass IT–Security Konzepte und Funktionen ein integraler Bestandteil der Anforderungsprofile sind und damit auch zum integralen Funktionsumfang automationstechnischer Komponenten und Lösungen gehören. So besteht die Chance, die Komplexität von Automatisierungslösungen erheblich zu reduzieren.

Diese NAMUR Empfehlung adressiert auch eine Reihe grundsätzlicher Anforderungen, die erst auf der Basis intensiver Forschung und Entwicklung erfüllbar sein werden. In diesem Zusammenhang werden hiermit auch neue oder erweiterte Handlungsfelder für Forschung und Entwicklung – auch in der konventionellen IT - aufgezeigt. Dennoch besteht die Erwartungshaltung seitens der Betreiber, dass Hersteller und Integratoren innovative Sicherheitstechnologien und -konzepte frühzeitig auf ihre Anwendbarkeit in der Automatisierungstechnik prüfen und in ihre Produkte integrieren. Dabei muss natürlich auch eine Abwägung zwischen dem erzielten Sicherheitsniveau einerseits und den resultierenden Kosten, der Komplexität, der Verfügbarkeit und dem Zeitverhalten andererseits erfolgen.

Während einige der Anforderungen durchaus schon heute umsetzbar sind, spiegeln andere die Vision einer zukünftigen Generation von Automatisierungslösungen wider. Letztere eignen sich somit nicht dafür, als Auswahlkriterien für heutige Systeme herangezogen zu werden. Bei der Anwendung der in diesem Dokument definierten Anforderungen muss zudem berücksichtigt werden, welche Kriterien sich für einzelne Komponenten und welche für eine gesamte Lösung eignen.

Insgesamt soll durch die Anforderungen die IT-Sicherheit über ein Basisniveau hinaus deutlich erhöht werden. Jedoch befreit dies die Anlagenbetreiber nicht von der Pflicht, ein ganzheitliches Sicherheitsmanagement als kontinuierlichen Prozess zu etablieren.

Da hierzu sowohl Betreiber und Lieferanten beitragen müssen, wurde diese NAMUR Empfehlung gemeinsam von Experten der NAMUR und des ZVEI mit Unterstützung des BSI erstellt.

quirements by defining IT security concepts and functions as an integral part of the requirement profiles and, consequently, also as part of the integral range of functions of automation components and solutions. It is therefore possible to reduce the complexity of automation solutions considerably in this manner.

This NAMUR recommendation addresses also a range of fundamental requirements which can only be met on the basis of intensive research and development. For this reason, new or expanded areas of activity for research and development – including in conventional IT - are also identified in this context. Nevertheless, operators still expect manufacturers and integrators to check innovative security technologies and concepts at an early stage to ascertain their applicability in automation and to integrate these in their products. Of course, the desired security level achieved in this respect should be placed against the resulting costs, complexity, availability and time response.

it is already possible to implement some requirements today, others reflect the vision of a future generation of automation solutions. The latter are therefore unsuitable for consideration as selection criteria for current systems. In addition, when applying the requirements defined in this document it should be taken into account which criteria are suitable for individual components and which are appropriate for a complete solution.

Overall, IT security should be raised considerably above a basic level through these requirements. However, this does not relieve system operators from the obligation to establish a holistic security management system as a continuous process.

As both operators and suppliers should contribute to this end, this NAMUR recommendation was compiled by NAMUR experts and ZVEI with the support of the Federal Office for Information Security in Germany (Bundesamt für Sicherheit in der Informationstechnik - BSI).

2 Secure by Default

Secure by Default bedeutet: Funktionen und Vorgehensweisen auf dem Stand der Technik der IT-Security für die Automation sind standardmäßig in den Komponenten und Systemen der Automatisierungslösungen verfügbar. Darüber hinaus sind folgende Anforderungen zu erfüllen:

2 Secure by Default

Secure by Default means functions and procedures meeting state-of-the-art technological standards in IT security are available as standard features for automation in the components and systems of automation solutions. Moreover, the following requirements should be met:

2.1. Eindeutige Spezifikation und Dokumentation der Funktionen von Geräten, Systemen oder Lösungen durch den Lieferanten

Bei einem Gerät, System oder Lösung ist grundsätzlich zwischen nach-außen-wirkenden Nutzfunktionen und inneren Eigenschaften zu unterscheiden. Nur wenn sämtliche verfügbaren Funktionen und Eigenschaften einer in-den-Verkehr gebrachten Komponente aktuell, dokumentiert und verifizierbar sind, kann diese Komponente effizient in ein IT-Security Konzept integriert werden.

Forderungen:

1. Alle zur Verfügung stehenden Funktionen einer Komponente sind zu spezifizieren und dokumentieren. Ihr grundsätzliches Systemverhalten unabhängig vom Use Case ist zu beschreiben. Fehlverhalten im Sinne Fehlbedienung darf keinen nicht vorhergesehenen (nicht bekannten und nicht erwarteten) Modus einleiten können
2. Funktionen einer Komponente, die für ihren individuellen, geplanten Einsatz in einer Automatisierungslösung nicht gefordert oder gewünscht sind, müssen nachweislich inklusive ihrer gesamten Auswirkungen deinstalliert bzw. nachhaltig deaktiviert sein. Dabei versteht man unter einer „nachhaltigen Deaktivierung“ auch, dass sichergestellt sein muss, dass weder ein einfacher Bedienfehler noch ein nicht autorisierter Zugriff den Funktionsumfang einer automationstechnischen Komponente verändern darf.
3. Die Dokumentation der Funktionen ist bei allen Änderungen fortzuschreiben (z.B.: Reaktivierung von abgeschalteten Funktionen, Funktionserweiterung des Gerätes, usw.).

2.1 Unambiguous specification and documentation of the functions of device, systems or solutions by the supplier

For a device, system or solution, a fundamental differentiation should be made between outwardly working user functions and internal characteristics. Only where all available functions and characteristics of a component placed on the market are current, documented and verifiable, than this component can be integrated efficiently into an IT security concept.

Requirements:

1. All available functions of a component should be specified and documented. Their fundamental system behaviour independent of the use case should be described. Incorrect behaviour in the sense of mal-operation should never initiate an unintentional (unknown and unexpected) mode.
2. Functions of a component which are not required or not desired for their individual and intended use in an automation solution should be verifiably deinstalled and/or permanently deactivated along with their entire effects. Permanent deactivation in this respect means that it should be ensured that neither a simple operating error nor an unauthorised intervention can alter the functional scope of an automation component.
3. Documentation of functions should be updated with all changes (e.g.: reactivation of deactivated functions, expansion of equipment functions, etc.).

2.2. Definition der Nutzfunktionen für den bestimmungsgemäßen Gebrauch, Rückwirkungsfreiheit von Zusatzfunktion

Komponenten der Automatisierungslösungen weisen in der Regel eine Multifunktionalität auf. Diese werden in einer Gesamtlösung vernetzt und in verschiedenen Funktionsausprägungen betrieben. Die Änderung einer Nutzfunktion hat unter systemtechnischen Gesichtspunkten oft auch Einfluss auf die Funktionen der anderen Komponenten.

Forderungen:

1. Bei der Integration von Komponenten in eine Automatisierungslösung ist sicher zu

2.2 Definition of utility functions for correct use, absence of interaction of additional function

Automation solution components generally exhibit multifunctionality. These are networked in an overall solution and operated at different functionality levels. From a technical point of view, modification of an user function often has an influence on the functions of other components.

Requirements:

1. When integrating components in an automation solution, it should be ensured that

stellen, dass die Anwendung aller aktivierten Nutzfunktionen dieser Komponenten nur in der für die geplante Anwendung vorgesehenen Kombination möglich ist.

2. Durch die Nutzung zulässiger Optionen dürfen keine nicht spezifizierten Funktionsänderungen ausgelöst werden. In jeder Kombination der verfügbaren Optionen muss ein nachvollziehbares deterministisches Verhalten der Nutzfunktionen der Automatisierungskomponente gewährleistet sein.

use of all active functions of these components is only possible in that combination intended for the intended application.

2. The use of approved options should not cause any not specified functional changes. Comprehensible deterministic behaviour of the automation component user functions must be assured in any combination of available options.

2.3. Einhaltung von Zuverlässigkeitsanforderungen an die Nutzfunktionen bei der Vernetzung von Komponenten

Forderungen:

1. Die zulässigen Kommunikationsbeziehungen einschließlich möglicher Redundanzen oder Ersatzwege müssen eindeutig definiert und auf das notwendige Minimum reduziert sein. Nicht zulässige Kommunikationen sind zu unterbinden.
2. Sind logische Kommunikationsbeziehungen über interne oder externe physikalische Schnittstellen Bestandteil einer automationstechnischen Funktion, so müssen die notwendigen Funktionen die Erfüllung der Anforderungen an den festgelegten zeitlichen Ablauf der Kommunikation sicherstellen.
3. Die im Rahmen der Automatisierungslösung geforderte Integrität und Vertraulichkeit der Daten und Funktionen sowie ihre Verfügbarkeit (im Sinne von Zugreifbarkeit) ist in allen Kommunikationszuständen zu gewährleisten.

2.3 Observance of reliability requirements with regard to user functions during networking of components

Requirements:

1. Allowed communication relationships, including potential redundancies or alternate routes, should be defined *unambiguously* and be reduced to a necessary minimum. Unapproved communications should be deactivated.
2. If logical communication relationships via internal or external physical interfaces are part of an automation engineering function, the necessary functions must meet the requirements for the defined timing of the communication.
3. The integrity and confidentiality of data and functions defined in the context of the automation solution as well as their availability (in the sense of accessibility) should be assured in all communication conditions.

2.4. Beherrschbarkeit der Betriebszustände von Komponenten und Lösungen

Die Beherrschbarkeit der Betriebszustände - auch im Notfall - einer Komponente und/oder einer Lösung setzt überschaubare funktionale Beziehungen voraus. Eine Funktion wird durch einen eindeutigen Algorithmus mit definierten Eingangs- und Ausgangsgrößen und -werten beschrieben.

Forderungen

1. Eine Veränderung einer Funktion muss auch weiterhin zu nachvollziehbaren Änderungen des Gesamtsystems oder der Automatisierungslösung führen (dies kann z.B. durch eine hierarchische Struktur der Funktionen erreicht werden).

2.4 Controllability of the operating conditions of components and solutions

Controllability of the operating conditions of a component and/or solution demands manageable functional relationships. This requirement is true also in case of an emergency situation. A function is described through an *univocal* algorithm with defined input and output variables and values.

Requirements

1. Modification of a function must continue to lead to comprehensible changes to the overall system or automation solution (this can, for example, be achieved through a hierarchical structure of functions).

2. Die Veränderung der Modalität (Parametrierung des Algorithmus) einer Funktion muss durch vorgegebene Regeln bestimmt werden.

2.5. Eindeutige Spezifikation und Abgrenzung der Betriebsdaten von den Konfigurationsdaten sowie dem zugehörigen Anwendungsprogramm

Die Datenhaltung innerhalb von Automatisierungskomponenten und -lösungen erfordert eine eindeutige und klare Unterscheidung zwischen Betriebsdaten, Konfigurationsdaten bzw. -parametern und Programmen.

Forderungen:

1. Programme beinhalten die Anweisungen, nach denen unter Berücksichtigung von Konfigurationsdaten und Betriebsdaten die Nutzfunktionen realisiert werden. Es muss sichergestellt sein, dass Veränderungen der Konfigurationsdaten oder der Betriebsdaten keinen ungewollten Einfluss auf das Anwenderprogramm oder seine Ausführung haben. Hieraus ergeben sich die Anforderungen an Betriebssysteme, Laufzeitsysteme, Programmiersprachen und Implementierungsregeln.
2. Konfigurationsdaten dürfen nur unter eindeutigen Bedingungen verändert werden. Dies bedeutet, dass das System zu jeder Zeit in einem definierten Zustand sein muss, in welchem die Konfigurationsdaten konsistent übernommen und geprüft werden können. Dazu muss sichergestellt sein, dass die Beherrschbarkeit, der zulässige Zeitpunkt sowie der Umfang und die Wirkung einer Veränderung definiert sind. Der Zugriff auf und die Veränderbarkeit von Konfigurationsdaten darf nur für zugelassene Teilnehmer nach erfolgter Autorisierung und Authentisierung des Eingriffs erfolgen.
3. Betriebsdaten sind Informationen (Parameter, Eingangsdaten und Ausgangsdaten), die sich dynamisch während des Betriebes einer Automatisierungslösung verändern. Es ist sicherzustellen, dass im Betrieb die Veränderung der Betriebsdaten keine Manipulation des Programmablaufs und der Konfigurationsdaten verursachen können.

3 Secure by Design

Konzepte und Funktionen der IT-Security für die Automation sind bei der Formulierung der Anforderungen bis hin zur Entwicklung von automationstechnischen Komponenten und Lösungen zu berücksichtigen. Als Grundlage dienen aktuelle Nor-

2. Changing of the modality (parameterising of the algorithm) of a function should be determined through specified rules.

2.5 Unambiguous specification and distinction of operating data from configuration data and the associated application program

Data storage within automation components and solutions requires a distinct and clear differentiation between operating data, configuration data and parameters and programs.

Requirements:

1. Programs contain the instructions according to which, taking account the configuration data and operating data, user functions are realised. It must be ensured that changes to configuration data or operating data do not have any undesired effect on the user program or its execution. This defines requirements for operating systems, runtime systems, programming languages and implementation rules.
2. Configuration data should only be changed under unambiguous conditions. This means the system must be in a defined status at any given time in which configuration data can be consistently adopted and checked. It should be ensured in this respect that the controllability, the permissible time and the scope and effect of a change are defined. Access to and the changing of configuration data should only be possible for authorised parties following authorisation and authentication of the change.
3. Operating data is information (parameters, input and output data) which changes dynamically during operation of an automation solution. It should be ensured that the changing of operating data during operation cannot result in any manipulation of the program sequence and configuration data.

3 Secure by Design

IT security concepts and functions for the automation should be taken into consideration through all process steps from specifying the requirements up to the final development of automation components and solutions. Current norms and standards serve

men und Standards wie z.B. die IEC 62443 oder die Richtlinie VDI/VDE 2182.

3.1. IT-Security Konzepte und Funktionen sind integraler Bestandteil der automationstechnischen Komponenten und Lösungen

Forderungen:

1. IT-Security Anforderungen sind in die Anforderungsspezifikationen zu integrieren und bei der Entwicklung der einzelnen Komponenten umzusetzen. Auf diesem Wege soll sichergestellt werden, dass Maßnahmen getroffen werden, die die Integrität und Verfügbarkeit der Nutzfunktionen einer Komponente oder einer Lösung entlang ihres Lebenszyklus sicherstellen. Die Leistungsmerkmale der Nutzfunktion dürfen dabei nicht beeinträchtigt werden.
2. Es müssen Konzepte zur Verfügung gestellt werden, um im Laufe der Lebensdauer einer Komponente bzw. Automatisierungslösung diese an die veränderten Bedrohungs- und Verwundbarkeitssituationen zu adaptieren.
3. Die realisierten IT-Security Funktionen automationstechnischer Komponenten müssen eindeutig identifizierbar und in ihrer Wirksamkeit von den Nutzfunktionen abgrenzbar sein.

3.2. Reduzierung der Systemkomplexität

In der Regel erhöhen, zusätzliche, sogenannte externe IT-Security Maßnahmen die Systemkomplexität.

Forderungen:

1. Es muss das Ziel zukünftiger Komponententenentwicklung sein, zu einer Reduzierung der Systemkomplexität beizutragen.
2. Werden externe IT-Security Maßnahmen eingesetzt, müssen auch sie unter den vorhersehbaren Betriebsbedingungen beschrieben und getestet werden.
3. Die definierten Leistungsmerkmale der automatisierungstechnischen Funktionen müssen stets nachweislich aufrechterhalten bleiben.
4. Werden ergänzende Maßnahmen eingesetzt, so sind die Aufwände für die Integration ergänzender Sicherheitsmaßnahmen bei erhöhtem Schutzbedarf zu minimieren.

as a basis (e.g. IEC 62443 or the VDI/VDE 2182 directive).

3.1 IT security concepts and functions are an integral part of automation components and solutions

Requirements:

1. IT security requirements should be integrated to the requirement specifications and implemented during the development of individual components. This approach should ensure that measures are taken which guarantee the integrity and availability of the user functions of a component or solution throughout its life cycle. The performance characteristics of the user function should not be impaired in this context.
2. Concepts should be provided which adapt changing threat and vulnerability situations, during the lifespan of a component or automation solution.
3. IT security functions realised for automation components should be clearly identifiable and definable in terms of their effectiveness to differentiate them from user functions.

3.2 Reduction of system complexity

In general, so-called external IT security measures add to system complexity.

Requirements:

1. The goal of future component development should be to contribute to a reduction of system complexity.
2. Where external IT security measures are employed, these should also be described and tested under the predicted operating conditions.
3. The defined performance characteristics of automation functions should be maintained at all times in a verifiable manner.
4. Where supplementary measures are employed, the effort and outlay for the integration of supplementary security measures should be minimised in the event of an increased security requirement.

3.3. Anwendungssoftware muss definierten und nachprüfbaren Qualitätsvorgaben entsprechen

Die Qualität der Anwendungssoftware von Automatisierungskomponenten und -lösungen beeinflussen maßgeblich die IT-Security in der Automation.

Forderung:

State-Of-The-Art Methoden zur Qualitätssicherung von Software sind nachweisbar anzuwenden.

3.4. Die Kommunikation zwischen den Software-Modulen einer automatisierungstechnischen Komponente ist über eindeutig spezifizierte Schnittstellen (Quelle, Ziel, Übertragungsweg) sichergestellt und geprüft

Forderungen:

1. Grundsätzlich ist ein deterministisches Zeitverhalten in der Kommunikationsbeziehung zwischen allen Modulen einer Komponente zu gewährleisten.
2. Für jede Kommunikation muss definiert sein, welche Kommunikationswege benutzt werden und aus welchen Modulen und/oder Komponenten diese Kommunikationswege bestehen.

4 Secure by Implementation

Dieser Abschnitt beschreibt einige grundlegende Anforderungen an die *Umsetzung* von IT-Security Konzepten und Funktionen in Komponenten und Lösungen.

4.1. Alle Funktionen einer Komponente oder Lösung einschließlich der integrierten IT-Security Funktionen müssen durch geeignete Programmiersprachen und Betriebssysteme umgesetzt werden

Dieser Teil wendet sich explizit an die Forschung und Entwicklung mit der Aufforderung die notwendigen Voraussetzungen für Verfügbarmachung von nutzbaren IT Werkzeugen zu schaffen.

Forderungen:

1. Es ist notwendig, dass Zuverlässigkeitskriterien für die Anforderungen der IT-Security in der Automation definiert werden, anhand derer die Eignung von Programmiersprachen und Betriebssystemen nachgewiesen werden können.

3.3 Application software should correspond to defined and verifiable quality specifications

The quality of the application software used for automation components and solutions considerably influences IT security in the automation.

Requirement:

State-of-the-art quality assurance methods for software should be employed in a verifiable manner.

3.4 Communication between the software modules of an automation component should be ensured and tested via univocal specified interfaces (source, target, transmission path).

Requirements:

1. Fundamentally speaking, deterministic time behaviour in the communication relationship between all modules of a component should be ensured.
2. The communication channels to be used and the modules and/or components from which these communication channels are created should be defined for each communication.

4 Secure by Implementation

This section describes a few fundamental requirements governing the *implementation* of IT security concepts and functions in components and solutions.

4.1 All functions of a component or solution, including integrated IT security functions, should be implemented through appropriate programming languages and operating systems

This section explicitly addresses research and development with the challenge of creating the preconditions necessary to make useful IT tools available.

Requirements:

1. It is necessary to define reliability criteria for IT security requirements in the automation which can be used as a basis for determining the suitability of programming languages and operating systems in a verifiable manner.

2. Werden Programmiersprachen mit bekannten Defiziten eingesetzt so sind zur Kompensation ergänzende Maßnahmen zu definieren und anzuwenden.
3. Werden Betriebssysteme oder Laufzeitumgebungen mit bekannten Defiziten eingesetzt, müssen diese kompensiert werden.

2. Where programming languages with known deficits are used, supplementary measures should be defined and exploited to compensate for this.
3. Where operating systems or runtime environments with known deficits are employed, these should be compensated for.

4.2. Die Identität und Integrität der Implementierung ist abzusichern

Forderungen:

1. In Abhängigkeit der zu erfüllenden Zuverlässigkeitsanforderungen müssen unzulässige Veränderungen von Programmen, Daten und Kommunikationsvorgängen verhindert oder wenigstens erkannt werden.
2. Die Prüfung der Identität sowie der Berechtigungen bei der Nutzung einer Funktion durch Personen, Komponenten, Module etc. muss entsprechend der Anforderungsspezifikation sicher gestellt sein.

4.2 The identity and integrity of the implementation should be secured

Requirements:

1. Impermissible changes to programs, data and communication procedures should be prevented or at least identified, depending on the reliability requirements to be met.
2. Checking of identity and authorisation during the use of a function by persons, components, modules, etc. should be ensured pursuant to the requirement specification.

4.3. IT-Security Tests müssen integraler Bestandteil bei der Entwicklung und Systemintegration von Automatisierungskomponenten sein

Dabei ist zu berücksichtigen, dass der Test von Komponenten auf typische, aktuelle Schwachstellen nicht ausreichend ist. Diese Schwachstellen sind methodisch und vollständig im Rahmen der Spezifikation und deren Umsetzung zu behandeln.

Forderung:

In Typprüfungen und Freigabeverfahren der Hersteller ist die Validierung der Einhaltung der IT-Security zu integrieren.

4.3 IT security tests should be an integral part of the development and system integration of automation components

It should be taken into consideration in this respect that the testing of components for typical, current vulnerabilities is inadequate. These vulnerabilities have to be addressed methodically and completely in the context of the specification and its implementation.

Requirement:

Validation of observance of IT security should be integrated in type testing and the approval procedure of manufacturers.

5 Secure in Deployment

Dieser Abschnitt befasst sich mit der sicheren betrieblichen Implementierung von Automatisierungskomponenten und -lösungen. Im Wesentlichen geht es um eine vertrauensvolle Zusammenarbeit zwischen Lieferanten und Betreiber über die Dauer des gesamten Lebenszyklus einer automationstechnischen Lösung. Die allgemeinen Standards zur IT Security in der Automation sind hierbei umzusetzen.

5 Secure in Deployment

This section addresses the secure operational implementation of automation components and solutions. Essentially, cooperation between suppliers and operators based on mutual trust for the duration of the entire life cycle of an automation solution. General standards for IT security in automation are to be implemented in this respect.

5.1. Mitgelieferte Dokumentationen und Tools unterstützen den Anwender bei der sicheren Konfiguration und dem sicheren Betrieb

Forderung:

Lieferanten müssen entlang aller Lebensphasen der Komponenten und Lösungen über integrierte IT-Security Maßnahmen und notwendige Voraussetzungen für ihren sicheren Einsatz kommunizieren. Dies bedeutet, dass zu jeder Komponente bzw. Lösung ein IT-Security Leitfaden zu Verfügung gestellt und dieser über geeignete Kommunikationsmethoden aktualisiert wird.

5.2. Umgang und Informationen zu Sicherheitslücken

Forderung:

Lieferanten müssen über mögliche IT-Security Schwachstellen, die zu einer Beeinträchtigung des Einsatzes oder Betriebs führen können, über geeignete Kommunikationspfade an die Betreiber zeitnah, offen und proaktiv berichten.

5.3. Aufbau eines geeigneten Patch- und Softwareupdatemanagements

Patch-Vorgänge und Software-Updates in automatisierungstechnischen Komponenten und Lösungen dienen im Allgemeinen dem Erhalt bzw. der Erweiterung des Funktionsumfangs oder zur Fehler- und Schwachstellenbereinigung. Durch die Umsetzung der in 1.-3. definierten Forderungen wird über den gesamten Lebenszyklus einer Software die Anzahl der Patches bzw. Updates minimiert.

Forderungen:

1. Patches bzw. Updates dürfen keine ungewollten, nicht spezifizierten Funktionsänderungen zur Folge haben.
2. Die vom Lieferanten in diesem Zusammenhang etablierten Prozesse und Maßnahmen müssen mit den Anforderungen und Rahmenbedingungen beim Betreiber abgestimmt und bezüglich der korrekten Abarbeitung überprüfbar und kontrollierbar sein.
3. Vom Lieferanten ist zu definieren, welche Konsequenzen die Ausführung dieser Patches bzw. Updates auf Zuverlässigkeit, Sicherheit und Verfügbarkeit der Automatisierungslösung haben. Ggf. ist die Risikoanalyse zum Betrieb einer Lösung in Zusammenarbeit mit dem Betreiber zu aktualisieren.

5.1 Documentation and tools supplied support the user during secure configuration and reliable operation

Requirement:

Suppliers should communicate throughout all life cycle phases of components and solutions the integrated IT security measures and the necessary preconditions for their reliable use. This means that an IT security guideline should be provided for each component or solution, and this should be updated through appropriate communication methods.

5.2 Handling of and information on security loopholes

Requirement:

Suppliers should report promptly, openly and proactively to operators, via suitable communication paths, on potential IT security vulnerabilities which could impair use or operation.

5.3 Development of suitable patch and software update management

In general, patches and software updates in automation components and solutions serve to maintain and expand the functional scope or eliminate errors and vulnerabilities. The number of patches and updates required over the entire life cycle of software is minimised through implementation of the Requirements defined in 1.-3.

Requirements:

1. Patches and updates should not result in any undesired and unspecified functional changes.
2. Processes and measures established by the supplier in this context should be coordinated with requirements and framework conditions at the operator’s facility and be suitable for inspection and verification with regard to their correct execution.
3. The supplier should define those consequences which the realisation of patches and updates has on the reliability, security and availability of the automation solution. The risk analysis of the operation of a solution should be updated together with the operator where appropriate.

4. Lieferanten einer Automatisierungslösung müssen Patches freigeben und dabei sicherstellen, die spezifizierte Funktionalität der Automatisierungslösung nicht beeinflusst wird. Dies gilt auch für damit verbundene Updates einer Softwareplattform eines anderen Lieferanten (z.B. Betriebssysteme, Programmierbibliotheken, etc.).

4. Suppliers of an automation solution should approve patches and ensure in this context that the specified functionality of the automation solution is not influenced. This also applies to associated updates of a software platform from another supplier (e.g. operating systems, programming libraries, etc.).

6 Literatur

[1] VDI/VDE 2182, *Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell*

[2] IEC 62443, *Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme*

6 Literature

[1] [1]VDI/VDE 2182, *IT-security for industrial automation - General model*

[2] IEC 62443, *Industrial communication networks - Network and system security*