ICS 35.030, 35.240.50

VDI/VDE-RICHTLINIEN

April 2020

VEREIN DEUTSCHER INGENIEURE

VERBAND DER ELEKTROTECHNIK ELEKTRONIK INFORMATIONSTECHNIK

# Informationssicherheit in der industriellen Automatisierung

## Empfehlungen zur Umsetzung von Security-Eigenschaften für Komponenten, Systeme und Anlagen

## IT security for industrial automation

## Recommendations for the implementation of security properties for components, systems, and equipment

VDI/VDE 2182

Blatt 4 / Part 4

Ausg. deutsch/englisch
Issue German/English



*Die deutsche Version dieser Richtlinie ist verbindlich.*

*The German version of this standard shall be taken as authoritative. No guarantee can be given with respect to the English translation.*

**Inhalt** Seite



**Contents** Page



VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA)

Fachbereich Industrielle Informationstechnik

 

**Inhalt** Seite



**Contents** Page

## Vorbemerkung

Der Inhalt dieser Richtlinie ist entstanden unter Beachtung der Vorgaben und Empfehlungen der Richtlinie VDI 1000.



Allen, die ehrenamtlich an der Erarbeitung dieser Richtlinie mitgewirkt haben, sei gedankt.

Eine Liste der aktuell verfügbaren Blätter dieser Richtlinienreihe ist im Internet abrufbar unter www.vdi.de/2182.

## Einleitung

Diese Richtlinie beschreibt für Anbieter von Automatisierungslösungen handhabbare Maßnahmen auf Basis der NAMUR NE 153 sowie der Richtlinie VDI/VDE 2182 Blatt 1. Sie erweitert die bestehende Richtlinienreihe VDI/VDE 2182.

Diese Richtlinie wurde vom Fachausschuss „Security“ der VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) erarbeitet, in dem Vertreter der herstellenden und der anwendenden Industrie sowie von Hochschulen und beratenden Unternehmen mitgewirkt haben.

Die NE 153 definiert allgemeine Anforderungen an zukünftige Automatisierungskomponenten, mit dem Ziel, Informationssicherheit als integralen Bestandteil zukünftiger Automatisierungslösungen zu etablieren. Die NE 153 nimmt dabei Bezug auf die Lebenszyklen Design, Implementierung und Betrieb einer Automatisierungslösung.

Die Richtlinie VDI/VDE 2182 Blatt 1 definiert dabei ein allgemeines Vorgehensmodell, mit dessen Anwendung die Informationssicherheit von Geräten, Maschinen und Anlagen erreicht werden kann. Weitere Blätter beschreiben die beispielhafte Anwendung des Vorgehensmodells sowohl für die Fabrikautomation (VDI/VDE 2182 Blatt 2.1, Blatt 2.2 und Blatt 2.3) als auch für die Prozessautomation (VDI/VDE 2182 Blatt 3.1, Blatt 3.2, Blatt 3.3) aus Sicht des Herstellers, des Integrators/Maschinenbauers und des Betreibers.

Die Richtlinie bezieht sich ausschließlich auf den Aspekt der IT-Security im Bereich der industriellen Automatisierung. In der Literatur sind neben IT-Security weitere synonyme Begriffe zu finden, z. B.

## Preliminary note

The content of this standard has been developed in strict accordance with the requirements and recommendations of the standard VDI 1000.



We wish to express our gratitude to all honorary contributors to this standard.

A catalogue of all available parts of this series of standards can be accessed on the Internet at www.vdi.de/2812.

## Introduction

This standard describes practicable security measures for the suppliers and providers of automation solutions and is based on NAMUR recommendation NE 153 and VDI/VDE 2182 Part 1. It forms an additional part of the existing VDI/VDE 2182 series of standards.

The standard was drafted by the Technical Committee “Security” of the VDI/VDE Society Measurement and Automatic Control, with contributions from representatives of manufacturing and user industries, as well as universities and consultancy companies.

NE 153 defines a set of general requirements for automation components with the aim of establishing IT security as an integral part of future automation solutions. NE 153 addresses the design, implementation and operation life cycles of automation solutions.

Standard VDI/VDE 2182 Part 1 defines a general model for achieving IT security in automation devices, machines and plants. Other parts of the standard describe examples of how the model can be applied, both in factory automation (VDI/VDE 2182 Part 2.1, Part 2.2 and Part 2.3) and process automation (VDI/VDE 2182 Part 3.1, Part 3.2, Part 3.3) from the perspective of product suppliers, integrators/machine builders and asset owners.

The standard addresses only those aspects of IT security which are relevant to the industrial automation sector. In relevant bibliography, IT security is also referred to synonymously as information

 

IT-Sicherheit, Informationssicherheit, Cyber Security, Industrial Security, OT Security.

## 1 Anwendungsbereich

Diese Richtlinie ist von Herstellern von Komponenten, Systemen und Anlagen industrieller Automatisierungstechnik (Akteure: Hersteller, Integrator/Maschinenbauer) anzuwenden. Sie richtet sich konkret an die Verantwortlichen für die Anforderungsspezifikation, Design, Implementation und Deployment von Komponenten, Systemen und Anlagen.

Sie basiert auf Anforderungen und Vorgaben der NE 153 und setzt sich im Besonderen mit den Randbedingungen aus der Sicht eines Herstellers auseinander. Im Ergebnis werden Maßnahmen zur Umsetzung aufgezeigt, die gleichermaßen für groß- als auch für klein- und mittelständische Unternehmen geeignet sind.

Diese Richtlinie steht dabei nicht im Widerspruch zur internationalen DIN IEC 62443.

Ziel ist es, dem Leser Denkanstöße zu vermitteln und seine Entwicklung bzw. seinen Entwicklungsprozess bezüglich IT-Security zu verbessern. Am Ende wird IT-Security eine Produkteigenschaft werden, die jedoch oft in Konkurrenz mit anderen bzw. weiteren Produkteigenschaften steht. So wird IT-Security ein Design-Ziel, genauso wie funktionale Sicherheit oder eine Messgenauigkeit.

**Anmerkung:** In Abschnitt 5 bis Abschnitt 8 werden Maßnahmen zur Umsetzung der NE 153 Anforderungen definiert. Dabei ist der Begriff „Umsetzungen“ wie folgt gekennzeichnet:

- keine Auflistung klassischer technischer bzw. organisatorischer Schutzmaßnahmen (Good- oder Best-Practice-Katalog)
- kein Kochrezept, das einfach nur abgearbeitet werden muss (Verlust der Individualität der Anwendung)

## 2 Normative Verweise

Das folgende zitierte Dokument ist für die Anwendung dieser Richtlinie erforderlich:

VDI/VDE 2182 Blatt 1:2020-01 Informationssicherheit in der industriellen Automatisierung; Allgemeines Vorgehensmodell

security, cyber-security, industrial security, or OT security (operational technology security), for example.

## 1 Scope

This standard addresses the suppliers of industrial automation technology components, systems and plants (actors: product suppliers, integrators/machine builders). It specifically addresses all those responsible for requirement specifications, design, implementation and deployment of components, systems and plants.

It is based on the requirements and guidelines of NE 153 and deals, in particular, with boundary conditions from the product supplier’s perspective. As a result, it shows implementation measures that are suitable for both large companies as well as small and medium-sized enterprises (SMEs).

At the same time, it remains consistent with international standard DIN IEC 62443.

The aim is to provide readers with food for thought to help them improve their development and/or development processes with regard to IT security. In the long run, IT security will become a product capability, albeit one which will often clash with other product capability. As a result, IT security will become another design goal, just like functional safety or measurement accuracy.

**Note:** Various measures for implementation of the NE 153 requirements are defined in Section 5 to Section 8. Here, the term “implementation” can be described as follows:

- no list of classical technical and/or organisational security measures (good or best practice catalogues)
- no recipe that simply needs to be followed (and which would lead to a loss of individuality in applications)

## 2 Normative references

The following referenced document is indispensable for the application of this standard:

VDI/VDE 2182 Part 1:2020-01 IT-security for industrial automation; General model