

VEREIN
DEUTSCHER
INGENIEURE

VERBAND DER
ELEKTROTECHNIK
ELEKTRONIK
INFORMATIONSTECHNIK

Informationssicherheit in der
industriellen Automatisierung

Allgemeines Vorgehensmodell

IT-security for industrial automation

General model

VDI/VDE 2182

Blatt 1 / Part 1

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
Vorbemerkung	2	Preliminary note.....	2
1 Anwendungsbereich	2	1 Scope	2
2 Begriffe	3	2 Terms and definitions	3
3 Vorbereitende Aufgaben	6	3 Preparatory tasks	6
3.1 Informationsaustausch	6	3.1 Information exchange	6
3.2 Rollen.....	8	3.2 Roles.....	8
3.3 Strukturanalyse	10	3.3 Structure analysis.....	10
3.4 Anlass.....	11	3.4 Trigger	11
4 Vorgehensbeschreibung	11	4 Procedure description	11
4.1 Assets identifizieren.....	12	4.1 Identify assets	12
4.2 Bedrohungen analysieren.....	13	4.2 Analyse threats	13
4.3 Relevante Schutzziele ermitteln.....	15	4.3 Determine relevant security objectives....	15
4.4 Risiken analysieren und bewerten.....	16	4.4 Analyse and assess risks	16
4.5 Schutzmaßnahmen aufzeigen und Wirksamkeit bewerten	19	4.5 Identify individual measures and assess their effectiveness	19
4.6 Schutzmaßnahmen auswählen	21	4.6 Select countermeasures.....	21
4.7 Schutzmaßnahmen umsetzen	23	4.7 Implement countermeasures	23
4.8 Prozessaudit durchführen.....	23	4.8 Perform process audit	23
5 Anforderungsdokumentation	25	5 Requirement specification	25
6 Prozessdokumentation	25	6 Process documentation	25
7 Technische Dokumentation	25	7 Technical documentation	25
Schrifttum	26	Bibliography	26
Benennungsindex	28	Term index.....	28

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

Fachbereich Industrielle Informationstechnik

VDI/VDE-Handbuch Automatisierungstechnik

VDI-Handbuch Informationstechnik, Band 1: Angewandte Informationstechnik

VDI-Handbuch Fabrikplanung und -betrieb, Band 1: Betriebsüberwachung/Instandhaltung

VDI-Handbuch Verfahrenstechnik und Chemieingenieurwesen, Band 4: Arbeitsschutz

Vorbemerkung

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

Alle Rechte, insbesondere die des Nachdrucks, der Fotokopie, der elektronischen Verwendung und der Übersetzung, jeweils auszugsweise oder vollständig, sind vorbehalten.

Die Nutzung dieser Richtlinie ist unter Wahrung des Urheberrechts und unter Beachtung der Lizenzbedingungen (www.vdi.de/richtlinien), die in den VDI-Merkblättern geregelt sind, möglich.

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.

1 Anwendungsbereich

Der Begriff „Sicherheit“ lässt sich im technischen Kontext aus mehreren Teilaspekten zusammenfassen, sodass der allgemeine Begriff „Sicherheit“ als eine Art Gesamtsicherheit beschrieben werden kann.

Die Gesamtsicherheit berücksichtigt die Aspekte

- Zuverlässigkeit,
- funktionale Sicherheit und
- Informationssicherheit.

In dieser Richtlinie wird ausschließlich die Informationssicherheit behandelt.

Diese Richtlinie beschreibt, wie die Informationssicherheit von automatisierten Anlagen durch die Umsetzung von konkreten Schutzmaßnahmen erreicht werden kann; dazu werden Aspekte der eingesetzten Automatisierungsgeräte, Automatisierungssysteme und Automatisierungslösungen betrachtet. Auf der Basis einer zwischen Herstellern von Automatisierungsgeräten und -systemen und deren Benutzern (z.B. Integratoren, Betreibern) abgestimmten, gemeinsamen Begriffsdefinition wird eine einheitliche, praktikable Vorgehensweise beschrieben, wie Informationssicherheit im gesamten Lebenszyklus von Automatisierungsgeräten, -systemen und -anwendungen gewährleistet werden kann. Der Lebenszyklus berücksichtigt die Phasen „Entwicklung“, „Integration“, „Betrieb“, „Migration“ und „Außerbetriebsetzung“.

Die Richtlinie definiert ein einfaches Vorgehensmodell zur Bearbeitung und Darstellung der Informationssicherheit. Das Modell besteht aus mehreren Prozessschritten. Die Anwendung dieses Vorgehensmodells aus Sicht des Herstellers, Integrators und Betreibers wird in den Richtlinien

Preliminary note

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

All rights are reserved, including those of reprinting, reproduction (photocopying, micro copying), storage in data processing systems and translation, either of the full text or of extracts.

The use of this standard without infringement of copyright is permitted subject to the licensing conditions (www.vdi.de/richtlinien) specified in the VDI Notices.

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/2182.

1 Scope

In a technical context, the term “security” covers many different aspects, so the universal term can be described as “overall security”.

Overall security takes account of issues of

- reliability,
- functional safety, and
- information security.

This standard deals only with IT-security.

This standard describes how specific measures can be implemented in order to guarantee the IT-security of automated plant; aspects of the automation devices, automation systems, and automation applications used are considered. A uniform, feasible procedure for ensuring IT-security throughout the entire life cycle of automation devices, systems, and applications is described, based on common terms and definitions agreed by the product suppliers of automation devices and systems and their users (e.g., integration service providers, asset owner). The life cycle covers the development, integration, operation, migration, and decommissioning phases.

This standard defines a simple procedure model for the development and description of IT-security. The model consists of eight steps. The implementation of this model from the viewpoint of product supplier, integrators and asset owner will be exemplarily described in the standard VDI/VDE 2182

VDI/VDE 2182 Blatt 2 bis Blatt 4 anhand konkreter Beispiele beschrieben.

Die Anwendung der hier beschriebenen Methoden und Schutzmaßnahmen führt systematisch zu Lösungen, die dem Schutzbedarf angemessen und damit wirtschaftlich sind.

Part 2 to Part 4.

Applying the methods and measures described in this standard will allow systematic solutions to be achieved, which are appropriate to the level of protection required, meaning that they are also cost-effective.

→plant