

VEREIN
DEUTSCHER
INGENIEURE

VERBAND DER
ELEKTROTECHNIK
ELEKTRONIK
INFORMATIONSTECHNIK

Informationssicherheit in der industriellen
Automatisierung

Anwendungsbeispiel des Vorgehensmodells in der
Fabrikautomation für Hersteller

Speicherprogrammierbare Steuerung (SPS)

IT-security for industrial automation

Example of use of the general model for
device manufacturer in factory automation

Programmable logic controller (PLC)

VDI/VDE 2182

Blatt 2.1 / Part 2.1

Ausz. deutsch/englisch
Issue German/English

Die deutsche Version dieser Richtlinie ist verbindlich.

The German version of this guideline 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
Einleitung.....	2	Introduction.....	2
1 Anwendungsbereich	2	1 Scope	2
2 Normative Verweise	3	2 Normative references	3
3 Begriffe	3	3 Terms and definitions	3
4 Vorbereitende Maßnahmen	4	4 Usability and ergonomic	4
4.1 Abhängigkeiten.....	4	4.1 Dependencies.....	4
4.2 Rollen.....	6	4.2 Roles.....	6
4.3 Strukturanalyse.....	6	4.3 Structure analysis.....	6
4.4 Anlass.....	14	4.4 Cause.....	14
5 Anwendung des Vorgehensmodells	16	5 Application of the general model	16
5.1 Assets identifizieren.....	16	5.1 Identify assets.....	16
5.2 Bedrohungen analysieren.....	18	5.2 Analyse threats.....	18
5.3 Relevante Schutzziele ermitteln.....	23	5.3 Determine relevant security objectives.....	23
5.4 Risiken analysieren und bewerten.....	26	5.4 Analyse and assess risks.....	26
5.5 Schutzmaßnahmen aufzeigen und Wirksamkeit bewerten.....	28	5.5 Identify individual measures and assess their effectiveness.....	28
6 Anforderungen	37	6 Requirements	37
7 Prozessdokumentation	37	7 Process documentation	37
8 Externe technische Dokumentation	39	8 External technical documentation	39
Schrifttum.....	42	Bibliography.....	42

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

Fachbereich Industrielle Informationstechnik

VDI-Handbuch Informationstechnik, Band 1: Angewandte Informationstechnik
VDI/VDE-Handbuch Automatisierungstechnik
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 VDI-Richtlinie ist unter Wahrung des Urheberrechts und unter Beachtung der Lizenzbedingungen (www.vdi-richtlinien.de), die in den VDI-Merkblättern geregelt sind, möglich.

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

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

Einleitung

Der Inhalt dieser Richtlinie beschreibt ein Anwendungsbeispiel der Richtlinie VDI/VDE 2182 Blatt 1 und stellt somit eine Ergänzung zum Blatt 1 dar.

VDI/VDE 2182 Blatt 1 definiert dabei ein allgemeines Vorgehensmodell, mit dessen Anwendung die Informationssicherheit von automatisierten Maschinen und Anlagen durch die Umsetzung von konkreten Maßnahmen erreicht werden kann.

Das allgemeine Vorgehensmodell der Richtlinie VDI/VDE 2182 Blatt 1 wird in diesem Dokument aus Sicht des Herstellers abgearbeitet, mit dem Ziel, die Relevanz von Blatt 1 und dessen Praktikabilität unter Beweis zu stellen.

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

1 Anwendungsbereich

Diese Richtlinie muss von Herstellern von Automatisierungsgeräten angewendet werden. Sie beschreibt die in der Richtlinie VDI/VDE 2182 Blatt 1 definierte Vorgehensweise und deren Randbedingungen aus Sicht eines Herstellers anhand eines konkreten Anwendungsbeispiels, hier einer speicherprogrammierbaren Steuerung (SPS).

Die Anwendung des Vorgehensmodells führt zu angemessenen Schutzmaßnahmen und zur Dokumentation der Security-relevanten Eigenschaften der SPS.

Preliminary note

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

All rights 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 guideline without infringement of copyright is permitted subject to the licensing conditions specified in the VDI Notices (www.vdi-richtlinien.de).

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

A catalogue of all available parts of this series of guidelines can be accessed on the internet at www.vdi.de/2182.

Introduction

This guideline describes an application example of the principles set out in guideline VDI/VDE 2182 Part 1 and thus supplements Part 1.

VDI/VDE 2182 Part 1 defines a general model that can be used to increase the IT security of devices, machines and plants by implementing specific measures.

The general model from guideline VDI/VDE 2182 Part 1 will be processed in this document from the viewpoint of the device manufacturer, with the aim of proving the relevance of Part 1 and its feasibility.

This guideline has been drafted by the Technical Committee “Security” of the VDI/VDE Society for Measurement and Automatic Control, in collaboration with representatives from the industries that manufacture and use the technologies in question, as well as from educational and consulting bodies.

1 Scope

This guideline is intended to be used by device manufacturers of automation devices. It describes the procedure defined in the guideline VDI/VDE 2182 Part 1 and its constraints from the viewpoint of a device manufacturer, using a specific application example, which is a programmable logic controller (PLC).

In this example, the application of the procedure model results in appropriate countermeasures and in documentation of the security-relevant properties of the PLC.

Dieses Dokument stellt kein Patentrezept dar und erhebt keinen Anspruch auf Vollständigkeit.

Weitere Blätter beschreiben die Anwendung des Vorgehensmodells aus VDI/VDE 2182 Blatt 1 sowohl für die Fabrikautomation (VDI/VDE 2182 Blatt 2.2 und Blatt 2.3) als auch für die Prozessautomation (Blatt 3.1, Blatt 3.2, Blatt 3.3) aus Sicht des Herstellers, des Integrators/Maschinenbauers und des Betreibers.

Die Richtlinie VDI/VDE 2182 Blatt 1 muss dem Leser/der Leserin vorliegen bzw. hinreichend bekannt sein. Sie bildet die Grundlage für diese Richtlinie.

This document is not a ready solution and does not make any claims to completeness.

In other parts of this guideline, we will describe the use of the procedure model from VDI/VDE 2182 Part 1 in factory automation (VDI/VDE 2182 Part 2.2 and Part 2.3) and in process automation (Part 3.1, Part 3.2, Part 3.3) from the viewpoints of the device manufacturer, the integrator/machine builder and the plant manager.

The reader should have access to or sufficient knowledge of guideline VDI/VDE 2182 Part 1, as it forms the basis of the present guideline.