ICS 25.040.40, 35.240.50

VDI/VDE-RICHTLINIEN

April 2019

VEREIN DEUTSCHER INGENIEURE

VERBAND DER ELEKTROTECHNIK ELEKTRONIK INFORMATIONSTECHNIK

Funktionale Sicherheit in der Prozessindustrie
Einführung, Begriffe, Konzeption

Functional safety in the process industry
Introduction, terms, conception

VDI/VDE 2180

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

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

Fachbereich Engineering und Betrieb automatisierter Anlagen

VDI/VDE-Handbuch Automatisierungstechnik
VDI-Handbuch Fabrikplanung und -betrieb, Band 1: Betriebsmittelüberwachung/Instandhaltung
VDI-Handbuch Verfahrenstechnik und Chemieingenieurwesen, Band 3: Verfügbarkeit/Schadensanalyse
VDI-Handbuch Zuverlässigkeit

Frühere Ausgaben: 04.07; 02.18 Entwurf, deutsch; VDI/VDE 2180 Blatt 2:2007-04 und Blatt 5:2010-05

Former editions: 04/07; 02/18 Draft, in German only; VDI/VDE 2180 Part 2:2007-04 and Part 5:2010-05

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/2180.

Einleitung

Gegenüber der vorherigen Ausgabe der Richtlinienreihe VDI/VDE 2180 wurde die Struktur verändert wie in Tabelle 1 dargestellt.

Tabelle 1. Der Inhalt dieser Richtlinienreihe im Vergleich zur vorherigen Ausgabe der Richtlinienreihe

VDI/VDE 2180 Vorausgabe	Änderung	VDI/VDE 2180 aktuell
Blatt 1 Einführung, Begriffe, Konzeption	Überführung nach Blatt 1 neu	Blatt 1 Einführung, Begriffe, Konzeption
Blatt 2 Managementsystem	Überführung nach Blatt 1 neu	
Blatt 3 Anlagenplanung, -errichtung und -betrieb	Überführung nach Blatt 2 neu	Blatt 2 Planung, Errichtung und Betrieb von PLT-Sicherheitsfunktionen
Blatt 4 Nachweis der Hardwaresicherheitsintegrität einer PLT-Schutzeinrichtung	Überführung nach Blatt 3 neu	Blatt 3 Nachweis der Ausfallwahrscheinlichkeit im Anforderungsfall (*PFD)*
Blatt 5 Empfehlungen zur Umsetzung in die Praxis	Überführung nach Blatt 1 neu und Blatt 2 neu	
Blatt 6 Anwendung der funktionalen Sicherheit im Rahmen von Explosionsschutzmaßnahmen	entfällt	

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/2180.

Introduction

Compared to the previous edition of the series of standards VDI/VDE 2180, the structure has been changed as shown in Table 1.

Table 1. The content of this series of standards compared to the previous edition of the series of standards

VDI/VDE 2180 advance	Change	VDI/VDE 2180 current
Part 1 Introduction, terms, concepts	transfer to Part 1 new	Part 1 Introduction, terms, conception
Part 2 Management system	transfer to Part 1 new	
Part 3 Plant engineering, realisation and operation	transfer to Part 2 new	Part 2 Planning, installation and operation of safety instrumented functions
Part 4 Verification of the hardware safety integrity of safety instrumented systems	transfer to page 3 new	Part 3 Verification of Probability of Failure on Demand (PFD)
Part 5 Recommendations for practical use	transfer to part 1 new and part 2 new	
Part 6 Application of functional safety in the context of explosion protection measures	withdrawn	

Weiterhin wurden Begriffe neu definiert. Diese Anpassung wurde erforderlich, um eine stärkere Übereinstimmung der deutschen mit der internationalen Normung herbeizuführen und Unklarheiten bei der Verwendung der einzelnen Begriffe zu beseitigen. Diese Anpassung betrifft zwei Punkte:

- Die „PLT-Betriebs- und Überwachungseinrichtungen“, die in der IEC 61511 unter dem Begriff „BPCS“ zusammengefasst sind, werden zukünftig als „PLT-Betriebseinrichtungen“ bezeichnet. Die bisherige Unterscheidung bezog sich ausschließlich auf die Aufgaben dieser Einrichtungen. Aus Sicht der funktionalen Sicherheit ist diese Unterscheidung nicht erforderlich, da sie sich nicht in Form unterschiedlicher Anforderungen oder unterschiedlicher praktischer Realisierungen auswirkt.
- Der englische Begriff „Safety“ wird im Allgemeinen mit „Sicherheit“, der Begriff „Protection“ mit „Schutz“ übersetzt. Beispiele sind die Begriffe „Protection Layer“ = „Schutzebene“, „safety valve“ = „Sicherheitsventil“, „safety instrumented system“ = „PLT-Sicherheitssystem“. Die Störfall-Verordnung benennt im § 4, Pkt. 2 „Warn- Alarm- und Sicherheitseinrichtungen“; zu den Letzteren gehören auch die bisherigen PLT-Schutzeinrichtungen gemäß VDI/VDE 2180. Gerade das letzte Beispiel führt aufgrund der unterschiedlichen Begriffe in der Praxis oft zu Diskussionen. Weiteres Beispiel AD 2000-Merkblatt A6: PLT-Sicherheitseinrichtungen. Deshalb werden in der Neuausgabe der Richtlinienreihe VDI/VDE 2180 und zeitgleich auch in der Übersetzung der IEC 61511 die genannten Unterschiede zur Richtlinienreihe VDI/VDE 2180 ausgeräumt und die deutschen Begriffe angepasst.

Tabelle 2 gibt einen Überblick über die terminologischen Veränderungen.

Der Begriff „hochverfügbare PLT- Überwachungseinrichtungen“ aus VDI/VDE 2180 Blatt 6 wurde aufgehoben. Dafür wurde der Begriff der „PLT-Betriebseinrichtung mit Sicherheitsfunktion“ eingeführt. Diese Einrichtung führt zwar Sicherheitsfunktionen aus und kann gemäß der IEC 61511 das verfahrenstechnische Risiko um maximal den Faktor 10 reduzieren, sie kann jedoch im Prozessleitsystem unter besonderen Bedingungen integriert sein.

Der Begriff „PLT-Betriebseinrichtung mit Sicherheitsfunktion“ soll die Besonderheit dieser PLT-Einrichtungen widerspiegeln, dass sie zur notwendigen Risikoreduzierung beitragen und somit sicherheitsrelevant sind.

Terms have also been redefined. This adaptation was necessary in order to achieve greater consistency between German and international standardisation and to eliminate ambiguities in the use of the individual terms. This adjustment concerns two points:

- The former “PLT-Betriebs- und Überwachungseinrichtungen”, which are summarised in IEC 61511 under the term “BPCS”, will in future be referred to as “PLT-Betriebseinrichtungen”. The previous distinction referred exclusively to the different functions of these devices. From the point of view of functional safety, this distinction is not necessary because it does not result in different requirements or different practical implementations.
- The English term “safety” is generally translated into German as “Sicherheit”, the term „Protection“ as “Schutz”. Examples are the terms “Protection Layer” (= Schutzebene), “safety valve” = (Sicherheitsventil) and “safety instrumented system“ (= PLT-Sicherheitssystem). The Major Accidents Ordinance speaks of “Warning, Alarming and Safety Devices” in § 4, point 2; the latter also include the previous “PLT-Schutzeinrichtungen” in accordance with old VDI/VDE 2180. The last example in particular often leads to discussions in practice due to the different terms used. Further example AD 2000-Merkblatt A6: PLT-Sicherheitseinrichtungen. Therefore, in the new edition of the standard series VDI/VDE 2180 and at the same time also in the translation of IEC 61511, the mentioned differences to the series of standards VDI/VDE 2180 are eliminated and the German terms are adapted.

Table 2 gives an overview of the terminological changes.

The term “Hochverfügbare PLT-Überwachungseinrichtung” from VDI/VDE 2180 Part 6 has been deleted. For this purpose, the term “PLT-Betriebseinrichtung mit Sicherheitsfunktion” (= “BPCS protection layer”) was introduced. Although this device performs safety functions and can reduce the process risk by a maximum factor of 10 in accordance with IEC 61511, it can be integrated in the process control system under special conditions.

The term “PLT-Betriebseinrichtung mit Sicherheitsfunktion” is intended to reflect the special purpose of these devices that they contribute to the necessary risk reduction and are therefore safety-relevant.

Tabelle 2. Änderungen in der Terminologie

VDI/VDE 2180, Ausgabe April 2007	VDI/VDE 2180, Ausgabe 2019	IEC 61511, Ed. 2, 2017
PLT-Betriebseinrichtung (Messen, Steuern, Regeln)	PLT-Betriebseinrichtung (PLT-B) (Messen, Steuern, Regeln, Alarmieren, Melden, Schalten)	basic process control system (BPCS) (Messen, Steuern, Regeln, Alarmieren, Melden, Schalten)
PLT-Überwachungseinrichtung (Alarmieren, Melden, Schalten)		
Hochverfügbare PLT-Überwachungseinrichtung	PLT-Betriebseinrichtung mit Sicherheitsfunktion (PLT-BS) (Risikominderung bis 10)	BPCS protection layer (BPCS-PL) (Risikominderung bis 10)
PLT-Schutzeinrichtung	PLT-Sicherheitseinrichtung (PLT-S) (Risikominderung > 10, SIL 1 bis SIL 4)	safety instrumented system (SIS) (Risikominderung > 10, SIL 1 bis SIL 4)

Table 2. Changes in terminology

VDI/VDE 2180, Edition April 2007	VDI/VDE 2180, Edition 2019	IEC 61511, Ed. 2, 2017
PLT-Betriebseinrichtung (measuring and controlling)	PLT-Betriebseinrichtung (PLT-B) (measuring, controlling, alarming, signalling, switching)	basic process control system (BPCS) (measuring, controlling, alarming, signalling, switching)
PLT monitoring device (alarming, signalling, switching)		
Hochverfügbare PLT-Überwachungseinrichtung	PLT-Betriebseinrichtung mit Sicherheitsfunktion (PLT-BS) (risk reduction up to 10)	BPCS protection layer (BPCS-PL) (risk reduction up to 10)
PLT-Schutzeinrichtung	PLT-Sicherheitseinrichtung (PLT-S) (risk reduction >10, SIL 1 to SIL 4)	safety instrumented system (SIS) (risk reduction >10, SIL 1 to SIL 4)

Die Richtlinienreihe VDI/VDE 2180 besteht aus folgenden Blättern:

Blatt 1 Einführung, Begriffe, Konzeption

Blatt 2 Planung, Errichtung und Betrieb von PLT-Sicherheitsfunktionen

Blatt 3 Nachweis der Ausfallwahrscheinlichkeit im Anforderungsfall (*PFD)*

Im Folgenden liegt der Schwerpunkt auf der Realisierung von PLT-Sicherheitsfunktionen mit einem SIL zwischen 1 und 3 in entsprechenden PLT-Sicherheitseinrichtungen und -systemen. SIL-4-Einrichtungen werden nur in begründeten Ausnahmefällen und unter Beachtung umfangreicher Zusatzmaßnamen (siehe IEC 61511) eingesetzt. In dieser Richtlinie wird auf die Realisierung von SIL-4-Funktionen deshalb nicht weiter eingegangen. Die Anforderungen an PLT-Betriebseinrichtungen mit Sicherheitsfunktion sind in einem gesonderten Abschnitt zusammengefasst.

1 Anwendungsbereich

Diese Richtlinie basiert auf IEC 61511 und gilt für Anlagen der Prozessindustrie, z.B. der chemischen und petrochemischen Industrie. Sie stellt eine bewährte Möglichkeit dar, die Anforderungen der 12. BlmSchV (Störfall-Verordnung) an PLT-Sicherheitseinrichtungen umzusetzen (siehe auch „Vollzugshilfe zur Störfall-Verordnung vom März 2004“, herausgegeben vom BMU).

Die Nutzung der Richtlinie setzt voraus, dass bei Planung, Errichtung und Betrieb alle einschlägigen

The standard series VDI/VDE 2180 consists of the following parts:

Part 1 Introduction, terms, conception

Part 2 Planning, installation and operation of safety instrumented functions

Part 3 Verification of probability of failure on demand (*PFD*)

In the following, the focus is on the implementation of safety instrumented functions with a SIL between 1 and 3 in corresponding safety instrumented systems. SIL 4 functions are only used in justified exceptional cases and with consideration of extensive additional measures (see IEC 61511). This standard therefore does not deal further with the implementation of SIL 4 functions. The requirements for BPCS protection layer are summarised in a separate Section.

1 Scope

This standard is based on IEC 61511 and applies to plants in the process industry, e.g. the chemical and petrochemical industries. It represents a proven possibility to implement the requirements of the 12. BlmSchV (Major Accidents Ordinance) for safety instrumented systems (see also “Implementation Aid to the Major Accidents Ordinance of March 2004”, published by BMU).

The use of the standard presupposes that all relevant laws, regulations, accident prevention regula-

Gesetze, Verordnungen, Unfallverhütungsvorschriften, sonstige Vorschriften, Normen, technische Regeln usw. beachtet werden.

PLT-Sicherheitseinrichtungen kommen üblicherweise dann zum Einsatz, wenn andere Maßnahmen nicht anwendbar, nicht ausreichend oder bei vergleichbarer Risikoreduzierung nicht wirtschaftlich sind. Die Anwendung möglichst einfacher, überschaubarer und unmittelbar wirkender Maßnahmen (z.B. Sicherheitsventile, druckfeste Absicherung) führt in der Regel zu sicheren und gleichzeitig wirtschaftlichen Lösungen.

In dieser Richtlinie werden die allgemeinen Grundsätze für die Sicherung von Anlagen der Prozessindustrie mit Mitteln der Prozessleittechnik (PLT) für den typischen Fall einer höchstens jährlichen Anforderung der PLT-Sicherheitsfunktion beschrieben.

Obwohl sich diese Richtlinie formal nur auf PLT-Einrichtungen bezieht, können die beschriebenen Grundsätze, Konzepte und Vorgehensweisen auch auf Einrichtungen anderer Gewerke angewendet werden. Dies betrifft ausschließlich die systematischen Aspekte und Managementaspekte (z.B. Einsatz geeigneten Personals, Managementsystem der funktionalen Sicherheit, Vorgehen bei erkannten Störungen), die hier beschrieben sind, und nicht die probabilistischen Gesichtspunkte.

tions, other regulations, standards, technical rules, etc. are observed during planning, construction, and operation.

Safety instrumented systems are usually used when other measures with comparable risk reduction are not applicable, not sufficient or not economical. The application of measures that are as simple, straightforward and directly acting as possible (e.g. safety valves, pressure-resistant protection) generally leads to safe and at the same time economical solutions.

This standard describes the general principles for plant protection in the process industry by use of process control technology for the typical case of a maximum annual demand for the safety instrumented function.

Although this standard formally refers only to process control equipment, the principles, concepts and procedures described can also be applied to equipment of other trades. This applies exclusively to the systematic aspects and management aspects (e.g. deployment of suitable personnel, management system of functional safety, procedure in the event of malfunctions detected) described here and not to the probabilistic aspects.