NeGSt

Neue Generation Signaltechnik - NeGSt

Sammlung zu

„Definition Betriebsbewährtheit“

Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

NeGSt

AP 2100, Arbeitsgruppe 1

„Anerkannte Regeln der Technik“

31. Juli 2013

Datei: NeGSt_ARdT_Sammlung_Betriebsbewaehrt_V1-00_20130731

BOMBARDIER DB NETZE Deutsches Zentrum für Luft- und Raumfahrt e.V. in der Helmholtz-Gemeinschaft fir/RWTH AACHEN funkwerk traffic & control communication PINTSCH BAMAG SCHEIDT&BACHMANN SIEMENS THALES

Inhaltsverzeichnis

Änderungsvermerke:

Version	Durchgeführt von	Anmerkung
V0-00	C. Hilgers	Veröffentlichte Fassung

1 Vorwort

Mit diesem Dokument werden Definitionen und Aussagen zum Begriff „Betriebsbewährtheit“ zusammengefasst. Es ist eine Zusammenstellung, die nicht den Anspruch auf Vollständigkeit erhebt.
Im Rahmen des Projektes NeGSt AP 2100, Arbeitsgruppe 1 „Anerkannte Regeln der Technik“ wird der Begriff „Betriebsbewährtheit“ diskutiert und führte zu einer Sammlung von Definitionen. Dieses Dokument ergänzt somit das Positionspapier „Positionspapier Entwicklung von anerkannten Regeln der Technik“, insbesondere die Aussagen zur Betriebsbewährtheit in Kapitel 4.1.

2 Sammlung Definition Betriebsbewährtheit[1]

2.1 Funktionale Sicherheit elektrotechnischer Komponenten - Ein Leitfaden für Anwender [A]

„Die IEC 61508 ist die Grundnorm und damit die Basis für die Sicherheitsnormierung. Daneben gibt es noch sektorspezifische Normen auf Basis der IEC 61508, die besonders für Planer und Betreiber wichtig sind. Für die Prozessindustrie gilt die IEC 61511. Mögliche Anwendungen und Validierungen für sicherheitsrelevante Schutzfunktionen sowie Regeln für (betriebs-)bewährte Technik werden durch europäische und internationale Normen (zum Beispiel DIN EN 50116 oder DIN ISO 13849-2) definiert.
…
In der IEC 61511 wird „betriebsbewährt“ definiert, jedoch kann nur der Betreiber eine Betriebsbewährung aussprechen, der Hersteller nicht. Betriebsbewährte Geräte werden zumeist durch die Anwender in Standardgerätelisten festgehalten. Betriebsbewährungen müssen lückenlos dokumentiert werden und in hinreichendem Maße die Einsatzerfahrungen über einen längeren Zeitraum wiedergeben.“

Quelle [A]:
http://www.namur.de/fileadmin/media/Pressespiegel/atp/atp_01_02_2011_Funktionale_Sicherheit_Knittel_Namur.pdf

2.2 IEC 61508

Zitat aus IEC 61508-2:2000 [15]:

> *„7.4.7.6 Eine Komponente oder ein Teilsystem kann dann als betriebsbewährt (Proven in Use) angesehen … Komponente ausreichende Nachweise … Einsatz in einem sicherheitstechnischen System eignet.*
>
> *….“*

Die weiteren Abschnitte 7.4.7.7 bis 7.4.7.12 der Norm beschreiben die Anwendungsbedingungen für das Kriterium „proven in use“.

In der EN 61508-2:2010 [5] sind geändert diese Aussagen zu finden:

> *„7.4.10 Anforderungen an betriebsbewährte Elemente*
>
> *Anmerkung Siehe 7.4.2.2. c) für Einzelheiten, wann die Anforderungen dieses Unterabschnitts gelten.*
>
> *7.4.10.1 Ein Element darf nur als betriebsbewährt betrachtet werden, wenn es eine klar beschränkte und festgelegte Funktionalität hat und wenn ein angemessener dokumentarischer Nachweis vorliegt, um zu zeigen, dass die Wahrscheinlichkeit aller gefahrbringenden systematischen Fehler gering genug ist, …“*

Zitat aus IEC 61508-7:2000 [16] der Norm:

> *„B.5.4 Felderfahrung*
>
> *Anmerkung 1 Siehe auch C.2.10 für eine ähnliche Maßnahme und Anhang D für einen statistischen Ansatz, beides im Zusammenhang mit Software.*

[1] engl. „proven in use“

Anmerkung 2 Dieses Verfahren/Maßnahme ist in den Tabellen B.3 und B.5 der IEC 61508-2 aufgeführt.

Ziel: Verwendung von Felderfahrungen …

Beschreibung: Verwendung von Bauteilen oder Untersystemen, … über ausreichend lange Zeit in zahlreichen verschiedenen Anwendungen keine oder nur unbedeutende Fehler …

Für die Angabe „Felderfahrung" müssen die folgenden Bedingungen erfüllt sein:

- *unveränderte Spezifikation;*
- *10 Systeme in verschiedenen Anwendungen;*
- *10^5 Betriebsstunden und mindestens ein Jahr Betriebsaufzeichnung.*

Die Felderfahrung wird durch Dokumentation des Herstellers und/oder der betreibenden Firma nachgewiesen.

… "

In der EN 61508-7:2010 [17] sind ähnliche Aussagen zu finden:

„…

Ziel: Verwendung von Felderfahrungen …

Beschreibung: Verwendung von Bauteilen oder Teilsystemen, … über ausreichend lange Zeit in zahlreichen verschiedenen Anwendungen keine oder nur unbedeutende Fehler gezeigt haben …

Für die Angabe „Felderfahrung" müssen die folgenden Bedingungen erfüllt sein:

- *unveränderte Spezifikation;*
- *10 Systeme in verschiedenen Anwendungen;*
- *10^5 Betriebsstunden und mindestens ein Jahr Betriebsaufzeichnung.*

…

Die Felderfahrung wird durch Dokumentation des Herstellers und/oder der betreibenden Firma nachgewiesen.

…"

2.3 IEC 61511 (Prozessindustrie)

Definition Betriebsbewährtheit nach E DIN EN 61511-1:2012-10 Kap. 3.2.55 [6]:

„Betriebsbewährt (en: prior use)

dokumentierte Beurteilung, beruhend auf Betriebserfahrungen in einer ähnlichen Umgebung, …"

„11.5.3 Anforderung hinsichtlich der auf Basis einer früheren Verwendung erfolgenden Auswahl von Komponenten und Teilsystemen

11.5.3.1 Es muss in geeigneter Weise nachgewiesen werden, dass die Komponenten und Teilsysteme für den Einsatz im sicherheitstechnischen System geeignet sind.

…

11.5.3.2 Der Nachweis muss Folgendes beinhalten:

- *Berücksichtigung des Qualitätsmanagements …*
- *…*
- *den Umfang der Betriebserfahrung;*

…“

EN 61511-1:2004 [15]:

„3.2.60 Eine Komponente ist dann betriebsbewährt, … für den Einsatz in einem sicherheitstechnischen System geeignet …“

2.4 Diskussion innerhalb der Normenfachexperten IEC 61508/61511

Anpassung der Definitionen zur früheren Nutzung und der Bedingungen, unter denen diese herangezogen werden kann. Die Benennung „frühere Nutzung“ wird in der zur Zeit gültigen DIN EN 61511 (VDE 0810):2004 für die Benennung „prior use“ nach IEC 61511 verwendet. DKE/GK 914 berät jedoch darüber, für die Neuausgabe der DIN EN 61511 (VDE 0810) diese Benennung „frühere Nutzung“ durch die in der deutschen Fachöffentlichkeit übliche Benennung „betriebsbewährt“ zu ersetzen.
Eine vom Hersteller festgestellte Betriebsbewährung (proven in use) wird in der künftigen IEC 61511 voraussichtlich nicht mehr beschrieben werden.

Quelle (Meldung vom 14.1.2013) [B]: http://www.dke.de/de/DKE-Arbeit/MitteilungenzurNormungsarbeit/2013/Seiten/Ueberarbeitung61511.aspx

Eine Diskussion der unterschiedlichen Aussagen der IEC 61508 und IEC 61511 zur Betriebsbewährtheit sowie einer möglichen Umsetzung erfolgt im englischsprachigen Artikel [13].

2.5 DIN EN 5012x (Bahn)

2.5.1 DIN EN 50126:2000

Keine Verwendung; in B5. ist ohne weitere Erläuterung die Rede von „erprobten Verfahren/Werkzeugen“

2.5.2 DIN EN 50128:2001 / EN 50128:2011

„Betriebsbewährter Übersetzer“ (Compiler) in Abschnitt B.65 der Norm von 2001 beschrieben; in der Norm von 2011 wurde der Abschnitt offensichtlich entfernt

2.5.3 DIN EN 50129:2003

- Verwendung im Kontext der Verwendung betriebsbewährter Computertools für SIL3/SIL4 in Tabelle E.7, vierte Zeile. Keine Definition des Begriffs.

„Bei SIL3 / 4: R: Verwendung von betriebsbewährten oder validierten Werkzeugen, allgemeine computerunterstützte Entwicklung“

- Die hier relevantere Verwendung ist diejenige als empfohlene Methode (Einstufung R = recommended) für die Verifikation und Validation von Systemen/Produktentwürfen in Tabelle E.9, zwölfte Zeile:

  "10.000 Betriebsstunden über mindestens 1 Jahr" für SIL 1/2-Systeme sowie "1 Million Betriebsstunden über mindestens 2 Jahre mit unterschiedlichen Einrichtungen, einschließlich Sicherheitsanalyse, detaillierte Dokumentation auch von kleineren Änderungen während der Betriebszeit" für SIL 3/4-Systeme.

2.6 ISO 26262 (Automotive)

Proven-in-Use, Betriebsbewährtheit: Wenn Komponenten eines Systems wiederverwendet werden sollen oder einige Zeit vor Inkrafttreten der Norm erfolgreich und fehlerfrei von Kunden verwendet wurden, kann man mit dieser Erfahrung den Entwicklungsaufwand bei Wiederverwendung reduzieren. Je nach Bedeutung können von der Norm geforderte Nachweise oder Maßnahmen entfallen. Voraussetzung ist eine Produktbeobachtung[2] und die Analyse der Ausfälle, die in der Hand des Kunden aufgetreten sind[6]. Komponenten können Hardwarekomponenten und Softwaremodule sein, aber auch Teile der früher erarbeiteten Dokumentation, die selbst nur dem Nachweis einer sicheren Entwicklung dient.

Quelle [C]: http://de.wikipedia.org/wiki/ISO_26262

Schließlich wird in der Leitnorm für die Risikobeurteilung (ISO 12100) ausdrücklich erwähnt, dass bei den notwendigerweise hypothetischen Analysen real existierende Praxisbefunde berücksichtigt werden sollen. Dies tut z. B. die funktionale Sicherheitsnorm ISO 26262 für Kraftfahrzeuge im Teil 8 Abschnitt 14 mit statistisch begründeten Methoden zum Nachweis der Betriebsbewährtheit.

Quelle [D]: http://www.industrie-forum.net/de/konstruktionentwicklungde/april042011/rubrik/betriebsbewaehrtheit-beruecksichtigen/;jsessionid=aT_fUTwaOMVdZig42f

Die aktuelle Dissertationsschrift [14] setzt sich ausführlich mit Theorie und Praxis der Betriebsbewährtheit im Automobilbereich auseinander.

2.7 EN 13849 (Anlagen-/Maschinensicherheit)

EN 13849-1: Betriebsbewährte Bauteile als eine Maßnahme (unter vielen) gegen CCF-Ausfälle

Quelle [E]: www.hs-augsburg.de/~gilles/.../Steuerungen%20EN%20**13849-1**.ppt

Betriebsbewährte Bauteile. In ähnlichen Anwendungen bereits eingesetzt (vgl. DIN EN ISO 13849-2 B.4)

Quelle [F]: http://www.festo.com/net/SupportPortal/Files/26977/Sicherheitstechnik%20135241%2003-2013%20DE.pdf

[2] http://de.wikipedia.org/wiki/Produktbeobachtung

Zitate aus EN ISO 13849-1:2008 [7]:

„4.5.1 Performance Level P

…

Dies kann erreicht werden durch Erhöhung der Zuverlässigkeit der Bauteile, z. B. durch Auswahl von bewährten Bauteilen und/oder die Anwendung von bewährten Sicherheitsprinzipien, …

6.2.4 Kategorie 1

… Ein bewährtes Bauteil für eine sicherheitsbezogene Anwendung ist ein Bauteil, das entweder:

a) in der Vergangenheit weit verbreitet mit erfolgreichen Ergebnissen …

b) unter Anwendung von Prinzipien hergestellt und verifiziert …

…“

Zitat aus EN ISO 13849-2:2003 [17]:

„8 Validierung der Umgebungsanforderungen

Die Anwendung von Betriebszuverlässigkeitsdaten … können den Validierungsprozess unterstützen.“

2.8 Im Kontext der (Chemie-)Anlagensicherheit

Als betriebsbewährt gelten Ausrüstungsteil, die bereits in einer Mindeststückzahl über einen definierten Zeitraum in gleichem oder zumindest vergleichbarem Einsatzbereich betrieben werden und als sicher in ihrer Funktion gelten. Die IEC 61511 beziffert hier die Summe der Einsatzzeit auf mindestens 30 Mio. Stunden (Einbeziehung aller eingesetzten Geräte). Neben der IEC 61511 behandelt auch die Namur-Empfehlung NE 93 die Kriterien für die Betriebsbewährtheit.

Quelle [G]: http://www.industrie.de/industrie/live/index2.php?set=goarticle&object_id=30095748

2.9 Im Kontext elektrotechnischer Komponenten

„Betriebsbewährtheit

Proven in Use (zur Konfiguration sicherheitsbezogener Systeme werden u. a. betriebsbewährte [proven-in-use] Bauteile verwendet. Das heißt Bauteile, die sich bereits in größerer Stückzahl über einen längeren Zeitraum unter gleichen oder ähnlichen Einsatzbedingungen bezüglich ihrer Funktionssicherheit bewährt haben. Die konkreten Kriterien für die Betriebsbewährtheit sind dabei in den verschiedenen Branchen nicht exakt gleich definiert. Nach der DIN EN 61511 (VDE 0810) beispielsweise werden in der Prozessindustrie unter Einbeziehung aller betrachteten Geräte mindestens 30 Mio. Stunden Betriebszeit vorausgesetzt. Im Bereich des Maschinenbaus dagegen werden Bauteile oder Komponenten als betriebsbewährt angesehen, wenn zehn Systeme in unterschiedlichen Anwendungen während 10 000 Betriebsstunden oder wenigstens einem Jahr Betriebsdauer keine sicherheitsrelevanten Fehlfunktionen gezeigt haben)“

Quelle [H]: http://www.etz.de/1111-0-Fachlexikon.html?alpha=B

2.10 Im Software-Kontext

„Der Begriff „Betriebsbewährtheit" und der Begriff „Erprobtheit" kommen eigentlich aus dem Gebiet der Hardware, vor allem in Bezug auf Bauelemente. Sie sind im Regelwerk festgelegt (siehe z.B. DIN 50116 und DIN 0801).

Der Beurteilung, ob eine Software betriebsbewährt ist (Es kann sich auch um ein einzelnes Modul oder z.B. um einen kompletten Compiler handeln), liegen drei Kriterien zugrunde:

- Zeitraum des Einsatzes mindestens zwei Jahre
- Große Anzahl von Installationen
- Unterschiedliche Anwendungen

Die Spezifikation darf nicht verändert werden, nur um diese Kriterien zu erfüllen. Außerdem dürfen keine oder nur unwesentliche Versagensfälle auftreten. Der Einsatz betriebsbewährter Software ist - wie bei Hardware - eine Maßnahme, die Verfügbarkeit und Zuverlässigkeit des Gesamtsystems erhöht.

Bei manchen Software-Produkten bedeutet das Zutreffen der obigen drei Kriterien nicht unbedingt das das Produkt „Betriebsbewährt" ist. So kann es sich bei einem Betriebssystem einer bekannten Firma aus Redmond nicht um eine „Betriebsbewährte" Software handelt, da auftretende Fehler meistens nicht selten und unwesentlich sind. Zwar überwiegt die Anzahl der Installation und die der Unterschiedlichen Anwendungen sicher denen anderer Hersteller, aber trotzdem sollte dieses Produkt nicht als „Betriebsbewährt" angesehen werden."

Quelle [l]: http://www.fh-wedel.de/archiv/wol/seminar/gruppe9-10/definition.html

3 Anhang

3.1 Literaturverzeichnis

[1] EN 50129:2003; Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante elektronische Systeme für Signaltechnik

[2] EN 50126:1999 und Berichtigungen; Bahnanwendungen - Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS);

[3] EN 50128:2008; Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Software für Eisenbahnsteuerungs- und Überwachungssysteme

[4] EN 50126 Reihe: prEN 50126-1, -2, -4 und -5, Entwurf 2012
Zusammenführung der EN 50126, EN 50128 und EN 50129

[5] EN 61508-2:2010 Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme

[6] E DIN EN 61511-1:2012-10: Europäische Norm; Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie

[7] EN 13849 Europäische Norm; Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen

[8] ISO 26262 Internationale Norm; Straßenfahrzeuge - Funktionale Sicherheit

[9] ISO 12100 Internationale Norm; Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung

[10] NE 93

[11] DIN 50116 Prüfung von Zink und Zinklegierungen; Schlagbiegeversuch

[12] DIN 0801 Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben.

[13] R. Amkreutz and I. Van Beurden: What does proven in use imply? Houston, TX, United States, 2004.

[14] Marco Heinz Schlummer: Beitrag zur Entwicklung einer alternativen Vorgehensweise für eine Proven-in-Use-Argumentation in der Automobilindustrie. Bergische Universität Wuppertal, 2012

[15] IEC 61508-2:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2

[16] IEC 61508-7:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7

[17] EN 61508-7:2010 Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer/programmierbarer elektronischer Systeme – Teil 7: Überblick über Verfahren und Maßnahmen

3.2 Quellenverzeichnis Internet

[A] http://www.namur.de/fileadmin/media/Pressespiegel/atp/atp_01_02_2011_Funktionale_Sicherheit_Knittel_Namur.pdf

[B] http://www.dke.de/de/DKE-Arbeit/MitteilungenzurNormungsarbeit/2013/Seiten/Ueberarbeitung61511.aspx

[C] http://www.dke.de/de/DKE-Arbeit/MitteilungenzurNormungsarbeit/2013/Seiten/Ueberarbeitung61511.aspx

[D] http://www.industrie-forum.net/de/konstruktionentwicklungde/april042011/rubrik/betriebsbewaehrtheit-berueecksichtigen/;jsessionid=aT_fUTwaOMVdZig42f

[E] www.hs-augsburg.de/~gilles/.../Steuerungen%20EN%2013849-1.ppt

[F] http://www.festo.com/net/SupportPortal/Files/26977/Sicherheitstechnik%20135241%2003-2013%20DE.pdf

[G] http://www.industrie.de/industrie/live/index2.php?set=goarticle&object_id=30095748

[H] http://www.etz.de/1111-0-Fachlexikon.html?alpha=B

[I] http://www.fh-wedel.de/archiv/wol/seminar/gruppe9-10/definition.html

3.3 Glossar

AP	Arbeitspaket
CCF	Common Cause Failure
DIN	Deutsche Industrienorm
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE
E/E/PES	Elektrische/Elektronische/Programmierbare Elektronische Systeme
EN	Europäische Norm
GK	Gemeinschaftskomitee
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
NeGSt	Neue Generation Signaltechnik
PL	Performance Level
SIL	Safety Integrity Level
SIS	Sicherheitstechnisches System
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e.V.