Neufassung der Norm DIN/IEC 61508 - Anforderungen an Software in sicherheitsrelevanten industriellen Rechensystemen

Wolfgang D. Ehrenberger
Fachbereich Angewandte Informatik, Fachhochschule
36012 Fulda

Abstract: Die Neufassung des Softwareteils der DIN/IEC 61508 betrifft neben der Korrektur allfälliger Schwächen der vorhandenen Fassung die Betonung der Möglichkeit von Sicherheitsnachweisen mit Hilfe von Betriebserfahrung, das Sicherheitshandbuch, Änderungen durch den Betreiber, die deutlichere Herauskehrung der verschiedenen Betrach-tungen von kontinuierlich arbeitender und auf Anforderung arbeitender Software, sowie verteilten Systeme und Zugriffe von außen. Die bei der Datenübertragung verwendeten Verfahren können auch bei der Verifikation von Betriebserfahrung verwendet werden und damit Genehmigungsaufwand sparen.

1. Erfordernis der Neufassung

Die Norm IEC 61508 wurde 1998 herausgegeben. Sie besteht aus sieben Teilen, von denen erste drei normativ sind, während die anderen erklärenden Charakter haben. Teil 1 beschäftigt sich vorwiegend mit Systemanforderungen, Teil 2 vor allem mit Hardware und Teil 3 mit Software. Gegenüber früheren Normen ist das Kennzeichen dieser Norm die Einführung probabilistisch definierter Sicherheitsstufen (Safety Integrity Levels, SILs). Sie soll gewährleisten, einerseits bei hohen Sicherheitsanforderungen nicht zu wenig an Sorgfalt aufzuwenden, andererseits bei niedrigen nicht zu viel.

Der Software-Teil ist von jeher heftig umkämpft gewesen. Angesichts des stetigen Vordringens von Software in neue Bereiche halten ihn viele auch für einen besonders wichtigen Teil. Wegen der regen Nachfrage nach dieser Norm wird ihre routinemäßig übliche Neufassung seitens der IEC nachdrücklich verlangt; zudem erfordert der technische Fortschritt die Einbeziehung neuer Gegebenheiten.

Im folgenden werden einige wichtige Punkte der Neufassung dargestellt. Die Darstellung ist naturgemäß unvollständig. Punkte 3 geht auf einen besonderen Punkt genauer ein.

2. Wesentliche Anforderungen allgemeiner Art

2.1 Sicherheitshandbuch

Es werden Hinweise für die Rechte und Einschränkungen gesucht, die ein Betreiber von sicherheitsrelevanter Software sinnvoller Weise haben sollte wenn er Software umkonfigurieren will. Solche Umkonfigurationen können sich im Laufe des Lebens einer Anlage oder einer Software erforderlich erweisen. Das angestrebte Handbuch soll

darauf eingehen. Es soll auch ganz allgemein Integrationsfragen behandeln, die durch die Zusammensetzung von Software aus bereits zertifizierten Bausteinen entstehen.

Dabei ist auch zu behandeln, *wer* Änderungen vornehmen darf: was etwa dem Anlagen*fahrer* erlaubt ist, was dem Anlagen*ingenieur* und was eine Neuverifikation und -Validation nach sich zu ziehen habe. Selbstverständlich sind dabei die jeweiligen Sicherheitsstufen (SILs) in Betracht zu ziehen, sowie die möglichen Auswirkungen von Änderungen.

2.3 Nicht-Abschaltung, kontinuierliche Regelung und Hilfssysteme

Die Norm soll leichter handhabbar gemacht werden für Anwendungen, die nicht mit der Regelung kontinuierlicher Vorgänge zu tun haben, etwa Dispositionssysteme. Des weiteren sollen Systeme mehr Beachtung finden, die keine sichere Seite haben, wie dies bei Verkehrsmitteln der Fall sein kann. Weiterhin sollen Hilfssysteme stärkere Beachtung finden, die zwar für sich keine Sicherheitsverantwortung tragen, die aber in bestimmten Zusammenhängen Sicherheitsbezug erreichen können, weil sie mit Sicherheitssystemen zusammen arbeiten. Ein Beispiel ist ein Gepäck-Handhabungs-System eines Flughafens. Schließlich ist die

2.4 Evidenzgrade

Derzeit ist zu wenig darüber ausgesagt, wann eine Behauptung als erwiesen angesehen werden darf. Wann etwa ist ein Spezifikation vollständig, wann ein Entwurf fehlerfrei, ein Test bestanden? Die anzustrebenden Kriterien sollen sowohl von der Sicherheitsstufe abhängen, als auch von der Software-Komplexität, von der vorliegenden Information und von der jeweils eingesetzten Methode.

3. Authentisierung und Kryptographie

Im Zuge der Fortentwicklung des elektronischen Handels in seinen verschiedenen Formen ist die Frage des Zugriffschutzes von Daten, die über ungeschützte Netze übertragen werden, wichtig geworden. Von den im kommerziellen Bereich gewonnenen Erfahrungen gilt es nun im sicherheitsbezogenen Rechnereinsatz Gebrauch zu machen. [ITSEC] gibt beispielsweise an, wie ein System zu klassifizieren sei, [RFC 2459] nennt Verschlüsselungsverfahren und [ISO/IEC10118] beschreibt Algorithmen zur Authentisierung.

3.1 Verteilte Systeme

Sicherheitsbezogene Software ist nicht nur in einzelnen stationären Anlagen zu finden, sondern auch in flächig oder räumlich verteilten Systemen, etwa bei Eisenbahnanwendungen oder im Flugverkehr. Für die Zukunft zeichnet sich der Wunsch ab, neue Software-Versionen für einzelne Anlagen von zentraler Stelle aus aufzuspielen.

Die hierbei durch Verfälschungen von Programmen und Daten möglichen Probleme müssen in überschaubaren Grenzen gehalten werden. In vielen Fällen wird es gelingen, die Datenübertragung und den Zugriffschutz auf interne Software von der Sicherheit

einer Anlage zu trennen indem man eine Rückfallebene einbaut; eine solche ist aber nicht immer möglich.
Vermutlich wird verlangt werden:

- Konsequente Einhaltung der Normen bezüglich des Elektronischen Handels, unter anderem der jeweiligen Signaturgesetze
- Berücksichtigung der Zugriffschutz-Fragen über den gesamten Lebenszyklus des Systems hinweg
- Einführung einer eigenen Zugriffschutz-Stufung (einer Threat-SIL(?)), die nicht probabilistisch, sondern deterministisch zu definieren ist, etwa nach [ITSEC]
- Implementation wesentlicher Funktionsteile in Hardware bzw. ASICS
- Berücksichtigung der Anlagen-Lebensdauer, regelmäßige Zugriffschutz-Revisionsprüfung
- Berücksichtigung der Anforderungen aufgrund elektronischer Kriegführung (electronic war fare)
- Trennung von Sicherheits-Funktionen und Zugriffschutz-Funktionen
- Überwachung der Einbruchs-Unversehrtheit und Meldung eventueller Einbrüche

3.2 Vorbenutzte Software

Ein zunehmend drängender Wunsch ist, Kosten bei der Genehmigung von Software einzusparen, indem man die mit Programmen bereits gesammelte Erfahrung mit heran zieht. Dies ist aber nur dann auf solider Grundlage möglich, wenn man sicher ist, eine ungeänderte Software vor sich zu haben. Die in [ISO/IEC10118] und [RFC 2459] dargestellten Verfahren eignen sich auch, um dies nachzuweisen. Man kann beispielsweise einen Hash-Wert eines Programms errechnen und ihn mit dem privaten Schlüssel des Herstellers signieren. Will man die Herstellungsgeschichte mit dokumentieren und den jeweils befassten Gutachter mit in die Pflicht nehmen, so geht dies, wie etwa [Daf98] beschreibt.

Zu berücksichtigen ist ferner, dass die Anforderungsprofile der alten und der neuen Umgebung abweichen. Wie man zwischen verschiedenen Anforderungsprofilen umrechnen kann, ist bei [Ehr02] angegeben.

3.3 Konfigurationsmanagement

Im Zusammenhang mit der Umkonfiguration von Software beim Betreiber treten ebenfalls Authentisierungsfragen auf. Sie nehmen die Gestalt an, *wer wo was dürfe*. Eine entsprechende Dokumentation verlangt nicht nur eine klare Zuordnung der verwendeten Software-Teile, sondern auch der Personen, die Eingriffe vorgenommen haben.

In vielen Fällen geht es nicht nur um die schließlich zu installierende Software, sondern auch um die

4. Schlußbemerkung

In vielen der oben genannten Probleme spielt die Frage eine Rolle, wann Software als *einfach* betrachtet werden dürfe. Unglücklicher Weise konnte hierzu noch keine brauchbare Definition gefunden werden.

Davon abgesehen aber schreitet die Neufassung der IEC 61508 voran; mit Ergebnissen ist 2004 zu rechnen. Selbstverständlich sind zu jederzeit Wünsche und Hinweise willkommen.

Literaturverzeichnis

[IEC 61508] Internationale Elektrotechnische Kommission: Functional Safety of electricsl/electronic/programmable electronic safety-related systems - Part 3: Software requirements, 1998, Reference number CEI/ICE 61508-3:1998

[ITSEC] Bundesamt für Sicherheit in der Informationstechnik: Kriterien für die Bewertung der Sicherheit von Systemen in der Informationstechnik (ITSEC). Vorläufige Form der harmonisierten Kriterien, EGKS-EWG.EAG, Brüssel, Luxemburg, ISBN 92-826-3003-X, 1991

[MT12] IEC SC 65A Maintenance Team 12 Technical Report: Issues arising from application software to appear at IEC 2002

[RFC 2459] Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Jan 1999

[ISO/IEC10118] Information technology - Security techniques - Hash Functions

[Daf98] Dafelmair. F.: Model and Implementation of a Secure SW.Development Process for Mission Critical Software, LNCS 1516, Springer-Verlag Heidelberg, 1998, ISBN 3-540-65110-1

[Ehr02] Ehrenberger, W.: Software Verifikationsverfahren, Carl Hanser Verlag, München 2002, ISBN 3-446-21624-3, 366 Seiten