KAPITEL 13

Kontextfreie SILs

Jan Sanders 2010

13.1 Zusammenfassung

Wir werden zeigen, dass es nicht möglich ist, probabilistische Sicherheitseigenschaften für Baugruppen festzulegen ohne das System zu kennen in dem sie eingebettet werden sollen. Der Prozess der Sicherheitsbewertung einer Baugruppe erschafft einen Kontext in dem die Bewertung Gültigkeit hat. Außerhalb diese Kontext hat die Bewertung keine Aussagekraft. Wir werden außerdem zeigen, dass die Übernahme einer vermeintlich kontextfreien Bewertung nicht notwendigerweise den Aufwand einer Sicherheitsanalyse, bzw. eines Sicherheitsnachweises verringert.

13.2 Einleitung

Wer sicherheitskritische Systeme entwickelt und vertreibt oder betreibt, der muss in Europa den Nachweis erbringen, dass das System ausreichend sicher ist. Neben anderen findet der IEC 61508 Standard breite Verwendung beim Sicherheitsnachweis von sicherheitskritischen Systemen.

Ein Konzept des Standards IEC 61508, der sog. Safety Integrity Level (kurz SIL) und sein Nachweis ist fortwährend Gegenstand von Missverständnissen, Diskussion und Kritik.

Ein SIL beschreibt, kurz gesagt, das Verhältnis von Anwesenheit zu Abwesenheit von Systemversagen welches zu Schaden führt.

Hier werden wir vornehmlich von SILs sprechen, weil sie ein prominentes Beispiel sind. Die Aussagen, die hier über SILs gemacht werden gelten aber ebenso für alle anderen probabilistisch fundierten Sicherheits-Labels.

Der Leser benötigt zum Verstehen dieses Arguments kein tiefes Verständnis des SIL-Konzeptes. Von hier an werden die Sicherheits-Labels allgemein als SLs bezeichnet. Wie werden den Begriff SIL nur dort verwenden wo wir ausdrücklich über SILs reden wollen.

Der Titel dieses Aufsatzes ist eine Anlehnung an eine Diskussion die auf der Safety Crititcal Mailing List [55] statt gefunden hat.

Das Thema SIL und IEC 61508 ist auf der SCML ein immer wiederkehrendes. Es steht immer die Frage im Raum, warum eine Baugruppe, die der Hersteller mit SIL X klassifiziert hat, nicht einfach in ein System integriert werden kann und dort einfach als eine Baugruppe behandelt werden kann die einen SIL von X aufweist.

Wenn dies möglich wäre, dann würde es den Aufwand eines Sicherheitsnachweises sehr erleichtern.

Hersteller von Beugruppen für sicherheitskritische Systeme verwenden vorbestimmte SILs gern als Marketingargument und um die Qualität ihrer Produkte zu unterstreichen.

Dies suggeriert, dass das vom Hersteller bestimmte SIL ohne Weiteres, als Sicherheitseigenschaft der Baugruppe in die Sicherhetsanalyse eines größeren Systems übernommen werden kann.

Wir geben einige Beispiele von Herstellern und Produkten, die mit dem Prädikat eines vorbestimmten SIL vertrieben werden:

- Der TÜV-SÜD-zertifizierte Esterel Code-Generator wird mit SIL 3 nach IEC 61508 [11] beworben: „The SCADE KCG code generator already has been certified by TÜV SÜD to Safety Integrity Level 3 (SIL 3) under IEC 61508“.
- Das sprichwörtliche, SIL-zertifizierte Ventil von [10].
- Der Eagle Logic Solver, ein digitales Kommunikationssystem [8].
- Man wird viele weitere Beispiele finden in dem man einfach seine bevorzugte Internetsuchmaschine nach ”SIL certified” suchen lässt.

13.3 Kontextfreie Bestimmung von Sicherheitslabels (SL)

Zuerst einige Begriffsklärungen.

Der Begriff *SL* bezeichnet eine quantitative Bestimmung des Verhältnisses von Anwesenheit und Abwesenheit von nicht gewolltem Verhalten einer Baugruppe.

Mit *Baugruppe* bezeichnen wir ein Objekt, welches benutzt wird oder gedacht ist, als eine Teil eines größeren Systems.

Wobei ein *System* ein zusammemgesetztes Objekt ist, dessen Gesamtsicherheit analysiert oder gezeigt werden soll.

Kontextfrei bedeutet, das ein SL vergeben wird, ohne Bezug auf ein System in das es eingebettet ist, bzw. ohne eine vollständige Beschreibung eine Systemklasse in der es verwendunge finden kann.

13.4 Das Gegenargument

Nehmen wir an jemand vergibt eine SL an eine Baugruppe.

Dieser Jemand, nennen wir ihn J, sagt, dass

> *es nachgewiesen wurde, dass die Baugruppe X mit dem Sicherheitslabel Y ausgezeichnet wird.*
>
> *Die unabhängige Klassifikationsgesellschaft K hat dies bestätigt und die Baugruppe zertifiziert.*

J wäre schlecht beraten diese Aussage ohne irgendeine Form von Qualitätsnachweis zu machen oder SLs gar willkürlich festzulegen.

Es muss also ein Argument — im philosophischen Sinn [57] — geben, welches die Behauptung stützt. Wir wollen ausdrücklich darauf hinweisen, dass J sich nicht der Arbeit von [57] bewusst sein muss. Aber welche Begründung auch immer hinter der Aussage steht, dass Baugruppe X das Sicherheitslabel Y bekommt, sie kann mit Hilfe von [57] ausgedrückt werden.

Parsons gibt eine Liste von fünf Punkten für ein erfolgreiches Argument [57, S. 171], von denen für uns das erste von Bedeutung ist:

> *Every premise is among the statements assumed in the setting“*

The setting in our case would be the justification for attributing a SaL to an object. Also the setting can be considered the unrefined argument.

Within a refined argument only premises may be used that originate in the setting. Because we are only interested in showing that SaLs cannot be context-free we do not need to examine the other four conditions for successful arguments.

Es muss mindestes eine Prämisse für das Sicherheitsargument geben. Von welcher Art diese Prämisse ist ist für unseren Fall unerheblich. Prämissen könnten quantitative Messungen aus Testreihen sein oder qualitative (Sub-)Argumente warum X die Eigenschaft E hat oder nicht.

Für das SL von Objekt X bedeutet dies, dass das Argument nur innerhalb der Prämissen gültig ist. In anderen Worten: Die Prämissen des Sicherheitsarguments geben den Kontext vor in dem das SL gerechtfertigter Weise anwendbar sist.

Es kann also keine kontextfreien SL geben.

13.5 Bedeutung für die Integration

Der Begriff Vorbestimmtes Sicherheitslabel (VSL) soll von hier an verwendet werden um eine SL zu bezeichnen, welches ein Hersteller für eine Baugruppe vergeben hat ohne, dass die Integrationsumgebung der Baugruppe bekannt oder abzusehen war.

Wenn die Baugruppe in ein System integriert wird, dann kann das System, also die Umgebung der Baugruppe, vollständig konsistenz zum VSL sein.

Dann ist es die Aufgabe des Integrators nachzuweisen, dass

1. die Umgebung der Baugruppe mit den Prämissen des VSL vereinbar ist

   oder,

2. dass Inkonsistenzen nicht das VSL Argument ungültig machen.

In hinreichend komplexen Systemen ist der Erfolg die beiden Punkte oben nachzuweisen nicht absehbar. Es grenzt an Glücksspiel zu versuchen den Nachweis von (1) und (2) zu erbringen.

Wenn der Nachweis nicht erbracht werden kann, dass das VSL und die Anforderungen an die Sicherheit eines Systems miteinander übereinstimmen, dann muss der Systemintegrator ein eigenes Argument entwickeln, dass die Integration von X der Sicherheit des Systems genügt.

Um in der Lage zu sein (1) oder (2) nachweisen zu können, muss der Integrator die gesamte Liste der Prämissen kennen, die in die Erstellung des VSL eingeflossen sind. Ohne kann der Nachweis von (1) oder (2) nicht gelingen und muss daher als nichtig angesehen werden. In anderen Worten: Der Nachweis von (1) oder (2) kann nicht nachgewiesen werden, selbst wenn das VSL gültig ist.

13.6 Schlussfolgerung

Es gibt kein Kontext-freies Sicherheitslabel oder Safety Integrity Level. Nichtsdestoweniger gibt es Unternehmen, die Baugruppen mit dem Hinweis auf Konformität mit einem bestimmten SL vertreiben.

Wenn die Baugruppe in ein größeres System integriert wird, wo liegt der Wert eines Sicherheitszertifikats, außerhalb des Marktetingwertes? Was der Anbieter bieten möchte ist eine Baugruppe deren Integration in ein Sicherheitsargument möglichst einfach sein soll.

Nebenher wird versucht mit einem scheinbar vergleichbaren Qualitätsmerkmal die Überlegenheit des eigenen Produktes gegenüber der Konkurrenz zu verdeutlichen. Für einen Ingenieur, der mit dem Nachweis der Sicherheit des Gesamtsystems betraut ist, ist ein VSL keine Hilfe. Es ist nicht immer klar, und hängt stark von der Baugruppe und dem Gesamtsystem ab, ob ein VSL eine Hilfe ist oder nicht.

Der Aufwand die Verwendbarkeit des VSL nachzuweisen ist nicht zwangsläufig niedriger, als der Aufwand die Sicherheit der Baugruppe im Gesamtsystem nachzuweisen. Ein Ingenieur der diese Einwände ignoriert entwickelt keinen gültigen Sicherheitsnachweis des Gesamtsystems. Ein Anbieter der den Käufer einer Baugruppe nicht mit den gesamten Prämissen, die zur Rechfertigung des verliehenen SL dienen, versorgt hilft seinem Kunden nicht. Wenn etwas schief geht werden die Lücken im Sicherheitsnachweis schnell offensichtlich werden.