Interview

SONDERDRUCK

06-2013

Computer & AUTOMATION

Fachmedium der Automatisierungstechnik

Safety unter Linux?

Das Open Source Automation Development Lab (OSADL), eine internationale Genossenschaft zur Unterstützung von Open Source Software in der Industrie, hat ein Projekt mit dem Namen SIL2LinuxMP gestartet. Ziel ist die Zertifizierung von Linux-basierten Systemen für den Einsatz im Safety-Umfeld. OSADL-Geschäftsführer Dr. Carsten Emde und Nicholas Mc Guire, Koordinator der entsprechenden Aktivitäten, erläutern die Hintergründe.

❑ *Herr Dr. Emde, was genau hat die OSADL dazu bewogen, das Projekt SIL2LinuxMP ins Leben zu rufen?*

■ **Emde:** Die OSADL wurde vor sieben Jahren gegründet. Obwohl zunächst der Fokus auf Linux und dessen Echtzeit-Eigenschaften lag, kamen schon bald andere Themen hinzu. Und so stand bereits im Jahre 2007 auch das Thema Zertifizierung auf der Tagesordnung, was zur Gründung der Safety Critical Working Group unter Leitung von Nicholas Mc Guire geführt hat.

Ursprünglich war die Idee, dass diese Arbeitsgruppe sich weiterentwickeln und schließlich auch über die Kompetenz verfügen würde, aktiven Support bei der individuellen Zertifizierung von Safety-Systemen mit Open Source Software zu liefern. Aber damit haben wir das Potenzial der Arbeitsgruppe wohl überschätzt.

Tatsächlich kann ein so komplexes und anspruchsvolles Projekt wie die Sicherheits-Zertifizierung eines kompletten GNU/Linux-Systems nur in einem formal geregelten Projekt mit klaren Vorgaben erfolgen. Und es war rasch klar, dass ein solches Projekt nicht einfach aus der pauschalen Dienstleistungsumlage der Mitglieder finanzierbar ist, sondern dass die Teilnehmer an einem solchen Projekt, die am Ende ja auch ein TÜV-Zertifikat für die spezifizierte Hardware/Software-Kombination erhalten, einen eigenen finanziellen Beitrag leisten müssen.

Carsten Emde, OSADL: „Sowohl die Industrie als auch wir betreten bei diesem Thema Neuland."

❑ *Wofür steht die Abkürzung MP im Projektnamen?*

■ **Mc Guire:** Traditionell kommen für Safety-Systeme Single-Core-Prozessoren zum Einsatz; die Ära dieser Prozessoren geht aber zu Ende und wir wollten von vornherein klarstellen, dass wir auch

Nicholas Mc Guire: „Wir sind zuversichtlich, dass eine Zertifizierung praktisch machbar ist."

auf Multi-Core beziehungsweise Multi-Processing setzen. Also steht SIL2-LinuxMP für SIL2-Zertifizierung von Linux mit Support für Multi-Processing.

❏ *Safety-Zertifizierung von Open Source Software – geht das überhaupt?*

■ **Mc Guire:** Das war lange Zeit nicht klar. Die Frage, wie Open Source im Safety-Umfeld konkret zu behandeln ist, war bestenfalls in der EN 50128 zur Qualifizierung von Software für Bahnanwendungen gut ausgeführt; in der IEC 61508 Ed 1 war dies hingegen sehr unscharf formuliert und daher mit einem relativ hohem Risiko behaftet. Erst die EN 50128 Ed 2 hat Open Source unmissverständlich als „pre-existing software" definiert und damit offiziell benannt und anerkannt. Und mit der Ed 2 der IEC 61508 ist nun auch festgelegt, dass „pre-existing software" jene Software-Komponenten betrifft, die nicht speziell für das in Entwicklung befindliche System geschrieben wurden und nicht den im Standard festgelegten Anforderungen an den Entwicklungsprozess gefolgt sind – und dies trifft natürlich perfekt auf Open Source Software zu.

Viel wichtiger als die reine Begriffsklärung ist aber, dass die Methodik zur Verifizierung der funktionalen Sicherheitseigenschaften von „pre-existing software" nun explizit ausgeführt wurde und damit erstmals ein klarer Pfad für den Nachweis der funktionalen Sicherheit definiert ist. Dies ist deshalb so wichtig, weil es hilft, das Erfolgsrisiko einer derartigen Zertifizierung besser abzuschätzen.

Nicht zuletzt wurde auch das Konzept der „systematic capabilities" eingeführt, das vorher zwar schon existierte, aber noch keinen Eingang in einen generischen Standard gefunden hatte. Die „systematic capabilities" erlauben es, eine bestimmte Komponente so zu spezifizieren, dass diese in ein Gesamtsystem unter Berücksichtigung der funktionalen Sicherheit eingebunden werden kann, ohne dass eine allumfassende Neubetrachtung der Komponente nötig ist. Mit diesem Schritt hat sich die IEC 61508 von einem monolithischen zu einem modularen Safety-Standard weiterentwickelt. Gerade diese Entwicklung ist für das SIL2LinuxMP-Projekt von großer Bedeutung und gibt uns die Zuversicht, dass eine Zertifizierung praktisch machbar ist.

❏ *Wie sieht das Konzept der angepeilten Zertifizierung konkret aus?*

■ **Emde:** Bei dem in enger Zusammenarbeit mit Spezialisten vom TÜV Rheinland und dem TÜV Süd sowie vielen anderen Safety-Experten initiierten Vorhaben handelt es sich um ein Zweiphasenkonzept, bei dem sowohl allgemein verwendbare als auch individuelle Materialien bereitgestellt werden. Der Grund hierfür: Während zum Beispiel der Linux-Kernel kein differenzierendes Know-how enthält und daher problemlos sogar mit dem Mitbewerber ausgetauscht werden kann, betrifft eine Sicherheits-Zertifizierung auch Know-Bereiche, die in den Safe des jeweiligen Unternehmens und nicht ins Internet gehören. Ergo haben wir die Arbeiten, die für die Zertifizierung erforderlich sind, in zwei Bereiche aufgeteilt.

Die allgemein verwendbaren Materialien werden in einem Community-Prozess ähnlich wie Open Source Software gemeinsam entwickelt. Dadurch reduziert sich der Aufwand erheblich, und wir können die enormen Vorteile des öffentlichen Peer-Reviews nutzen. Bei diesen Materialien handelt es sich in erster Linie um Methoden, Argumente und Anforderungen. Im Gegensatz dazu können individuelle Materialien, die sich auf Details der eingesetzten Hardware und Software beziehen und die im Zusammenhang mit dem jeweiligen Safety-Case stehen, vertraulich behandelt werden. Hierfür steht dann natürlich auch kein Community-Prozess zur Verfügung.

❏ *Welche Herausforderungen waren und sind grundsätzlich zu lösen, um die Voraussetzungen für eine Safety-Zertifizierung unter Linux zu schaffen?*

■ **Mc Guire:** Aus jetziger Sicht sehen wir kein grundsätzliches Gegenargument, warum ein GNU/Linux-System nicht für SIL2 zertifiziert werden kann. Die wesentlichen funktionalen Eigenschaften, die ein GNU/Linux-System mitbringt, sind standardisiert – zum Beispiel POSIX.1-2001 oder die Single Unix Specification V3. Die Frage, die sich stellt, ist also nicht, ob GNU/Linux geeignet ist, sondern ob die Funktionen, die von den Safety-relevanten Applikationen genutzt werden, auch so implementiert sind, wie der Standard es vorschreibt.

Bei den Herausforderungen sind technische und prozedurale Aspekte zu unterscheiden: Technisch gesehen bringt GNU/Linux hervorragende Voraussetzungen mit. Dies bezieht sich auf die starken Anlehnungen an weit verbreitete und akzeptierte Standards und an die Fülle an etablierten Tools. Außerdem ist es eine große Stärke von Linux, dass viele Entwickler überall auf der Welt ihr Wissen und Können für die Linux-Entwicklung zur Verfügung stellen. Nicht zuletzt ist klar geregelt und einfach nachvollziehbar, welche

„OSADL 2.0"

Bei der Gründung der OSADL eG vor sieben Jahren stand zunächst die Idee im Vordergrund, gemeinsam Open Source Software für Embedded-Systeme zu entwickeln und auf diese Weise sowohl den Mitgliedern Kosten zu sparen als auch vom Peer-Review einer großen Expertengemeinschaft zu profitieren. Nachdem dieses Ziel erreicht ist, haben sich im Dezember 2012 etwa 20 OSADL-Mitglieder zu einem Strategie-Workshop getroffen und als Ergebnis die Ausweitung der OSADL-Geschäftstätigkeit zu einem Allround-Service-Provider für Open Source Software in Embedded-Systemen angeregt. Wesentliche Schritte auf diesem Weg sind inzwischen gegangen:

- Anmietung eigener Labor- und Geschäftsräume im Technologiepark Heidelberg,
- Beschäftigung von weiteren eigenen und freien Mitarbeitern für Vertrieb und Entwicklung
- sowie Entwicklung eines eigenen Produkt-Portfolios mit zur Zeit drei wesentlichen Angeboten: Qualitäts-Kontrolle von Embedded-Systemen in der OSADL QA-Farm, Rechtssicherheit bei der Lizenzierung durch das OSADL License Compliance Audit (LCA) sowie Engineering- und Consulting-Angebote im Zusammenhang mit der System-Integration von Embedded-Systemen mit Open Source Software.

Komponente warum und durch wen eingebracht wurde – Stichwort „traceability“. Hinzu kommt, dass der Prozess für die Aufnahme von Schlüsselkomponenten sehr strikt ist. Dies gilt für den Kernel selbst, aber auch für den Compiler und die Bibliotheken.
Auf der prozeduralen Seite hingegen ist noch viel zu tun – Linux wurde eindeutig nicht nach einem Safety-Standard entwickelt. Es müssen also die Schwächen des Prozesses analysiert werden; eventuell sind Gegenmaßnahmen einzuleiten. Dies kann zusätzliche Analysen erfordern, aber es ist auch denkbar, dass Funktions-Wrapper eingeführt oder Nutzungseinschränkungen auferlegt werden müssen.
Die größte Herausforderung für SIL2LinuxMP wird vermutlich sein, einen Funktionsumfang zu definieren, der eine für den Safety-Case optimale Größe hat. Er darf nicht zu klein sein, damit nicht Safety-relevante Funktionalität ausgespart wird; aber er darf auch nicht zu groß sein, damit keine unnötige Komplexität entsteht.

❏ *Das Projekt zielt zunächst auf SIL2-Lösungen. Was ist notwendig, um Linux auch für SIL3 zu ertüchtigen?*

■ **Emde:** Die Frage ist sehr treffend formuliert – es ist tatsächlich eine Ertüchtigung nötig, um mit vertretbarem Aufwand SIL3 argumentieren zu können. Ein möglicher Weg könnte darin bestehen, durch die Bereitstellung von in unserer QA-Farm und im Feld gewonnenen langfristigen Betriebsdaten eine Höherqualifizierung zu erreichen. Aber im Gegensatz zur SIL2-Zertifizierung, die wir für absolut machbar halten, ist dies aus heutiger Sicht keineswegs ein gesicherter Plan. Lassen Sie uns also erst einmal das SIL2-Projekt zum Laufen bringen und den Spatz in der Hand halten. Dann kümmern wir uns um die Taube auf dem Dach.

❏ *Wie sieht die genaue Roadmap des Projektes aus?*

■ **Emde:** Stand der Planung ist ein 18-monatiger Prozess. Bei unserem ersten Treffen mit Vertretern des TÜV Rheinland haben wir das Gefühl bekommen, dass dies sicher ein ehrgeiziges Ziel ist, aber nicht völlig abwegig. Wann wir starten können, ab wann also die 18 Monate gerechnet werden können, kann ich Ihnen allerdings nicht sagen. Das Projekt beginnt in dem Moment, in dem die Finanzierung gesichert ist. Wir gehen von einem Finanzierungsbedarf in Höhe von insgesamt 320.000 Euro aus. Vier Fünftel dieser Summe übernehmen sogenannte „Full Participants“, das heißt Firmen, die Hardware und Software spezifizieren und am Ende des Projekts Anrecht auf ein TÜV-Zertifikat haben. Den Rest teilen sich „Reviewing Partners“ und OSADL zu gleichen Teilen. Wenn wir mal annehmen, dass wir vier „Full Participants“ und vier „Reviewing Partners“ gewinnen können, kämen jeweils 64.000 Euro für erstere und 8.000 Euro für letztere an Kostenbeteiligung auf die Unternehmen zu.

❏ *Die Modalitäten der Gemeinschaftsentwicklung sind in einem „Letter of Intent“ festgelegt – was genau fordert dieser von den Unterzeichnern?*

■ **Mc Guire:** Das Unternehmen erklärt hier definitiv seine Bereitschaft, am Projekt mit der angegebenen Aktivität – entweder als „Full Participant“ oder als „Reviewing Partner“ – teilzunehmen. Wenn die erwartete Anzahl an Teilnehmern nicht zustande kommt oder sich keine Mehrheit für den gewünschten Standard ergibt, entfällt die Verpflichtung. Nur Teilnehmer mit der Aktivität „Full Participant“ können ihre Anforderungen in Bezug auf Hardware und Software spezifizieren und erhalten am Ende des Projekts im Erfolgsfall ein vom TÜV Rheinland ausgestelltes Zertifikat.

❏ *Wie viele Unternehmen beziehungsweise Organisationen haben diese Absichtserklärung bereits unterzeichnet? Welche Namen können Sie nennen?*

■ **Emde:** Aktuell*) liegen definitive Teilnahme-Erklärungen von einem „Full Participant“, zwei akademischen Teilnehmern und zwei Zertifizierungsstellen – dem TÜV Rheinland und dem TÜV Süd – vor. Mit den industriellen Partnern ist verabredet, dass wir die Namen der Teilnehmer frühestens publizieren, wenn das Projekt offiziell gestartet sein wird. Dies hat unter anderem auch mit vertraglich zugesicherten Vereinbarungen unserer Teilnehmer gegenüber deren Kunden zu tun. Aktive Teilnehmer am Projekt erfahren natürlich grundsätzlich die Namen der anderen Partner.

❏ *Worin sehen Sie denn die Gründe für die doch sehr zögerliche Resonanz auf die Thematik? Ein „Full Participant“ momentan ist ja nicht gerade viel!*

■ **Emde:** Hier müssen beide Seiten wohl noch lernen. Die Industrie muss auf der Managementebene ein wenig umdenken, um ein derartiges Projekt mitzutragen – dabei geht es vermutlich in erster Linie gar nicht um die Bereitstellung des finanziellen Beitrags, sondern darum, dass hier Neuland zu betreten ist. Auch auf unserer Seite handelt es sich durchaus um Neuland, was die Größe und die organisatorischen Abläufe anbelangt. Aber wenn nicht wir ein solches Projekt in Angriff nehmen, wer soll es denn tun?
Und sollte das Projekt wider Erwarten nicht zustande kommen, werden wir dennoch viele wichtige Erfahrungen gesammelt haben. Wenn es aber gelingt, ist dies sicher ein bedeutsamer Meilenstein auf dem Erfolgsweg von Open Source Software in der Industrie. *gh*

*) Anm. d. Red.: zum Redaktionsschluss Mitte Mai

Safety-Zertifizierung von Open Source Software? Geht das überhaupt?

- → **Was sagen Zertifizierungsstellen dazu?**
- → **Welche Safety Integrity Level (SIL) sind überhaupt möglich?**
- → **Muss das jeder für sich machen oder gibt es einen Community-Ansatz?**
- → **Welche Standards kommen in Frage?**

Kommen Ihnen diese Fragen bekannt vor, und haben Sie bisher keine Antwort gefunden?
Dann schließen Sie sich am besten dem SIL2LinuxMP-Projekt bei OSADL an.

Weitere Informationen zum OSADL SIL2Linux MP-Projekt finden Sie auf www.osadl.org.

Dieses Zertifikat schafft Vertrauen.

Sie setzen Linux in Ihren Produkten ein?
Ja, sicher!

Sie erfüllen alle Lizenzbedingungen der GPL und LGPL?
Auch sicher?

Das OSADL License Compliance Audit (LCA) überprüft zuverlässig, ob alle Lizenzbedingungen eingehalten werden. Sollten Lücken existieren, hilft OSADL doppelt:

Sie erhalten:
1. konkrete Vorschläge, um diese Lücken zu schließen, und
2. klare Konzepte, die betroffenen Prozesse zu optimieren.

Mehr Informationen zum OSADL LCA finden Sie auf lca.osadl.de oder senden Sie uns eine E-Mail mit Ihren Fragen an info@osadl.org.

open source meets industry
osadl.org

OSADL
Open Source Automation Development Lab eG

Open Source Automation Development Lab (OSADL) eG
Im Neuenheimer Feld 583, 69120 Heidelberg
Telefon: +49 (0) 6221 98504-0
www.osadl.org, info@osadl.org