

SONDERDRUCK

# A *Computer &* AUTOMATION

Fachmedium der Automatisierungstechnik



TITEL:

**NACHGEHAKT  
BEI DR. CARSTEN EMDE -  
DAS SAFETY-PROJEKT  
UNTER LINUX**

# Das Safety-Projekt unter Linux

Im Juni vergangenen Jahres hatte die Organisation OSADL (Open Source Automation Development Lab) angekündigt, ein Projekt zur Zertifizierung von Linux-basierten Systemen für den Einsatz im Safety-Umfeld starten zu wollen (siehe Computer&AUTOMATION, Ausgabe 06/2013, Seite 37ff). Wie weit ist dieser Plan gediehen? OSADL-Geschäftsführer Dr. Carsten Emde bezieht Stellung.

□ *Herr Emde, nach der Ankündigung des Projektes „SIL2LinuxMP“ Im Juni 2013 ist es ruhig um das Thema Safety unter Linux geworden. Ist das Thema noch aktuell beziehungsweise sind Sie im Plan?*

■ **Emde:** Ja, das Thema ist noch aktuell; obwohl ich zugeben muss, dass wir den Zeitbedarf für Prüfung und Akzeptanz unseres Vorhabens zu optimistisch eingeschätzt haben. Die aktuelle Versionsnummer 11 des ‚Letter of Intent‘ spricht sicher Bände. Aber der Zeitrahmen steht, und aus heutiger Sicht halten wir einen Start noch 2014 für realistisch, was einen Abschluss bis 2016 ermöglichen würde.

□ *Was konkret ist in den vergangenen 14 Monaten passiert?*

■ **Emde:** Hinter den Kulissen hat sich einiges getan. Unter anderem sind hier zwei Dinge zu nennen: Erstens sind unsere Bedenken, ARM-Plattformen einzusetzen, in der Zwischenzeit weitgehend zerstreut worden. Dies hat damit zu tun, dass in Frage kommende Prozessoren wie zum Beispiel AM335x oder i.MX6 vor einem Jahr nur mit einem so genannten Vendor-Kernel betrieben werden konnten. Dafür haben wir uns ein adäquates Mapping auf konformante Entwicklungsprozesse nicht zugetraut. Dies hat sich Ende des letzten Jahres mit der Verfügbarkeit des Linuxkernels in der Version 3.12 drastisch geändert; denn ab dieser Version laufen die genannten ARM-Prozessoren ohne großen Aufwand direkt auf dem Mainline-Kernel. Zweitens sind – auch ohne dass das eigentliche Projekt gestartet wurde – einige der benötigten Vorarbeiten getätigt worden. Unter anderem ist hier die Mitwirkung des TÜV Süd zu nennen, der wesentliche Impulse gegeben hat. Zur Erinnerung: Vom TÜV Süd und vom TÜV Rheinland

liegen Bestätigungen zur Projektteilnahme vor. Letzterer wird die Zertifizierung vornehmen.

□ *Als Finanzierungsbedarf nannten Sie damals 320.000 Euro, welcher maßgeblich von vier ‚Full Partnern‘ mit je 64.000 Euro sowie von weiteren vier ‚Reviewing Partnern‘ mit jeweils 8.000 Euro gestemmt werden sollte. Haben Sie diese Firmen mittlerweile zusammen bekommen?*

■ **Emde:** Inzwischen haben drei ‚Full Partner‘ den Letter of Intent verbindlich unterschrieben, und zwar die Firmen A&R Tech in Wien, BMW Car IT in München und Sensor-Technik Wiedemann in Kaufbeuren. Darüber hinaus haben wir eine vertragliche und drei schriftliche Zusagen

für insgesamt vier ‚Reviewing Partner‘. Soweit wir wissen, sind außerdem weitere Firmen aktuell im Entscheidungsprozess.

” **Hinter den Kulissen hat sich einiges getan.** “

□ *Steht damit nun der eigentliche Startschuss für die Projektdurchführung unmittelbar bevor?*

■ **Emde:** Ja, davon gehen wir aus.

□ *Bei den Namen der ‚Full Partner‘ fällt auf, dass es sich ausnahmslos um Unternehmen handelt, die primär auf dem Fahrzeugsektor unterwegs sind. Die klassische Fertigungsindustrie zeigt offenbar nach wie vor wenig Interesse am Thema Safety unter Linux?!*

■ **Emde:** Darüber haben wir auch schon nachgedacht. Vielleicht liegt es daran, dass die klassischen Automatisierer, deren Anlagen zertifizierungspflichtig sind, bereits über funktionsfähige Lösungen verfügen und diese erst einmal amortisieren wollen. Die ISO 26262 in der Fahrzeugindustrie ist dagegen erst jetzt aktuell geworden. Hinzu kommt, dass in der Fahrzeugindustrie ein Umbruch in



Richtung autonomer Systeme stattfindet, wodurch fundamental höhere Anforderungen an die Rechenleistung und Komplexität der Programme gestellt werden, die Entwicklungskosten aber nicht steigen dürfen. Und genau dadurch entsteht jetzt die Forderung nach einem „Open Source Realtime“-Betriebssystem mit Multicore-Support, wofür GNU/Linux RTOS zur Zeit offensichtlich erste Wahl ist – fehlt ‚nur noch‘ die Zertifizierung.

□ *Vorausgesetzt der Projektstart erfolgt im September – wie sieht der konkrete Projektablauf dann aus?*

■ **Emde:** Zunächst werden in Zusammenarbeit mit den TÜVs die erforderlichen Prozesse entwickelt. Voraussichtlich werden nicht wenige davon unter eine freie Lizenz – zum Beispiel Common Creative - gestellt. In dieser

Phase sollte aber auch schon an den jeweiligen Plattformen gearbeitet und der Codeumfang festgelegt werden. Überspitzt gesagt müssen wir 17 Millionen Zeilen Code auf unter 100.000 Zeilen herunterverhandeln.

Am Ende der ersten Phase wird es spannend. Dann erwarten wir nämlich vom TÜV Rheinland eine Stellungnahme, ob die bis dahin erarbeiteten Prozesse sowie die jeweiligen Plattformen mit einer ausreichenden Wahrscheinlichkeit eine Chance zur erfolgreichen Zertifizierung haben. Wenn ja, geht es weiter mit Phase 2, sprich der eigentlichen Zertifizierung. Wenn nein, brechen wir ab, und alle Teilnehmer erhalten die Hälfte der eingezahlten Projektkosten zurück. OSADL's Vision für die Zukunft des Einsatzes von Open Source im Safety-kritischen Umfeld: Mit dem SIL2LinuxMP-Projekt verfolgt OSADL zunächst die Absicht, die Zertifizierbarkeit von Linux am praktischen Beispiel nachzuweisen. Darüber hinaus soll aber auch ein dem Stand der Technik entsprechender wiederholbarer Prozess etabliert werden, so dass zertifizierte Linux-Systeme in Zukunft zur Normalität werden. gh

## Open Source Automation Development Lab (OSADL) eG

Im Neuenheimer Feld 583

D-69120 Heidelberg

Telefon: +49 6221 98504 0

Telefax: +49 6221 98504 80

info@osadl.org – www.osadl.org



# 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 SIL2LinuxMP-Projekt finden Sie auf [www.osadl.org](http://www.osadl.org).



Open Source Automation Development Lab (OSADL) eG  
Im Neuenheimer Feld 583, 69120 Heidelberg  
Telefon: +49 (0) 6221 98504-0  
[www.osadl.org](http://www.osadl.org), [info@osadl.org](mailto:info@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](http://lca.osadl.de) oder senden Sie uns eine E-Mail mit Ihren Fragen an [info@osadl.org](mailto:info@osadl.org).



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