# Life Cycle Support und Security-Monitoring

Embedded Open Source-Systeme profitieren von den enormen Entwicklungskapazitäten und der Innovationskraft der Open Source Community. Um diese Vorteile optimal nutzen zu können, braucht man jedoch auf Ebene der Geräte-Software ein geeignetes Wartungs- und Weiterentwicklungskonzept.

Die Geräte und Anlagen aus ganz unterschiedlichen Zielbranchen haben in der Regel einen Lebenszyklus, der – zum Teil auch deutlich – oberhalb von fünf Jahren liegt. Immer häufiger sind sie in Weitverkehrs-Netzwerke eingebunden und müssen branchenüblichen Zertifizierungsanforderungen oder IT-Compliance-Anforderungen der Betreiber genügen.

Im Rahmen von Wartungsvereinbarungen hält emlix nicht nur Entwickler-Kapazitäten vor, die mit dem konkreten Software-System vertraut sind. Zum Leistungsumfang gehört auch das kontinuierliche Monitoring der relevanten Communities, Mailinglisten und weiterer Informationsquellen für sämtliche in der Software enthaltenen Open Source-Komponenten.

## Security- und Maintenance-Report

Einmal monatlich erhält jeder Wartungskunde einen Maintenance- und Security-Report, in dem für sein System relevante Updates, Bugs bzw. Bugfixes und weitere Patches im Überblick dargestellt werden.

Sie sind jeweils versehen mit einer Empfehlung für resultierende Maßnahmen: Ein Sicherheits-Bug kann den konkreten Anwendungskontext eines Gerätes gar nicht betreffen oder einen Bugfix beim kommenden planmäßigen Release sinnvoll erscheinen lassen oder aber auch ein sofortiges Ausrollen einer gefixten Software-Version erforderlich machen.

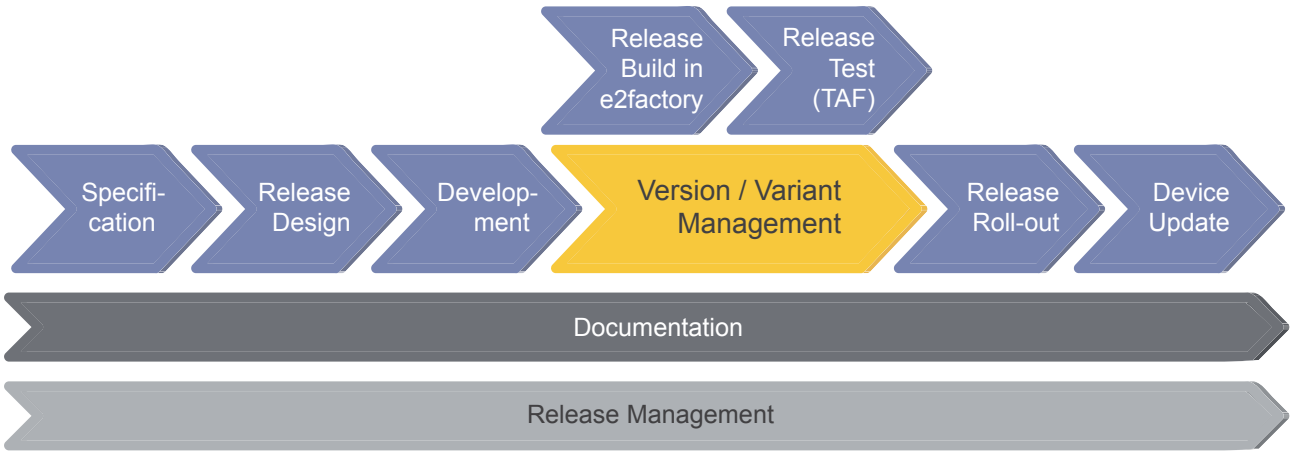
## *Kontinuierliches Security-Monitoring*

Grundsätzlich wird emlix nur nach Abstimmung tätig und führt niemals unabgestimmt Modifikationen an der Software durch. Des Weiteren wird einmal monatlich die Integrität der Software und des Build-Prozesses überprüft.

## Änderungsverfolgung

Neben Neuerungen in der Community können beispielsweise die Anpassung an neue Hardware-Revisionen aufgrund von Bauteilabkündigungen, die Integration neuer Features oder endkundenspezifische Erweiterungen im Rahmen eines Wartungsvertrages umgesetzt werden.

Sämtliche Änderungen, die in der Wartungsphase an den Software-Komponenten vorgenommen werden, sind reproduzierbar und ebenso versioniert wie der Bauprozess selbst. Damit sind typische Anforderungen an die Rückverfolgbarkeit („traceability“) erfüllt.




*Bei netzwerkintegrierten Produkten sind regelmäßige Sicherheits-Updates unumgänglich. Um aufwändige Rezertifizierungen zu vermeiden, ist dazu gerade in der Medizintechnik ein valides Software Management obligatorisch.*

Die gesamte hierfür notwendige technische und Prozess-Infrastruktur kann im Anschluss an eine Wartungsvereinbarung an den Kunden übergeben werden, sodass er unabhängig von emlix diesen Prozess mit eigenen Kapazitäten fortsetzen kann.

Zusätzlicher Bestandteil eines Wartungsvertrages kann auf Wunsch eine Subscription für das emlix Test Application Framework (TAF) mit dem projektrelevanten Testset sein. Dies ermöglicht den Projektingenieuren beim Kunden, unabhängig von emlix regelmäßige, automatisierte Testzyklen zu fahren und weitere Tests in das Framework zu integrieren.

Eine Wartungsvereinbarung stellt auch sicher, dass der Know how-Transfer zwischen emlix und dem Entwickler-Team beim Kunden nicht abreißt. Gerade in Feldtest- oder frühen Markteinführungsphasen können in diesem Rahmen auftretende Probleme sofort gemeinsam beurteilt und behoben werden.

## emlix GmbH

solutions @ emlix.com
http://www.emlix.com

Phone +49 (0) 551 / 30664-0
Fax +49 (0) 551 / 30664-11

# Konsolidierung von Linux-Systemen

In Unternehmen, die schon längere Zeit Embedded Linux-Systeme verwenden, sind häufig mehrere unterschiedliche Hersteller- und Community-Distributionen sowie eigene Zusammenstellungen im Einsatz. Hier kann es lohnend sein, diese Linux-Systeme zu konsolidieren und Build- und Software Management-Prozesse zu vereinheitlichen. Resultat ist in der Regel ein „Kern-Linux-System“, das zentral gewartet und beispielsweise mit Bugfixes versehen werden kann, sowie daraus abgeleitete BSPs für konkrete Geräte.

Typische Ziele einer solchen Konsolidierung sind:

- die Dokumentations-, Wartungs- und Weiterentwicklungsaufwände zu minimieren
- durch Transparenz und gute Dokumentation die Personen-Abhängigkeit zu reduzieren
- „zentrale“ Bugfixes und Paket-Updates für eine ganze Produktfamilie
- die Anpassungsaufwände der Embedded Linux-Plattform für ein neues Produkt zu minimieren
- gegebenenfalls Zertifizierungs- und Rezertifizierungsaufwände zu reduzieren
- eine weitgehende Hardware-Abstraktion und damit Unabhängigkeit von einem Hardware-Hersteller
- größtmögliche Transparenz bezüglich der im Unternehmen verwendeten Embedded Linux Systeme

Ziel ist es, dass sich Software-Plattformen über ihren Lebenszyklus kostenminimal an die Anforderungen des zu entwickelnden Produktes anpassen können. Mehraufwände und Risiken, die aus der wiederholten Anpassung, der häufig fehlenden Dokumentation und der hohen Komplexität einer Distribution oder eines Hersteller-BSPs resultieren, werden ausgeschlossen.