emlix
embedded linux systems

Embedded Linux Security

Hersteller, Integratoren und Betreiber von Industrieprodukten müssen im Kontext Industrie 4.0, Industrial Internet und Cyber Security vermehrt neuen gesetzlichen und marktlichen Anforderungen genügen. Die IT- und Systemsicherheit und die sichere M2M-Kommunikation werden damit wettbewerbsrelevant.

emlix bietet anpassbare Systemkomponenten zur Steigerung der Systemsicherheit für industriell genutzte Embedded Linux-Systeme. Hinzu kommen Tools und Prozesse, um die erreichte Sicherheit über den gesamten Produktlebenszyklus aufrecht erhalten zu können.

Skalierbare Sicherheitslösungen

Das Spektrum von emlix Security-Lösungen reicht von der Anlagenvernetzung mit „industriellem Basisschutz“ bis hin zum Hochsicherheitssystem. Die definierte Security muss dabei wirtschaftlich und skalierbar, aber auch wartbar sein.

Security Komponenten

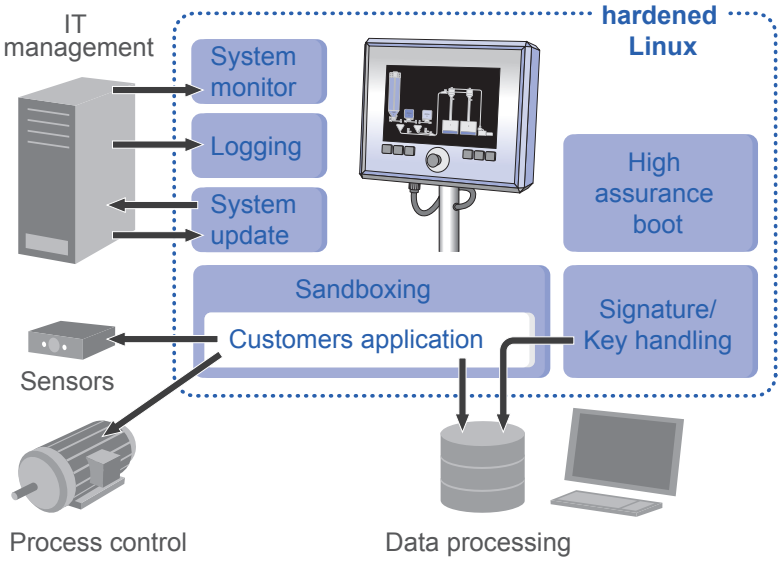
Für die Entwicklung neuer Produkte bieten unsere adaptierbaren Security Komponenten zentrale, vorkonfigurierte Bausteine zur schnellen und wirtschaftlichen Umsetzung einer sinnvollen Systemsicherheit.

Durch die Nutzung von Mainline-basierten Komponenten bieten die emlix-Lösungen Investitionssicherheit und sind leicht wartbar: Innovationen und Fixes aus der Community können direkt übernommen werden.

Die verfügbaren Security Komponenten umfassen unter anderem:

- Infrastruktur für gehärtete Linux-Systeme
- Secure Boot für Integrität des Linux und der Anwendung
- Sandbox-Umgebung und Container-Konzepte zur Isolation von Anwendungen
- Sichere Interprozesskommunikation
- Verschlüsselte Diagnosedaten interner Systemzustände
- Verschlüsselte Logs zu Ereignissen wie Wartungszugriffen
- Abgesicherte Netzwerkanbindung
- Infrastruktur für signierte Security Patches
- Verfahren zur Integritätsprüfung von Updates
- Automatisierte Tests der Systemintegrität

In enger Zusammenarbeit mit dem Kunden werden diese an die individuellen Anforderungen des jeweiligen Produkts und Einsatzkontextes angepasst.



emlix
embedded linux systems

Security Monitoring

Das emlix Security Monitoring unterstützt Sie in der Betriebs- und Wartungsphase von Embedded Linux-basierten Industrieprodukten bei der Aufrechterhaltung eines definierten Sicherheitsstatus.

Wir überwachen hierzu relevante Informationsquellen sowie Security Findings (CVEs, Common Vulnerabilities and Exposures) und bewerten mögliche Risiken vor dem Hintergrund des produktspezifischen Einsatzkontextes und Risikoprofils Ihres Produktes. Ein Security Report gibt Ihnen konkrete Empfehlungen für Sicherheits-Patches und Updates.

Das IT-Sicherheitsgesetz fordert ein Security Lifecycle Management für Industrial Control Systems (ICS). Das Security Monitoring sichert diesen Prozess ab.

Das IT-Sicherheitsgesetz fordert ein Security Lifecycle Management für Industrial Control Systems (ICS). Das Security Monitoring sichert diesen Prozess ab.

Zielsetzung ist, relevante Security-Fixes, neue Software-Versionen und Verbesserungen relevanter Komponenten zeitnah zu identifizieren und daraufhin zu prüfen, ob und wann sie ins Produktivsystem übernommen werden müssen (Security Patch Management).

Unser Build Automation System e2factory gewährleistet dabei Nachvollziehbarkeit dieser Änderungen und ermöglichen eine definierte Systemsicherheit für Board Support Packages.

Security Review

Für eine Bewertung der System- und Netzwerksicherheit eines Open Source-basierten Industrieproduktes bieten wir ein differenziertes Security Review an. Dazu werden entsprechende Netzwerktests und eine Analyse der eingesetzten Linux Software-Plattform durchgeführt. Neben einer Analyse des Ist-Zustandes der Produkt-Sicherheit sowie Hinweise zu Risiken gehören konkrete Empfehlungen zum Leistungsumfang.

Industrieprodukte werden durch Betreiber verstärkt auf IT-Sicherheit geprüft. Ein Security Review hilft, Sicherheitslücken vorab zu erkennen und zu schließen.

Industrieprodukte werden durch Betreiber verstärkt auf IT-Sicherheit geprüft. Unser Security Review hilft, Sicherheitslücken vorab zu erkennen und schließen.

Das Security Review orientiert sich dabei an industriellen Best Practices. Entwicklung, Produktmanagement und Marketing unserer Kunden sollen in die Lage versetzt werden, den aktuellen Entwicklungsstand vor dem Hintergrund von Kundenwünschen hinsichtlich „Cyber Security“, „Embedded IT Compliance“ oder „Industrial Security“ zu bewerten.

Ein emlix Scurity Review umfasst unter anderem die folgenden Leistungen:

- Analyse des Produktes und seines Einsatzumfeldes
- Durchführung von Netzwerk- und Schnittstellentests
- Analyse der verwendeten Software-Pakete und CVEs
- Bewertung der verwendeten Softwarearchitektur und -basis

Die Reviewergebnisse werden in einem Bericht mit konkreten Handlungsempfehlungen zusammengefasst. Den Abschluss bildet stets die Bewertung von Risiken und Abwehrmaßnahmen zusammen mit Entwicklern und Produktmanagern des Kunden.

emlix GmbH
solutions @ emlix.com
http://www.emlix.com
Phone +49 (0) 551 / 30664-0
Fax +49 (0) 551 / 30664-11