

Embedded Software im Anlagenbetrieb

Wie Hersteller den Software-Lifecycle managen



Embedded Software begleitet industrielle Anlagen über ihren gesamten Lebenszyklus. © Revenera/FreePik, lizenzfrei

Industriemaschinen laufen oft Jahrzehnte – die darin integrierte Software verändert sich jedoch kontinuierlich. Für Hersteller entsteht daraus eine neue operative Herausforderung: Software muss über den gesamten Lebenszyklus einer Anlage transparent, konsistent und revisionssicher verwaltet werden.

Embedded-Systeme in industriellen Maschinen sind typischerweise auf lange Einsatzzeiten von zehn bis zwanzig Jahren ausgelegt. In dieser Zeit bleibt die Hardware weitgehend konstant, während sich die darauf laufende Software mehrfach ändert. Sie ist längst kein bloßes Zubehör mehr, sondern ein zentraler Faktor für Funktionalität, Sicherheit und Verfügbarkeit im laufenden Betrieb.

Mit der zunehmenden Integration von KI verschärft sich diese Abhängigkeit weiter. KI-basierte Funktionen lassen sich im industriellen Umfeld nur dann skalieren, wenn Software- und Systemzustände eindeutig definiert und reproduzierbar sind. In manchen Fällen fehlt es an konsistenten Softwareständen und Systemkontext, auf denen KI sinnvoll aufsetzen kann.

Zentrale Steuerungsebene für Software

Um integrierte Software über ihren gesamten Lebenszyklus hinweg nachvollziehbar zu managen, braucht es eine technische Steuerungsebene. Maschinen- und Anlagenhersteller setzen hierfür auf sogenanntes Entitlement Management. Darunter versteht man die zentrale Verwaltung und Durchsetzung von Nutzungsrechten für Softwarefunktionen in Echtzeit. Das Berechtigungsmanagement regelt, welche Softwarefunktionen in welchem Umfang auf welcher

Maschine und für welchen Nutzer freigeschaltet sind – unabhängig davon, ob diese lokal, verteilt oder über Updates bereitgestellt werden.

In der Praxis bildet dies die Grundlage für Lizenzierung, Compliance-Kontrolle und die Monetarisierung von Software. Bei Embedded Software ist diese Form der zentralen Rechteverwaltung auch deshalb relevant, weil industrielle Maschinen heute häufig über eine identische Basissoftware verfügen. Welche Funktionen, Leistungsstufen oder Optionen tatsächlich zum Einsatz kommen, richtet sich nach den Produktionsanforderungen.

Die jeweils benötigten Funktionen lassen sich gezielt freischalten oder upgraden. Eine zentrale Plattform bündelt diese Aufgaben in einer Steuerungsoberfläche, über die Anlagen- und Maschinenhersteller Lizenzen verwalten, Zugriffsrechte steuern, Nutzer authentifizieren und Berechtigungen zuweisen. Der laufende Betrieb in der Produktion bleibt dabei unbeeinträchtigt.

Mehrwert für Anlagenbetreiber

Für Maschinen- und Anlagenhersteller liegt der Nutzen eines zentralen Berechtigungsmanagements auf der Hand: Sie optimieren betriebliche Abläufe, bündeln die Bereitstellung von Softwarefunktionen und behalten den Überblick über die beim Kunden genutzten Varianten. Davon profitieren jedoch auch die Anwender: Ein strukturiertes Entitlement Management verbessert das Service-Level, da Funktionen, Updates oder Anpassungen schneller und gezielter bereitgestellt werden können. Gleichzeitig sinkt der Abstimmungsaufwand zwischen Betreiber und Hersteller, weil Berechtigungen eindeutig definiert und systemseitig nachvollziehbar sind.

Selfservice-Funktionen

Viele Lösungen ergänzen diese Steuerungsebene um Selfservice-Funktionen. Über entsprechende Portale können Anwender Funktionsumfänge einsehen, Zugriffsrechte verwalten oder Erweiterungen

anfordern – teilweise auch unternehmensintern für verschiedene Standorte, Linien oder Nutzergruppen. Das schafft Transparenz über aktive Funktionen, Nutzungsrechte und laufende Kosten.

Fünf Ansatzpunkte für den Betrieb

Im laufenden Betrieb beeinflusst Entitlement Management mehrere zentrale Bereiche gleichzeitig. Die folgenden fünf Ansatzpunkte verdeutlichen, wo diese Steuerung konkret ansetzt und welche operativen Effekte sich daraus ergeben.

1. Skalierbare Performance

Die Auslastung von Anlagen ist in der Praxis selten ein statischer Wert. Taktzahlen, Module und Produktionsmodi unterliegen Schwankungen, Aufträgen und Auslastungsspitzen. Klare Regeln für die Nutzung von Softwarefunktionen ermöglichen es, auf diese Veränderungen planbar zu reagieren. Je nach vertraglichem Rahmen lassen sich höhere Durchsätze, temporäre Kapazitätserweiterungen oder optionale Funktionen gezielt aktivieren – zeitlich begrenzt und unter definierten Bedingungen.

Änderungen am Softwarestand passieren entlang definierter Update- und Freigabepfade. Produktkonfigurationen (z. B. Standard- und Light-Version) lassen sich dynamisch erstellen bzw. vorbereiten, testen und schrittweise einführen, ohne den freigegebenen Grundzustand der Anlage zu verlassen. Genauso wichtig wie das Aktivieren ist das Zurücknehmen (Rollback). Wenn Anpassungen nicht greifen oder Lastspitzen vorbei sind, führen Betreiber die Anlage gezielt auf einen bekannten, freigegebenen Zustand zurück.

2. Systematische Sicherheit

Allein im letzten Jahr meldeten Sicherheitsexperten über 2450 neue Sicherheitslücken in ICS (Industrial Control Systems) bei 152 Anbietern [1]. Damit hat sich die Zahl der Bedrohungen in industriellen Netzwerken nahezu verdoppelt. Ohne klar definierte Softwarezustände gibt es keinen wirksamen Hebel, um solche



© Nicole Segerer

Autorin:
Nicole Segerer
SVP und General Manager
Revenera
www.revenera.de

Cyberangriffe zu managen. Sicherheitsmeldungen, Herstellerhinweise oder Ergebnisse aus Security-Tools lassen sich eindeutig zuordnen:

- Welche Anlagen sind betroffen?
- Welche Softwarekombination ist im Einsatz?
- Wo besteht tatsächlich Handlungsbedarf?

Security-Updates werden nicht isoliert ausgerollt, sondern immer im Kontext freigegebener Systemzustände bewertet. Betreiber aktivieren Patches nur dort, wo der Hersteller die jeweilige Kombination geprüft und freigegeben hat. Auch Zugriffs- und Nutzungsrechte folgen diesem Prinzip. Fernzugriffe, Schnittstellen oder Diagnosefunktionen sind nur dort aktiv, wo sie explizit erlaubt sind – zeitlich begrenzt, anlagenbezogen oder zweckgebunden. Dauerhaft offene Systeme werden zur Ausnahme. Die Angriffsfläche in vernetzten OT/IT-Umgebungen schrumpft messbar.

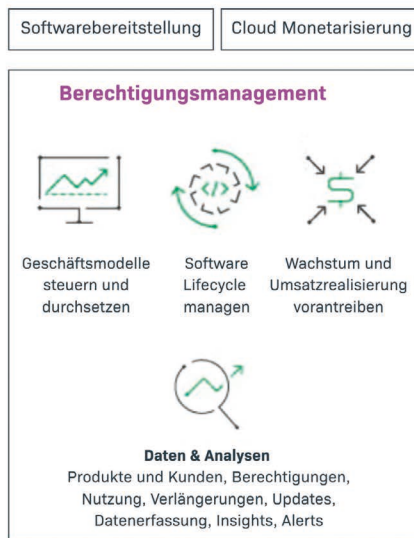
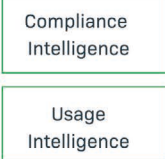
3. Auditfähig im laufenden Betrieb

Hersteller von Software müssen Compliance sicherstellen und jederzeit wissen, über welche Software- und Funktionsausprägungen der Betreiber einer Anlage verfügt. Ziel ist es, Übernutzung zu vermeiden und das Kosten-Nutzen-Verhältnis im Sinne eines fairen Kundenservices zu gestalten. Auf Betreiberseite geht es darum, im laufenden Betrieb auditfähig zu sein und aufwendige nachträgliche Lizenzprüfungen (True-ups) zu vermeiden.

Transparenz über die vertraglichen Nutzungsbedingungen ist daher das A und O. Eine eindeutig definierte Referenz für den zulässigen Funktionsumfang bildet den dokumentierten Soll-Zustand, auf den Betreiber jederzeit zurückgreifen können, statt Versionen oder Funktionen im Nachhinein rekonstruieren zu müssen. Updates, Funktionsfreischaltungen und sicherheitsrelevante Anpassungen erfolgen auf dieser Grundlage ausschließlich nach expliziter Freigabe. Interne Audits und externe Prüfungen stützen sich damit auf konsistente Systeminformationen, sodass Compliance nicht nur punktuell nachgewiesen, sondern dauerhaft im laufenden Betrieb verankert ist.



Usage Analytics



Portal Kunden- / Anlagenbetreiber

Lizenzierung

Cloud / Lokal



Entitlement-Management: Lizenzierung, Bereitstellung, Aktualisierung und Analyse auf Basis von Berechtigungen,
© Revenera

4. Transparente Kostenkontrolle

Nach einer Revenera-Umfrage [2] planen mehr als die Hälfte der Softwareanbieter, innerhalb der nächsten 18 Monate neue Geschäftsmodelle einzuführen. Im Zentrum stehen nutzungsbasierte Ansätze wie Pay-per-Use oder Pay-per-Outcome. Abgerechnet wird nicht mehr pauschal, sondern entlang tatsächlicher Nutzung oder erzielter Ergebnisse.

Gerade bei Embedded Software gewinnt diese Logik massiv an Bedeutung. Doch nutzungsbasierte Modelle funktionieren nur, wenn Nutzung eindeutig messbar und technisch kontrollierbar ist. Anbieter müssen wissen, wofür sie abrechnen. Betreiber müssen jederzeit nachvollziehen können, wofür sie zahlen. Ohne saubere Steuerung zehrt das Modell – nicht betriebswirtschaftlich, sondern operativ.

Entitlement Management liefert die technische Grundlage, um Nutzung und Kosten auf beiden Seiten transparent abzubilden. Es definiert präzise, welche Kosten durch welche Nutzung entstehen. Gleichzeitig ermöglicht es hybride Modelle: Ein Abonnement deckt die Grundnutzung einer Maschine ab, zusätzliche Funktionen oder Leistungsspitzen lassen sich über Prepaid-Kontingente flexibel aktivieren – etwa zur Abdeckung saisonaler Lasten oder kurzfristiger Produktionsanforderungen (Elastic-Access-Model).

Auch neue KI-Funktionen lassen sich so zunächst testweise nutzen und erst bei nachweislichem Mehrwert dauerhaft aktivieren – ohne langfristige Kostenfolgen.

5. Sauber aufgesetzte Maintenance

Im laufenden Betrieb liefert eine zentrale Verwaltung der Software- und Funktionszustände eine verlässliche Übersicht darüber, welche Software und Funktionen zu einer Anlage gehören. Diese Transparenz verändert Wartung und Service grundlegend. Service-Teams arbeiten nicht länger mit Annahmen, sondern mit überprüfbaren Zuständen. Sie erkennen sofort, welche Software-, Betriebssystem- und Hardwareebenen betroffen sind – und welche nicht. Die saubere Trennung dieser Ebenen reduziert Fehlkonfigurationen, beschleunigt Fehleranalysen und verkürzt Serviceeinsätze messbar.

Auch bei Instandhaltungs- und Retrofit-Entscheidungen entsteht dadurch eine belastbare Grundlage. Betreiber sehen auf einen Blick, welche Anlagen softwareseitig erweiterbar sind, wo technische oder lizenzielle Grenzen liegen und welche Maßnahmen wirtschaftlich sinnvoll bleiben. Entscheidungen basieren auf reproduzierbaren Systemzuständen – nicht auf projektspezifischen Sonderlösungen oder historisch gewachsenen Ausnahmen.

Fazit

Wer industrielle Anlagen heute noch ohne klar definierten Software-Sollzustand betreibt, verzichtet auf Kontrolle. Ein systematisch aufgesetztes Berechtigungs- und Entitlement Management macht Embedded Software im Feld steuerbar – technisch, wirtschaftlich und organisatorisch. Es entscheidet darüber, ob sich Maschinen gezielt weiterentwickeln lassen oder als Legacy-Systeme in historisch gewachsener Komplexität erstarren.

Wer schreibt:

Nicole Segerer ist General Manager von Revenera, Anbieter von Lösungen für Softwaremonetarisierung, Compliance und Nutzungsanalyse. Sie ist Experte für Monetarisierungsmodelle für Software, SaaS und IoT-Unternehmen. Mit ihrem Team unterstützt sie Softwareanbieter und IoT-Hersteller bei der Umstellung auf neue Geschäftsmodelle und der Optimierung der Softwaremonetarisierung und Compliance. ◀

Referenzen

[1] Cycle Research & Intelligence Labs (CRIL) Annual Threat Landscape Report 2025

[2] Revenera Monetization Monitor 2026 Outlook: Software Monetization Models and Strategies