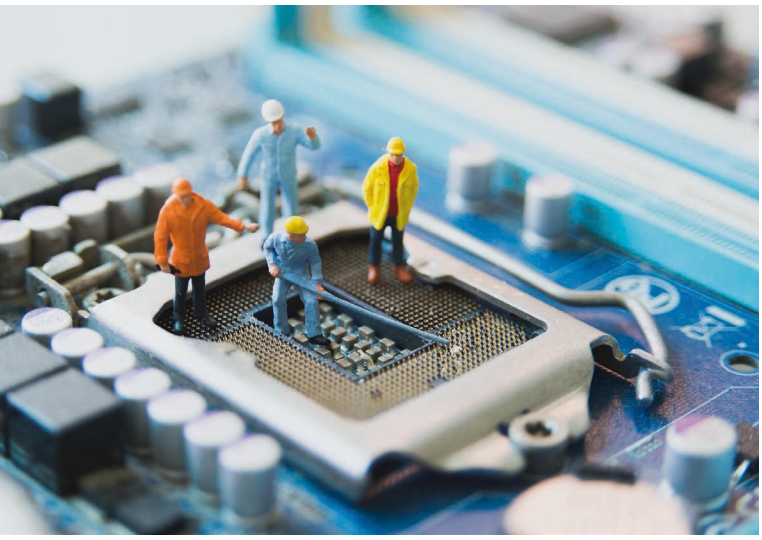
# Wenn ein USB-Stick das (größte) Risiko ist

***IT-Technologien für die OT-Welt***



In der Industrie prallen zwei Welten aufeinander, die nicht unterschiedlicher sein könnten: OT und IT. Damit Fertigungsstraßen effizienter und sicherer werden, braucht es einen neuen Ansatz – nämlich Software-definiert, containerisiert und KI-gestützt. Nur so lassen sich alle Aufgaben entlang des Lebenszyklus-Managements optimieren und automatisieren.

*Autor:*
*Stefan Bergstein*
*Chief Architect Manufacturing*
*Red Hat*
*www.redhat.com/de*

Ein USB-Stick für sicherheitsrelevante Patches? Was sich in der IT-Welt nach einem Relikt aus vergangenen Zeiten anhört, ist in der OT-Umgebung durchaus noch Realität. Denn die Fertigungsstrukturen im Shopfloor sind teilweise über Jahrzehnte gewachsen und werden nur angefasst, wenn unbedingt notwendig. Änderungen gelten allgemein als Risiko, Upgrades finden im besten Fall im Rahmen eines geplanten Stillstandes statt. Hinzu kommt, dass Maschinen unterschiedlichster Hersteller im Einsatz sind. Die haben teilweise ihre ganz eigenen Protokolle, und nicht jeder Controller spricht mit dem anderen.

Die IT dagegen hat in den letzten Jahren eine ziemliche Transformation durchlaufen: Technologien und Ansätze wie Cloud-native Entwicklung, Microservices, Automatisierung und DevOps sind darauf ausgerichtet, Systeme schneller und flexibler zu machen. Die Diskrepanz zwischen beiden Welten führt im Fertigungsalltag zu einer Vielzahl von Problemen. Produktionsdaten bleiben in Maschinen gefangen, statt in betriebsweiten Pipelines zu landen. Updates erfordern manuelles Eingreifen, lokale Freigaben und individuelle Abstimmungen. Jede Linie, jedes Werk, manchmal sogar jede Maschine bildet ein eigenes Ökosystem mit eigener Hardware, eigenem Patch-Stand und eigener Betriebslogik. Das Ergebnis sind unvereinbare Lebenszyklen, die Prozesse verlangsamen und Innovationen ausbremsen, bevor sie überhaupt operative Relevanz entfalten.

## Trennung verhindert ein konsistentes Lifecycle-Management

Was in der IT selbstverständlich ist – Standardisierung, reproduzierbare Deployments und einheitliches Monitoring – ist folglich in der OT nur bedingt möglich. Damit steigt aber auch der Integrations- und Verwaltungsaufwand: Jedes System erfordert Einzelanpassungen, manuelle Konfigurationen und individuelle Schnittstellenlösungen. Gleichzeitig steigt der Modernisierungsdruck angesichts der technologischen Entwicklungen der letzten Jahre. Anwendungen, die früher zentral liefen, wandern näher an die Maschinen. KI-Inferenzen beispielsweise müssen lokal ausgeführt werden, um Latenzen und Verfügbarkeiten sicherzustellen. Digitale Zwillinge benötigen konsistente Datenströme über alle Ebenen hinweg. Generative KI wiederum erfordert einen Zugang zu dokumentiertem, versioniertem und qualitätsgesichertem Unternehmenswissen. Dringend notwendig ist deshalb eine Plattform, die die OT- und IT-Umgebung technisch und organisatorisch miteinander verbindet. Diese Plattform sollte Software-definiert sein, damit die vielen Recheninstanzen in einer Fertigungslinie in einem Cluster konsolidiert werden können.

## Vereinheitlichung

Der Vergleich mit der Automobilindustrie zeigt eindrucksvoll, was eine Vereinheitlichung des technischen Unterbaus bewirken kann. Früher hatten Fahrzeuge dutzende proprietäre Steuergeräte, jedes mit eigener Hardware, eigener Software und eigenem Lebenszyklus. Updates waren aufwendig, teuer und riskant – ein Zustand, der der heutigen Situation im Shopfloor ziemlich ähnelt. Moderne Fahrzeugarchitekturen gehen inzwischen einen anderen Weg: Sie konsolidieren Steuergeräte, zentralisieren Logik und setzen auf Software-definierte Komponenten. Funktionen werden also nicht mehr in Hardware gegossen, sondern als Software verteilt, aktualisiert und erweitert. Dadurch wird das Auto zu einer Plattform, die problemlos skalierbar und damit effizienter ist.

## Software-defined als gemeinsamer Nenner

Von diesem Gedanken profitiert auch die Industrie. Eine Software-definierte Fertigung entkoppelt die Hardware- und Software-Lebenszyklen, sodass die aufwendige Administration und Steuerung einzelner Industrie-PCs und Controller entfällt. Gleichzeitig schafft dieser Ansatz auch die Basis für die Umsetzung einer virtuellen speicherprogrammierbaren Steuerung (vSPS). Physische Geräte für jede einzelne Einheit sind nicht mehr

notwendig, vielmehr läuft eine Software-Steuerung auf einer Serverlösung am Edge. So können neue SPS-Instanzen leichter gewartet werden, wenn es die Produktion erfordert.

## Effizienter Aktualisieren

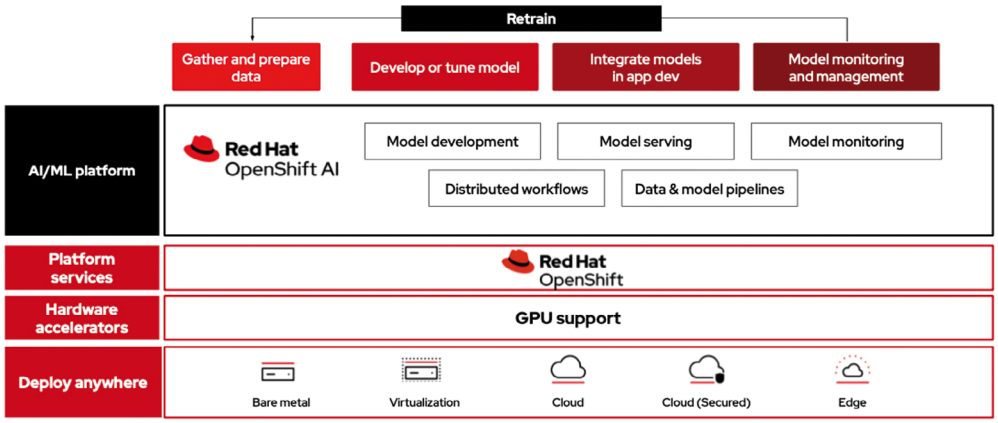
In einer solchen Fertigungsumgebung laufen zudem Wartung und Weiterentwicklung deutlich effizienter ab: Aktualisierungen lassen sich gebündelt und weitgehend automatisiert auf dem gesamten Cluster ausrollen. Die bislang gängige Praxis, einzelne Steuerungen manuell – in manchen Fällen sogar per USB-Stick – zu patchen, entfällt vollständig. Gleichzeitig verkürzt sich die Time-to-Value: Neue Funktionen oder Verbesserungen können als zentrale Services bereitgestellt und sofort im gesamten Cluster aktiviert werden.

## Zusammenführung verteilter Industrie-PCs

Durch die Zusammenführung ehemals verteilter Industrie-PCs entsteht zudem eine homogene Ressourcenlandschaft, die Überkapazitäten reduziert und die vorhandene Rechenleistung besser ausschöpft – ein Vorteil gegenüber fragmentierten Einzelrechnern, die häufig zu groß dimensioniert und deshalb schlecht ausgelastet sind. Darüber hinaus eröffnet die Virtualisierung neue Möglichkeiten in der Systemintegration. Steuerungslogik, die als virtuelle Instanz vorliegt, lässt sich leichter mit MES-, SCADA- oder Qualitätsmanagementsystemen verbinden, da Schnittstellen standardisiert und nicht mehr an die Eigenheiten physischer Hardware gebunden sind. Dies schafft eine flexiblere, besser orchestrierbare Produktionslandschaft.

## Containerisierung vereinfacht den KI-Einstieg

Wenn ein Fertigungsunternehmen auf eine softwaredefinierte Architektur setzt, eröffnet sich der Zugang zu modernen Container-Technologien. Über eine einfache Beschreibungssprache lassen sich Container-Images für Betriebssystem und Applikationsplattform erzeugen. Diese können anschließend automatisiert über die Edge-Infrastruktur verteilt werden. Der entscheidende Vorteil liegt in der Standardisierung: Anwendungen lassen sich als definierte Images ausrollen, Aktualisierungen erfolgen kontrolliert und rückverfolgbar, und das komplette Lifecycle-Management – von der Entwicklung über Tests bis zum produktiven Rollout – wird zum wiederholbaren Prozess. Damit gewinnt die Produktion jene Agilität, die bisher nur in IT-Umgebungen möglich war. Gleichzeitig wird MLOps in der Fertigung zum neuen Standard. Das heißt: KI-Modelle können in Container-Images gepackt und flexibel auf Edge-Geräten, Gateways oder Produktionsservern ausgerollt werden. Innovation lassen sich schnell und sicher in den Shopfloor bringen, ohne jedes Mal ein Risiko in Bezug auf die Stabilität der Produktion einzugehen.




***Mit Red Hat OpenShift AI, einer flexiblen, skalierbaren Plattform, können Fertigungsunternehmen KI-gestützte Anwendungen entwickeln und bereitstellen. © Red Hat***

## Automatisierung

ist wiederum in puncto Sicherheit extrem wichtig. Mithilfe von Frameworks oder Ansätzen wie GitOps lassen sich Sicherheitsrichtlinien zentral definieren und durchsetzen. Das reduziert nicht nur menschliche Fehler, sondern sorgt auch dafür, dass Systeme lückenlos auf dem aktuellen Stand bleiben, um Angriffsflächen gar nicht erst entstehen zu lassen. Eine KI-gestützte Anomalie-Erkennung wiederum hilft dabei, verdächtige Muster in Netzwerk- oder Prozessdaten in Echtzeit zu erkennen. Gegenmaßnahmen können dann automatisch angestoßen werden. Generative KI-Assistenten und Co-Piloten verkürzen zudem Troubleshooting-Zeiten spürbar, weil Maschinendaten und Logfiles kontextbezogen aufbereitet werden.

Ein häufiges Missverständnis ist allerdings, dass Containerisierung automatisch sichere Updates bedeutet. Tatsächlich sind feingranulare Policies erforderlich: Signaturen, Hardware-Root-of-Trust an Edge-Gateways, Rollback-Mechanismen, und - für die Produktion entscheidend - abgestimmte Freigabeschritte, die die Functional Safety abbilden. Werden KI-Modelle eingesetzt, müssen zusätzlich Guardrails implementiert werden, die Halluzinationen verhindern, Eingriffe in Steuerungslogik nur über genehmigte Schnittstellen erlauben und Entscheidungswege auditierbar machen. Grundsätzlich sollten sich Fertiger an den Zero-Trust-Prinzipien aus der IT orientieren.

## Der Weg zur echten OT-Agilität

Eine Software-definierte Plattform ist jedenfalls nicht nur ein technologischer Schritt, sondern ein struktureller. Sie verändert, wie Unternehmen Workloads entwickeln, testen, betreiben und überwachen. Sie schafft eine gemeinsame Sprache zwischen OT und IT, einheitliche Compliance-Mechanismen und eine klare Governance über Zuständigkeiten hinweg. Gleichzeitig erlaubt sie es, bestehende Anlagen weiter zu nutzen, statt sie abzulösen – ein entscheidender Punkt in einer Umgebung mit langen Investitionszyklen.

Vor allem aber löst sie den zentralen Konflikt der industriellen Digitalisierung: Sie verbindet Stabilität mit Innovation. Sie ermöglicht, dass Fertigungsunternehmen ihren hohen Sicherheits- und Verfügbarkeitsanforderungen treu bleiben und dennoch die Geschwindigkeit moderner Softwareentwicklung nutzen können. Damit wird die Produktionshalle zum skalierbaren, digitalen Ökosystem. ◄