

computer & automation

Fachmedium der Automatisierungstechnik

01/02-2026 • 11 € • computer-automation.de

Der Weg zur KI-gesteuerten Anlage



 MathWorks®

Im Fokus: Distribution
**E-Procurement als
Effizienzfaktor**

Radarsensoren
**Dicke und Flächengewicht
gleichzeitig messen**

Systemdesign
**Der Unterbau für
virtuelle Steuerungen**

Retrofit von Industrierechnern

von Stefan Niermann



Bild: NAIMAH/stock.adobe.com/inosoft

Wenn bewährte IPCs in die Jahre kommen, steigt nicht nur das Ausfallrisiko, auch fehlende Sicherheitsupdates werden zum Problem. Ein durchdachter Retrofit kann helfen, bestehende Anlagen wirtschaftlich und regulatorisch konform weiter zu betreiben.

In vielen Produktionsumgebungen sind Industrierechner im Einsatz, die seit zehn oder mehr Jahren zuverlässig ihren Dienst verrichten. In den meisten Fällen läuft auf ihnen eine HMI-Software zur Maschinenbedienung, häufig ergänzt um übergeordnete SCADA-Funktionen. Fällt ein solcher Rechner aus, steht nicht selten eine komplette Maschine oder ein ganzer Fertigungsabschnitt still. Neben dem altersbedingten Ausfallrisiko der Hardware stellt die fehlende Aktualisierung der Betriebssysteme ein zusätzliches Risiko dar.

Egal ob Panel-PC oder IPC mit abgesetztem Display – diese Rechner basieren meist auf dem Betriebssystem Windows sowie einer HMI-/SCADA-Grundsoftware wie VisiWin inklusive einer maschinenspezifischen Applikation und Konfiguration. Diese Komponenten und die daraus resultierenden Risiken sollen im Folgenden betrachtet werden.

Mit zunehmendem Alter der Hardware steigt die Wahrscheinlichkeit eines ungeplanten Ausfalls. Mechanische Komponenten wie Lüfter oder Festplatten unterliegen einem natürlichen Verschleiß, Ersatzteile sind häufig nur eingeschränkt verfügbar. Der Ausfall einzelner Komponenten kann in diesem Fall zum Stillstand der Maschine führen.

Alte Windows-Versionen erhalten keine Sicherheitsupdates mehr und stellen damit ein wachsendes Risiko dar, insbeson-

dere wenn sie direkt oder indirekt mit anderen Systemen vernetzt sind. Vor dem Hintergrund regulatorischer Anforderungen wie dem Cyber Resilience Act (CRA) wird deutlich, dass der Weiterbetrieb veralteter Betriebssysteme langfristig keine tragfähige Option mehr ist.

Der Kauf eines neuen Rechners mit aktuellem Betriebssystem und ein Software-Upgrade der bestehenden Anwendung ist nicht in allen Fällen möglich. Wenn über Jahre hinweg mehrere Versionssprünge ausgelassen wurden, lassen sich ältere Applikationen häufig nicht mehr wirtschaftlich oder technisch sinnvoll aktualisieren.

Viele Maschinenbauer bieten aktuelle Rechner als Ersatzteil an. Das ist die einfachste Lösung, da alle im Folgenden beschriebenen Gesichtspunkte bereits bedacht wurden und man ein lauffähiges System geliefert bekommt. Ist dies nicht möglich, wird der Retrofit des Rechners zum zentralen Baustein, um bestehende Anlagen weiterhin sicher betreiben zu können.

Retrofit-Variante 1: Bestehender Rechner, neues Betriebssystem

Wurde die vorhandene Hardware bereits erneuert, verfügt jedoch noch über ein veraltetes Windows-System, kann zunächst ein Betriebssystem-Upgrade in Betracht gezogen

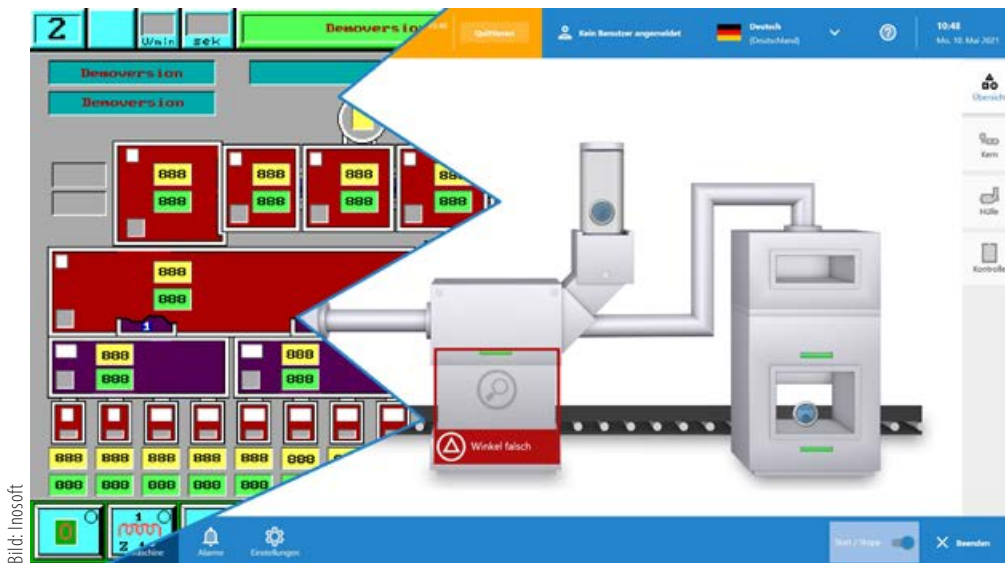


Bild: Insooft

Neben IT-Sicherheitsaspekten ist auch die Modernisierung der HMI- und SCADA-Oberfläche ein zentraler Anlass für Retrofit-Projekte in der industriellen Automatisierung.

werden. Ziel ist es, wieder einen unterstützten Windows-Stand zu erreichen.

Dabei sind mehrere Punkte kritisch zu prüfen. Zum einen muss die Leistungsfähigkeit des Rechners ausreichend sein, um ein modernes Betriebssystem stabil zu betreiben. Zum anderen stellen Treiber ein häufig unterschätztes Problem dar: Proprietäre Hardwarekomponenten, etwa spezielle Kommunikationskarten oder I/O-Erweiterungen, verfügen unter Umständen nicht mehr über kompatible Treiber für aktuelle Windows-Versionen. Sind keine geeigneten Treiber verfügbar, ist diese Retrofit-Variante technisch nicht umsetzbar.

Retrofit-Variante 2: Neuer Rechner mit aktuellem Betriebssystem

In vielen Fällen ist ein vollständiger Austausch der Rechnerhardware erforderlich. Ein neuer Industrie-PC mit aktuellem Windows kann die Betriebssicherheit erhöhen und eine langfristige Ersatzteilverfügbarkeit verbessern.

Viele ältere Systeme nutzen Schnittstellen wie LPT- oder COM-Ports oder proprietäre Steckkarten, beispielsweise Profibus-Karten für ISA-Steckplätze. Moderne Rechner verfügen in der Regel nicht mehr über diese Anschlüsse. Selbst wenn entsprechende Karten mechanisch noch eingesetzt werden können, ist die Kompatibilität der Systemtreiber häufig nicht mehr gegeben. Die Bereitstellung von COM-Ports über USB-Adapter kann zudem Schwierigkeiten durch verändertes Timing-Verhalten nach sich ziehen.

Diese Schnittstellen wurden vielfach zur direkten Kommunikation mit der angebundenen SPS genutzt. Dies ist eine

INTER NATIONAL



Automation 24/7 on



Bild: Damia/stock.adobe.com



IT-Sicherheit in der industriellen Produktion gewinnt durch regulatorische Vorgaben wie den Cyber Resilience Act zunehmend an Bedeutung.

der wichtigsten Anforderungen, die gelöst werden muss. Da ältere SPSen häufig nicht über Ethernet-Schnittstellen verfügen, muss ein alternativer Kommunikationsweg geschaffen werden. Hier bieten sich Adapterlösungen verschiedener Hersteller an, etwa zur Umsetzung von MPI (Message Passing Interface) auf Ethernet. Solche Adapter ermöglichen es, bestehende Steuerungen weiter zu nutzen, ohne tief in die Maschinenhardware eingreifen zu müssen.

Zentrale Herausforderung: Installation der bestehenden Software

Unabhängig von der gewählten Hardware ist die Übernahme der bestehenden Software meist ein kritischer Punkt im Retrofit-Projekt. Zunächst ist zu prüfen, ob die ursprünglichen Installationsmedien noch vorhanden und lesbar sind. Disketten oder CDs können über die Jahre beschädigt worden sein, zudem besteht die Software häufig aus mehreren getrennten Installationspaketen, die vollständig benötigt werden.

Darüber hinaus ist zu klären, ob die Installationsroutinen selbst noch mit dem neuen Betriebssystem lauffähig sind. Ältere Setups setzen häufig veraltete Installer-Technologien oder Systemfunktionen voraus, die in aktuellen Windows-Versionen nicht mehr verfügbar oder aus Sicherheitsgründen deaktiviert sind.

Ist die Software installiert, folgt die Übertragung der maschinenspezifischen Applikation oder zumindest der zugehörigen Konfigurationsdaten. Dabei ist zu prüfen, ob die Daten noch vorhanden und unverändert genutzt werden können.

Im nächsten Schritt wird getestet, ob die Software korrekt startet und stabil läuft. Ältere Anwendungen greifen häufig auf Verzeichnisse zu, die unter aktuellen Sicherheitsrichtlinien nicht ohne Weiteres beschreibbar sind. Auch zusätzliche Software-Komponenten, etwa für Datenbankzugriffe oder Kommunikationsdienste, müssen kompatibel sein.

Nicht zuletzt spielt die grafische Darstellung eine Rolle. Viele ältere Applikationen wurden für geringe Bildschirmauflösungen entwickelt. Auf modernen Displays belegen sie dann nur die obere linke Ecke, oder es kommt zu unschönen Skalierungseffekten beziehungsweise Darstellungsfehlern, die die Bedienbarkeit beeinträchtigen.

Lizenzierung – oft nicht bedacht, aber wichtig

Ein weiterer Aspekt beim Retrofit ist die Lizenzierung der bestehenden Software. In der Praxis existieren unterschiedliche Verfahren – von hardwarebasierten Lizenz-Dongles am LPT-Port bis zu Lizenzmechanismen, die ursprünglich von Disketten in ein FAT-Dateisystem übertragen wurden.

Solche Verfahren funktionieren auf modernen Systemen häufig nicht mehr. Teilweise können Dongles ersetzt oder Lizenzmechanismen auf andere Schutzmechanismen umgestellt werden, sofern der Hersteller entsprechende Optionen anbietet. In anderen Fällen ist dies nicht möglich. Daher sollte frühzeitig geprüft werden, ob alle notwendigen Lizenzschlüssel vorhanden sind und technisch weiter genutzt werden können.

Neuerstellung als Alternative

Alle bisher beschriebenen Möglichkeiten nutzen die bestehende Software auf dem alten Stand. Diese wird häufig nicht mehr vom Hersteller unterstützt und muss gegebenenfalls von der Außenwelt abgeschottet werden. Wenn dann noch der Aufwand für den Erhalt der bestehenden Software unverhältnismäßig hoch wird, kann eine Neuerstellung der Applikation die sinnvollste Alternative sein. Sie erfordert zwar das größte Budget, bietet aber gleichzeitig den größten Nutzen.

Das Ergebnis ist ein aktueller Softwarestand mit aktivem Herstellersupport. Inhalte und Struktur können überarbeitet, nicht mehr benötigte Funktionen entfernt und Bedienkonzepte angepasst werden. Zudem können alternative Architekturansätze geprüft werden, etwa der Einsatz von Linux als Betriebssystem in Kombination mit Container-Technologien wie Docker. Beispielsweise kann der VisiWin Cross-Platform-Server als Container bereitgestellt und bei Bedarf durch eine andere Version ersetzt werden. Sollte ein Rollback auf die Vorgängerversion notwendig sein, erfolgt dieser durch Austausch des Containers. In Verbindung mit gängigen Administrations- und Orchestrierungswerkzeugen lassen sich Aktualisierungen strukturiert durchführen.

Fazit

Eine veraltete Hard- und Softwareumgebung stellt ein erhebliches technisches und organisatorisches Risiko dar. Industrierechner und eingesetzte Software müssen daher regelmäßig auf Aktualität und Sicherheitslücken geprüft werden. Hersteller sind verpflichtet, Schwachstellen zu beheben, Betreiber müssen verfügbare Updates jedoch auch zeitnah installieren. Diese Anforderungen sind ein zentraler Bestandteil des Cyber Resilience Act und setzen stets aktuelle Softwarestände voraus. ag



Stefan Niermann

ist Head of Business Development und Prokurist bei Inosoft.