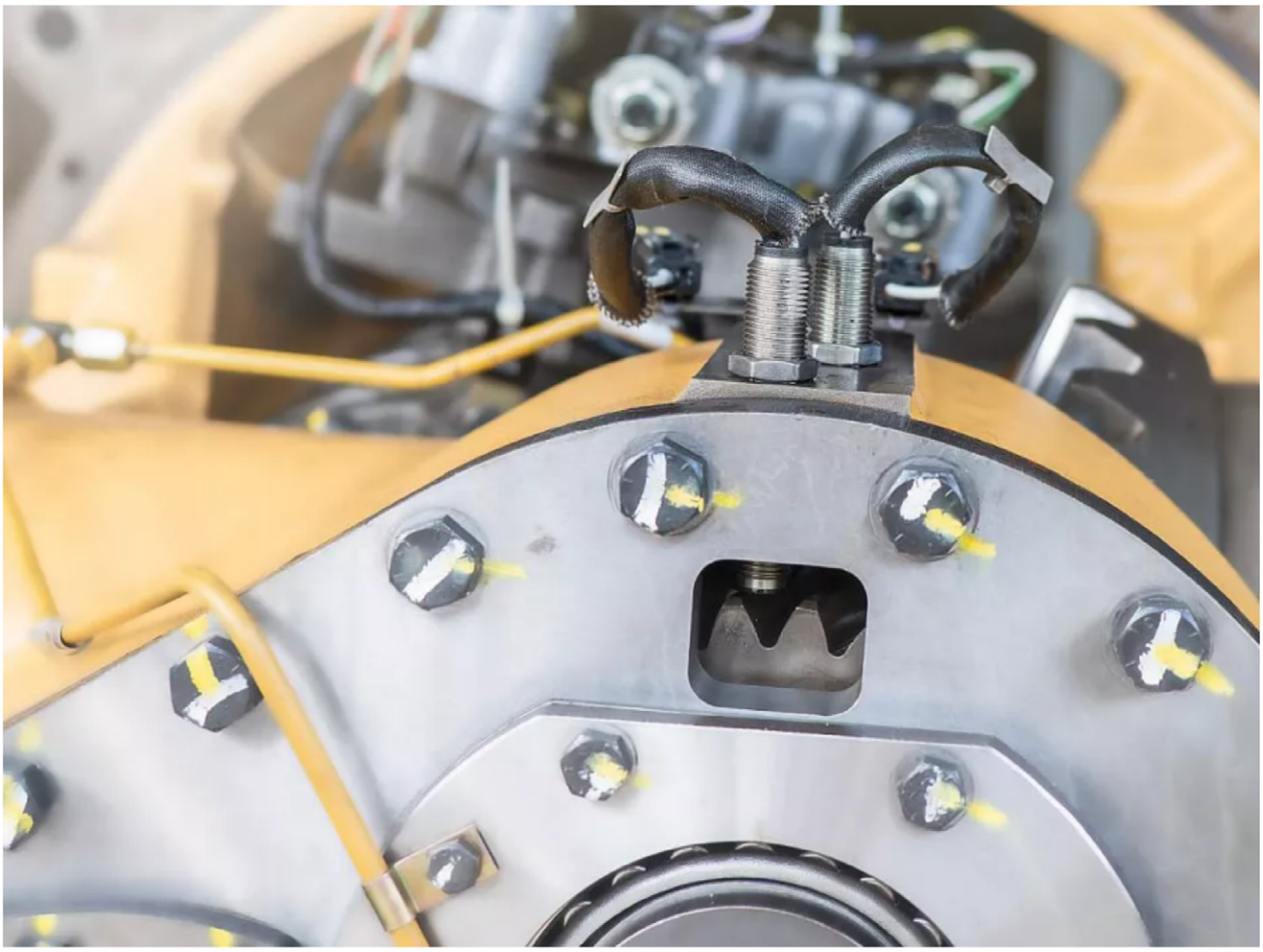
Wirtschaft

25. Jul. 2022 | 09:51 Uhr | von Siegfried Müller

Kolumne

Per Retrofit sicher zukunftsfähig werden

Machen Sie Ihre betagte Maschine per Retrofit tauglich und sicher für die Digitalisierung, rät unser Kolumnist Siegfried Müller. Denn so können Bestandsanlagen auch in Zeiten der Digitalisierung effektiv weiter betrieben werden.



Auch an schon länger betriebenen Maschinen ist ein Retrofit - wie hier, mit neuer Sensorik - sehr oft ein lohnendes Unterfangen. (Bild: Kanemme6 - stock.adobe.com)

War früher alles besser? Erscheint einem bisweilen so, denn Retro als kulturelle Strömung ist gerade wieder sehr en vogue – in der Mode, bei Spielzeug und natürlich auch bei Möbeln. Doch was verbirgt sich tatsächlich dahinter? Retro-Möbeln beispielsweise zeichnen sich dadurch aus, dass hier die Form- und Farbgebung alter Design-Klassiker aufgegriffen wird – also zum Beispiel die organische Ausprägung, die einen Nierentisch ausmacht –, um diese dann zu transformieren. Retro-Möbelstücke sind somit lediglich an das alte Design angelehnt, de facto werden sie neu produziert. Doch was vermutlich bei den meisten – auch diejenigen, die nicht unbedingt für Retro-Klassiker schwärmen – früher mit hoher Wahrscheinlichkeit besser gewesen sein wird, zumindest in der Retroperspektive betrachtet, ist die körperliche Verfassung. Wenigstens bezogen auf Ausdauer und eine gute Kondition. Wer denkt nicht ab und zu, dass er auch schon mal fitter war?

Was ist ein Retrofit?
Bei einem Retrofit (lat. retro - rückwärts und engl. fit - anpassen) wird eine bestehende Anlage oder eine bereits seit längerem eingesetzte Maschine im Hinblick auf nun bestehende Anforderungen nachgerüstet und verbessert. Diese "Modernisierung" von Anlagen ist eine im Vergleich zur Neuanschaffung oftmals monetär günstigere Möglichkeit, Energieeffizienz zu erhöhen, Produktionsqualität zu verbessern, Lebensdauer zu verlängern und aktuelle gesetzliche Vorgaben zu erfüllen. Außerdem sind in vielen Fertigungen bestimmte Maschinen nicht ersetzbar, müssen aber zum Beispiel in die Digitalisierungsmaßnahmen eingebunden werden. Hier kommt nur ein Retrofit in Frage.

Doch Retro ist nicht nur in nahezu allen Bereichen kultureller Produktion anzutreffen, sondern auch im Maschinenbau. Seit mindestens zwei bis drei Jahren taucht dieser Begriff immer häufiger auf – allerdings mit einem Zusatz, nämlich als Retrofit. Gut, mit Bezug auf die eingangs gemachten Erläuterungen stellt sich die Frage, ob diese Begrifflichkeit treffend ist. Andererseits im Sinne der Definition von Fitness im Prinzip vielleicht schon eher – denn sich fit halten führt dazu, im Alltag leistungsfähig zu sein und Belastungen eher standhalten zu können. Genau das ist das anvisierte Ziel: ältere Maschinen via Retrofitting für einen Einsatz im digitalen Umfeld tauglich zu machen.

Mit diesem Ansatz ist es möglich, früher oder später, aber auf jeden Fall absehbar alle Maschinen in vernetzte Produktionsstraßen zu integrieren. Mit hoher Wahrscheinlichkeit viel früher lässt sich das Ziel einer ‚Intelligenten Fabrik' erreichen, da es nicht unbedingt erforderlich ist, die alten Maschinen aufgrund ihrer fehlenden

Konnektivität komplett gegen moderne austauschen zu müssen – was sehr kostenintensiv wäre, sondern die Bestandsanlagen mit entsprechenden Sensoren und geeigneter Kommunikationstechnologie (digital) so aufzurüsten, dass eine Vernetzung möglich ist. Natürlich jeweils abhängig von den individuellen Rahmenbedingungen im Unternehmen ist es somit möglich, durch diese Nachrüstung eine Steigerung der Wirtschaftlichkeit zu erreichen.

Zugleich gibt es vom Grundsatz her noch einen triftigen Grund, der für die adäquate Aufrüstung der Maschinen spricht: die Befähigung zum Erheben von verwendbaren Maschinendaten, die für Analysezwecken erforderlich sind – unter anderem um Prognosen erstellen zu können, zum Beispiel hinsichtlich Verschleißdaten. Auf Basis dieser zusammengetragenen Daten lassen sich im Weiteren Maßnahmen ableiten, etwa zur Qualitätskontrolle sowie -verbesserung oder um Prozesse zu optimieren und dadurch Kosten zu reduzieren.

Mehr Überwachung, aber höherer IT-Sicherheitsbedarf

Daran lässt sich ablesen, dass die – mittels der Sensoren ermöglichte – Erfassung von Daten der Bestandsmaschinen insgesamt ausgesprochen relevant ist. Der daraus resultierende Nutzwert steht in vielerlei Hinsicht außer Frage. Doch das Potenzial lässt sich tatsächlich nur dann vollumfänglich realisieren, wenn ein wichtiger Aspekt dabei Berücksichtigung findet: die Cybersicherheit. Denn mit dem zunehmenden Digitalisierungs- und Vernetzungsgrad steigt das Risiko Opfer eines Cyberangriffs zu werden. Dessen müssen Unternehmen sich bewusst sein und entsprechende Vorbereitungen treffen, unter anderem, indem sie sowohl ihr individuelles Gefährdungspotential analysieren als auch die Wirksamkeit ihrer getroffenen IT-Schutzmaßnahmen daraufhin überprüfen.

Dies fängt bei dem (richtigen) Umgang mit den Daten an. Zu deren Absicherung gibt es konkret eine Fülle von IT-Sicherheitsmaßnahmen, die empfehlenswert sind. Doch vor Erstellung und Umsetzung eines entsprechenden IT-Schutzkonzepts müssen Unternehmen nicht nur erkennen, dass sie über ausgesprochen sensible und wertvolle Daten verfügen, sondern auch genau wissen, wo diese generiert werden. Denn nur auf Basis der daraus resultierenden Erkenntnisse lassen dann im Weiteren adäquate Entscheidungen treffen. Zum Beispiel dahingehend, wie der Zugriff – auch aus der Ferne – auf die Maschinen erfolgen soll oder wie beziehungsweise wo die Daten sicher abgespeichert werden können. In diesem Kontext ist es meiner Meinung nach für Unternehmen elementar, ausgereifte Datensicherheitsrichtlinien abzufassen sowie darüber hinaus ein Verfahren zur Reaktion auf Vor- beziehungsweise Krisenfälle erarbeitet zu haben.

Der Autor Siegfried Müller ist Vice-President Advanced Technologies bei der MB Connect Line GmbH Fernwartungssysteme. (Bild: MB Connect Line)

In Bezug auf die Datensicherheit gibt es bestimmte Maßnahmen, die an vorderster Stelle stehen müssen: Das ist zum einen, die Zugriffsrechte dergestalt zu beschränken, dass der Zugang zu IT-Systemen und Informationen nur autorisierten Mitarbeitern im Rahmen der Erfüllung ihrer Aufgaben gestattet wird. Denn im Ranking der kritischen Angriffspunkte stehen zu weit gefasste Zugriffsrechte immer ganz weit vorne, da dies die Risiken im Hinblick auf Datendiebstahl enorm erhöht. Des Weiteren sollten nicht mehr benötigte, aber noch existente Nutzerkonten und Daten gelöscht sowie zeitlich unbegrenzte Passwörter gut vor Angriffe der Cyberkriminellen geschützt werden.

Selbstverständlich gibt es darüber hinaus noch grundlegende IT-Sicherheitsmaßnahmen, die effektiv sind und sich zudem relativ einfach umsetzen lassen: Netzwerksegmentierung inklusive Einsatz von dedizierten Firewalls, Verschlüsselung der Daten während der Übertragung und bei der Speicherung sowie die Authentifikation der Mitarbeiter und Maschinen.

Ergo: Bestandsanlagen nicht zum Cyber-Risiko werden lassen

Ob früher alles besser war, bleibt dahingestellt. Rückblickend gab es natürlich mal eine Zeit, in der die Maschinen in der Produktion nicht angreifbar waren. Doch mittlerweile haben sich die Gegebenheiten geändert – das gilt es zu akzeptieren. Daraus ergibt sich unter anderem die Konsequenz, dass aufgrund der zunehmenden Komplexität – die nicht zuletzt auch daraus resultiert, dass Maschinen, Netzwerk- und IT-Technologie verschiedener Generationen in einer gemeinsamen IT-Umgebung miteinander verbunden sind – eine angemessene Absicherung der Produktionsanlagen zunehmend unabdingbar wird. Oder anders ausgedrückt: Je weiter also die Digitalisierung in Produktion und Fertigung fortschreitet, desto mehr wird eine mangelhafte Cyber-Sicherheit zu einem hohen Risiko.

Dies gilt erst recht für Bestandsmaschinen und -anlagen, die originär nicht für eine Integration in das Netzwerk ausgelegt waren.

Aus dem Grund ist es unerlässlich, hier so schnell wie möglich ein hinreichendes IT-Schutzniveau zu etablieren – was aufgrund von vermehrt vorhandenen Standard-Sicherheitsprodukten realisierbar ist, da sich diese relativ problemlos integrieren lassen.