Gut geplant, vernetzt und digitalisiert

Robuste und zuverlässige Verpackungslinien für die Petrochemie

Maschinen in petrochemischen Betrieben müssen außerordentlich zuverlässig und robust sein. Denn kommt es zu Ausfällen, können auf den Betreiber Kosten in Millionenhöhe zukommen. Die Beumer Group liefert von der Absackung bis zur Verpackung komplette Verpackungslinien inklusive Service. Der Anwender profitiert von der modularen Bauweise der Maschinen und weiteren Vorteilen durch die zunehmende Vernetzung und Digitalisierung.

Rafael Imberg, Beumer Group

© BEUMER Group GmbH & Co. KG

Am Ende der Prozesskette ist die Verpackungslinie. Steht diese still, weil eine Maschine defekt ist, müssen oft auch andere Anlagen abgeschaltet werden, bspw. die Extruder. Jede Stunde, in der die Produktion stillsteht, kann ein Unternehmen mehrere 100.000 EUR kosten. Dazu kommen Kosten, um das Problem zu beseitigen – etwa für Betriebsmittel, Ersatzteile und Instandhaltung. Nicht zu unterschätzen sind entgangene Geschäftsgelegenheiten und ein geschädigtes Kundenvertrauen. In der Petrochemie wird eine robuste und ausfallsichere Arbeitsweise der Maschinen immer wichtiger, deshalb hat die Beumer Group das Design ihrer Verpackungsanlagen überarbeitet und sie modular aufgebaut.

Der Beumer Fillpac FFS z.B. formt Säcke aus einer vorgefertigten PE-Schlauchfolie und füllt diese zuverlässig und schonend ab. Anschließend werden sie automatisch verschweißt. Bis zu 2.800 Säcke pro Stunde kann die Maschine auf diese Weise handhaben. Nach dem Verschließen werden die Säcke für den Transport sicher und zuverlässig auf einer Palette gestapelt, wofür sich der Beumer Paletpac besonders eignet. Auch dieses System lässt sich individuell an die unterschiedlichen Anforderungen der chemischen Industrie anpassen. Die Anlage erreicht einen Durchsatz von bis zu 3.200 Säcken pro Stunde. Für die Endverpackung hat der Systemanbieter seine Hochleistungsverpackungsanlage Stretch Hood im Programm. Die Stretchfolie passt sich an jeden Stapel an. Sie ist sehr dehnbar und fixiert das Material sowohl durch die horizontalen als auch die vertikalen Rückstellkräfte auf der Palette. Dieses Verfahren bietet so eine hohe Ladungsstabilität.

Modular und intelligent

Alle Baureihen haben die Beumer-Spezialisten nicht nur robust gestaltet, mit der neuen modularen Bauweise sind in den Anlagen auch gleiche oder ähnliche Komponenten und Module verbaut. Das reduziert die Anzahl der Ersatzteile, beschleunigt deren Lieferzeiten und erleichtert dem kundenseitigen Personal die Wartung. Durch das gleiche Look and Feel kann der Mitarbeitende ganz leicht einen Paletpac bedienen, obwohl er bspw. bisher nur mit der Handhabung des Beumer Stretch Hood vertraut war. Das Personal lernt so auch die verschiedenen Maschinen schneller kennen. Die modulare Bauweise schafft noch weitere Vorteile: Fordert der Anwender mehr Leistung, kann diese bei den Maschinen nachträglich relativ einfach gesteigert werden. Ob die Anlage nun nachgerüstet oder ein Schaden behoben werden muss – die Modularität sorgt für einen deutlichen Zeitvorteil.

Auf Wunsch lassen sich auch alle Maschinen und Komponenten mit einer übergeordneten Steuerung – der BG Software Suite – vernetzen. Mit der Visualisierung BG Fusion steht dem Bediener zudem eine webfähige Benutzeroberfläche für Konfiguration, Monitoring und Reporting zur Verfügung. Damit lassen sich alle Informationen, die der Systemanbieter mittels Data Analytics in der Maschine sammelt, transparent darstellen. Maschinendaten, Störmeldungen sowie Hinweise zum Betrieb und zur Wartung werden so aufbereitet, dass der Anwender sie einfach nutzen kann – z.B. für eine vorausschauende Wartung.

©vegefox.com - stock.adobe.com

Wissen, wann die Maschine ausfällt

Denn die Frage lautet: Wie lässt sich die Wartung so planen, dass wir einen plötzlichen Stillstand ausschließen können? Der Kunde möchte z.B. einmal im Monat eine Wartungsschicht. Das heißt, er setzt die Maschinen bewusst still, will aber sichergehen, dass diese danach störungsfrei arbeiten. Bei einem ungeplanten Ausfall hat er nicht immer das erforderliche Werkzeug oder Personal parat, um die Anlage wieder instand zu setzen.

Mit der Datenanalyse lässt sich auch die Einsatzdauer der Komponenten verlängern. Die Kunden wollen wissen, nach wie vielen Betriebsstunden eine bestimmte Komponente, etwa ein Motor, ausgetauscht werden muss. Das lässt sich in der Regel nicht pauschal vorhersagen, weil das immer von den Umgebungsbedingungen abhängt. Wie ist die Maschine eingestellt, wie ist sie gewartet? Besteht die Möglichkeit, etwa Motoren, Sensoren und Zylinder im Betrieb zu überwachen und Schwachstellen elektronisch festzustellen, lässt sich der Austausch auf den optimalen Zeitpunkt festlegen. Ein Beispiel: Wird der Motor ungewöhnlich warm, können die Service-Techniker daraus auf seinen Zustand schließen. Mit dieser Information kann ein plötzlicher Ausfall vermieden werden, denn die Software gibt rechtzeitig Alarm.

Vernetzt vom Silo bis zum Lager

Der Lieferumfang des Systemanbieters Beumer beginnt beim Kunden unterhalb des Silos. Das Produkt fällt in den Sack, dieser wird palettiert und der gesamte Stapel mit einer Stretchfolienhaube überzogen. Über die Beumer Software lässt sich zudem das Warehouse-Management-System (WMS) anbinden. Dieses kann für die Einlagerung etwa über Barcode, RFID oder QR-Code die Waren eindeutig zuordnen. Mit Lesegeräten ausgestatte Gabelstapler „wissen“, wohin sie die Paletten transportieren müssen und geben die Informationen über die Einlagerung zurück ans System. Mit der Software lässt sich das Gesamtsystem vom Silo bis zum Lager vernetzen. Ziel ist es, Schnittstellen zu minimieren und dem Kunden alles aus einer Hand bieten zu können.

Unter dem Stichwort Smart Factory will der Systemanbieter seinen Kunden in Sachen Bedienung und Wartung so viele Aufgaben wie möglich abnehmen. Denn je nach Einsatzort sind auch immer weniger Einsatzkräfte verfügbar.

Service über “voice and picture”

Doch was, wenn trotzdem eine Störung eintritt oder die Maschine komplett ausfällt? Um Betreiber zu unterstützen und längere Ausfallzeiten zu verhindern, schickt Beumer seine weltweit lokalisierten Techniker zum Kunden. Dazu bietet der Customer Support eine 24/7-Hotline. Häufig ist es jedoch nicht möglich, ein komplexes Problem am Telefon schnell und eindeutig zu beschreiben. Für solche Fälle wurde das zukunftsweisende Produkt Beumer Smart Glasses entwickelt. Damit blicken die Servicemitarbeiter virtuell dem kundenseitigen Techniker über die Schulter und gehen gemeinsam mit ihm über Bild und Ton auf Fehlersuche, um diesen zu beheben. Mit den Smart Glasses kann der Kunde schnell ein Bild zum Experten des Systemanbieters schicken, der wiederum auch ein Bild zurücksenden kann. Diese digitale Lösung reduziert zeitaufwändige Anreisen und hohe Zusatzkosten. Next Level of Remote Diagnostic – was früher das Telefon war, ist heute „voice and picture“.

Doch Lösungen werden nicht nur für Greenfield-, sondern auch für Brownfield-Projekte entwickelt. Das ist wichtig, da der Systemanbieter weltweit zahlreiche bereits installierte Anlagen betreut. Viele Kunden entscheiden sich nach Jahren oft für einen Retrofit. Meist ist dies auch unumgänglich aufgrund der Ersatzteilsituation oder Prozessänderungen. Dabei tauschen die Beumer Techniker nicht nur Komponenten, sondern erhöhen über die Software auch die Leistung.

Rafael Imberg, Head of Sales Petrochemie, Beumer Group, Beckum

■ www.beumergroup.de

Cyberbedrohung in der Operational Technology

Schutz vor Angriffen auf Prozessanlagen muss intensiviert werden

Die Cybergefahr für industrielle Systeme steigt seit Jahren. Hacker haben es häufig auf Unternehmensgeheimnisse oder Lösegelder abgesehen. Beim Thema OT-Security muss zügig aufgeholt werden, was lange vernachlässigt wurde.

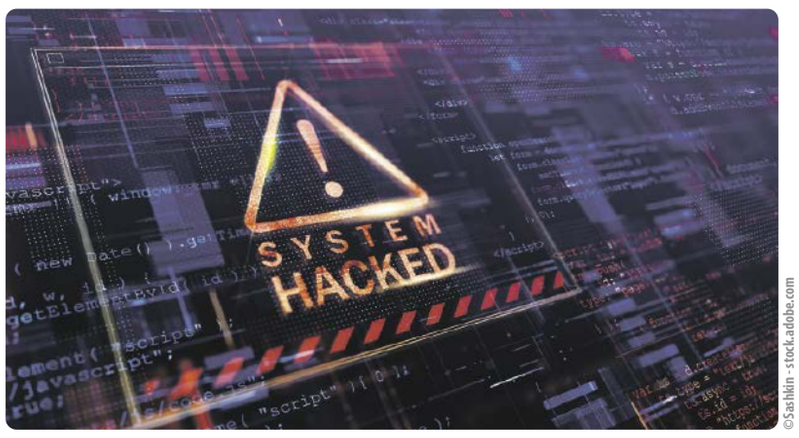
Im vergangenen Jahr hat die Anzahl der Cyberstraftaten in der Bundesrepublik Deutschland einen neuen Höchststand erreicht. 146.363 Delikte zählte das Bundeskriminalamt (BKA) 2021. Diese Bedrohung macht auch vor der Chemie- und Pharmaindustrie nicht Halt: Schon 2019 enthüllten Datenjournalisten von Norddeutschem Rundfunk (NDR) und Bayerischem Rundfunk (BR), dass eine professionelle Hackergruppe über Jahre hinweg große deutsche Chemie- und Pharmakonzerne ausspioniert hatte. Dazu gehörten Bayer, BASF, Covestro und Henkel. Systeme an der Schnittstelle vom Intranet zum Internet sowie Autorisierungssysteme waren mit Schadsoftware infiziert. Auch Unternehmen im Ausland waren betroffen, darunter der Schweizer Pharmakonzern Roche, der französische Klebstoffhersteller Bostik oder der japanische Chemieriese Shin-Etsu. Der verantwortlichen Gruppe „Winnti“ wird eine Nähe zum chinesischen Staat zugeschrieben.

Sicherheitslage bleibt angespannt

Eine vom Gesamtverband der Versicherer (GDV) in Auftrag gegebene repräsentative Forsa-Umfrage aus dem Jahr 2020 zeigt, wie brisant die Gefahrenlage zu diesem Zeitpunkt bereits war. Dafür wurden die jeweiligen Verantwortlichen für IT-Security in 100 kleinen und mittleren deutschen Chemieunternehmen befragt. 30 % der Befragten gaben an, dass ihr Unternehmen schon einmal Opfer eines Cyberangriffs geworden ist. Während einer Cybersicherheitsanalyse unter 510 mittelständischen Chemieunternehmen wurden zudem bei 41 % der Unternehmen Daten im Darknet gefunden. Darunter waren über 10.000 E-Mail-/Passwort-Kombinationen von Mitarbeitern. Die Situation hat sich mit Beginn des russischen Angriffskrieges in der Ukraine weiter verschärft.

Bewusstsein für OT-Security wächst

Zusätzlich zu den reinen IT-Infrastrukturen sind von der Cybergefahr zunehmend auch industrielle Anlagen betroffen, also Operational Technology (OT). Das verantwortliche OT-Personal war jahrelang allein dafür zuständig, dass Maschinen und Produktionsanlagen zuverlässig laufen. Weil die Systeme komplett abgekoppelt von der IT funktionierten, reichte dies auch aus. OT-Security war deshalb schlichtweg kein Thema. Einhergehend mit Entwicklungen wie der Digitalisierung und der Industrie 4.0 werden Herstellungsanlagen aber seit den Neunzigerjahren zunehmend mit IT-Infrastrukturen und Office-Netzwerken gekoppelt.



©Sashkin - stock.adobe.com

Immer mehr Schnittstellen zwischen OT und IT sorgen auch im Chemie- und Pharmabereich für eine steigende Anzahl an sensiblen Punkten, an denen auch die Operational Technology von außen angreifbar und verwundbar ist. Zukünftig ist daher zu erwarten, dass Sicherheitslücken hier noch gnadenloser ausgenutzt werden. Besonders Angriffe mit Ransomware (Erpressungssoftware) dürften immer spezieller auf OT-Systeme ausgerichtet werden. Die Angreifer können deutlich mehr finanziellen Druck auf Unternehmen mit systemrelevanten Produktionsanlagen ausüben, auch, weil die Systeme beim Patchen erfahrungsgemäß immer hinterherhängen.

Wertvolle Daten im Visier

OT-Sicherheit umfasst zum einen die Produktionssicherheit und zum anderen die Datensicherheit. Beides hängt miteinander zusammen. Denn die intelligente Vernetzung von Chemieanlagen führt dazu, dass die Produktion ohne digitale Datenströme lahmliegt. Kriminelle Hacker können sich Zugriff auf diese Daten verschaffen und folgendes bewirken: unwiederbringlichen Datenverlust, Datendiebstahl (Spionage) oder Datenverfälschung (Manipulation).

Bis vor einigen Jahren existierten noch keine spezifischen Programme für OT-Systeme, die kontrollieren, ob Daten manipuliert wurden. IT-Programme mussten entsprechend umständlich und aufwendig konfiguriert werden. Daher waren Angriffe mittels Datenmanipulation, die bis hin zum Herunterfahren der OT-Umgebung führen können, das größte Problem. Dies hat sich jedoch geändert: Hacker nehmen gegenwärtig neben Lösegelderpressung die Industriespionage stärker in den Fokus. Dabei lassen sie über Wochen oder Monate unbemerkt Daten abfließen, um diese im Darknet zum Verkauf anzubieten. Von Interesse kann z.B. ein patentgeschütztes Verfahren zur Impfstoffherstellung sein oder Informationen zum Aufbau chemischer Anlagen. Der Datenabfluss kann durch einen berechtigten Zugang eines Mitarbeiters erfolgen – Remote-Zugriffe über VPN-Verbindungen stellen hier eine Herausforderung dar – oder durch unberechtigte Infiltrierung von außen.

Normen schaffen Sicherheit

Nicht alle Chemie- und Pharmaunternehmen gehören zur Kritischen Infrastruktur (KRITIS) nach dem IT-Sicherheitsgesetz 2.0 bzw. der Kritisverordnung des Bundesamtes für Informationstechnik (BSI). Dennoch können viele als systemrelevant bezeichnet werden: Wenn z.B. bei einem Hersteller von Plastikgranulat die Produktion ausfällt, führt dies dazu, dass Lieferketten negativ beeinflusst werden. Bestimmtes medizinisches Werkzeug, wie Spritzen, kann dann nicht mehr hergestellt werden. Der IT-Grundschutz BSI bietet auch für Chemie- und Pharmaunternehmen außerhalb der KRITIS einen wertvollen Leitfaden, um die IT- und OT-Sicherheit zu verbessern.

Normen wie die ISO 27001 für Informationssicherheit oder die IEC 62443 für industrielle Sicherheit fordern schon lange einen besonderen Schutz für produzierende Unternehmen. Speziell ausgebildete und zertifizierte Experten können bei der Umsetzung dieser Vorgaben

Fortsetzung auf Seite 35 ▶