Industrie 4.0: mit Sicherheit aus der Krise

Von Johannes Näumann

Druckbehälter und Dampfkesselanlagen gehören nach wie vor zur technischen Grundausstattung vieler Unternehmen. Durch die Digitalisierung werden konventionelle Anlagen immer stärker miteinander vernetzt. Die Einbindung von Industrieanlagen in eine globale IoT-Architektur bietet die Chance, effizienter, umweltschonender und weniger krisenanfällig zu produzieren. Das hat sich während des Lockdowns infolge der Corona-Pandemie sehr deutlich gezeigt. Die Industrie 4.0 erfordert aber auch Investitionen in die Sicherheit und einen neuen Ansatz bei technischen Prüfungen. Safety und Cybersecurity müssen dabei in Einklang gebracht werden.

Jedes Jahr prüfen die Zugelassenen Überwachungsstellen mehr als 300.000 Druckbehälter und Dampfkesselanlagen. Das zeigt: Die Digitalisierung lässt herkömmliche Technologien nicht vom Markt verschwinden. Zur Stromproduktion oder zur Erzeugung von Prozessdampf durch Kraft-Wärme-Kopplung werden in der Industrie auch künftig konventionelle Druckanlagen eingesetzt. Allerdings werden sie zunehmend um digitale Eigenschaften ergänzt, miteinander vernetzt und in ein globales IoT-System (Internet of Things) eingebunden.

Die Vorteile der digitalen Vernetzung liegen vor allem in einer höheren Effizienz und einer niedrigeren Umweltbelastung durch Industrieanlagen. Obwohl ein Dampfkessel in seinem Grundprinzip seit der Industrialisierung fast unverändert ist, lassen sich die Kesseleffizienz und die Energieeinsparpotenziale etwa durch eine konsequente Erfassung und digitale Auswertung von Betriebsdaten optimal ausnutzen. Studien der TU Wien, des Austrian Institute of Technology (AIT) und der Montanuniversität Leoben aus dem Jahr 2020 belegen, dass sich durch den konsequenten Einsatz digitaler Technologien der Energieverbrauch im Industriesektor drastisch senken lässt – eine Voraussetzung, um die weltweiten Klimaziele zu erreichen. Künstliche Intelligenz, Blockchain, datengetriebene Modellrechnungen, digitale Zwillinge, offene Plattformen oder der Einsatz von Sensoren und digitalen Stromzählern gehören hier zu den technologischen Treibern.

Spätestens im Jahr 2020 stellte sich aber noch eine weitere Herausforderung: Die Corona-Pandemie verursachte laut dem Institut der Deutschen Wirtschaft allein in den ersten beiden Krisenmonaten einen Produktionsrückgang von 30 Prozent, das statistische Bundesamt stellte im zweiten Quartal 2020 einen Einbruch des Bruttoinlandsprodukts (BIP) um 10,1 Prozent im Vergleich zum ersten Vierteljahr fest – ein Rekordwert seit Beginn der regelmäßigen BIP-Berechnung im Jahr 1970. Um diese Krise zu bewältigen und künftig im Wettbewerb bestehen zu können, ist die Digitalisierung in der Industrie eine wichtige Voraussetzung.

So kommt der Digitalverband Bitkom in einer kürzlich veröffentlichten Studie zu dem Ergebnis, dass eine überwältigende Mehrheit (94 Prozent) der befragten Unternehmen in der Digitalisierung die Voraussetzung für den Erhalt der Wettbewerbsfähigkeit der deutschen Industrie sieht. Die Zahl der Industrieunternehmen mit mehr als 100 Mitarbeitern, die Industrie-4.0-Anwendungen nutzen, sind in Deutschland in den letzten zwei Jahren von 49 Prozent auf 59 Prozent gestiegen, weitere 22 Prozent planen den Einsatz von Industrie 4.0. „Je digitaler die Industrieunternehmen aufgestellt sind, desto schneller werden sie sich von den Folgen des Shutdowns erholen“, sagte Verbandschef Achim Berg.

Der Münchner Digital-Pionier Lin Kayser geht sogar noch einen Schritt weiter. Für ihn hat die Corona-Krise den Raum für visionäres Denken geöffnet. „Digitale Lieferketten und eine dezentrale automatisierte Produktion“ könnten künftig die globalen

wirtschaftlichen Prozessabläufe krisenfest machen. Anstatt fertige Bauteile in Containern um die Welt zu verschiffen sieht er die Zukunft in „digitalen physischen Produkten (DPP)“, die digital entwickelt, je nach Bedarf modifiziert und später lokal im additiven 3D-Druckverfahren produziert werden. Eine effiziente Methode, die während der Corona-Krise in Italien zur Beschaffung dringend benötigter Ersatzteile für Beatmungsgeräte bereits erfolgreich praktiziert wurde.

Es werden daher nicht mehr nur die funktionalen Mängel bei einem Druckbehälter oder einer Dampfkesselanlage zu Sicherheitsrisiken führen, sondern auch Lücken im Bereich Cybersecurity. Laut einer Studie des TÜV-Verbands beklagte jedes achte Unternehmen (13 Prozent) innerhalb der letzten 12 Monate vor der Befragung einen IT-Sicherheitsvorfall. Jedes vierte betroffene Unternehmen (26 Prozent) berichtet von Phishing-Angriffen, bei denen – in der Regel per E-Mail – Schadsoftware in die Organisation eingeschleust wird. An zweiter Stelle steht Ransomware (19 Prozent), mit deren Hilfe Cyberkriminelle die IT-Systeme einer Organisation lahmlegen und die Unternehmen dann erpressen. Weitere Bedrohungsszenarien seien „Social Engeneering“, Man-in-the-middle-, Passwort- und DDoS-Angriffe.

Für den Bereich der intelligenten Energieversorgung forderte daher das IEC-Systemkomitee Smart Energy (IEC/SyC Smart Energy) im April 2020 zum Schutz des Stromnetzes vor Cyberangriffen „einen ganzheitlichen Ansatz zum Aufbau von Cyberwiderstandsfähigkeit, der bewährte Verfahren mit Prüfungen und Zertifizierungen kombiniert.“ Digitale Sicherheit müsse bereits im Design angelegt sein und von Anfang an in die Systeme und in den Betrieb integriert werden, anstatt sie erst nach der Implementierung der Systeme anzuwenden.

Durch die Corona-Krise befinden sich nun viele Unternehmen in einem Dilemma: Der wirtschaftliche Einbruch zwingt sie zu harten Sparmaßnahmen, wobei andererseits Investitionen in die Krisenbewältigung und Resilienz bei künftigen Pandemien notwendig sind. Hier müssen die Prioritäten richtig gesetzt werden. „Es wäre fatal, wenn die Unternehmen in wirtschaftlich schwierigen Zeiten die Sicherheit ihrer digitalen Systeme vernachlässigen würden“, sagte TÜV-Verbandschef Joachim Bühler. „Jeder Euro, der jetzt in die IT-Security fließt, ist eine Investition in eine krisensichere Zukunft.“

Prüfungen an Druckanlagen müssen künftig neben „Safety“, also dem sicheren Funktionieren aller technischen Komponenten, auch die „IT-Security“ im Blick haben. Bei diesem Paradigmenwechsel, der alle überwachungsbedürftigen Anlagen betrifft, ist auch der Gesetzgeber gefragt. Die Prüforganisationen fordern daher eine Anpassung der Rechtsvorschriften und Normen in Deutschland und der EU. Im Bereich von Industrie 4.0 müssen vor allem Standards entwickelt und Referenzarchitekturen für die vernetzte Technologie cyber-physikalischer Systeme (CPS) aufgebaut werden. „Unabhängige Zertifizierungen durch akkreditierte neutrale Dritte liefern den verlässlichen Nachweis, dass diese Standards eingehalten werden“, sagte Bühler. „Dadurch entsteht Transparenz und das notwendige Vertrauen in Produkte, Prozesse und neue Technologien.“

Johannes Näumann
Büro für strategische Kommunikation
jn@naeumann.de