PODIUMSDISKUSSION VON DER SPS|IPC|DRIVES 2012

Industrie 4.0 – ein neues Konzept für mehr Flexibilität

Integrativ denken, interdisziplinär forschen. Bisher gab es drei revolutionäre Erfindungen, die die Industrie entscheidend geprägt haben und wesentliche Produktivitätsfortschritte brachten: Dampfmaschine, Fließband und speicherprogrammierbare Steuerungen. Mit Industrie 4.0 zieht nun die moderne Informationstechnik in klassische industrielle Prozesse ein. Grundlage dafür sind Cyber-Physical Systems (CPS). Sie können eigenständig Informationen aufnehmen, Aktionen auslösen und sich wechselseitig steuern. Sie bilden künftig das Nervensystem von Industrie 4.0. Ein Nachbericht von der SPS|IPC|Drives 2012.

Die erste industrielle Revolution begann mit der Erfindung der Dampfmaschine. Sie revolutionierte mit ihrer Kraft vor allem den Bergbau und die textile Massenproduktion. Industrie 2.0 war wesentlich durch Arbeitsteilung und Elektrizität geprägt. Elektrischer Strom brachte die Ortsunabhängigkeit und das Fließband einen neuen Takt in die Fabriken. Siebzig Jahre später steuerten dann erstmals speicherprogrammierbare Steuerungen und Mikroprozessoren Maschinen und Anlagen. Dies steigerte die Produktivität der Herstellungsprozesse und die Qualität der Produkte enorm. Jetzt rufen in Deutschland Verbände, Politik und Industrie die vierte industrielle Revolution aus.

Ein Paradigmenwechsel

„Mit Industrie 4.0 bekommen wir einen deutlichen Paradigmenwechsel: Von bisher hierarchisch organisierten Strukturen hin zu Netzwerken“, sagt Prof. Dr.-Ing. Detlef Zühlke vom Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI). Das Zukunftsprojekt Industrie 4.0 treibt die produzierende Industrie und die Automatisierungstechnik voran. Im Gegensatz zum Computer integrated manufactoring (CIM)-Ansatz vor dreißig Jahren sind heute die Möglichkeiten, auf denen Informationen ausgetauscht werden, wesentlich größer. Während CIM mit seinem technokratischen Ansatz nur Insellösungen einzelner Hersteller lauffähig gemacht hat, liegt der wesentliche Fortschritt bei Industrie 4.0 in seinem industrieübergreifenden Ansatz. „CIM ist damals gescheitert, weil wir die Komplexität der Systeme nicht händeln konnten“, sagt Roland Bent, Geschäftsführer von Phoenix Contact. „Ganzheitlich betrachtet, bietet Industrie 4.0 hierarchielose Kommunikationsstrukturen, wie sie im Internet üblich sind. Wir versuchen autonome Gruppen zu schaffen, die für sich auch entsprechende Entscheidungen treffen können.“ Im Klartext heißt das, dass nicht mehr eine zentrale Steuerung, sondern das zu fertigende Produkt selbst die Produktion steuert. Doch Autonomie ist nicht gleichzusetzen mit Anarchie. Es bestehen noch Regeln, innerhalb derer – abhängig von den Rahmenbedingungen – Entscheidungen getroffen werden können. Dazu gehören auch Konzepte, die die horizontale Integration innerhalb von Wertschöpfungsnetzwerken und die vertikale Integration der Systeme in flexiblen und rekonfigurierbaren Produktionssystemen vorantreiben. Doch gibt es inzwischen Tendenzen, dass sich die Ränder der klassisch abgegrenzten Ebenen langsam auflösen, beobachtet Olaf Sauer, stellvertretender Leiter des Fraunhofer Instituts IOSB. „Typische MES-Funktionen wie Fertigungssteuerung, Qualitätsmanagement oder Tracking & Tracing wandern als CPS-Dienste in die Automatisierungs- und Feldebene, während sich die Fertigungsplanung in die ERP-Ebene verlagert“, so Sauer.

„Typische MES-Funktionen wie Fertigungssteuerung, Qualitätsmanagement oder Tracking & Tracing wandern als CPS-Dienste in die Automatisierungs- und Feldebene, während sich die Fertigungsplanung in die ERP-Ebene verlagert.“

OLAF SAUER
Stellvertretender Leiter des Fraunhofer Instituts IOSB

Mobilität als Kernthese

Dem Paradigma des Internets der Dinge folgend, wird alles mobil werden. Smarte Objekte vernetzen sich mit einem IT-Standard und tragen alle Eigenschafts-, Produktions- und Logistik-Informationen in sich. „Wir lesen einfach den Speicher aus und wissen, wo das Objekt hergekommen ist, wo es hingeht, wie es hergestellt worden ist“, sagt Detlef Zühlke. Es sei nur noch eine Frage der Zeit und des Preises, bis auch Maschinentaster und Sensoren mit einer kleinen Steuerung und einem eigenen Server ausgestattet seien, so der Hauptinitiator der Technologie-Initiative SmartFactory KL weiter.

„Mit Industrie 4.0 schaffen wir die Voraussetzung für eine wirkliche vertikale Integration. Mit einer smarten Vernetzung kann man einen Sensorwert direkt über das Netzwerk liefern“, so Zühlke. Essenziell sei aber auch, dass alle Prozesse und Komponenten standardisiert werden. „Das wirkt sich natürlich auch auf unsere Geräte aus, denn wir werden ein Gerät nicht mehr als ein physikalisches Gerät an der Klemme XY23 sehen, sondern wir werden das Gerät mit Modellen ausstatten müssen, die wir dem Kunden mitliefern. Das machen wir heute schon“, so Zühlke. Schon heute haben Elektromotoren oder Sensoren ein elektronisches

„Heute sehen wir die höchsten Wachstumsraten im Bereich After Sales. Mit dem Konzept Industrie 4.0 könnte ein Maschinenbauer zusätzliche IT-Dienstleistungen anbietet, die ihm dafür ein Alleinstellungsmerkmal gegenüber seinem Mitbewerb bieten.“

KLAUS BAUER
Leiter der Entwicklung Basistechnologie bei Trumpf Werkzeugmaschinen

„Ganzheitlich betrachtet, bietet Industrie 4.0 hierarchielose Kommunikationsstrukturen, wie sie im Internet üblich sind. Wir versuchen autonome Gruppen zu schaffen, die für sich auch entsprechende Entscheidungen treffen können."

ROLAND BENT
Geschäftsführer von Phoenix Contact.

Datenblatt, mit dem sie sich selbst konfigurieren. „Was fehlt, ist die Software, mit der man den Sensor in ein Netzwerk einbinden und gleichzeitig als Objekt in der Engineering-Phase betrachteten kann. Dazu kommt noch ein Dienste-, Ressourcen und Energiemodell, bei dem wir nicht mehr von Signalen reden, sondern von abstrakten Diensten, die wir von einem solchen Gerät anfordern", so Zühlke. „Ich vergleiche dies immer gern mit einem Legostein, d. h. wir versuchen, unsere Geräte zu abstrahieren – wir trennen damit die Hardwareerscheinung von der Kommunikationserscheinung und der Funktionalität, die dahinter steht. Das ist etwas, was wir in der Informatik schon lange machen." Dies hat dann den Vorteil, dass man zeitoptimiert und parallelisiert entwickeln und in Betrieb nehmen kann.

„Mit SmartFactory existiert heute schon die entsprechende Basistechnologie für eine serviceorientierte Architektur (SOA), auf die man jetzt zurückgreifen kann", erklärt Zühlke und verweist auf den neuen SOA-Demonstrator. „Das Teil ist jetzt so groß wie drei Zuckerwürfel nebeneinander, kostet 36 Euro als Einzelstück, hat WLAN- und Kabelanschluss und als Software OPC UA mit entsprechenden Dienstarchitekturen." Als Mittler zwischen der Feld- und der Automatisierungsebene baut das Deutsche Forschungszentrum für Künstliche Inteligenz (DFKI) gerade eine SOA-SPS auf, die auf der einen Seite wie eine handelsübliche SPS fungiert und auf der anderen Seite ein SOA-Interface hat. Nach oben betrachtet, ist sie ein SOA-Teilnehmer in einem Netzwerk und nach unten hin eine klassische SPS mit der entsprechenden Funktionalität. Damit trennt sich die Hardware von der Kommunikation und der Funktionalität.

„Wenn demnächst jeder Sensor, jeder Motor oder jedes Fertigungsaggregat Zeichnungen, Revisionsstände, Ersatzteillisten, Soft- und Hardware, Kapazitäten, Bewegungsräume etc. in sich trägt und dies bei Bedarf anderen mitteilen kann, dann lassen sich daraus recht einfach autonome Maschinenaggregate konfigurieren", erklärt Gerd Hoppe von Beckhoff Automation. Diese geben dann Fertigungsaufträge oder Service-Requests an die Fertigungseinrichtung. „Damit schaffen wir eine Verbindung zwischen den Methoden der virtuellen Welt, der Informationstechnologie und einem physischen System." Dies gelte auch unabhängig davon, ob es sich um eine Produktionsumgebung oder eine städtische Infrastruktur handelt. Der Begriff Industrie 4.0 sei nicht auf die Automatisierung begrenzt, so Hoppe weiter. „Die Zukunft wird zeigen, ob sich das alles so strukturiert, wie wir es wollen – von der Top-down-Architektur bis zum völlig freien Kommunizieren zwischen autonomen Systemen ist alles möglich."

Sicherheit ist die Basis

Allerdings ist dies noch nicht so weit, „denn man muss sich fragen, wie man mit dem iPad eine sichere Bedienung hinbekommt", sagt Klaus Bauer, Leiter der Entwicklung Basistechnologie bei Trumpf Werkzeugmaschinen. „Entsprechende Regularien gibt es nicht. Diese müssen wir jetzt gemeinsam erarbeiten, damit eine Technik, die eigentlich funktioniert, auch akzeptiert wird." Bisher betrachtete man IT-Sicherheit als Sicherheit der Anlage oder des Zugriffsschutzes auf Steuerung und Hardware. Mit Industrie 4.0 spannt sich der Bogen weiter, denn verbundene Systeme haben mehr Angriffsmöglichkeiten, die mit der Zahl der Verbindungen und den unterschiedlichsten Technologien wachsen. Damit wird Cybersicherheit zum zentralen Thema von Industrie 4.0 – dies unabhängig davon, ob man einen microsoftbasierenden Industrie-PC einsetzt oder eine klassische Industriesteuerung. „Wenn wir als Industrie dieses Thema nicht angehen, dann kann es zum Show-Stopper für die durchgängige Vernetzung einer Industrie 4.0 werden", meint Roland Bent.

„Doch keiner lässt seine Fertigungseinrichtung frei im Internet zugreifbar erscheinen, sondern baut mit den entsprechenden IT-Mitteln eine In-House-Cloud auf", entgegnet Gerd Hoppe. Grundsätzlich müssten die Sicherheitsmaßnahmen auch nicht anders sein als in der Office-IT. Als Wichtigstes müssten die Informationen, die auf der Anlage liegen, so verschlüsselt sein, dass keiner darauf zugreifen kann. Gleichzeitig müsse auch der Transportweg so abgesichert sein, dass sich niemand einwählen kann, laut Hoppe. „Wichtig ist, dass man das Sicherheitsniveau als Basistechnologie nutzt", so Olaf Sauer. Man müsse sich daran gewöhnen, dass jeder solche Verschlüsselungsmechanismen für sich auch nutze, damit auch das gesamte System sicher sei. Dies sei aber auch ein Erziehungsprozess, sagt Sauer weiter.

Neue Geschäftsmodelle

„Heute sehen wir die höchsten Wachstumsraten im Bereich After Sales. Mit dem Konzept Industrie 4.0 könnte ein Maschinenbauer zusätzliche IT-Dienstleistungen anbieten, die ihm dafür ein Alleinstellungsmerkmal gegenüber seinem Mitbewerb bieten", kann sich Klaus Bauer vorstellen. Worüber man aber durchaus kontrovers diskutieren müsse, sei das Vertriebsmodell von Software – beispielsweise solcher, die ein Maschinen- oder Anlagenbauer erstellt, um damit beispielsweise seinem Kunden die Fernwartung und die Auswertung der Daten zu ermöglichen. „Ob man diese Software jetzt verschenkt oder auch zusätzlich verkauft, diese Frage ist aus meiner Sicht noch nicht beantwortet", so Bauer weiter. „Doch eins ist klar: Sobald wir an Technologiegrenzen kommen, müssen wir unsere Produkte stärken – und im Konzept von Industrie 4.0 heißt das, das Kernprodukt durch einen Dienst stärken."

Noch ist Industrie 4.0 ein deutscher Begriff, der in der deutschen Öffentlichkeit geprägt worden ist. „Doch wir haben die komfortable Situation, dass Deutschland eines der führenden Maschinenbauländer der Erde und gut vernetzt ist mit einer breitgefächerten Zulieferindustrie. Zudem sind hier auch alle Industriebereiche von der Erzaufbereitung bis zur Solarindustrie und den Consumer-Produkten vertreten", so Hoppe. „Dies gibt uns die Chance, integrativ zu denken interdisziplinär zu forschen und die Technologie voranzutreiben. Die Zukunft wird zeigen, ob sich das alles so strukturiert, wie wir es wollen – als Top-Down-Architektur oder ob es ein völlig freies Kommunizieren zwischen autonomen Geräten gibt. Wenn die Integration der Produktionsprozesse gelingt, haben deutsche Unternehmen auch in einem Hochlohnland die Chance, wettbewerbsfähig zu produzieren", schlussfolgert Hoppe. **R. H.**

„Wenn die Integration der Produktionsprozesse gelingt, haben deutsche Unternehmen auch in einem Hochlohnland die Chance, wettbewerbsfähig zu produzieren"

GERD HOPPE
Corporate Management bei Beckhoff Automation.

IT-SICHERHEIT IM PRODUKTIONSUMFELD

Verfügbarkeit & Vertraulichkeit

Cyber-Sicherheit in der Fabrikumgebung. Sicherheit ist nicht nur Aufgabe des Herstellers und Systemintegrators sondern auch des Betreibers und der Bediener. In der Vergangenheit wurden in der Industrie Aspekte der Cyber-Sicherheit nachrangig behandelt oder gar vernachlässigt. Doch angesichts zunehmender Sicherheitsvorfälle und Schwachstellen müssen Betreiber von Industrieanlagen sich dringend dieser Thematik annehmen. Dies gilt sowohl für Infrastrukturen, die unmittelbar mit dem Internet verbunden sind, als auch für diejenigen, welche auf mittelbarem Wege durch Cyber-Angriffe attackiert werden können. Ein heiß diskutiertes Thema zur SPS|IPC|Drives in Nürnberg.

Bisher stand für einen Anlagenbetreiber immer die Verfügbarkeit und der sichere Anlagenbetrieb im Vordergrund. Doch mit steigender Flexibilität und Offenheit der Anlagen rückt die IT-Sicherheit auch in die Fabrikumgebung vor. Und plötzlich ergibt sich die Frage, wer für industrielle Sicherheit verantwortlich ist. „Noch zu häufig verlassen sich Anwender darauf, dass die Komponentenhersteller fertige Lösungen liefern. Sicherheit ist aber kein Produkt, Sicherheit kann man nicht kaufen, Sicherheit muss man schaffen“, sagt Holger Junker vom Bundesamt für Sichernheit in der Informationstechnik (BSI). Sicherheit beginnt beim Management und endet nicht beim Maschinenbediener, beim Pförtner oder der Putzfrau. Sicherheit ist nicht nur Aufgabe des Herstellers und Systemintegrators, sondern auch des Betreibers und der Bediener. Alle haben dafür zu sorgen, dass die Gateways ausreichend gehärtet und die Ports geschlossen sind, eine mehrstufige Firewall das industrielle Netz schützt und der Zugang zu den Schaltschränken versperrt ist. Wie hoch dann das Risiko eines Angriffs über vorhandene Schwachstellen immer noch ist, lässt sich nicht pauschal beantworten.

Nach einer Studie der ARC Advisory Group, „Risiko als Anstoß für verstärkte Investitionen in die Cybersicherheit von Industriesteuerungen“, geben Unternehmen derzeit über 2 % ihrer Steuerungsanlagen-Budgets für IT-Sicherheit aus. Interne Personalkosten sind dabei nicht berücksichtigt. Dies ist immer noch 1,5 % weniger, als im Office-Bereich für IT-Sicherheit ausgegeben wird. Die Analysten schätzen, dass in Zukunft die Aufwendungen für IT-Sicherheit noch weiter steigen werden. Dabei gelte es für alle Unternehmen abzuwägen, wie wahrscheinlich ein Schadensfall ist, welche Kosten dadurch entstehen können und was es kosten würde, den Schadensfall durch Sicherheitsmaßnahmen abzuwehren.

„Man muss das Risiko in einer Anlage ganz individuell betrachten“, sagt Stefan Ditting, Produktmanager bei HIMA Paul Hildebrand GmbH. „Als Vertreter eines Herstellers sicherheitsgerichteter Steuerungen geht es für uns vor allem um die Integrität der Daten. Deshalb sehen wir bei unseren Automatisierungsgeräten die Sicherheitsmaßnahmen schon vor, damit der Betreiber sie so integrieren kann, dass es kaum Angriffe geben kann.“

„Sicherheit ist aber kein Produkt, Sicherheit kann man nicht kaufen, Sicherheit muss man schaffen.“

HOLGER JUNKER
Bundesamt für Sichernheit in der Informationstechnik (BSI)

Doch in der Regel denkt der Betreiber beim Kauf nicht an Risikoprozesse oder Deeskalation von Sicherheitsmaßnahmen, um das Produkt sicherer zu machen. „Man nimmt das, was am Markt verfügbar ist, gut passt und preiswert ist. Das ist der falsche Ansatz“, sagt Steffen Zimmermann, beim VDMA zuständig für IT-Sicherheit. Das große Problem dahinter ist, dass Betreiber von Maschinen und Anlagen ihre Anforderungen nicht formulieren können. D. h. derjenige, der als Maschinenbauer die erste sichere Maschine anbietet, ist in der Regel noch viel zu früh dran. „Ich kann kein Rezept anbieten, aber der VDMA ruft sowohl die Anbieter von Komponenten als auch die Maschinenbauer auf, entsprechende Anforderungen zu formulieren“, so Zimmermann.

Zusammenspiel innerhalb der Produktionskette ist wichtig

„Es gibt im Produktionsumfeld die gleichen Mittel und Mechanismen, die man auch in der Office-Welt einsetzt. Jetzt muss man diese Mittel auch in der Produktion so einsetzen, dass das Thema Verfügbarkeit gewährleistet ist und die Rahmenbedingungen der Produktion berücksichtigt werden“, sagt Dr. Pierre Kobes von Siemens Industry Automation. Dies berücksichtige auch, dass die Rechner im Kontrollraum ausreichend geschützt sind, die Bildschirmschoner mit Passwortschutz aktiviert sind, nur eine begrenzte Zahl von Mitarbeitern Zugang hat und die Informationen verschlüsselt sind. Insgesamt gesehen, ist es immer ein Zusammenspiel zwischen technischen Gegebenheiten und organisatorischen Maßnahmen. Dabei ist das Bewusstsein für Sicherheit ein ganz zentrales Thema. „Wenn man sich einmal bewusst ist über die Gefahren, dann kann man mit wenig Aufwand eine ganze Reihe Maßnahmen ergreifen“, so Kobes weiter. „Als Hersteller legen wir unseren Produkten immer eine Beschreibung bei, wie diese Produkte sicher

„Es gibt im Produktionsumfeld die gleichen Mittel und Mechanismen, die man auch in der Office-Welt einsetzt. Jetzt muss man diese Mittel auch in der Produktion so einsetzen, dass das Thema Verfügbarkeit gewährleistet ist .“

DR. PIERRE KOBES
Siemens Industry Automation

Umfassendes Informationsangebot zur SPS/IPC/Drives: Die Messeforen des VDMA und des ZVEI standen wieder für ein hochkarätiges Vortragsprogramm. Unter der Regie von Verbänden und Fachverlagen fanden über die drei Messetage verteilt Podiumsdiskussionen, Produktpräsentationen sowie Diskussionsrunden zu aktuellen Themen der Branche statt.

einzusetzen sind – und falls dies nicht reicht, bieten wir auch entsprechende Dienstleistungen an."

Der Schutz einer Anlage ist dann gegeben, wenn auch in den Produkten und Systemen die technischen Möglichkeiten gegeben sind. Dabei müssen natürlich auch die Funktionalitäten richtig ausgelegt werden. Man kann es einem Hersteller von Netzwerkprodukten nicht ankreiden, wenn in der Produktion die Netzwerkarchitektur nicht so ausgelegt ist, dass sie sicher ist. Wer auf der sicheren Seite sein will, muss Sicherheitszellen bilden und so die Produktion segmentieren. Das sind Maßnahmen, die in der Verantwortung des Systemintegrators liegen. Danach ist letztendlich der Betreiber zuständig, die Anlage auch sicher zu betreiben. Dazu gehört ein User-Management, bei dem genau festgelegt ist, wer was wann tun darf. Insgesamt bedeutet dies, dass der Hersteller die technischen Möglichkeiten zur Verfügung stellen muss. Der Systemintegrator muss sie entsprechend auslegen und der Betreiber muss während der gesamten Lebenszeit der Anlagen dafür sorgen, dass die Anwendung entsprechend gepflegt wird. So ist der Betreiber auch dafür zuständig, dass die Bediener beim Verlassen des Unternehmens auch ausgetragen werden. „Erst wenn alle drei Genannten gemeinsam an einem Strang ziehen, gibt es optimale Sicherheit", so Kobes.

In der VDI-Richtlinie 2182 zur IT-Sicherheit in der Automation wird genau beschrieben, dass diese drei Rollen miteinander kommunizieren müssen. Wenn der Betreiber ein Sicherheitsproblem feststellt, dann muss er dies auch dem Integrator und Hersteller mitteilen. Ansonsten kann dieser seine Produkte nicht wirklich verbessern. Gleichzeitig stellt sich auch die Frage, was spezifiziert ist? „Wenn der Anwender keine Steuerung fordert, die für Security ausgelegt ist, bekommt er auch keine", sagt Stefan Ditting. „Wer ein Auto kauft, kann nicht erwarten, dass es kugelsichere Scheiben hat. Der Kunde muss schon seine Anforderung exakt formulieren und auch bereit sein, einen Mehrpreis zu bezahlen."

Allerdings werden die Steuerungssysteme der Zukunft ein Grundlevel an Sicherheit mitbringen müssen. Allerdings sollte man, bevor man das Thema „Schützen" angeht, eine Risikoanalyse voranstellen. „Genauso wenig wie es die Automation gibt, genauso wenig gibt es die Schutzmaßnahme. Sicherheit ist ein Prozess, der einmal eingeführt über den gesamten Lebenszyklus einer Anlage immer wieder geprüft, erneuert und gelebt werden muss", ergänzt Ditting.

Top 10 der kritischsten Bedrohungen

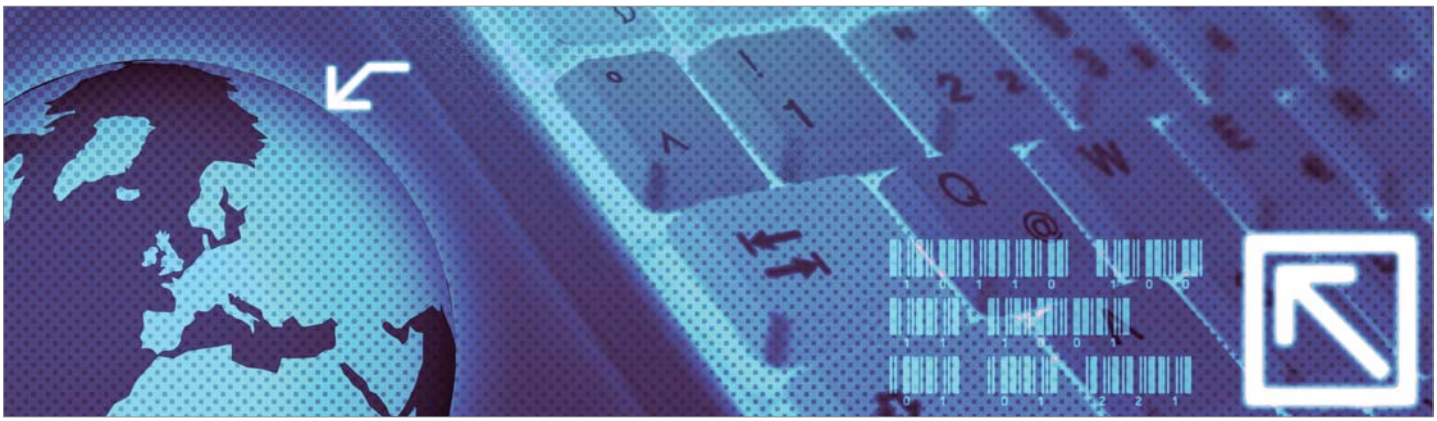
Das BSI hat deshalb in jahrelanger Arbeit mit dem Grundschutzkatalog eine allgemeine Vorgehensweise für eine Office-Umgebung geschaffen. Einen solchen Katalog gibt es für die Automation noch nicht. „Dies liegt einerseits daran, dass die Automation vielfältiger ist als eine Office-Umgebung, zum anderen konzentriert man sich im industriellen Bereich zu sehr auf die technische Lösung des Problems und vernachlässigt die organisatorischen Maßnahmen und die Sensibilisierung der Mitarbeiter", sagt Holger Junker vom BSI. Im Rahmen seiner Analysen zur Cyber-Sicherheit hat das BSI die aktuellen Bedrohungen mit der höchsten Kritikalität zusammengestellt, denen Automatisierungs-, Prozesssteuerungs- und -leitsysteme derzeit ausgesetzt sind. Im Zuge der geplanten Fortschreibung dieser Top 10 sollen zudem Trends bzgl. der kritischsten Bedrohungen aufgezeigt werden. Die Rangordnung der Bedrohungen ergibt sich aus einer Betrachtung von Aspekten wie beispielsweise Täterkreis, Verbreitung und Ausnutzbarkeit der Schwachstellen sowie der möglichen technischen und wirtschaftlichen Folgen eines Angriffs. Dabei wurden u. a. etablierte Vorfallsdatenbanken ausgewertet.

Die Top 10-Liste ist aus Sicht des BSI kein umfassendes Standardwerk und erhebt auch keinen Anspruch auf Vollständigkeit. „Sie ist

bewusst sehr kurz gehalten, listet die zehn relevantesten Bedrohungen von industriellen Anlagen auf und nennt entsprechende Gegenmaßnahmen. Dies soll einfach mal eine Diskussions- oder Sensibilisierungsmaßnahme sein", so Junker weiter. Es sei nicht erklärtes Ziel, dass alle aufgeführten Maßnahmen umgesetzt werden müssen, denn das würde sicher zu teuer werden. Es gehe eher darum, die kritischsten Punkte für das jeweilige Unternehmen zu identifizieren. Dann könne man entsprechend der höchsten Priorität Maßnahmen umsetzen. In der Regel wird es überhaupt kein Produkt sein, das man kaufen kann, sondern es sind Zuständigkeiten, Rollen, Rechte etc. Allein dadurch kann man schon ein deutliches Plus an Sicherheit erzielen. Es geht ganz einfach darum, den Einstieg zu bekommen und sukzessive für mehr Sicherheit zu sorgen. Welche Auswahl von Maßnahmen konkret geeignet ist und welche alternativen Maßnahmen möglicherweise notwendig sind, muss letztendlich am jeweiligen konkreten Anwendungsfall geprüft werden. „Irgendwann wird man feststellen, dass Sicherheit als Prozess sich institutionalisiert hat", so Junker. R.H.

Top 10 Bedrohungen

Nr.	Bedrohung	Erläuterung
1	Unberechtigte Nutzung von Fernwartungszugängen	Wartungszugänge sind bewusst geschaffene Öffnungen des ICS-Netzes nach außen, die häufig jedoch nicht hinreichend abgesichert sind.
2	Online-Angriffe über Office-/ Enterprise-Netze	Office-IT ist i. d. R. auf vielen Wegen mit dem Internet verbunden. Meist bestehen auch Netzwerkverbindungen vom Office- ins ICS-Netz, sodass Angreifer über diesen Weg eindringen können.
3	Angriffe auf eingesetzte Standardkomponenten im ICS-Netz	IT-Standardkomponenten (commercial off-the-shelf, COTS) wie Betriebssysteme, Application Server oder Datenbanken enthalten in der Regel Fehler und Schwachstellen, die von Angreifern ausgenutzt werden. Kommen diese Standardkomponenten auch im ICS-Netz zum Einsatz, so erhöht dies das Risiko eines erfolgreichen Angriffs auf die ICS-Systeme.
4	(D)DoS Angriffe	Durch (Distributed) Denial-of-Service-Angriffe können Netzwerkverbindungen und benötigte Ressourcen beeinträchtigt und Systeme zum Absturz gebracht werden, z. B. um die Funktionsfähigkeit eines ICS zu stören.
5	Menschliches Fehlverhalten und Sabotage	Vorsätzliche Handlungen – ganz gleich ob durch interne oder externe Täter – sind eine massive Bedrohung für sämtliche Schutzziele. Daneben sind Fahrlässigkeit und menschliches Versagen eine große Bedrohung insbesondere bzgl. der Schutzziele Vertraulichkeit und Verfügbarkeit.
6	Einschleusen eines Schadcodes über Wechseldatenträger und externe Hardware	Der Einsatz von Wechseldatenträgern und mobilen IT-Komponenten externer Mitarbeiter stellt stets eine große Gefahr bzgl. Malware-Infektionen dar. Dieser Aspekt kam z. B. bei Stuxnet zum Tragen.
7	Lesen und Schreiben von Nachrichten im ICS-Netz	Da die meisten Steuerungskomponenten derzeit über Klartextprotokolle und somit ungeschützt kommunizieren, ist das Mitlesen und Einspielen von Steuerbefehlen oftmals ohne größeren Aufwand möglich.
8	Unberechtigter Zugriff auf Ressourcen	Insbesondere Innentäter oder Folgeangriffe nach einer Penetration von außen haben leichtes Spiel, wenn Dienste und Komponenten im Prozessnetz keine bzw. unsichere Methoden zur Authentisierung und Autorisierung implementieren.
9	Angriffe auf Netzwerkkomponenten	Netzwerkkomponenten können durch Angreifer manipuliert werden, um z. B. Man-in-the-Middle-Angriffe durchzuführen oder um Sniffing zu erleichtern.
10	Technisches Fehlverhalten und höhere Gewalt	Ausfälle durch extreme Umwelteinflüsse oder technische Defekte sind immer möglich – Risiko und Schadenspotenzial können hier lediglich minimiert werden.

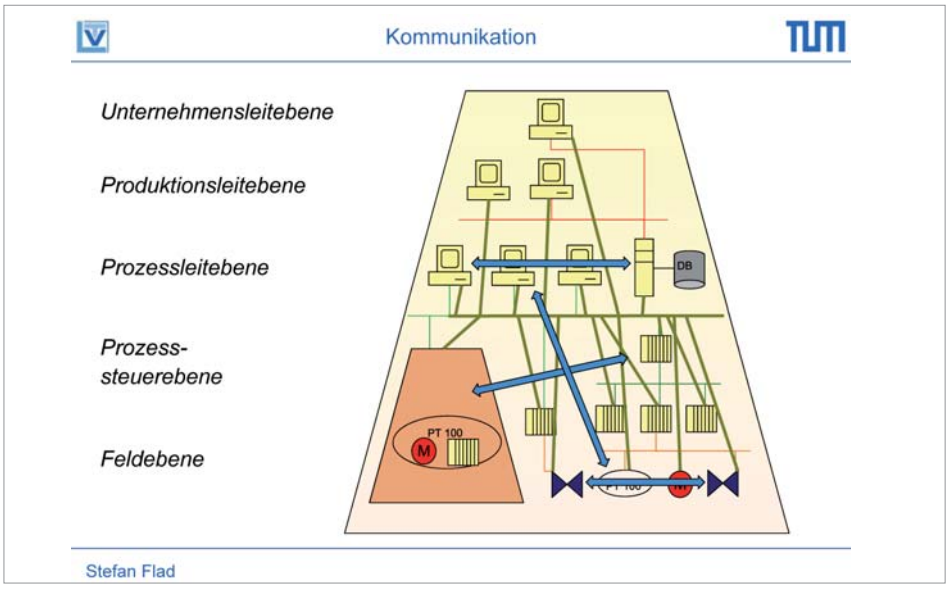


6. IT-SYMPOSIUM DER TU MÜNCHEN

Möglichkeiten moderner Produktionseinrichtungen

Anforderungen an die Informationstechnologie in der Getränke- und Lebensmittelproduktion. Ohne ausreichende informationstechnische Unterstützung ist eine effiziente, flexible und qualitativ hochwertige Produktion kaum noch machbar. Deshalb beschäftigte sich das 6. Symposium für Informationstechnologie in der Lebensmittelindustrie der TU München besonders mit der Praxis von Manufacturing Execution (MES)- und Supply Chain-Anwendungen. Neben wissenschaftlichen Betrachtungen berichteten vor allem Praktiker über ihre Erfahrungen aus aktuellen IT-Projekten und zeigten, wie man Kosten spart, Aufwände reduziert und die Flexibilität der Produktion erhöht.

Inzwischen haben Branchennormen und Standards wie IEC 62264-3, S95, VDI 5600, NAMUR, etc. dazu beigetragen, die Aufgaben und Funktionen der prozessnah operierenden Produktionsleitsysteme zu optimieren. Insofern sind MES-Lösungen heute in vielen Unternehmen eingeführt; und mit dem geeigneten Kennzahlensystem lassen sich Schwachstellen in der Produktion identifizieren. Doch bei der Frage, was die Herstellung der Flasche Apfelsaft mit der Artikelnummer 1234 kostet und wie viel CO_2-Äquivalente bei ihrer Abfüllung entstehen, müssen die meisten Systeme passen. „Es reicht heute nicht mehr, nur zu wissen, wie effizient die Anlagen arbeiten", erklärte **Dr.-Ing. Tobias Voigt** von der **Technischen Universität München** in seinem Einführungsvortrag. Bei den heutigen niedrigen Margen müsse man auch zu günstigsten Kosten produzieren können und wissen, wie effizient die Produktion eines Artikels war. „Im Moment weiß keiner, unter welchen konkreten Randbedingungen die Artikel produziert wurden und was sie, ganz konkret auf die Palette bezogen, kosten", so Voigt. Mit dem bisherigen Kennzahlensystem komme man nicht weiter, deshalb wurde das OEE-Kennzahlenmodell des Weihenstephaner Standards erweitert: Zum einen gibt es einen zusätzlichen Planungsfaktor, der die Verluste in geplante und ungeplante Stillstände unterteilt. Dann gibt es noch die Nennausbringung/Sollleistung als Bezugsgröße, die auch von der Flaschengröße abhängig ist. Der Weihenstephaner Standard definiert hierzu Datenpunkte, mit denen man die Anlageneffizienz als Verhältnis von geplanter Betriebszeit zu theoretischer Produktionszeit berechnen kann. Und zum Schluss wurde noch die Kostenberechnung pro Produkt mit einem Auftragsbezug bzw. Artikelbezug versehen. Dies gestattet es, die Verluste auch verursachergerecht einem Artikel zuzuordnen. Aus der genauen Kenntnis der Ist-Kosten pro Produktionsauftrag/Artikel kann man Mindestlosgrößen einführen und so unnötige Rüstzeiten



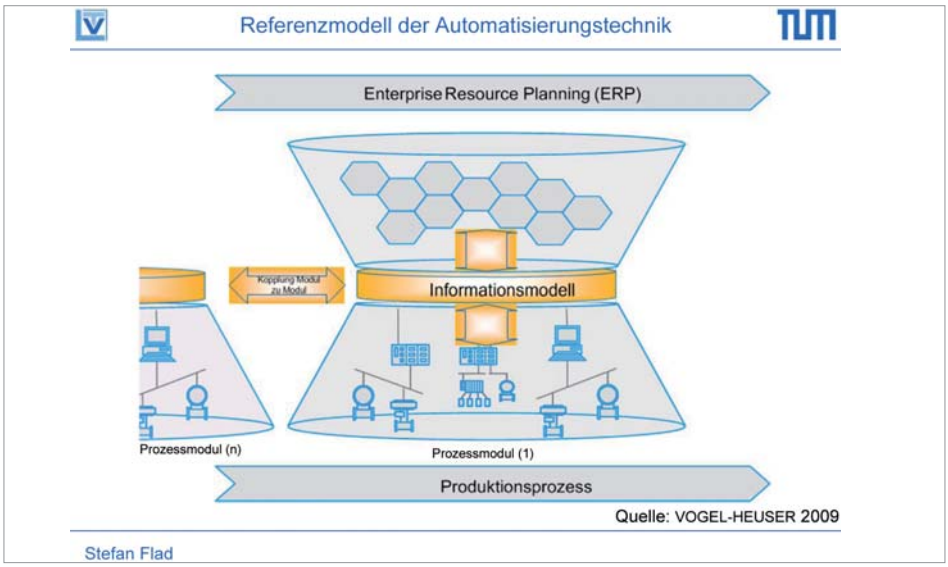
vermeiden, die Maschinenausrüstung verbessern oder die Preise erhöhen. Wie dies in der Praxis funktioniert, erläuterte **Matthias Führ** von der **H.&E. Reinert Unternehmensgruppe** am Beispiel der Produktion von Rohwurst.

Kennzahlen schaffen notwendige Transparenz

Bei geringer Verfügbarkeit der Anlage sollte die Instandhaltungsstrategie überdacht werden, so Voigt. Eine Brauerei-Studie von T.A. Cook Consultants zeigt auf, dass Anlagen mit einem Anteil an reaktiver Instandhaltung von 80 % sehr kritisch zu betrachten sind. Die Ausfallkosten übersteigen hier bei Weitem die eingesparten Instandhaltungskosten. „Rein reaktive Instandhaltung ist nicht mehr zeitgemäß. Eine Kombination aus reaktiver, periodischer und zustandsorientierter Instandhaltung, in die auch die Wartung der Software einbezogen wird, hat sich in der Praxis bewährt", versichert Voigt.

„Wenn man sich Gedanken über Kennzahlen macht, muss man sich auch über die Strategie des Unternehmens Gedanken machen", ergänzt **Ralf Siegmund** von **Krones**. Es helfe nichts, einem Unternehmen ein Kennzahlensystem überzustülpen. Die Mitarbeiter müssten Kennzahlen auch verstehen, die Philosophie teilen und aktiv an der Lösung von Problemen mitarbeiten. Am Beispiel einer südamerikanischen Brauerei zeigte er, wie das Unternehmen mittels eines zentralen KPI-Benchmarkings eine standortübergreifende Transparenz erhielt. Hier ging der Impuls entscheidend vom Management aus, das sich mit der Einführung des Systems ein MVV-Programm (Motivation–Value–Vision) aufgelegt hat und das inzwischen auch in allen Unternehmensteilen gelebt wird.

Insgesamt ist das Unternehmen schnell gewachsen und hat eine ständig steigende Artikelzahl. Bisher wurden alle Daten manuell erfasst. Feinplanung und Auswertung wurden in Excel erstellt. Es war keine durchgängige Transparenz vorhanden. Teilweise wurden unterschiedliche Berechnungsmethoden an unterschiedlichen Standorten verwendet, was die Datenqualität nicht vergleichbar machte. Verständlich, dass die Auswertungen vom Management mit Misstrauen betrachtet wurden. Nach einer Ist-Analyse wurden die verschiedenen Zähler in einer einheitlichen Systematik aufgenommen, in die Zentrale übertragen und ausgewertet. „Sofort nach einer ersten Auswertung der OEE zeigten sich Fehler in der Wartungsstrategie eines Betriebes", sagt **Dieter Bischkopf**, **Krones**-Projektleiter. „Gerade wenn man die OEE auflöst bis in die Nebenzeiten wie Reinigen und Rüsten, die nicht technisch bedingt sind, sondern organisatorisch, zeigt sich das Optimierungspotenzial. Durch gezieltes Training kann man die Rüst- oder Reinigungsvorgänge deutlich reduzieren. Daraus kann man dann Standardvorgaben und Abläufe festlegen, wie lange eine Reinigung zu dauern hat." Auf einem Dashboard sowohl im Management als auch beim Werker wird die Produktivität als Trendverlauf im Vergleich zur Vorwoche oder dem Vormonat angezeigt.



Quelle: Vogel-Heuser 2009

Wie kommt man zu einem erfolgreichen MES-System?

„Wer in IT investiert, sollte es wie eine Anlageninvestition sehen. Niemand würde ohne genaue Spezifikationen eine Produktionsmaschine kaufen", sagt Tobias Voigt. Doch die Praxis sieht anders aus und die Systeme werden ohne Anforderungsdefinition installiert. Besser sei eine intensive Zusammenarbeit mit dem Lieferanten, mit dem man das Lasten- und Pflichtenheft schreibt, rät Voigt. „Helfen kann die TU München im Bereich der Funktionsempfehlungen für MES und im Bereich der Schnittstellen an den Maschinen mit den Weihenstephaner Standards."

Standardisierte Software, die alle Systeme und Prozesse miteinander verbindet, ist auch das Thema von **Christian Maurer**, MES Champion F&B bei **Siemens**. Am Beispiel der österreichischen Brau Union zeigte er, dass es sich lohnt, Schlüsselelemente der Kunden-IT zu standardisieren. So entwickelte Siemens mit der Manufacturing Operation Management Platform (MOM) eine Schnittstelle zum ERP und zum Prozess. Die Manufacturing IT-Plattform verbindet die PLM, ERO- und Automatisierungsinseln zu einem koordinierten Unternehmensmodell. Bisher erfolgte bei Brau Union die Datenerfassung an den Maschinen zu 100 % manuell. Es war keine Verbindung zu SAP vorhanden, es erfolgte kein automatisches Update der überlagerten Systeme und das Berichtswesen basierte auf Excel. Dies sollte mit der Implementierung von Simatic IT geändert werden.

Als Erstes wurde ein MES-Pilot in der Brauerei Wieselburg implementiert. Es bildet mehrere Chargengebiete pro Linie ab und berichtet in einem Heinecken spezifischen Kennzahlensystem. Das Projekt wurde mit dem höchstmöglichen Return on Investment (ROI) und dem geringstmöglichen Total Cost of Ownership (TCO) abgewickelt. D.h., das Projekt wird mit dem potenziellen Ertrag gerechtfertigt, den es mit sich

bringt. Der Erfolg des Projekts wird nach den Gesamtkosten inklusive Kosten für Support, Wartung und Weiterentwicklung beurteilt. Um nun als Systemintegrator auf der sicheren Seite zu sein, setzte Siemens auf modulare, skalierbare Architektur und Funktionalität mit dem Simatic IT-Portfolio, das alle Anforderungen der Brau Union abdeckt.

„Schlüsselfaktoren für die Auftragsvergabe an Siemens war der konkurrenzfähige TCO und die Kompetenz für das MES-Rollout", sagt Maurer. Standard-Software braucht weniger Anpassungen an bestehende Systeme, hat die entsprechende Flexibilität und Wartungsfähigkeit, da sie auf Standards aufsetzt. Damit ist die Möglichkeit für die Entwicklung eines Templates für einen unternehmensweiten Rollout und die Etablierung einer Systembasis als Plattform für weitere MES-Funktionen gegeben.

Doch es geht auch mit einem eher universitären Forschungsansatz, wie **Stefan Flad** von der **TU München** erklärt: „Betrachtet man einfach mal den Einsatz von Programmen in der Industrie, so stellt man fest, dass sehr viele programmtechnische Insellösungen existieren. Wir gehen davon aus, dass durch die individuellen Anpassungen und Schnittstellenrealisierung sowie durch die Nachbesserung aufgrund unzureichender Projektspezifikationen 10 % Kosten für Hard- und Software anfallen, aber die restlichen 90 % Personalkosten sind." Aus diesem Grunde versucht die Wissenschaft gerade, die strenge Hierarchie der Automatisierungspyramide aufzubrechen und immer mehr Komponenten zu modularisieren. Als Referenzmodell gilt – auch im Hinblick auf die Herausforderungen bei Industrie 4.0 – das sogenannte Automatisierungsdiabolo, bei dem die Kopplung von Modul zu Modul über ein Informationsmodell geschaffen wird. Dies reduziere die Anzahl der Schnittstellen von n x m auf n + m, so Flad. In Zusammenarbeit mit Copadata entwickelt die TUM einen OEE-Wizard, der sowohl die Anlagenbeschreibung als auch das Informationsmodell für die MES-Instanz enthält. Auf der Basis des Weihenstephaner Standards entsteht beim Import der Anlagenstruktur automatisch ein OEE-Client, der beispielsweise für das Tracking & Tracing oder das Energiemanagement eingesetzt werden kann. Die generische MES-Spezifikation wird über je einen Codegenerator von ProLeit und Artschwager & Kohl in die Automatisierungsebene übertragen.

Blick in die Zukunft

Die Wirtschaft steht an der Schwelle zur vierten industriellen Revolution. Durch das Internet getrieben, wachsen die reale und virtuelle Welt immer weiter zu einem Internet der Dinge zusammen. Kennzeichen zukünftiger Industrieproduktion wird die hoch flexibilisierte Serienproduktion stark individualisierter Produkte und die weitgehende Integration von Kunden und Geschäftspartnern in Geschäfts- und Wertschöpfungsprozesse sein. Als Beispiel nannte Voigt einen klassischen Verbraucher, der ein individuelles Bier verschenken möchte. Dies ist heute schon möglich mit der Braufabrik oder anderen Shops im Web. Damit wird sich die Getränke- und Lebensmittelproduktion der Zukunft deutlich verändern: Weg von der Großserienproduktion, vom Großhandel etc. hin zur kundenorientierten Produktion. Dies vereinfacht zunächst die Lieferkette, stellt aber zusätzliche Anforderungen an die IT in der Lebensmittelproduktion. Für die Chargenverfolgung heißt das nicht mehr, dass eine große Produktionscharge verfolgt wird, sondern das einzelne Six-Pack mit einem individuellen Etikett. Aus der starren Automatisierungspyramide wird ein Diabolo (siehe Abb.).

Neue Geschäftsmodelle nehmen immer mehr Raum ein. So berichtete **Dr. Klemens van Betteray** von **CBS-Systems** über Anwendungsmöglichkeiten im Cloud Computing. Als Komplett-IT-Dienstleister stellt CBS eine IT-Komplett-Lösung mit einem ERP und MES her, die die Belieferung von 1250 Edeka-Märkte koordiniert. Diese oder ähnliche Applikationen können natürlich auch in einer Cloud laufen. „Dies bringt vor allem für mittelständische Unternehmen große Einsparpotenziale", weiß van Betteray zu berichten. „Besonders die Investitionskosten können halbiert werden, die Betriebskosten lassen sich mit Cloud Computing sogar um 60 % senken." Erste Kunden nutzen die Cloud-Software des CBS-Rechenzentrums schon für Telematik- und Logistikanwendungen. So lassen sich beispielsweise Fahrzeuge/LKW mit einer Telematik-Box über Mobilfunk an den Telematik-Server des Rechenzentrums anbinden. Relevante Daten werden automatisch ermittelt und als elektronisches Fahrtenbuch geführt, das manipulationssicher allen steuerlichen und gesetzlichen Rahmenbedingungen entspricht. Nach der Übergabe von ERP-Daten an das Planungssystem werden Touren und Abfolge geplant und an das ERP-System und die Fahrzeuge versendet. Einsparungen von rund 16 % oder 5.000 bis 7.000 Euro pro LKW und Jahr schlagen zu Buche, so van Betteray. Andere Cloud-Anwendungen zielen auf die Bereitstellung von ERP- und MES-Funktionalitäten. So rechnet CBS-Systems bei der Umsetzung des elektronischen Geschäftsverkehrs bei Handelsunternehmen mit bis zu einem Euro Einsparung pro Rechnung. Und mit der internationalen Vernetzung kommen auch noch weitere mobile Anwendungen hinzu. **R.H.** ■