Effektive Angriffe zielen inzwischen nicht mehr auf Schwachstellen in der Kryptographie, sondern auf die Integrität des Gesamtsystems. Gelingt es dabei dem Angreifer den Code oder die Systemstruktur durch Schadsoftware oder geänderte Hardware in seinem Sinne zu verändern, so kann er damit alle konventionellen Schutzmaßnamen umgehen. Der in IUNO entwickelte Sicherheitschip enthält deshalb eine kryptographische Funktion um die Integrität des Codes und indirekt auch den Status von Soft- und Hardware zu messen. Durch Überprüfen der Signatur können dann ungewollte Veränderungen erkannt und Gegenmaßnamen eingeleitet werden.

Hans Brandl,
sichere Prozessoren / Chipkartenchips, Infineon Technologies AG

Der in IUNO entwickelte visuelle Security-Leitstand erfasst Datenströme in der Produktion in Echtzeit mit dem Ziel, relevante Daten über den aktuellen Stand der Informationssicherheit ganzheitlich und übersichtlich abzubilden. So werden Abweichungen in der Produktion sofort sichtbar und können korrigiert werden. Die Teilnehmer eines Produktionsnetzes sind transparent und eindeutig identifizierbar, sowie Störeinflüsse erkennbar. Die Überwachung des aktuellen IT-Sicherheitsstands ist notwendig, um die langfristige unternehmerische Sicherheit zu gewährleisten. Produktionsausfälle und Marketingschäden werden dadurch effektiv vermieden.

Ricardo Hormann und Stephan Teuber,
Doktoranden, Volkswagen AG

Die vielfältigen positiven Auswirkungen und Chancen durch die Digitalisierung und Vernetzung in der Produktion sollte man nicht durch ein vages Gefühl der Unsicherheit verwirken. Daher ist es generell ratsam, sich bei Unklarheiten ganz einfach fachliche Unterstützung zu holen. Es gibt sowohl organisatorische als auch technologische Möglichkeiten, mit denen das Schutzniveau sehr stark verbessert werden kann. Bereits bei der Planung von neuen Produktionsprozessen ist es empfehlenswert auch die Sicherheitsaspekte mit zu betrachten.

Bartol Filipovic,
Leiter Produtschutz und Industrial Security, Fraunhofer AISEC

Die Priorisierung der Themen rund um IT-Sicherheit wird an Wert gewinnen, wenn mit der Zeit größere Angriffe und folglich auch Schäden bei den Firmen zu beobachten sein werden. Solange die Kosten für die Absicherung höher sind, als möglicher Schaden, werden die für die Verteidigung benötigten Maßnahmen nicht ergriffen. Die zum Teil fehlende IT-Infrastruktur in Unternehmen hat uns in IUNO dazu veranlasst, eine Cloud-Lösung für die Fernwartung zu entwickeln. Bei einer cloudbasierten Lösung muss sich der Betreiber der Anlage nicht um die Verfügbarkeit der Fernwartungslösung, das Updatemanagement und die Anbindung an unterschiedliche Fernwartungsdienstleister kümmern.

Alexander Borisov,
Kryptografie und IT-Sicherheit für Industrie 4.0, Robert Bosch GmbH

Der kleine Mittelstand muss unbedingt darüber nachdenken, welchen Mehrwert er seinen Kunden durch flexiblere Produktion, Digitalisierung und Zusammenarbeit mit anderen Unternehmen in der Produktionskette bieten kann. Dabei hilft es, sich Pilotprojekte und Forschungsergebnisse genau anzusehen sowie Leitfäden und Hilfestellungen von Verbänden wie dem VDMA zu nutzen. Abzuwarten wäre fatal.

Oliver Winzenried,
Mitbegründer und Vorstand, WIBU-SYSTEMS AG

Für uns als Beratungshaus liegt es in der Natur der Sache, aus IUNO heraus Entwicklungsarbeit im Mittelstand zu leisten und die Unternehmer darüber aufzuklären, welche Mehrwerte sie aus Industrie 4.0 ableiten können. IUNO trägt hier viel zur Sichtbarkeit von nachhaltiger IT-Sicherheit als Anforderung bei. Auch Hersteller fragen vermehrt nach Unterstützung bei der Umsetzung von Sicherheitsanforderungen in ihren Produkten, während Betreiber von Anlagen sich ihre Einkaufsrichtlinien mit den Erkenntnissen aus IUNO erweitern lassen. Hier sehen wir den besonderen Beitrag von IUNO: die direkte Übertragung der Forschungsergebnisse auf die Industrie – und das bereits heute und nicht erst nach Abschluss des Projektes.

Sebastian Rohr,
Technischer Geschäftsführer, accessec GmbH

Als IT-Schutzziel steht im Produktionsbereich die Verfügbarkeit ganz oben. Die Maschinen produzieren am effizientesten, wenn sie ohne ungewollte Unterbrechung betrieben werden können. Weiterhin kommt der Integrität der Daten eine besondere Bedeutung zu. Hier wird im Rahmen des IUNO-Projekts betrachtet, wie sich die Manipulation von Daten auf Maschinen auswirkt. Für den Informationsaustausch zwischen Unternehmen im Rahmen der Industrie 4.0-Szenarien ist die Einhaltung der Schutzziele Vertraulichkeit und Verbindlichkeit wichtig.

Hermann Köhne,
Leiter IT-Sicherheit, nobilia-Werke

Zu allererst müssen sich die Unternehmen über ihre zu schützenden Werte klar werden. Das scheint selbstverständlich, ist aber selbst bei großen Konzernen oft nicht abschließend ermittelt und beschrieben. Erst wenn das feststeht, kann man abschätzen, welche Bedrohungen auf diese Werte einwirken und welche Rolle IT-Sicherheit dabei spielt. Auf der Basis kann man dann eine Risikoabschätzung vornehmen und eine entsprechend abgestimmte Sicherheitspolitik entwickeln.

Dr. Thorsten Henkel,
Datenmanagement, Datenschutz und Datensicherheit,
Fraunhofer SIT

IUNO beschäftigt sich mit einem ganz wesentlichen Aspekt der intelligenten Produktion von morgen. Grundvoraussetzung für Industrie 4.0 ist die Vernetzung aller Komponenten innerhalb einer Produktionsanlage und auch die nahtlose Einbindung in die Geschäftsprozesse der Unternehmen und das über den ganzen product life cycle. Die damit immer weiter voranschreitende Vernetzung aller Systeme innerhalb eines Unternehmens bietet auch immer mehr potentielle Einfallstore für Angreifer. IUNO hilft, Bewusstsein für IT-Sicherheit zu schaffen sowie Lösungsvorschläge zu erarbeiten, diese zu erproben und zu standardisieren.

Martin Müller,
Vice President I/O and Networks, Phoenix Contact

Die Sicherstellung der Geräte- und Systemintegrität von industriellen Komponenten ist essentiell für die Güte und Qualität des automatisierten Produktionsprozesses. Unter „Integrität“ ist hierbei zu verstehen, dass sich die Komponenten und Systeme funktional wie gewünscht und beschrieben verhalten. Im Projekt IUNO untersuchen wir verschiedene Mechanismen für den Integritätsschutz, die miteinander kombiniert einem Defense-in-Depth-Prinzip auf Komponentenebene folgen.

Kai Fischer,
Senior Key Expert Research Scientist, Siemens Corporate Technology

Ohne vernünftige Konzepte zur IT-Sicherheit wird Industrie 4.0 scheitern. Die dazu notwendige Vernetzung über die Unternehmensgrenzen hinaus macht die Produktion in zunehmendem Maße anfällig für Gefahren aus dem Internet. Im Office-Bereich hat man damit sicherlich schon länger Erfahrung und auch Technologien zum Schutz entwickelt. Diese müssen nun auf ihre Tauglichkeit im Produktionsbereich untersucht werden. Aus dieser Motivation heraus ist IUNO entstanden, um Lösungen für eine sichere Industrie 4.0 zu entwickeln.

Ernst Esslinger,
Director Methods/Tools, HOMAG und IUNO-Konsortialführer

Der primäre Nutzen der Einführung eines Technologiedatenmarktplatzes ist die Verfügbarkeit eines sehr breiten Angebots verschiedenster Daten, die in der Produktion benötigt werden. So hat ein Produktionsleiter die Vielzahl aller potentiellen Datenlieferanten in einem System vereint und kann dort einfach nach passenden Datensätzen suchen. Mit dem Einkauf der Daten auf der Plattform spart der Produktionsleiter zudem Geld, da er die benötigten Daten bedarfsgerecht, also pro Stück oder pro Zeiteinheit, zur Nutzung lizenzieren kann.

Hans-Peter Bock,
Experte für Industrie-4.0-Kommunikation und Security, TRUMPF

In Zukunft wird die Vernetzung in Produktionsanlagen weiter stark steigen. Hinzu kommt, dass Angreifer immer diversifizierter und spezialisierter vorgehen. Angriffe sind heutzutage oft maßgeschneidert auf den Anwendungsfall angepasst und werden von weit verbreiteten Angriffserkennungssystemen, die auf Signaturerkennung basieren, nicht detektiert. Methoden der Künstlichen Intelligenz sind geeignet, auch neuartige und bislang nicht dokumentierte Angriffe zuverlässig zu erkennen.

Prof. Dr.-Ing. Hans Dieter Schotten,
wissenschaftlicher Direktor, DFKI

Vor der Dritten Industriellen Revolution sagte damals der 36. US-Präsident Lyndon B. Johnson: „Die Automatisierung ist nicht unser Feind. Unsere Feinde sind Unwissenheit, Gleichgültigkeit und Trägheit." Anhand dieser aufrüttelnden Worte möchte ich nur zeigen, dass wir und nicht die Technik bei jedem Wandel die Hauptrolle spielen und genügend gesellschaftlicher und politischer Diskussionsstoff von Fachkräftemangel bis hin zu „German Angst" vorhanden ist, um Gründe zu finden, warum die Vorteile des digitalen Wandels noch nicht genutzt werden.

Daniel Marschalleck,
Leiter Digitalisierung Möbel, Duravit

Bei der Umstellung auf die vernetzte Produktion sehe ich die Hauptgefahr in den zahlreichen Kanälen, Schnittstellen und Protokollen, die das Unternehmen seinen Kooperationspartnern anbieten muss, um eine vernetzte Produktion im großen Stil zu realisieren. Gelingt es einem Angreifer, in solche Verbindungen einzudringen, so sind alle Systeme, die mit diesen in IT-Verbindung stehen, gefährdet. Um diese Schäden abzuwenden, bedarf es eines gestaffelten Schutzkonzepts. Im IUNO-Projekt forschen wir an den nötigen Verteidigungsfronten, um dafür praktikable Lösungen zu entwickeln.

Dr. Reinhard Schwarz,
Senior Engineer am Fraunhofer-Institut IESE

Der Grad der höheren Automatisierung in Industrie 4.0 wird mit der Vernetzung bisher separater, unvernetzter Entitäten an das Internet und damit mit einem erhöhten Datenaufkommen erkauft. Big Data –Analysen versprechen dann nicht nur Chancen im Hinblick auf die Verbesserung eigener Wirtschaftstätigkeit, sie bieten gleichfalls Risiken durch die Auswertung etwa von Konkurrenten. Das Ausspähen von Daten, Kopieren oder Nachahmen von Geschäftsmodellen, die auf digitale Produkte setzen, ist dann ebenso ein Risiko, wie auch die Ausfuhr digitaler Produkte mit starker Verschlüsselung, die ihrerseits gegen Ausfuhrbestimmungen verstoßen können.

Ass. iur. Johannes Müller MLE,
provet, Universität Kassel