Risiko: Das Ende eines Konzeptes?

Smarte Systeme kennzeichnen einen tiefgreifenden Wandel von Produktions- und Dienstleistungssystemen. Zudem steigen Erwartungen an Resilienz und Nachhaltigkeit. Das etablierte Risikokonzept reicht vermutlich nicht aus, um als Management-Werkzeug für Organisation und Kontrolle smarter Produktions- und Dienstleistungssysteme dienen zu können.

Von Ralf Mock und Christian Zipper

Schlagwörter wie Smart Manufacturing und Industrie 4.0 deuten bevorstehende Umwälzungen und Automatisierung in der produzierenden Industrie und im Dienstleistungssektor an. Die Erwartungen an solche smarten Systeme sind neben ökonomischen Vorteilen eine ausgewiesene Resilienz und Nachhaltigkeit. Eine wesentliche Rolle spielt dabei der umfassende Einsatz von Informations- und Kommunikationstechnik (IKT). Eine Frage für Unternehmen und Organisationen ist, ob das etablierte Konzept des Risikomanagements für diese neue Produktions- und Dienstleistungswelt methodisch und konzeptionell geeignet ist. Die Grundlage für die folgende Diskussion ist somit der Stand der Technik, wobei für diesen Beitrag vor allem Standards der International Organization for Standardization (ISO) eine Rolle spielen.

Risikomanagement

Risikomanagement nach ISO 31000:2009 umfasst «koordinierte Aktivitäten zur Lenkung und Steuerung einer Organisation in Bezug auf Risiken». Dieses Konzept hilft, Risiken zu finden, zu analysieren und zu bewerten. Die Ergebnisse aus dieser Beurteilung dienen letztlich dazu, Risiken zu minimieren und die Wirksamkeit von Massnahmen zu kontrollieren. Die Aktivitäten sind Teil einer umfassenderen Kommunikation über alle Unternehmens- und Entscheidungsebenen. Hierfür haben sich Managementprozesse und Analysemethoden etabliert. Ein Beispiel für eine Methode, die diesen Ansatz abdeckt, ist die verbreitete Failure Mode and Effects Analysis (FMEA).

Die ISO 31000:2009 definiert Risiko allgemein als «Auswirkung von Unsicherheit auf Ziele» (effect of uncertainty on objectives). Ziele sind dabei alle Arten von Unternehmenszielen, zum Beispiel strategische und prozessbezogene Ziele. Konzentriert man sich jedoch auf den Umgang mit technischen Risiken, wie im Risk Engineering üblich, so ist Risiko definiert als Ausmass und Häufigkeit eines (unerwünschten) Ereignisses. In der ISO 31000:2009 findet man diesen Ansatz unter dem Begriff Risiko unter Anmerkung 4.

Anforderungen an smarte Systeme

Die Produktionssysteme der (nahen) Zukunft sind durch Smartness gekennzeichnet. Einen Hinweis darauf, was unter smarten Systemen zu verstehen ist, gibt die ISO/TS 37151:2015 «Smart Community Infrastructures». Leicht verallgemeinert ist ein smartes System eine «[…] Infrastruktur mit erweiterter technischer Leistungsfähigkeit, die dafür ausgelegt ist, betrieben und unterhalten wird, um zur nachhaltigen Entwicklung und Resilienz […] beizutragen». Somit erfordert eine Analyse smarter Systeme den Nachweis

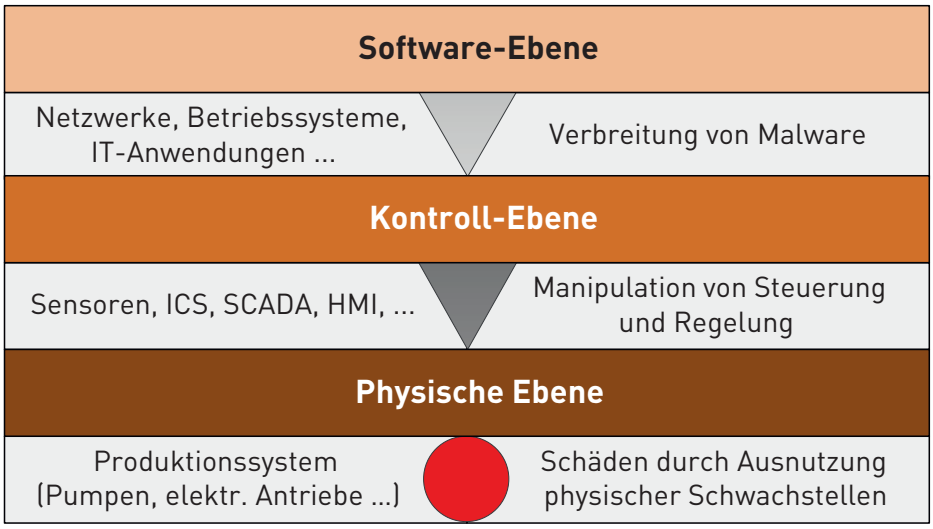

Abb. 1: Mehrschichtenmodell computergesteuerter und vernetzter Systeme

ICS: Industrial Control System; SCADA: Supervisory Control and Data Acquisition; HMI: Human-Machine-Interface

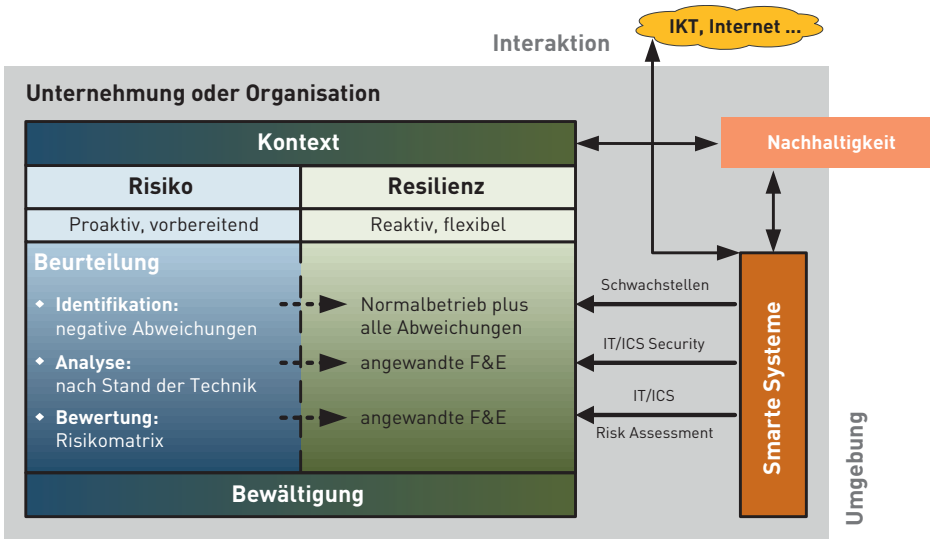

Abb. 2: Einfluss smarter Systeme auf Managementprozesse

IT: Informationstechnik; IKT: Informations- und Kommunikationstechnik; ICS: Industrial Control System

von Resilienz und Nachhaltigkeit als betriebliche Anforderungen. Auch hier klärt die ISO/TS 37151:2015 die Begrifflichkeiten. Resilienz bedeutet, «[…] dass Systeme dafür ausgelegt sind, Dienste in Notfällen weiterhin zu erbringen und sich rasch von Schäden und der Einstellung von Diensten erholen». Die ISO/TS 37151:2015 definiert Nachhaltigkeit als die «Beschaffenheit des globalen Systems, einschliesslich ökologischer, gesellschaftlicher und wirtschaftlicher Aspekte, bei dem die Bedürfnisse der Gegenwart erfüllt werden, ohne das Vermögen künftiger Generationen zu gefährden, ihre eigenen Bedürfnisse erfüllen zu können». Dies entspricht der Definition von Nachhaltigkeit nach Brundtland. Künftige Geschäftsleitungen sollten somit nachweisen können, dass die smarten (Industrie-)Systeme inhärent mit dynamischen Einflüssen umgehen können (Resilienz) und dass die Managementprozesse umfassendere Anforderungen und Kriterien als bis anhin üblich berücksichtigen (Nachhaltigkeit).

Technik smarter Systeme

Smarte Systeme kennzeichnen den aktuellen Schritt der industriellen Entwicklung in Richtung Automatisierung und Vernetzung. Funktion und Aufbau smarter Systeme sind mehrschichtig und erfordern die Analyse (mindestens) dreier Ebenen, wie in Abbildung 1 skizziert. Das Risk Engineering hat sich bisher auf die physische Ebene konzentriert. Smartness bedeutet auch den Einsatz des Internets der Dinge. Solche Systeme kommunizieren untereinander (Machine-to-Machine; M2M) und sind in der Lage, ohne Hilfe des Menschen Entscheidungen zu treffen. Vor allem die Kontrollebene ist somit einem massiven Wandel unterworfen. Damit bekommt die (virtuelle) Welt der Informatik massiven Einfluss auf die physische Welt der Produktion und smarte Produktionssysteme entwickeln sich zu (nichtkritischen) Infrastruktursystemen.

Die Abbildung 1 ist stark vereinfachend und jede Ebene lässt sich weiter unterteilen. So umfasst das OSI-Referenzmodell (Open Systems Interconnection Model) allein von der Bit-Übertragung bis zur IT-Anwendung sieben Schichten für die Software-Ebene.

Analyse smarter Systeme

Smarte Systeme erfordern in Unternehmen und Organisationen ein dem Risikomanagement entsprechendes Konzept, also Identifikations-, Analyse- und Beurteilungsprozesse, um mit diesen Systemen umgehen zu können. Es stellt sich die Frage, ob das Risikokonzept für smarte Systeme anpassungsfähig genug ist und einen passenden Rahmen für Managementaktivitäten bereitstellt.

Das etablierte Konzept des technischen Risikomanagements stammt aus einer Zeit ohne Internet und Smartness. So gehen die Ursprünge der FMEA auf Ende der 1940er-Jahre zurück. Es wundert daher nicht, dass solche Methoden wenig geeignet sind, IKT-abhängige Systeme in ihrer Vielschichtigkeit, Komplexität und Dynamik abzubilden. In der Informatik werden diese Methoden daher auch wenig verwendet. Zudem weicht das Interesse der IT-Security von den Zielen des Risk Engineerings ab. IT-Security ist eng auf die Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit (confidentiality, integrity, availability; CIA) von Informationen und Daten ausgerichtet, wobei Bedrohungen (threats) die dazu passenden Schwachstellen (vulnerabilities) ausnutzen. Eine Ausnahme ist der Ansatz des «Guide for Conducting Risk Assessments – Information Security» des National Institute of Standards and Technology (NIST SP 800-30 Rev 1.; 2012). Zur Systemanalyse von Kommunikationsarchitekturen und für die Software-Entwicklung nutzt die Informatik sonst eigene Methoden, zum Beispiel die UML-System-Diagramme (Unified Modeling Language).

Analyse	Abweichungen vom Soll-Zustand			
	gefährlich/ negativ	ungefährlich/ negativ	ungefährlich/ positiv	mit Erholbarkeit
Zuverlässigkeit	X	X	–	X
Risiko$_{RE}$	X	–	–	–
Risiko$_{ISO}$	X	X	X	–
Resilienz	X	X	X	X

Tab. 1: Ziele typischer Systemanalysen

Risiko$_{RE}$: Analyse gem. Risk Engineering;
Risiko$_{ISO}$: Analyse nach ISO 31000:2009 allg.

Ein besonderes Problem für die Risikoanalyse smarter Systeme stellt das Verschwimmen von System- und Komponentengrenzen dar. (Wo ist das Internet bzw. Intranet lokalisiert?) Sich mit der Zeit einen Erfahrungsschatz aufzubauen, um künftiges Ausfallverhalten besser einschätzen zu können, passt ebenfalls nicht mehr zu den technischen Gegebenheiten. Ein Software-Patch oder ein Update der Firmware beseitigt eine Schwachstelle und ist dann für Analysen nicht mehr relevant.

Management smarter Systeme

Managementsysteme nutzen Resultate aus Analysen, wobei die Analysen auf bestimmte Ziele ausgerichtet sind. Tabelle 1 fasst die Kernziele im Risk Engineering üblicher Systemanalysen zusammen. So befasst sich eine Zuverlässigkeitsanalyse mit gefährlichen und ungefährlichen negativen Systemabweichungen, zum Beispiel dem Ausfall von Systemkomponenten. Der Einfluss von Instandhaltung als technischem Erholungsprozess gehört dazu.

Nach Tabelle 1 richtet sich der Blickwinkel im Risk Engineering auf die Analyse ungeplanter Abweichungen eines Systems vom Sollzustand. (Warum versagt es?) Das etablierte Risikomanagement ist dabei präventiv ausgelegt, das heisst im Sinne einer Vorsorge (preparedness) und geht damit fliessend ins Kontinuitätsmanagement über, zum Beispiel nach ISO 22301:2012 «Societal security – Business continuity management systems – Requirements». Resilienzanalysen hingegen richten ihr Interesse auf die inhärente Fähigkeit sozio-technischer Systeme aus, reaktiv mit sich ändernden Rahmen- und Betriebsbedingungen zurechtzukommen, und gehen vom Sollbetrieb des Systems aus. (Warum funktioniert es?) Die typischen Systemanalysen des Risk Engineerings sind somit nicht für Resilienzanalysen ausgelegt. Nachhaltigkeit erweitert den Rahmen nochmals. Kernpostulate nachhaltiger Entwicklung sind Effizienz, Suffizienz und Konsistenz. Effizienz bedeutet ein möglichst optimales Verhältnis von Input zu Output. Konsistenz ist im Sinne der Verträglichkeit mit der Umwelt zu verstehen, zum Beispiel eine Produktion ohne umweltbelastende Stoffe. Konsistenz ist eine klassische ingenieurtechnische und (umwelt-)naturwissenschaftliche Disziplin der Systemoptimierung. Suffizienz hingegen verweist auf den verstärkten Einfluss eines fliessenden gesellschaftlich-normativen Beurteilungsprozesses auf das Management und hinterfragt das Mass der Angemessenheit. Die Abbildung 2 skizziert Zusammenhänge nach Einführung smarter Systeme auf Managementprozesse in einer Unternehmung oder Organisation und zeigt unter anderem Schnittstellen zu Resilienz und Nachhaltigkeit auf. Von aussen wirken Informations- und Kommunikationssysteme (das Internet) sowie Nachhaltigkeitsanforderungen auf das Management ein.

Die Entscheidung einer Geschäftsleitung für smarte Systeme heisst auch, sich auf faktisch unbegrenzte und vielschichtige Infrastruktursysteme einzulassen (vgl. Abb. 1). Solche Systeme sind schon jetzt mit etablierten Methoden des Risk Engineerings schwer oder nur ungenügend zu untersuchen. Damit werden Methoden aus dem Software Engineering und der Informatik, der IT- und ICS-Security (Industrial Control System) bei Prozessen des Unternehmens- und Produktionsmanagements eine bedeutendere Rolle als bisher spielen.

Ein vorläufiges Fazit

Nimmt man die Begriffe beim Wort, dann reicht nach Ansicht der Autoren das etablierte Risikokonzept nicht aus, um als Management-Werkzeug für Organisation und Kontrolle smarter, resilienter und nachhaltiger Produktions- und Dienstleistungssysteme zu dienen. Der Einbezug des erweiterten sozio-technischen Rahmens erschwert den Einsatz zusätzlich und lässt spätestens dann die Frage nach den erforderlichen Ansätzen und Ressourcen für die Durchführung von Analysen prominent werden. Dieses Fazit gilt übergreifend für alle Branchen, die smarte Technik einsetzen, zum Beispiel auch im Dienstleistungssektor. Zum einen sind Versicherer und Beratungsunternehmen direkt davon betroffen und müssen ihre Werkzeuge an die Erwartungen ihrer Kunden anpassen, zum anderen sind sie dann selbst smart und nutzen automatisierte Prozesse.

In Zeiten des Wandels sollte das Organisationsmanagement in der Lage sein, Gültigkeit und Aussagewert laufender Risikomanagementprozesse kompetent hinterfragen zu können, um Wissenslücken frühzeitig zu schliessen. Wie soll ein solches Management aussehen? Welche methodischen Ansätze der Beurteilung liefern die nötigen Entscheidungshilfen? Welche strategischen und strukturellen Prozesse sind zu implementieren? Nach Meinung der Autoren bedeutet der Einzug von Smartness in Unternehmen und Organisationen, dass das gewohnte Risikokonzept als Basis für das (technische) Risikomanagement möglicherweise unzureichend ist. Umfassende konzeptionelle und methodische Änderungen und Neuerungen, wie man die neuen Systeme handhaben soll, deuten sich an. Fachhochschulen, wie die ZHAW Zürcher Hochschule für Angewandte Wissenschaften, zeigen anwendungsorientierte Ansätze in ihren Forschungs- und Entwicklungsprojekten auf und vermitteln methodische Grundlagen und neue Konzepte, zum Beispiel in Weiterbildungskursen zum Integrierten Risikomanagement oder zur Industrie 4.0. ■


RALF MOCK
Dr.-Ing., Sicherheitsingenieur, Dozent Integriertes Risikomanagement, ZHAW, Institut für Nachhaltige Entwicklung INE, Winterthur.
CHRISTIAN ZIPPER
Dr. sc. nat. ETH, Umweltnaturwissenschaftler, Studiengangleitung MAS Integriertes Risikomanagement, Dozent, ZHAW, Institut für Nachhaltige Entwicklung INE, Winterthur.