Foto: Fotolia

Siegfried Vössner

IT Security und Safety 4.0 Herausforderungen und Bedrohungen im dämmernden Zeitalter von Cyber-Physischen Systemen von Systemen

Welche Sicherheitskonzepte brauchen IT-Systeme zur Unterstützung von Industrie 4.0?

Ein Blick zurück

In der Geschichte der Menschheit hat es schon immer ein Auf und Ab von Kulturen und Strömungen gegeben. Meist wellenförmig bildeten sich Zentren kultureller und wirtschaftlicher Aktivität, verteilt über die ganze Erde. Einige der Inhalte werden im Laufe der Zeit explizit oder implizit wiederentdeckt. Man denke zum Beispiel nur an das Sprichwort der Griechen: „Alter Wein in neuen Schläuchen", die Renaissance oder das Biedermeier.

Auch in Technik und Wissenschaft ist das so. Viele „neue" Ideen sind in Wirklichkeit Jahrzehnte, gar Jahrhunderte alt und kehren immer wieder. So auch als Zukunftsvisionen von Leonardo da Vinci bis Jules Verne, Gene Roddenberry und wie sie alle heißen.

An dieser Stelle kam und kommt die Technologie ins Spiel, die es durch ihre, besonders in den letzten zwei Jahrhunderten, rasante Weiterentwicklung ermöglicht hat, dass sich mehr und mehr der Ideen immer besser umsetzen lassen. Die Faszination der Technik hat dazu geführt, dass sich die Wissenschaft hauptsächlich auf die Entwicklung von Technologie konzentriert und deren Nutzen, Auswirkungen und Risiken aus dem Blickfeld verloren hat.

Dabei sind diese Themen genauso in den oben erwähnten Zukunftsvisionen größtenteils schon vorhanden und thematisiert. Seit vergleichsweise kurzer Zeit befasst sich die Wissenschaft mit technischen Systemen als Ganzes, ihren Architekturen, Eigenschaften und Interaktionen mit Mensch und Umwelt.

Systeme und Systeme von Systemen umgeben uns

Unter einem System verstehen wir eine Ansammlung von Elementen/Objekten und deren Eigenschaften, die durch Wechselbeziehungen miteinander verbunden sind (Hall und Fagen 1956). Manche Systeme sind zudem auch noch aus Teilsystemen aufgebaut bzw. sind ein System von Systemen. Seit jeher sind wir von solchen Systemen umgeben oder ein Teil davon. Man denke beispielsweise nur an das Ökosystem. Seit vergleichsweise kurzer Zeit haben die Menschen nun begonnen, diese Systeme selbst zu schaffen und sind dabei erst ganz am Anfang, die Eigenschaften dieser als Ganzes zu verstehen. Die meisten Technischen Universitäten sind dabei, dafür Lehrstühle einzurichten – so beispielsweise auch die Technische Universität Graz zum Thema *Systemarchitektur.*

Cyber-Physische Systeme

Die größten, von Menschen geschaffenen Systeme waren historisch gesehen Bauwerke und Maschinen und in letzter Zeit vernetzte Informationssysteme.

Was liegt nun näher als diese Werke zu verbinden? Somit könnte es möglich werden, alle von Menschen geschaffenen Systeme zu wenigen, großen Systemen zu verbinden.

Eine der ersten Ideen, *„intelligente"* Maschinen zu vernetzen, findet man beispielsweise beim Schriftsteller Karel Capek (1920) oder in den Kurzgeschichten „I, Robot" von Isaac Asimov 1950. Konkreter werden diese Systeme in der Hightech-Strategie „Industrie 4.0" des deutschen Bundesministeriums für Bildung und Forschung beschrieben (2011). Dort heißt es unter anderem:

„ ...Cyber-Physische Systeme (CPS) sind Netzwerke kleiner mit Sensoren und Aktoren ausgestatteter Computer, die als sogenannte Eingebettete Systeme in Materialien, Gegenstände, Geräte und Maschinenteile eingebaut und über das Internet miteinander verbunden werden. In einem derartigen Internet der Dinge verbinden sich die physische und die digitale Welt. Anlagen, Maschinen und einzelne Werkstücke tauschen kontinuierlich Informationen aus. Sämtliche Produktions- und Logistikprozesse werden integriert. Aus dieser Schlüsseltechnologie leiten sich zahlreiche industrielle Anwendungen ab: In Zukunft werden viele Prozesse in Echtzeit über große Entfernungen gesteuert und koordiniert...."

Dazu muss angemerkt werden, dass diese Vision Teil einer Strategie ist, die bis ins Jahr 2025 blickt und auch explizit den notwendigen Forschungsbedarf betont. Seit etwa einem Jahr hat sich massiv der Ergebnisdruck von der Anwenderseite erhöht, und es entstehen mit Unterstützung von Systemlieferanten erste pragmatische Lösungen. Lösungen, die neben den technischen Herausforderungen auch eine beträchtliche Sicherheitsherausforderung darstellen.

Sicherheitsherausforderungen und Bedrohungen

Einige der Grundrisiken, die bei solchen Systemen auftreten können, sind schon ebenso lange bekannt, wie die eingangs beschriebenen Zukunftsvisionen. Beispielsweise die Gefährlichkeit des von Menschen geschaffenen Wesens Golem (im Talmud nachzulesen), die Gefahr des Informationsmissbrauchs in George Orwells „1984", den Science Fiction Filmen *„The Matrix* (1999) oder *„Terminator 3: Rise of the Machines* (2003)", um nur ein paar wenige zu nennen. Nachdem einige dieser Zukunftsvisionen reale Wirklichkeit geworden sind, wurden aus Risiken auch konkrete Bedrohungen.

Da hier die Verhinderung von System-Fehlfunktionen mit signifikanten Auswirkungen auf Systemfunktion und Umwelt im Vordergrund stehen, erscheint es sinnvoll, den Begriff System-„Sicherheit" gemeinsam für beide Bereiche „Safety" und „Security" zu verwenden. Dabei sei auch angemerkt, dass viele Systeme, die wir heute bauen auch ohne Angreifer instabil und gefährlich sind. Menschliche Aktivitäten können dies noch verstärken. Hier wäre beispielsweise die Cyberkriminalität zu nennen, ob sie nun kriminelle Beweggründe oder solche der Staatssicherheit hat.

Waren es bei IT-Systemen „lediglich" Angriffe auf Daten und Rechneranlagen, sind es nun IT-basierte Angriffe auf physische Systeme. Cyber-physische Angriffe sind heute Realität geworden. Auch gibt es bereits eine Reihe von Ausfällen kritischer Infrastruktur (z.B. Kraftwerke), welche durch IT-Angriffe durchgeführt wurden.

Angesichts der bereits bestehenden Realität ist es notwendig, das bestehende Risiko methodisch zu klassifizieren, analysieren, bewerten und gezielt Gegenmaßnahmen zu ergreifen. In diesem Bereich gibt es bereits einige Konzepte für den Schutz von IT-Systemen und den Schutz von kritischer Infrastruktur, die sich auf cyber-physische Systeme, wie I4.0 sie entwirft, übertragen lassen.

Nach einer methodischen und (möglichst) umfassenden Schwachstellen- und Fehleranalyse, werden im Zuge einer Risikobewertung die möglichen Fehlfunktionen von Systemen hinsichtlich ihrer Auswirkungen und der Auftretenswahrscheinlichkeit bewertet. Dabei spielt es zuerst einmal keine Rolle, ob die Fehlfunktion aufgrund eines Designfehlers, von höherer Gewalt oder bewusst durch Angreifer verursacht wurde.

Im Folgenden sollen speziell die für cyber-physische Systeme besonders relevanten Sicherheitsrisiken einzeln hervorgehoben werden.

Steigende Komplexität

Ein inhärentes Risiko ist die dramatisch gestiegene Komplexität von Einzelkomponenten. Intelligente Algorithmen, die komplexe Systemfunktionen ermöglichen, werden mit immer komplexeren Computerprogrammen umgesetzt. Neben der Fehleranfälligkeit durch die immens gestiegene Anzahl an Programmzeilen, wird ein methodisches Testen sehr aufwändig und aus Kostengründen selten durchgeführt.

Daneben gelingt es noch weniger, die Interaktion und gegenseitige Beeinflussung der Einzelkomponenten im Gesamtsystem zu testen. Ein modernes, numerisch gesteuertes Bearbeitungszentrum beispielsweise, wird von einem hochkomplexen Computersystem gesteuert. Somit wird Wartung und Fehlersuche sehr, sehr aufwändig bzw. unmöglich.

Mangelnde Fehlertoleranz durch mangelnde Diversität

Ein weiteres Problem liegt in den vermeintlichen Vorteilen der Wiederverwendung von Systemkomponenten. Dieses Konzept kommt aus der Massenfertigung und hat dort hauptsächlich aus Kostengründen seine Berechtigung. Gefährlich wird ein solches Konzept, wenn man daraus große Systeme baut. Alle mit den gleichen Fehlern, alle mit den gleichen Schwachstellen, alle gleich angreifbar (Abbildungen 1 und 2).

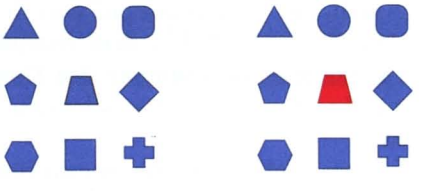

Abb. 1: Systemstabilität durch Diversität. Durch die vorgesehene Diversität der Systemkomponenten wirken sich Ausfälle (symbolisiert durch das rote Trapez) nur lokal aus

Ein gutes Beispiel dafür sind unsere mobilen Kommunikationsnetzwerke, deren Sicherheit an der Sicherheit der SIM-Karten (subscriber identity module) hängt. Ein erfolgreicher Angriff auf ein Einzelsystem lässt sich auch auf unzählige andere replizieren. Gleiches gilt für andere Netzwerkkomponenten wie Server, Router oder Internetmodems

Abb. 2: System-Monokulturen durch Wiederverwendung von Systemkomponenten. Neben den offensichtlichen Kosteneinsparungs- und Vereinheitlichungseffekten, führt ein solches Design zu systemweiten, simultanen Auswirkungen von Komponentenausfällen (symbolisiert durch das rote sowie die orangen Trapeze).

und sogar für Großserienprodukte, wie die im Editorial erwähnten Autos. Dies ist die Kehrseite von „Copy & Paste".

Netzwerkeffekte

Durch die Verbindung von Einzelsystemen entstehen darüber hinaus noch eine Reihe anderer Sicherheitsrisiken.
An erster Stelle sei hier systemisches Versagen zu nennen. So kann es beispielsweise zu unbeabsichtigten Kettenreaktionen, wie dem Abschalten von Energiesystemen und Leitungsknoten und damit auch zu gefährlichen Netzschwankungen bzw. Ausfällen kommen. So brachen beispielsweise im August 2003 im Nordosten der USA weite Teile des Stromversorgungsnetzes zusammen. Auslöser war eine Kettenreaktion bei der die Steuerungen einzelner Verteilerknoten andere im Netzwerk dazu brachten, sich ebenfalls abzuschalten. Ein weiteres Beispiel wäre der „Flash-Crash 2010", bei dem computergestützte Handelssysteme den Dow Jones Index um fast 10 % schwanken ließen.
Mit einer solchen Vernetzung geht eine gesteigerte Fehlerwahrscheinlichkeit einher. Die Ausfallswahrscheinlichkeit eines vernetzten, von allen Einzelkomponenten abhängigen Systems ist in der Regel viel höher als die von Einzelsystemen (Abbildung 3).

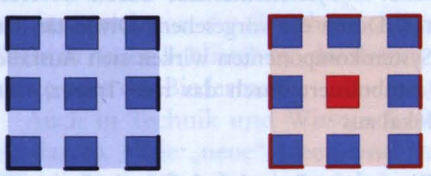

Abb. 3: Ausfallsrisiko eines stark vernetzten Systems. Durch die Abhängigkeit der Systemgesamtfunktion von allen einzelnen Systemkomponenten, führt schon die Fehlfunktion einer einzigen Komponente zum Gesamtausfall des Systems. Dabei ist die Systemzuverlässigkeit weit geringer als die seiner Einzelkomponenten.

Zwar können in solchen Systemen Redundanzen durch identische Systeme eingebaut werden, jedoch muss dabei oft aus Kostengründen auf vollständige Redundanz verzichtet werden. Das damit verbundene Risiko ist die „Globalisierung" der von Fehlfunktionen beeinflussten Bereiche durch weitreichende Vernetzungen. Lokale Fehler führen nunmehr zu globalen, oft fatalen Effekten.

Darüber hinaus bieten vernetzte Systeme eben durch die Vernetzung eine deutlich höhere Erfolgschance für Angriffe. Einerseits sind in der Regel nicht alle Systemkomponenten auf dem technisch sichersten Stand. Eine Schwachstelle führt nicht zum Ausfall bzw. zum Eindringen von Angreifern in ein Subsystem (Abbildung 4), sondern ermöglicht es Angreifern, dieses System als Ausgangsbasis für weitere Angriffe aus dem Inneren zu verwenden (Abbildung 5).
Andererseits lässt sich aufgrund gleicher Systemarchitekturen bzw. -konzepte oftmals mit einem Angriff ein weitreichender Schaden anrichten.

Ansätze für Sicherheitskonzepte für Industrie 4.0

Nicht nur aus Platzgründen überwiegt in diesem Beitrag die Analyse von Herausforderungen und Bedrohungen. Ansätze für Sicherheitskonzepte für zukünftige Industrie 4.0 Konzepte stehen bereits jetzt im Mittelpunkt umfangreicher Forschungen. Besonders etablierte Wissenschaftsrichtungen, wie *Systems Engineering* und die *Betriebs- bzw. Wirtschaftsinformatik*, können hier auf bestehenden Konzepten und Ergebnissen aufbauen. Die wichtigsten Ansätze mit dem größten Verbesserungspotenzial und mit der größten Relevanz aus heutiger Sicht sind:

Architektur-Maßnahmen: Weiterentwicklung von bestehenden Systemarchitekturansätzen für große, verteilte Systeme mit dem Ziel, nützliche (Anwenderfokus) testbare, wartbare und zukunftssichere Systeme zu bauen.

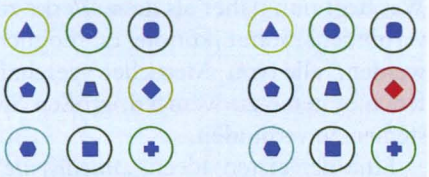

Abb. 4: Sicherheitsrisiko bei Angriff auf ein Teilsystem eines nicht vernetzten, heterogenen Systems. Obwohl es gelingt, die Sicherungseinrichtungen eines Teilsystems (dargestellt durch den roten Kreis im rechten Teil) zu überwinden, ist die Sicherheit der anderen Teilsysteme dadurch nicht kompromittiert.

Gestaltungsmaßnahmen: Weitere Verschränkung der Methoden der mechanischen und der Software-Entwicklung mit dem Ziel, die Informations- und Kommunikationstechnologien besser in die (physischen) Systemfunktionalitäten zu integrieren.

Verbesserung von Betriebssicherheit (Safety) und von Schutzmechanismen (Security) sowohl von Einzelkomponenten als auch von sie verbindenden Netzwerken. Dies gilt sowohl für die zugrunde liegende Technologie als auch für die Implementierung (Prozesse und Prozessdisziplin).

Ausblick und Schlussbemerkung

Selten verlaufen positive und nachhaltige Veränderungen „revolutionär". Selten sind sie von vorn herein planbar – weder in Ort noch Zeit. Genauso wie Karl Marx enttäuscht war, dass die von ihm erhoffte Revolution nicht in Deutschland sondern in Russland stattgefunden hat, kann es sein, dass auch

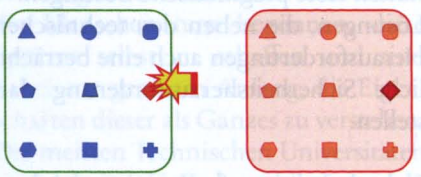

Abb. 5: Sicherheitsrisiko bei Angriff auf ein Teilsystem eines vernetzten Systems mit gemeinsamem Sicherheitsmechanismus. Trotz der einfacheren Administrierbarkeit und des in Summe oftmals höheren Sicherheitsstandards, bedeutet ein erfolgreicher Angriff auf ein Teilsystem (gelber Pfeil im linken Teilbild) eine Gefährdung aller Komponenten des Gesamtsystems. Dieses hier abgebildete Szenario ist in der Praxis häufig zu beobachten.

die „4. Industrielle Revolution" anders abläuft als geplant.

Die Informationstechnologie und die sie begleitende wissenschaftliche Forschung wird jedenfalls alles in ihren Möglichkeiten stehende tun, um zum Erfolg dieses Konzeptes beizutragen. Ob es nun eine Revolution oder einfach „nur" ein wichtiger Fort-Schritt wird, die wissenschaftlichen Erkenntnisse werden jedenfalls wiederum den Produktionswissenschaften und der Informatik gleichermaßen zugutekommen.

Autor:

Univ.-Prof. Dipl.-Ing. Dr. techn. Siegfried Vössner, Studien an der Technischen Universität Graz und der Stanford University, USA.
Forschungs- und Lehraufenthalte an der Stanford University, USA und Auckland University, Neuseeland.
Consulting Projekte (McKinsey & Company und selbständig): Konzeption und Durchführung internationaler Projekte in den Bereichen Strategie, Logistik und IKT sowie Business Information Systems.
Im Jahre 2003 Berufung als ordentlicher Professor an die Technische Universität Graz.
Vorstand des Instituts für Maschinenbau- und Betriebsinformatik, Technische Universität Graz.
Vize-Dekan der Fakultät für Maschinenbau und Wirtschaftswissenschaften.

Autor vieler Fachartikel und Mitautor eines Fachbuches für IT-Organisation sowie eines Standardwerkes für Systems-Engineering.

Univ.-Prof.
Dipl.-Ing. Dr.techn.
Siegfried Vössner
Vorstand des Instituts für Maschinenbau- und Betriebsinformatik TU Graz

LEUTE/KÖPFE

Dipl.-Ing. Herbert Steiner

Herbert Steiner ist Wirtschaftsingenieur in Maschinenbau mit Abschluss an der Technischen Universität Graz.
1997 startete er seine berufliche Laufbahn bei Volkswagen do Brasil. 1998 wechselte er zur AUDI AG nach Ingolstadt. Dort war Herbert Steiner in verschiedenen Bereichen wie Controlling, Finanzen und Einkauf tätig. 2002 folgte die Berufung zum Assistenten des Vorstands für Beschaffung. Im Jahr 2004 übernahm er die Leitung des Beschaffungsbereiches Einkaufsstrategie und -systeme.
2006 wechselte der heute 41-Jährige zur SEAT S.A. nach Matorell und übernahm dort für vier Jahre die Leitung des Generalsekretariats des Unternehmens. Anschließend war Herbert Steiner Geschäftsführer der Seat Componentes, eines der Getriebewerke des Volkswagen-Konzerns.
Seit 2014 ist Herbert Steiner Geschäftsführer der Motorenproduktion von Audi Hungaria, welches bei einer jährlichen Produktion von rund zwei Millionen Motoren das größten Motorenwerk der Welt ist. Seine Freizeit verbringt der gebürtige Salzburger mit Wintersport, Mountainbiken und Motorradfahren.