gwi
gaswärme
international
Zeitschrift für gasbeheizte Thermoprozesse

SCHWERPUNKT
Thermoprozesstechnik

ISSN 0020-9384
www.gaswaerme-online.de
Sonderdruck
Vulkan-Verlag

AICHELIN
Heat Treatment Systems

Sichere Thermoprozessanlagen 2.0

von Hartmut Steck-Winter

Bericht erschienen in der gwi gaswärme international 05/2012
Vulkan-Verlag GmbH, Essen (Germany)
Editor: Dipl.-Ing. Stephan Schalm, Tel. +49 201 82002-12, E-Mail: s.schalm@vulkan-verlag.de

Sichere Thermoprozessanlagen 2.0

von **Hartmut Steck-Winter**

Der Einsatz von IT-Komponenten hat sich mehr und mehr in der Automatisierungstechnik etabliert. Hackerangriffe und Computerviren sind die negativen Begleiterscheinungen. Durch die Verschmelzung der Automatisierungs- und Sicherheitstechnik, bei gleichzeitiger Verwendung von IT-Komponenten, ist das von böswillig angegriffenen IT-Systemen ausgehende Gefahrenpotential auf die funktionale Sicherheit immens und droht die Effizienzgewinne zu ersticken.

Safe thermal processing plants 2.0

Utilizing IT components in automation technology has become more and more common. Hacker attacks and computer viruses are negative side effects. Due to the merger of automation systems with safety technology, together with the utilization of IT components, the potential risk to functional safety by maliciously attacked IT systems is enormous and threatens to suffocate all efficiency gains.

Mit der Veröffentlichung des Fachartikels „Sicherer Betrieb von Thermoprozessanlagen mit Schutzgasatmosphären“ im April 2010 [1] wurde versucht, die wichtigsten Maßnahmen für den sicheren Betrieb von Thermoprozessanlagen aufzuzeigen.

Seither ist ein weiterer, aus dem bisherigen Rahmen fallender, Aspekt hinzugekommen: Die IT-Sicherheit. Die Schadsoftware Stuxnet hat die Betreiber und Hersteller von automatisierten Maschinen und Anlagen in aller Welt aufgerüttelt. Stuxnet fand weit über Fachkreise hinaus auch in der breiten Öffentlichkeit Beachtung, weil das Computervirus im Sommer 2010 Schäden an Automatisierungssystemen iranischer Atomanlagen verursacht hatte. Auch hierzulande kam daher schnell die Frage auf, inwiefern die deutsche Industrie durch Schadsoftware bedroht sein könnte.

(NEUE) ASPEKTE DER SICHERHEIT

Die englische Sprache unterscheidet zwischen safety und security. Gemeint sind damit die funktionale Sicherheit und die IT-Sicherheit. Funktionale Sicherheit (Safety) dient zur Abwehr von eher zufälligen technisch funktionalen Gefahren bzw. sicherheitskritischen Ereignissen. Der Gegenspieler ist also der meist zufällige Ausfall von Komponenten, d.h. die Ausfallwahrscheinlichkeit. Sicherheit im Prozessumfeld bedeutet daher in erster Linie Schutz von Personen und Anlagen vor Schäden durch unbeabsichtigte Fehler und Geräteausfälle.

Im Gegensatz dazu ist in der klassischen IT-Technologie mit „Sicherheit“ (Security) der Schutz von Daten und Systemen vor Verlust durch Hardwareschäden, besonders aber vor unberechtigten böswilligen Angriffen, gemeint. Lässt man also die Hardwareausfälle einmal außer Acht (auch weil sie der funktionalen Sicherheit zugeordnet werden müssten), dann wird die Existenz eines Angreifers vorausgesetzt. Der Angriff erfolgt beispielsweise, um in den Besitz von Daten und Informationen zu kommen oder aber, um das System zu schädigen.

Safety bezieht sich also auf die Reaktion eines Systems in Bezug auf dessen Gefährdungspotential. Security bezeichnet dagegen den Schutz eines Systems vor beabsichtigten Angriffen. Die beiden Begriffe sind nicht völlig unabhängig voneinander: Safety schließt auch Security mit ein, was bedeutet, dass ohne einem gewissen Level an Security keine ausreichenden Safety Eigenschaften erzielt werden können [2].

Die Möglichkeiten, ein Automatisierungssystem gegen Angriffe mit Schadsoftware zu schützen, sollen nun im Weiteren untersucht werden.

AUTOMATISIERUNGSSYSTEME FÜR THERMOPROZESSANLAGEN

Kennzeichnend für moderne Automatisierungssysteme ist, dass sie verteilt d.h. dezentral aufgebaut sind [3]. Die einzelnen Automatisierungskomponenten sind über Bussysteme verbunden. Speicherprogrammierbare Steuerungen (SPS) steuern und regeln den Prozess, erfassen Messwerte, Produktionsdaten, Alarmmeldungen etc. und übermitteln Daten an ein zentrales Leit- und Überwachungssystem (SCADA), beispielsweise FOCOS. Hier werden die aggregierten Daten unter anderem zu einem Wärmebehandlungsnachweis oder zu Statistiken weiter verarbeitet.

Auf so genannten Mensch-Maschine-Interfaces (MMI) wird, wie beispielhaft in **Bild 1** dargestellt, das Abbild des Gesamtprozesses visualisiert. Das Bedienpersonal kann gegebenenfalls manuell eingreifen und vom MMI aus Steuerungsvorgänge auslösen. Je nach räumlicher Ausdehnung der Anlage existieren mehrere ggf. auch mobile MMI an unterschiedlichen Standorten, die miteinander vernetzt sind und die ggf. auch redundant die Aufgaben eines anderen MMI übernehmen können.

Die Verschmelzung der Automatisierungstechnik mit der Sicherheitstechnik ist Stand der Technik. SPS verarbeiten Standard- und Sicherheitsfunktionen im Mischbetrieb. Sicherheitsgerichtete und nicht sicherheitsrelevante Signale werden über ein (und dasselbe) Bussystem ausgetauscht. Standard- und Sicherheitssoftware wird mit dem gleichen Programmiergerät erstellt.

Information ist ein wichtiger Produktionsfaktor, der eine offene Kommunikation und eine zunehmende Vernetzung von Automatisierungssystemen voraussetzt. Mitarbeiter und Servicedienstleister können sich von Zuhause, firmenfremden Standorten oder gar mobil über das Internet einwählen und Automatisierungssysteme aus der Ferne steuern bzw. sich mit Informationen versorgen. Automatisierungssysteme setzen selbsttätig Betriebs- und Störungsmeldungen per Email oder SMS ab. Verschiedene Firmensitze sind wie selbstverständlich über das Internet miteinander verbunden.

Während vor wenigen Jahren nur sehr spezialisierte proprietäre Automatisierungskomponenten verwendet wurden, werden jetzt vermehrt offene Standards und Standardprodukte aus der IT-Technik verwendet. Deshalb findet man in den SPS, MMI und Prozessleitsystemen heute auch Windowsbetriebssysteme, Industrial Ethernet

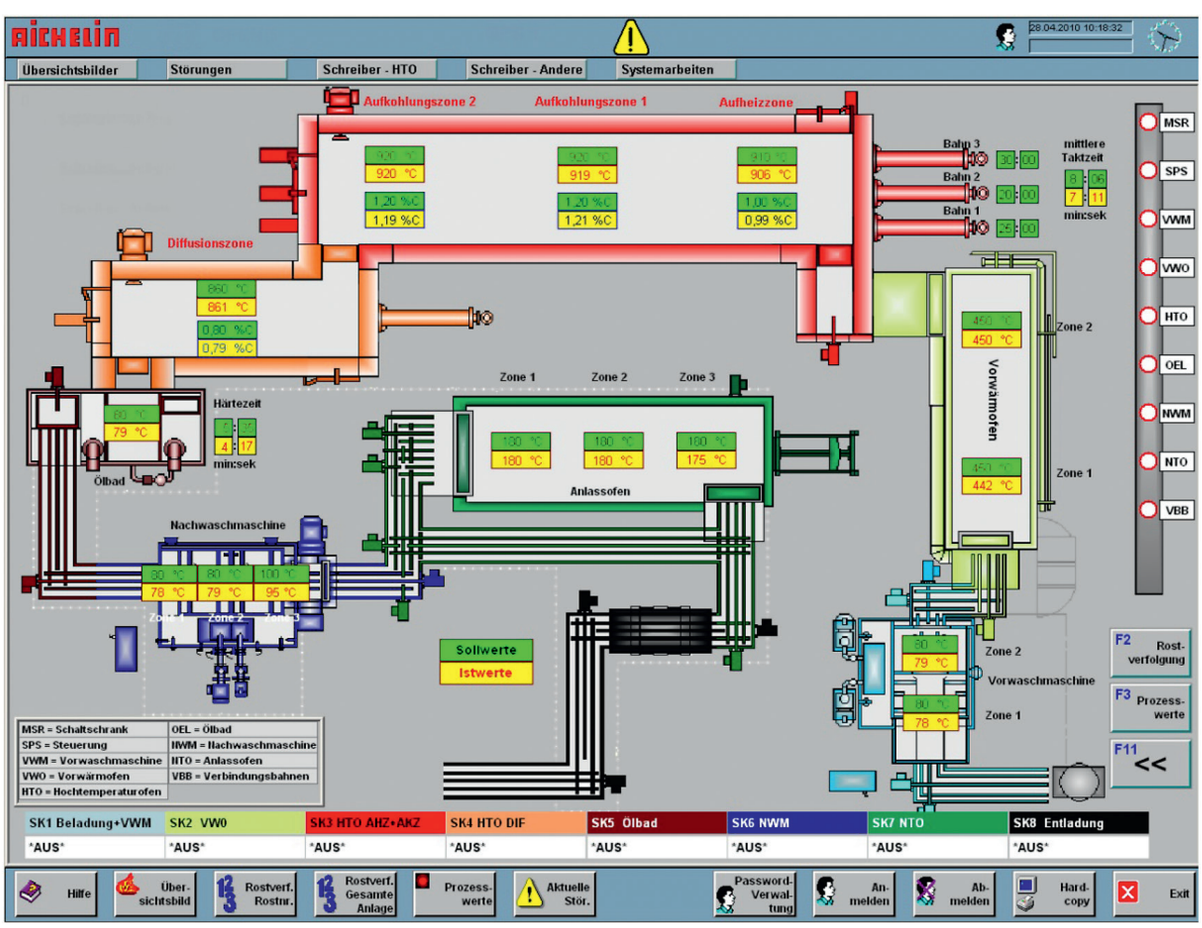

Bild 1: Beispiel eines MMI für eine Gasaufkohlung-Durchstoßofenanlage

mit TCP/IP-Standards (**Bild 2**) und andere Produkte aus der Office-Welt.

Die Verwendung von Techniken aus der klassischen IT-Welt bringt neben den Vorteilen aber offensichtlich auch neue Risiken mit sich. Ein böswilliger Angriff auf das Automatisierungssystem kann dann auch die Sicherheitstechnik aushebeln. Dies ist vor allem auf folgende Punkte zurückzuführen:

- Durch die einheitliche Kommunikationsinfrastruktur werden Grenzen überbrückt. Störungen und Bedrohungen sind somit nicht mehr auf lokale Bereiche begrenzt.
- Der Einsatz von mobilen Bediensystemen nimmt stetig zu. Besonders drahtlose Übertragungstechniken laden aber geradezu zum Angriff ein.
- Technische und andere Geschäftsprozesse wachsen mehr und mehr zusammen. Für den Datenaustausch zwischen Standorten wird meist öffentliche Infrastruktur (Internet) verwendet.
- Der wachsende Einsatz von Remote Control (Teleservice) über das Internet schafft neue Herausforderungen. Dazu gehört auch der zunehmende Einsatz von Web-Technologien für externe Benutzerschnittstellen.
- Zu den neuartigen Bedrohungen der vernetzten Automatisierungstechnik zählen nun aber auch absichtliche und unabsichtliche Angriffe von Mitarbeitern. Beispielsweise könnte eine Schadsoftware durch den Laptop eines Servicetechnikers eingeschleppt werden, die das HMI zum Absturz bringt und in Folge die Anlage der Kontrolle durch das Bedienungspersonal entzieht.

Wie „sicherheitskritisch“ sind automatisierte Thermoprozessanlagen?

Zur eigenen Beruhigung könnte man annehmen, dass die Folgen eines Cyberangriffs auf ein Atomkraftwerks im Vergleich zu einer Thermoprozessanlage riesengroß sind

Authentisierung

Der Nachweis eines Kommunikationspartners, dass er tatsächlich derjenige ist, der er vorgibt zu sein. Dies kann unter anderem durch Passwort-Eingabe erfolgen.

Computer-Virus

Ein Computer-Virus ist eine Schadsoftware, die sich selbst reproduziert, und dadurch vom Anwender nicht kontrollierbare Manipulationen an Programmen vornimmt.

Firewall

Firewalls (besser mit Sicherheitsgateway bezeichnet) sind Filter-Systeme, die alle grenzüberschreitenden Verbindungen kontrollieren und protokollieren. Insbesondere für die Abschottung des Internets vom Unternehmensnetzwerk sind sie unumgänglich. Eine Firewall lässt nur vorher erlaubte Zugriffe zu und steuert wer mit wem über welches Protokoll kommunizieren darf. Eine Firewall besteht aus einer oder mehreren Hard- und/oder Softwarekomponenten.

Industrial Ethernet

Das klassische Ethernet ist ein lokales Netz, an dem alle Teilnehmer gleichberechtigt sind. Die Datenübertragung erfolgt mit einem stochastischen Zugangsverfahren, bei dem die Teilnehmer Signale auf dem Netz erkennen, und dann, wenn kein anderes Signal vorhanden ist, es für die eigene Datenübertragung nutzen. Industrial Ethernet ist ein Oberbegriff für unterschiedliche ethernetbasierten Bussysteme in der Automatisierungstechnik.

TCP/IP

Abkürzung für Transmission Control Protocol/Internet Protocol. Es wurde entwickelt, um Computer in verschiedenen Netzwerken miteinander zu verbinden. TCP/IP ist die Basis für das Internet.

Virenscanner

Ein Virenscanner ist ein Antischadsoftwareprogramm, das Dateien nach Computer-Viren und anderer Schadsoftware absucht. Der Virenscanner überprüft, ob die Datenspeicher und eingehende Dateien von Schadsoftware befallen sind.

VPN-Verbindung

Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (meist des Internet) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In VPNs können Daten geschützt und die Kommunikationspartner sicher authentisiert werden, auch wenn diese über öffentliche Netze miteinander verbunden sind.

Bild 2: Fachbegriffe der IT-Sicherheit

und dass die Gefahr überschätzt wird. Aber hier ist Vorsicht geraten.

Eine Maschine könnte ganz generell als sicherheitskritisch bezeichnet werden, wenn eine Fehlfunktion zu folgenden Konsequenzen führt:

- Verlust von Menschenleben
- Verletzung oder Gesundheitsgefährdung von Menschen
- schwerwiegende Schädigung der Umgebung
- Nichterfüllung einer wichtigen Aufgabe oder Verpflichtung
- großer wirtschaftlicher oder finanzieller Verlust.

Es wird wohl kaum einen Disput darüber geben, dass die meisten, wenn nicht alle, der vorgenannten Kriterien auf Thermoprozessanlagen mit Schutzgasatmosphäre zutreffen, dass also von außer Kontrolle geratenen Thermoprozessanlagen große Gefahren ausgehen können und dass daher auch präventiv gehandelt werden muss. Diese Überlegungen gelten nicht nur für die Konstruktion und Herstellung neuer Thermoprozessanlagen, sondern auch für Thermoprozessanlagen im Betrieb.

SICHERHEIT VERSUS EFFIZIENZ

Steuerungssysteme, von denen die Sicherheit abhängt, müssen so konstruiert und instand gehalten werden, dass die Wahrscheinlichkeit von Funktionsfehlern ausreichend gering ist. Warum, so könnte man fragen, verwenden wir dann eine so sicherheitsanfällige Technik? Diese Problematik gab es doch früher nicht. Dass man bisher böswillige Attacken auf das Automatisierungssystem bei Risikoanalysen nicht berücksichtig hat, ist kein Grund dafür, dies weiterhin so zu handhaben.

Hinzu kommt, dass „nur Abschalten" als einzige Alternative, um eine Anlage in einen sicheren Zustand zu fahren, so wie es traditionell gehandhabt wurde, nach heutigen Maßstäben definitiv zu wenig und ineffizient ist. Möglicherweise kann die Anlage unter eingeschränkten Bedingungen auch weiterhin sicher betrieben werden.

Jeder der sich damit auseinander setzt weiß, mit traditioneller Sicherheitstechnik sinkt oft die Effizienz, nicht selten weil sie nicht genügend selektiv ist oder gar die Arbeit behindert. Warum sonst werden Schutzeinrichtungen seit es sie gibt umgangen oder manipuliert?

Die Erfahrung zeigt, dass Sicherheit und Effizienz immer dann nicht zusammen passen, wenn beide getrennt und nacheinander betrachtet werden, wenn also die Sicherheitstechnik wie ein lästiger Rucksack aufgesattelt wird.

Oberstes Ziel moderner funktionaler Sicherheitstechnik muss es sein, Gefahrenpotentiale für Mensch, Anlage und Umwelt durch technische Einrichtungen zu minimieren, dies aber mit der gleichrangigen Zielsetzung, den Produktionsprozess möglichst nicht negativ zu beeinträchtigen. Integrierte funktionale Sicherheit gehört aus diesem Grund mit zu den Megatrends moderner Automatisierungstechnik. Herkömmliche und sicherheitsgerichtete Automatisierung werden dabei zu einem durchgängigen Gesamtsystem verschmolzen.

Für die Automatisierung der Steuerungsabläufe und der Prozessregelung, aber auch der Sicherheitsfunktionen, werden gemeinsame Hardware und Engineering Systeme genutzt. Dies ermöglicht Einsparungen beim Hersteller und beim Betreiber. Insbesondere aber erleichtert das Zusammenspiel aller Komponenten eines Automatisierungssystems den ungehinderten Datenfluss und ermöglicht damit frühzeitig und intelligent auf Abweichungen zu reagieren und Fehlverhalten zu erkennen [4]. Das integrierte Zusammenspiel aus Sicherheitstechnik und Standardautomatisierung verringert dann dank besserer Diagnose auch etwaige Stillstandszeiten, erhöht die Verfügbarkeit und vereinfacht späteres Umrüsten und Modernisieren.

FUNKTIONALE SICHERHEIT (SAFETY)

Die Teile von Maschinensteuerungen, die Sicherheitsaufgaben übernehmen, werden als „sicherheitsbezogene Teile von Steuerungen" bezeichnet. Diese Teile können aus Hardware oder Software bzw. aus beidem bestehen und separater oder integraler Bestandteil der Steuerung sein. Sicherheitsbezogene Steuerungsteile umfassen jeweils die gesamte Wirkungskette einer Sicherheitsfunktion, bestehend aus der Eingangsebene mit der Sensorik, der Verknüpfungslogik mit einer sicheren Signalverarbeitung und der Ausgangsebene mit den Aktoren.

Zielsetzung ist es, diese drei Steuerungsteile so zu gestalten, dass die Sicherheit der Steuerungsfunktion, insbesondere das Verhalten der Steuerung im Fehlerfall, dem in der Risikobeurteilung ermittelten Grad an Risikoreduzierung entspricht. Je höher also die von dem sicherheitsbezogenen Steuerungsteil zu leistende Risikoverringerung ist, desto höher ist die geforderte Sicherheitsstufe oder das sicherheitstechnische Leistungsniveau des Steuerungsteils.

DIE NEUE EN-746-2:2010

Die EN 746 mit ihren insgesamt acht Teilen konkretisiert die Sicherheitsanforderungen der MRL an neue industrielle Thermoprozessanlagen. Gegenüber der DIN EN 746-2:1997 enthält die neue EN-746-2:2010 im Absatz 5.7 ein umfangreiches Kapitel mit der Überschrift „Konstruktive Anforderungen an die elektrische und elektronische Ausrüstung für Steuerungs- und Schutzsysteme".

Für Komponenten, die keiner Produktnorm entsprechen, wurden Mindestanforderungen vorgeschrieben. Überwachungsfunktionen (z.B. Gasdruck, Temperatur) müssen mindestens SIL 2 bzw. PL d entsprechen und Funktionen, deren Ausfall unmittelbar zu einer Gefähr-

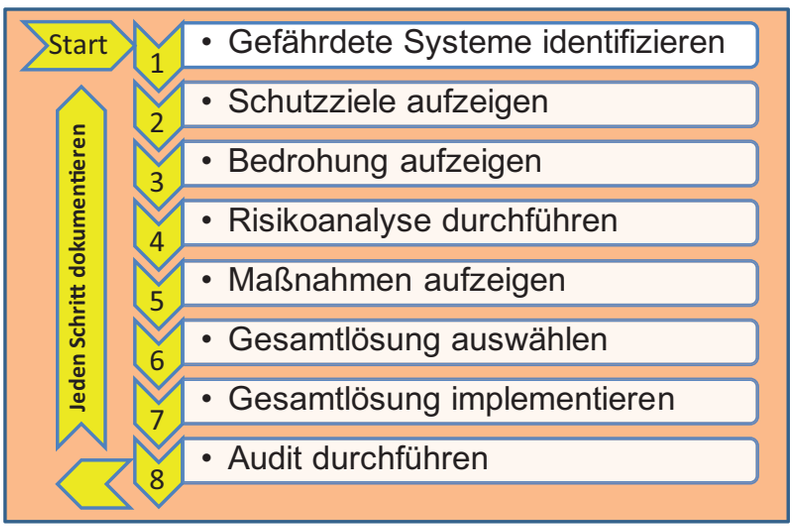

Bild 3: Vorgehensweise zur Erhöhung der IT-Sicherheit

dung führen kann (z.B. Flammenwächter), müssen mindestens SIL 3 bzw. PL e entsprechen.

Die Einsatzmöglichkeit SPS-basierender Systeme, die mit einem definierten SIL/PL-Level übereinstimmen, wird in der neuen Norm explizit aufgeführt. Möglich, wenn auch selten realisiert, war dies allerding auch schon früher. Die neue EN-746-2 trägt damit sowohl den gestiegenen Sicherheitsanforderungen als auch den höheren Effizienzanforderungen Rechnung. Es liegt aber auch auf der Hand, dass bei der Verwendung von SPS für Sicherheitsfunktionen auch beabsichtigte Angriffe auf die SPS mit in Betracht gezogen werden müssen.

IT-SICHERHEIT (SECURITY)

Viele Betreiber von Thermoprozessanlagen schließen möglicherweise vorschnell aus, dass sie auch das Ziel von Hackern sein könnten, weil so ein Angriff ja doch recht kompliziert und das eigene Unternehmen vergleichsweise unbedeutend wäre. Eine kurze Recherche im Internet zeigt Seiten mit erschreckend genauen Anleitungen, wie man in Prozessleitsysteme und SPS eindringen kann, schön sortiert nach Typ und Modell. Scheinbare Komplexität ist also kein Ausschlusskriterium.

Die in **Bild 3** vorgeschlagene Vorgehensweise in Anlehnung an Richtlinie VDI/VDE 2182 „Informationssicherheit in der Automatisierung" gibt Hinweise, wie die IT-Sicherheit von automatisierten Maschinen und Anlagen durch konkrete Maßnahmen erreicht werden kann.

SCHUTZMASSNAHMEN GEGEN SCHADSOFTWARE

Stuxnet wurde gezielt zur Sabotage programmiert. Die Schadsoftware hatte das Ziel, Automatisierungssysteme umzuprogrammieren und die funktionale Sicherheit anzugreifen. Durch böswillige Angriffe können Automatisierungssysteme mit allen denkbaren Folgen, beispielsweise Datenverlust oder gefährliche Fehlfunktionen, beeinflusst werden. Daher ist die IT-Sicherheit, zur Verhinderung derartiger Manipulationen, eine wesentliche Voraussetzung für den sicheren Betrieb von allen automatisierten Maschinen und Anlagen.

Prinzipiell kann ein Automatisierungssystem aus zwei Richtungen bedroht werden. Entweder durch Eingriff auf der höheren Ebene in der Automatisierungspyramide (**Bild 4**), also dem Prozessleitsystem, oder direkt auf der Steuerungsebene, beispielsweise am Feldbus, meist Industrial Ethernet.

Auf der höheren Ebene werden hauptsächlich Standard-IT-Technologien (PCs, Ethernet etc.) eingesetzt. Solche Technologien können mit Schutzmaßnahmen aus dem Standard-IT-Bereich adäquat abgesichert werden. Die auf der höheren Ebene gängigen vorbeugenden Maßnahmen, um die Verwundbarkeit eines Systems bei einem Angriff zu verringern, sind Firewalls und Virenscanner. Mit Hilfe einer Firewall wird die gesamte Interaktion zwischen internen und externen Systemen nach bestimmten Regeln eingeschränkt und analysiert. Das interne System ist somit weitgehend von der Außenwelt isoliert.

Virenscanner können einen Angriff selbst zwar nicht verhindern, jedoch die Folgen einer Attacke neutralisieren und somit die Gefahr für das System bannen. Bei PC-basierenden SCADA-Systemen und SPS verbietet sich allerdings häufig der Einsatz von Virenscannern, weil sie eine zusätzliche Systemlast erzeugen, die für die Echtzeitanwendung nicht tolerierbar ist.

Absicherungen gegen einen Angriff von unten, also von der Feldbusebene ausgehend, sind schwieriger. Ein Zugriff auf den Feldbus ist von einem geschulten Mitarbeiter, beispielsweise einem Instandhalter, an jedem Knotenpunkt der Feldebene möglich. In der Praxis ist nicht vorhersehbar, von welchem Punkt in der Feldebene ein Angriff erfolgt. Da der Feldbus dazu noch echtzeitfähig sein muss, sind die Ressourcen für Firewall und Virenscanner limitiert bzw. ausgeschlossen. D.h. die bekannten Schutzmechanismen der Standard-IT können auf der Feldebene meist nicht verwendet werden.

Nicht zuletzt aus diesen Gründen müssen darüber hinaus auch organisatorische Schutzmaßnahmen getroffen werden. Daten und Programme, die in die Automatisierungssysteme importiert werden sollen, zum Beispiel Software-Updates, müssen grundsätzlich vorher auf einem isolierten Rechner auf Schadsoftware geprüft werden, bevor sie ins Automatisierungssystem übertragen werden. Programmiergeräte (in der Regel Notebooks), die an die Automatisierungssysteme angeschlossen werden, müssen schadsoftwarefrei sein und über aktuelle Sicherheitspatches und Anti Virus-Software verfügen.

Kommt es trotz Sicherheitsvorkehrungen zu einem erfolgreichen Angriff, sind aktuelle Backups erforderlich, die eine schnelle Wiederaufnahme des Systems ermöglichen. Dann ist es auch sehr wichtig, möglichst viele Informationen zu erlangen, wie der Angriff erfolgt ist, um den Vorgang rekonstruieren zu können, damit eine Wiederholung verhindert werden kann.

SICHERHEITSRISIKEN IM REMOTE ACCESS

Kaum ein Betreiber und noch viel weniger ein Hersteller will und kann heute auf Remote Access (Teleservice) verzichten. Während vor einigen Jahren noch Modems üblich waren, mit denen eine geschützte Punkt zu Punkt Verbindung über das Telefonnetz aufgebaut wurde, erfolgt der Remote Access jetzt meist mit VPN über das Internet. Der Vorteil ist, dass keine teureren Telefonverbindungen oder gar angemietete Standleitungen nötig sind, die zudem nur eine relativ langsame Datenübertragung zulassen, sondern lediglich eine Internetverbindung. Der Mitarbeiter stellt nur über die Internetadresse eine Verbindung zum externen Teilnehmer her.

Vor jedem Fernzugriff müssen sich die Benutzer identifizieren. Die Authentifizierung des Benutzers erfolgt durch etwas, was nur der Benutzer weiß, beispielsweise ein Passwort, durch etwas was nur der Benutzer besitzt, z.B. ein Dongel oder durch etwas, was zum Benutzer gehört, z.B. ein Fingerabdruck. Am sichersten ist die Kombination dieser Möglichkeiten [2].

In der Regel findet keine weitere Überprüfung statt, ob ein Remote Access berechtigt ist, die Ausführung eines Befehls anzufordern. Dies gilt auch für die Steuerbefehle. Dazu kommt, dass auch im Remote Access Verriegelungen im Programmiermodus gesetzt oder geändert werden können (dazu ist er ja vorgesehen). Damit ist es für einen Angreifer im Remote Access einfach, beliebige Steuerkommandos abzusetzen. Ein Angreifer kann beispielsweise die SPS stoppen und starten, laufende SPS-Programme löschen oder verändern.

Die Zahl von Remote Control Berechtigten nimmt unter anderem wegen des Zeit- und Kostendrucks in einem Störungsfall gerade im Produktionsumfeld stark zu. Aber auch innerhalb der Betriebe werden immer häufiger Forderungen laut, von jedem Standort und auch von mobilen Systemen aus auf die Automatisierungssysteme zugreifen zu können [5].

Es ist also offensichtlich, dass die Automatisierungssysteme einerseits zur Außenwelt hin besser abgeschottet werden müssen, dass aber anderseits die Abschottung durch Remote Access auch wieder absichtlich geöffnet wird. Es liegt daher auf der Hand, dass der Remote Control Zugang möglichst sicher und limitiert sein muss. Eine ungeschützte Verbindung über öffentliche Internetverbindungen darf nie und nimmer erfolgen.

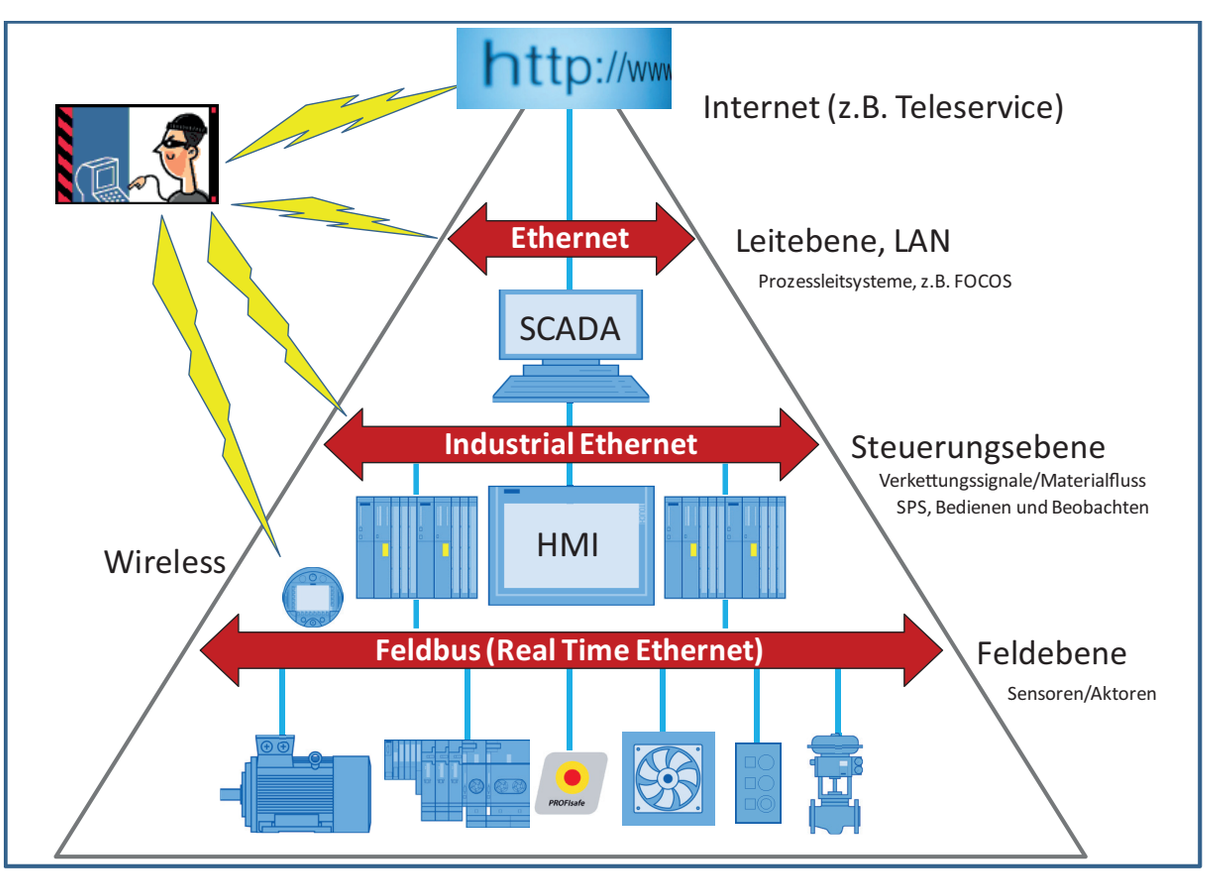

Bild 4: Angriffsmöglichkeiten auf die Automatisierungssysteme

MODERNISIERUNG DER SICHERHEITS- UND AUTOMATISIERUNGSTECHNIK

Sowohl die Betriebssicherheitsverordnung als auch das über ihr stehende Arbeitsschutzgesetz und die Arbeitsmittelbenutzungsrichtlinie verpflichten die Betreiber von allen Maschinen und Anlagen, auf der Basis einer Gefährdungsanalyse, konkrete Schutzmaßnahmen festzulegen, ihre Wirksamkeit zu überprüfen und gegebenenfalls an veränderte Bedingungen anzupassen. Die Prüfung und Modernisierungen von Schutzeinrichtungen sollte daher von keinem Betreiber einer Thermoprozessanlage aus den Augen verloren werden, sie ist nicht nur eine moralische, sondern auch eine gesetzliche Pflicht [6].

MODERNISIERUNG VON IT-SYSTEMEN IN THERMOPROZESSANLAGEN

Komponenten und Systeme in Thermoprozessanlagen sind für deutlich längere Nutzungszeiten vorgesehen, als dies im IT-Bereich üblich ist. Niemand würde auf die Idee kommen, eine Thermoprozessanlage alle zehn Jahre zu ersetzten, weil der Stand der Technik sie überholt hat. Für die Automatisierungstechnik einer Thermoprozessanlage, besonders für die Komponenten aus dem IT-Bereich, beispielsweise PC oder Netzwerkkomponenten gilt dies nicht. Zehn Jahre alte PCs sind schon echte Methusalems.

Die Automatisierungssysteme sind, bezogen auf die Möglichkeit eines böswilligen Angriffs, oftmals total veraltet, also offen für Cyberangriffe aller Art. Diese Systeme wurden wahrscheinlich noch als isolierte Inseln geplant, in denen es nur vertrauenswürdige Nutzer gab. Die heute üblichen Schutzmechanismen sind nicht vorhanden und können meist auch nicht einfach nachgerüstet werden. Die Konsequenzen liegen dann auf der Hand: Es gibt Sicherheitslücken, die von Angreifern ausgenutzt werden können.

Eingriffe in die Sicherheitstechnik, egal ob funktionale oder IT-Sicherheit, sollten nicht so nebenher ohne ausreichende Fachkenntnisse erfolgen. Es ist daher zu empfehlen, die Instandhaltung, besonders aber Umbau und Modernisierung von Sicherheitssystemen, von Fachfirmen mit sachkundigem Personal durchführen zu lassen.

FAZIT

„Ist die Sicherheit unserer Mitarbeiter, unsere Produktion und unser Know-how auch vor Cyberangriffen sicher?“ sind die berechtigten Fragen, die seit Stuxnet einen Paradigmenwechsel in der Automatisierungstechnik eingeleitet haben. Dies gilt auch für automatisierte Thermoprozessanlagen, egal ob neu oder schon länger in Betrieb.

Die zunehmende Vermischung und Vernetzung von Automatisierungssystemen mit IT-Systemen birgt nämlich nicht nur enorme Chancen, sondern auch einige Risiken. Neben den offensichtlichen Vorteilen, wie Kostenreduktion und höhere Flexibilität, wird die funktionale Sicherheit durch die IT-Sicherheit beeinflusst.

Hackerangriffe und Computerviren sind die negativen Begleiterscheinungen der fortschreitenden Standardisierung und Vernetzung. Das davon ausgehende Gefahrenpotential für die funktionale Sicherheit einer Anlage hat enorm zugenommen. Die Bedrohungen durch Schadprogramme oder unbefugte Personen beschränken sich nicht nur auf das Ausspionieren von Passwörtern oder Daten. Auch unerlaubte Eingriffe in die Steuerung und gezielte Sabotage sind denkbar. Die möglichen Folgen wären nicht nur materielle Schäden, sondern auch Gefahren für Mensch und Umwelt.

Um diese Risiken zu minimieren, sind sowohl eine gute Kenntnis des Stands der Technik als auch regelmäßige Prüfungen und Modernisierungen durch befähigte Personen notwendig. Dies erfordert ein umfangreiches Expertenwissen und eine langjährige Erfahrung, die in der Regel nur bei einem professionellen Hersteller oder Servicedienstleister vorhanden ist.

LITERATUR

[1] Steck-Winter, H.; Treptow, F.: Sicherer Betrieb von Thermoprozessanlagen mit Schutzgasatmosphären. Gaswärme International, 4/2010, Seite 250-262, Vulkan-Verlag Essen, 2010

[2] Sternberger, D.: Security in Safety Critical Systems, TU Wien, 2003

[3] Steck-Winter, H.; Unger, G.: Steuern, Regeln, Überwachen und Visualisieren von Ofenanlagen. In Praxishandbuch Thermoprozesstechnik, Seite 347-349, Vulkan Verlag, 2003

[4] Safety Integrated for Process Automation, Siemens AG Nürnberg, 2010

[5] S. Beirer: IT-Security in Automatisierungs- und Prozesssteuerungssystemen, GAI NetConsult GmbH, Berlin 2008

[6] Steck-Winter, H.: Modernisierung der Steuerung von Thermoprozessanlagen. Gaswärme International, Jahrgang 4-2008,Seite 232-236, Vulkan Verlag Essen, 2008

AUTOR

Dr. **Hartmut Steck-Winter**, MBA
Aichelin Service GmbH
Ludwigsburg
Tel.: 07141/ 6437-104
hartmut.steck-winter@aichelin.com