Industrie 4.0 - Schutz von schweißtechnischem Knowhow und QM-Sicherheit in Schweißanlagen.

J. Göppert, Auenwald, Deutschland

Kurzfassung: Moderne Schweißgeräte sind programmier- und konfigurierbar, ihre Schweißprogramme enthalten sensible Daten und Einstellwerte, und sie sind zur Steuerung, Dokumentation und Wartung vernetzt und weltweit erreichbar. Damit haben sie die Voraussetzungen um flexibel genutzt und im Zuge von Industrie 4.0 in Fertigungssysteme eingebunden zu werden. Allerdings birgt dieser Trend auch Risiken. Ohne entsprechenden Schutz kann firmensensitives Knowhow auf unsicheren Übertragungswegen (Ethernet, Email, USB-Sticks, Cloud-Speicher[3)] etc..) ausgespäht werden, Schadsoftware kann in Anlagen eingeschleust werden und geheime Daten offenlegen oder die sichere Funktion beeinträchtigen. Angriffsszenarien, wie wir sie aus der Tagespresse für PCs, Mobilgeräten und Fahrzeuge kennen, können in naher Zukunft auch ungeschützte Automatisierungskomponenten wie Schweißgeräte betreffen. Der Nutzen dieser neuen Technologien ist beträchtlich, was dazu führen wird, dass sich diese trotz aller Bedenken auch durchsetzen werden. Moderne Methoden der Verschlüsselung[7)], der sicheren Identifikation[10)], und der Zertifizierung[11)] bieten hingegen einen erprobten und wirksamen Schutz. Richtig konzeptioniert und angewendet werden sie sich in der Nutzung der Anlagen nicht nachteilig auswirken. Anlagenhersteller und Anlagenbetreiber haben ein gemeinsames Interesse und die Branche wird hier effiziente und sichere Methoden etablieren müssen. Die Gefahren wachsen mit dem Grad der Vernetzung[1)]. Dieser Beitrag will die beteiligten Personen und Unternehmen für diese Gefahren sensibilisieren und Wege für die Umsetzung aufzeigen.

1. Allgemeine technologische Entwicklungen

Die letzten Jahrzehnte sind geprägt von rasanten technologischen Entwicklungen, die sowohl den privaten Bereich als auch den industriellen Bereich betreffen. Eingeleitet wurde diese Entwicklung durch eine Digitalisierung von immer mehr Produkten, die allgemeine Nutzung von Computertechnologie, die Verfügbarkeit von Kommunikationstechniken und Speichermedien sowie die Verlagerung von immer mehr Funktionen in die Cloud[3)].

Beispielhaft kann hier der Konsum von Musik und das Speichern von Fotos genannt werden. Ausgehend von hardwarebasierten Lösungen führten technologische Umwälzungen zu mehr Flexibilität, zu zunehmender Digitalisierung, weiter über mobile Nutzungskonzepte hin zu cloudbasierten Diensten und Plattformen[5)]. Beim Hören von Musik werden diese technologischen Evolutionsschritte repräsentiert durch Spielautomaten, die Schallplatte, die Compact-Disc, MP3 Player und Musik-Streaming Dienste. Beim Speichern von Bildern ist ausgehend von Wandbildern, über Papierabzüge, die Speicherung auf PCs, auf Speicherkarten und USB-Sticks bis hin zum Austausch über soziale Netzwerke[5)] ein ähnlicher technologischer Umbruch zu beobachten.

Was bewegt Menschen wichtige Dinge, die sie früher physikalisch besessen haben und sicher kontrollieren konnten, auf unsichere Medien zu verlagern, über die sie keine Kontrolle mehr haben? Es sind die unschlagbaren Vorteile, die diese neuen Technologien mit sich bringen. Es ist die einfache Anwendbarkeit, die Verfügbarkeit zu jeder Zeit, an jedem Ort und die Unabhängigkeit von spezialisierten Endgeräten. Die Informationen sind unabhängig von Zeit, Ort und Installation verfügbar und können über Sprachbarrieren, Grenzen und Zeitzonen hinweg ausgetauscht werden. Weitere wichtige Erfolgsfaktoren sind nicht zuletzt die minimalen Kosten durch zentrale Installationen und die Möglichkeit der Finanzierung über neue Modelle wie Werbung, Data Mining, Pay-Per-Use oder Flatrates.

Wer diese technologische Entwicklung beobachtet, wird feststellen, dass dieser Prozess nicht aufzuhalten ist. Trotz großer Bedenken und Risiken setzen sich diese neuen Technologien auf breiter Front durch. Bedenken werden technisch gelöst in Kauf genommen oder ignoriert. Die Frage ist nicht „ob“, sondern „wie schnell“ sich dieser Trend auch in anderen Bereichen durchsetzen wird.

2. Industrie 4.0

Eine vergleichbare technologische Entwicklung ist unter dem Stichwort Industrie 4.0 zu beobachten [1] [3]. Diese zeichnet sich aus durch die Vernetzung[1)] der digitalen und physikalischen Welt, durch die stärkere Integration von IT Systemen und die Kommunikation zwischen „Smart Objects“[2)]. Hier spielt die Cloud Technologie[3)] und Big Data Analyse[4)] in Echtzeit eine zentrale Rolle. Autonome Systeme, Eigenkonfiguration und selbstlernende Systeme stehen im Zentrum der ambitionierten technologischen Pläne. Der Standort Deutschland soll über eine Flexibilisierung der Produktion gesichert werden. Als Beispiel wird oft die Fertigung der Losgröße 1 zum Preis der Serie genannt.

Wenngleich die Ziele sehr ambitioniert erscheinen, so muss doch festgestellt werden, dass die Technologie und Infrastruktur verfügbar ist. Die Basis stellt eine weltweite Vernetzung[1)] mit ausreichender Bandbreite und die Verfügbarkeit von großer Rechenleistung und großen Speichern dar. Big Data[4)] Technologien, Plattformenstrategien[5)] und Webshops sind im Web bereits erfolgreich im Einsatz und innovative Medien und Interaktionsgeräte sind vorhanden. Kostengünstige Identifikations-, Funk- und Vernetzungstechnologien[1)] stehen zur Verfügung. Standardisierte Protokolle für

die Konnektivität der Industrie 4.0 sind mit OPC-UA und RAMI 4.0 spezifiziert [2].

Industrie 4.0 verfolgt das Ziel, die Produktion zeitlich räumlich und inhaltlich zu flexibilisieren. Neue Prozesse und Möglichkeiten in der Logistik öffnen die Wertschöpfungsketten und ermöglichen eine stärkere Nutzung und die zunehmende Integration von Dienstleistern, Lieferanten und Kunden. Neue datenbasierte Prozesse für Service, Instandhaltung und Energieeffizienz werden ermöglicht. In der Arbeitswelt wird auch in Zukunft der Mensch als Entscheider im Mittelpunkt stehen, aber er wird sich zunehmend auf Kerntätigkeiten fokussieren und er muss weiter qualifiziert werden. Nicht zuletzt durch die neuen Möglichkeiten der Web-Portale[5)] werden neue Geschäftsmodelle mit kundenkonfigurierten Produkten und neuen Abrechnungskonzepten entstehen.

3. Realitäten und Visionen für die Schweißtechnik

Welche neue Möglichkeiten und Anwendungen ergeben sich daraus für die Schweißtechnik und die Schweißanlagen?

Die zunehmende Zusammenarbeit von Herstellern mit Fertigungsdienstleistern und Auftraggebern wird neue Anforderungen an die Wertschöpfungsketten stellen und zunehmende Anforderungen an den Austausch von Auftrags- und Qualitätsdaten stellen. Auch die Überwachung von Verbrauchsmaterial und die Rückmeldung von Arbeitsergebnissen in Form von Auftrags- und Schichtberichten wird künftig gefordert werden. Im Service von Schweißanlagen werden sich neue Prozesse und Standards etablieren. Genannt werden können hier Themen der Funktionserweiterung durch Software Update[15)] der Anlage im Feld und neue Ansätze in der vorbeugenden Instandhaltung. Durch erfasste und automatisch übermittelte Nutzungszeiten und Verbrauchsdaten werden sich neue Konzepte der Abrechnung für Auftragsfertiger und Vermieter und damit neue Geschäftsmodelle ergeben.

Abbildung: Datenaustausch einer Schweißanlage.

Eine moderne Schweißanlage bietet vielfach Schnittstellen[19)] zum elektronischen Austausch von Daten. Die Vorteile für die Anwendung für den Benutzer werden anhand einiger Beispiele dargestellt.

Die offensichtlichste und vielfach genutzte Möglichkeit betrifft die Erweiterung der Software-Funktionalität durch Updates und Upgrades[15)]. In der Vergangenheit war die Änderung des Funktionsumfangs zumeist verbunden mit elektrischen und konstruktiven Änderungen an der Anlage. Heute erlauben digitale Steuerungen und Vernetzung eine Erweiterungen durch eine Änderung der Software. So ist es möglich, zu geringen Kosten auch Anlagen im Feld nachzurüsten. Derartige Maßnahmen nehmen zu und sie müssen in einfacher Art und Weise auch vom Kunden direkt ausgeführt werden können. Eine Vernetzung[1)] der Anlage im Zuge von Industrie 4.0 bietet neue Möglichkeiten um Software Update Prozesse, wie wir sie aus der PC Welt und von mobilen Geräten her kennen, einfach und ohne manuelle Interaktion umsetzen zu können. Sicherheitsbetrachtungen werden hier von zentraler Bedeutung sein, um die Vertrauenswürdigkeit und Verlässlichkeit derart aufgespielter Programme und Funktionen gewährleisten zu können.

	Erweiterung Funktionalität	Schweißdaten Überwachung	Zugang Einstellung
Hardware	Hardware Modifikation	Manuelle Aufzeichnung	Schlüsselschalter
Digital	Digital gesteuert	Extern PC-Lösungen	SW Passwort
	Höhere Flexibilität und Konfiguration		
Mobil	Flashbar über Datenbus oder USB Speicher	Integriert. Speicherkaten	RFID Karte Personalisiertert
	Einfache Anwendung, erweiterte Funktionen		
Cloud	Online Automatisiert	Server Global	Online Integration
	Zentrale Verwaltung, aktuell, globaler Zugang		

Abbildung: Technologische Entwicklung

Die Bereitstellung von fertigungsbezogenen Daten und die Unterstützung von Qualitätsprozessen werden neue Anforderungen an die Schweißdatendokumentation und die Schweißdatenüberwachung stellen. Diese Daten werden zukünftig verstärkt durch offene Protokolle über öffentlich zugängliche Netzwerke oder Funktechnologien zu firmeninternen Datenbanken oder Cloud-basierten Datenbanken[3)] weitergeleitet. Im Baustelleneinsatz können Speicherkarten oder öffentliche Funknetzwerke zum Einsatz kommen. Dadurch sind produkt- oder prozessspezifische sensible Daten auf schwer kontrollierbaren Speicherbausteinen und in öffentlichen Netzwerken verfügbar. Um diese Risiken zu kontrollieren, sind geeignete Maßnahmen zu ergreifen.

Auch bei der Bedienung und Steuerung der Anlage etablieren sich durch Industrie 4.0 neue Möglichkeiten. Im Fokus stehen hier zum einen Technologien die den Schweißer bei der Bedienung der Anlage unterstützen und das Risiko von falschen Einstellungen deutlich reduzieren. Zum anderen wird dadurch auch eine nahtlose Integration der Schweißanlage in eine Industrie 4.0 Fertigungsumgebung und Qualitätsmanagementprozesse ermöglicht. Derartige Prozesse überwachen die Autorisierung und Qualifizierung der Schweißers bzw. des Bedienpersonals sowie die Berechtigung der mit der Schweißanlage interagierenden Steuerungen und intelligenten „Dinge“[2)]. Aufbauend auf Autorisierungskonzepten[10)] werden die Berechtigungen zur Konfiguration und Einstellung der Anlage

vergeben sowie die Konsistenz der übertragenen Daten sichergestellt. Der Einsatz von digitalen Möglichkeiten, Cloud-Technologien und portablen Speicherelementen ermöglicht den Aufbau von sicheren Abläufen ohne fehlerträchtige manuelle Eingaben, flexiblen Fertigungsabläufen, sowie die zentrale Verwaltung von Berechtigungen und Qualifikationen von Schweißern und auftragsbezogenen WPS Vorgaben. Auch hier ist besonderer Schutz der Daten erforderlich.

4. Sicherheitsüberlegungen

Es kann zusammengefasst werden, dass sich für die Schweißtechnik die gleichen Entwicklungen einstellen werden wie für technische Produkte aus anderen Bereichen. Das wird zu mehr Flexibilität, einem größeren Funktionsumfang, neuen Prozessen und einer verbesserten Nutzung führen. Während früher Funktionen und Informationen sicher in Schweißgeräten integriert waren und damit auch klar räumlich verortet werden konnten, wandern diese nun und zunehmend in mobile Speichermedien und werden über öffentliche Netzwerke verteilt.

Der Schutz der Informationen vor dem Ausspähen und vor unberechtigter Modifikation wird zunehmend schwieriger. Transportierbare Speicher können einfach verloren gehen, entwendet werden und sie können mit einfachen Mitteln vervielfältigt werden. Trotzdem bieten sie immer noch den Vorteil, dass die Information an ein physikalisches Objekt gebunden ist, das besonders geschützt werden kann. Ganz andere Methoden müssen angewendet werden, wenn die Informationen über Datennetze fließen. Falls keine Schutzmaßnahmen ergriffen werden, haben Sender und Empfänger der Daten auf dem öffentlichen Übertragungsweg keinerlei Möglichkeiten, ungerechtfertigtes Modifizieren oder Kopieren der Daten zu vermeiden. Meist besteht nicht einmal die Möglichkeit, letzteres zu erkennen. Während in der Vergangenheit das Ausspähen von Daten in der Regel einen physikalischen Zugang zu den Anlagen erfordert hat, können die Angreifer heute sicher aus der Entfernung und unerkannt agieren. Es ist folglich unabdingbar, dass die Daten aktiv geschützt und geeignete Maßnahmen ergriffen werden.

Trotz aller Risiken und Bedenken bezüglich der Sicherheit, des Schutzes von Knowhow und der Vertraulichkeit von Daten wird sich dieser Trend weiter fortsetzen. Die neuen Technologien werden sich durchsetzen. Die Frage ist nicht, ob sie sich durchsetzen, sondern wie schnell. Die Vorteile und neuen Möglichkeiten dominieren! Es ist Aufgabe der Technologielieferanten und der Verantwortlichen für die technologische Umsetzung in den Fertigungsbetrieben diese Sicherheitsaspekte zu lösen.

5. Angriffsziele und Schutz

Zunächst ist ein Angriff auf die Software der Anlage zu betrachten. Das Risiko ist hier die Betriebssicherheit, die Sicherheit der Daten und das Ausspionieren von Knowhow. Ein Angriff könnte hier über das Aufspielen oder in Verkehr bringen von modifizierter Firmware[15)] Software oder Applikationen erfolgen. Geeignete Schutzmaßnahmen sind die Nutzung von verschlüsselter Übertragung[7)], von Zertifikaten[11)] und von Softwareverifikation[13)] beim Startup der Programme. Es muss zwischen sicherer Hardware und unsicherer Hardware unterschieden werden. Der Hersteller der Anlage muss Maßnahmen ergreifen, um die verwendete Hardware und die darauf lauffähige Software abzusichern.

Ein weiteres Angriffsziel sind die im Web lokalisierten Datenbanken in Form von Webservern oder Portalen[5)]. Auch hier können Daten ausspioniert oder gelöscht werden oder es besteht das Risiko, Geschäftsmodelle zu unterhöhlen, indem eigentlich kostenpflichtige Funktionen erschlichen werden. Um das zu unterbinden, muss eine geeignete Sicherheitsarchitektur für die eingesetzte Server Infrastruktur gewählt werden. Besondere Aufmerksamkeit ist auf die Sicherheit der verwendeten Passwörter und Geheimnisse[9)] zu legen und es sind die üblichen Abwehrmaßnahmen gegen Viren und Angriffe zum Beispiel in Form von Firewalls[16)], Virenscanner[17)] und regelmäßigen Backups zu ergreifen.

Auch viele Bediengeräte, Speicher- oder Übertragungsmedien sind angreifbar. Hier geht es um das Ausspionieren von Knowhow, betrieblichen oder persönlichen Daten. Die Daten auf PC, Mobiltelefonen oder tragbaren Speichermedien können meist einfach dupliziert oder modifiziert werden. Ein Ausspionieren von Daten auf öffentlichen Übertragungswegen ist für den Angreifer oft risikolos, weil es aus der Entfernung und anonym erfolgen kann. Um das zu unterbinden, müssen Lösungen umgesetzt werden, die Sicherheitsfeatures der Speichermedien nutzen oder eine gesicherte und verschlüsselte Speicherung und Übertragung[7)] der Daten nutzt.

Ein wichtiges Ziel von IT-Sicherheit ist die Sicherstellung der Vertraulichkeit. Es geht darum, dass der Inhalt der Daten für Unberechtigte nicht lesbar sein darf. Das wird typischerweise erreicht durch eine Verschlüsselung[7)] der Daten. Um ein derartiges Konzept zu erarbeiten, muss klar analysiert werden, auf welchen Medien und welchen Wegen die Daten verfügbar sind. Die Vertrauenswürdigkeit jedes einzelnen dieser Medien wird ermittelt und es ist sicherzustellen, dass bei allen nicht vertrauenswürdigen Medien die Daten nur in geschützter Form vorliegen. Besondere Beachtung muss hier auch die Vertrauenswürdigkeit von PC-Programmen oder mobilen Applikationen gewidmet werden. Eine sichere Methode ist die sogenannte End-to-End Verschlüsselung[8)], bei der die zu schützenden Daten beim Sender innerhalb einer vertrauenswürdigen Umgebung verschlüsselt werden und

erst wieder beim Empfänger in der vertrauenswürdigen Umgebung entschlüsselt werden. Zur Ver- und Entschlüsselung kommen bei beiden Kommunikationspartnern entsprechende Geheimnisse[9)] zum Einsatz, die einen besonderen Schutz gegen Ausspionieren unterliegen müssen.

Abbildung: End-to-End Verschlüsselung

Eine andere Fragestellung ergibt sich wenn die Konsistenz der Daten und die Autorisierung[10)] des Absenders sichergestellt werden müssen. In diesem Fall kann es akzeptabel oder zu logistischen prozesstechnischen Zwecken sogar gewünscht sein, dass die Daten unterwegs gelesen werden können. Trotzdem müssen die Kommunikationspartner einen Nachweis haben, dass die Daten von einem autorisierten Sender versendet wurden und auf dem Weg zum Empfänger nicht verändert wurden. Dieser Nachweis kann durch ein Zertifikat[11)] geführt werden. Mit Hilfe eines Zertifikats kann der Empfänger überprüfen, ob der Sender der Daten autorisiert ist, und ob die Daten auf dem Weg vom Sender zum Empfänger nicht verändert wurden. Letzteres wird durch einen verschlüsselten Hashcode[12)] der Daten erreicht. Eine gute Verschlüsselung kann oft auch die Funktion eines Zertifikats abdecken, jedoch kann durch die Nutzung beider Methoden mit unterschiedlichen Verschlüsselungsgeheimnissen und Verschlüsselungsmethoden eine doppelte Sicherheit erreicht werden.

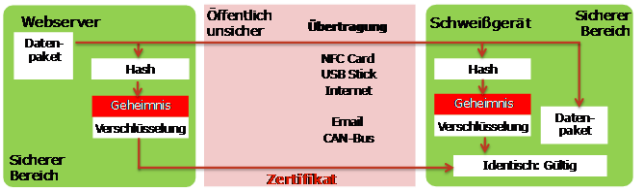

Abbildung: Zertifikat und Autorisierung

Sowohl die Verschlüsselung als auch die Zertifikatserstellung und -prüfung basiert auf Geheimnissen[9)]. Diese Geheimnisse müssen geschützt werden. Wer in den Besitz dieser Geheimnisse kommt, kann die Sicherheitsmechanismen umgehen oder außer Kraft setzen. Zum Schutz dieser Geheimnisse und der dazugehörenden Verschlüsselungsalgorithmen können verschiedene Sicherheitsstufen unterschieden werden:

- Unveränderliche Geheimnisse, die in der Software hinterlegt sind, bergen ein Sicherheitsrisiko. Sollte dieses Geheimnis bei einem beliebigen Partner ausspioniert werden, so fällt der Schutz für die komplette Anwendung.
- Veränderliche Geheimnisse, die eine Eigenschaft des Endgerätes nutzen (z.B. Seriennummer). Hier wird das Risiko beträchtlich reduziert, da ein ausspioniertes Geheimnis nur dieses individuelle Gerät betrifft.

Auch der Ort an dem die Geheimnisse gespeichert und die kritischen Berechnungen vorgenommen werden, ist genauer zu betrachten:

- Als kritisch einzustufen sind Geräte, die öffentlich verfügbar und von dritter Seite programmierbar sind (z.B. Personal Computer oder mobile Geräte). Jegliche Programme, die auf derartigen Systemen ausgeführt werden, können mit mehr oder weniger hohem Aufwand ausspioniert werden.
- Eine höhere Hürde stellen herstellerspezifische Endgeräte dar, da hier vielfach die nötige Detailkenntnis fehlt, um erfolgreiche Angriffe zu konzipieren. Mit besonderer Aufmerksamkeit muss hier jedoch nachladbare Software betrachtet werden, da derartige „Flash-Files“ oft über öffentliche Netzwerke ausgetauscht werden. Um die Vertraulichkeit und Sicherheit dieser Software herzustellen sind Methoden anzuwenden die in diesem Artikel unter dem Begriff „Secure-Boot“[14)] beschrieben sind.
- Die maximale Sicherheit ist nur mit spezieller kryptographischer Hardware zu erreichen. Hier handelt es sich um spezielle integrierte Bausteine oder Funktionen von Mikrocontrollern, die die Verschlüsselung in einer besonders angriffssicheren Umgebung vornehmen und die Geheimnisse unzugänglich von außen verwalten und schützen. In diesem Fall würde selbst das ausspionieren der kompletten Software die Geheimnisse nicht offenlegen.

Eine hohe Aufmerksamkeit ist auch der Sicherheit der herstellerspezifischen Endgeräte zu widmen. Es sind Maßnahmen erforderlich, die unterbinden, dass ein Angreifer modifizierte Software auf die Maschine aufspielt und diese nutzt, um das Sicherheitskonzept zu unterhöhlen oder Verschlüsselungsalgorithmus und Geheimnisse auszuspähen. Hier bietet sich auch ein Verfahren zur Softwareverifikation[11)] an, mit dem die Konsistenz und Modifikationsfreiheit aller ausführbaren Programme überprüft wird. In einer Basisausführung kann das einmalig beim Aufspielen des Programms geschehen. Im Idealfall würde aber die Konsistenz bei jedem einzelnen Programmstart verifiziert werden. Durch diese Methode ist es möglich eine von außen auf die Anlage aufgespielte Software als sicher zu deklarieren und entsprechende sicherheitskritische Funktionen in dieser Software auszuführen. Derartige Firmware-Verifikation wird in der Fachliteratur als „Secure-Boot“ [14)] bezeichnet.

Abbildung: Firmware Verifikation und Secure-Boot.

Ein gut konzipiertes Konzept arbeitet für den Anwender unbemerkt im Hintergrund. Allerdings ist hier mit zusätzlichem einmaligem Aufwand in der Konzeption und der logischen Abwicklung zu rechnen.

6. Maßnahmen und Empfehlungen.

Das Gefährdungspotential durch Angriffe auf Daten und Komponenten in einer Industrie 4.0 Umgebung steigt beträchtlich. Sowohl die Analyse der Angriffsszenarien, als auch das Entwickeln von Abwehrstrategien erfordert Aufmerksamkeit und Fachwissen. Eine Prävention von Angriffen umfasst den Knowhow-Schutz, Verschlüsselungs- und Autorisierungsprozesse, Firewalls, Spamfilter und Virenscanner. Darüber hinaus ist es erforderlich, bei den Mitarbeitern ein entsprechendes Risikobewusstsein zu schaffen und Unternehmensprozesse zur Schadensabwehr zu etablieren. Ein zweiter wichtiger Baustein ist die Detektion von potentiellen Angriffen. Das umfasst die Überwachung von Benutzeraktivitäten und Schwachstellen. Sobald ein Angriff erkannt wurde, ist eine entsprechende Reaktion erforderlich in Form eines Notfallplans oder in Form der Wiederherstellung von Backup. Zukünftige Standards von IT-Sicherheit in der Industrie 4.0 werden im nationalen Referenzprojekt IUNO definiert und standardisiert [4].

Aus diesem Grund sollte bei Industrie 4.0 Unternehmen die IT-Sicherheit zur Chefsache erklärt werden. Es ist ein entsprechendes Bewusstsein in der gesamten Firma bis hin zum letzten Mitarbeiter zu schaffen. Bei der Konzeption von Industrie 4.0 Lösungen in einem Unternehmen muss Sicherheit von Anfang an Teil des Gesamtkonzeptes sein. Das Sicherheitskonzept der beteiligten Anlagen und Dingen ist zu prüfen und in das Gesamtkonzept einzugehen. Nachträgliche Erweiterungen erfordern meist Kompromisse und sind teuer. Besonders wichtig ist das bei Systemen, die Möglichkeiten zum Datenaustausch bieten, öffentliche Übertragungswege nutzen oder Daten in Cloud-Diensten abspeichern. Es müssen kompetente Partner Lieferanten und Berater mit Erfahrung im Thema Datensicherheit gesucht werden und ein umfassendes Sicherheitsaudit erstellt werden. Für eine Gesamtlösung sind Systeme mit integriertem Datensicherheitskonzept zu bevorzugen.

Für die Firma Lorch Schweißtechnik steht das Thema Datensicherheit im Zentrum aller neuen Entwicklungsprojekte. So kommen beispielsweise in der Geräteserie MicorMig alle hier vorgestellten Methoden der verschlüsselten Datenübertragung[7] zum Einsatz. Besonders kritische Daten werden mit einem hardwarebasierten Zertifikat[11] abgesichert. Die Update- und Flash-Prozesse[15] nutzen Methoden der Firmware Verifikation[13] und Secure Boot[14]. Ein qualitätssicherndes Konzept stellt die Berechtigungen der Schweißer sicher und die Schweißanweisungen und Job-Einstellungen der Anlagen werden durch kopiergesicherte NFC-Karten[20] gesichert und übertragen [5]. Eine End-to-End Verschlüsselung[8] garantiert den Knowhow Schutz von Prozessparametern, Schweißprogrammen und Funktionserweiterungen. Der umfassende Schutz von Persönlichkeitsdaten, Prozess-Knowhow und schweißtechnischen Betriebsdaten ist sichergestellt. Damit existiert eine solide Basis für zukünftige Erweiterungen, insbesondere auch mit Blick auf die neuen Anforderungen aus dem wachsenden Bereich Industrie 4.0.

7. Begriffe Datenverarbeitung und IT-Sicherheit

[1] *Vernetzung:* Datenverbindung von Geräten untereinander. Die Vernetzung kann Drahtgebunden oder drahtlos sein. Die Verbindung kann lokal zwischen den Anlagen in räumlicher Nachbarschaft sein oder global eine Verbindung in das Internet umfassen.

[2] *Smart Objects, "Dinge"*: Sensoren, Aktoren, Komponenten, die einen klaren Funktionsumfang haben und nach herkömmlichem Verständnis keine IT-Komponenten sind. Im Zuge von „Industrie 4.0" und „Internet of Things" werden diese mit zusätzlicher Vernetzung und Datenverarbeitung erweitert und sind als autonome Komponenten eingebunden und flexibel einsetzbar.

[3] *Cloud, Clouddienste*: Anwendungen oder Datenbanken, die über das Internet dauerhaft weltweit erreichbar sind. Sie verfolgen das Ziel, Funktionen global bereitzustellen, Daten global zu sammeln oder Information global auszutauschen. Üblicherweise werden diese Dienste in großen Rechenzentren ausgeführt und werden außerhalb des Firmennetzwerkes der Anwender betrieben.

[4] *Big Data Analyse, Data Mining*: Auswertung von großen Datenmengen. Auffinden von Informationen in Daten, die meist über lange Zeiträume, für andere Zwecke gesammelt wurden und unstrukturiert vorliegen. Beispiel ist die Auswertung von Internet Suchanfragen um Zielgruppen für bestimmte Marketingaktionen zu identifizieren.

[5] *Plattformen, Web Portale*: Offene IT Systeme, für die Drittanbieter Software erstellen oder Dienste anbieten können. Beispiele für Plattformen sind PC-Systeme, mobile Kommunikationssysteme oder Internetdienste wie Verkaufsportale und soziale Medien.

[6] *Verschlüsselte Übertragung*: Übertragung von Daten in nicht lesbarer Form. Falls die Daten unterwegs kopiert oder mitgehört werden, sind sie unbrauchbar.

[7] *Verschlüsselung*: Übersetzung von Daten in eine andere nicht lesbare Form. Der Prozess der Verschlüsselung ist umkehrbar. Wer in Kenntnis des passenden Geheimnisses ist, kann die ursprünglichen Daten wieder herstellen.

[8] *End-to-End Verschlüsselung*: Verschlüsselte Übertragung oder Speicherung von Daten über alle Übertragungsstationen hinweg. Ver- und Entschlüsselung nur im sicheren Bereich beim Sender und Empfänger. Alle Zwischenstationen sind sicherheitsunkritisch.

[9] *Geheimnis, Passwort*: Informationen, die für eine erfolgreiche Verschlüsselung, Entschlüsselung oder Autorisierung erforderlich sind. Geheimnisse müssen besonders geschützt werden. Wenn die Geheimnisse ausgespäht oder veröffentlicht werden, verlieren die Schutzmechanismen ihre Wirkung.

[10] *Identifikation, Autorisierung*: Bestätigung, dass der Kommunikationspartner derjenige ist für den er sich ausgibt, bzw. dass er über die erforderliche Berechtigung verfügt.

[11] *Zertifizierung*: Bestätigung der Echtheit von Daten, realisiert in Form einer verschlüsselten Prüfsumme. Ein Zertifikat kann nur von einem Kommunikationspartner erstellt worden sein, der in Kenntnis eines gemeinsamen Geheimnisses ist.

[12] *Hashcode*: Prüfsumme von Daten. Eine Veränderung führt zu einem anderen Hashcode. Es nicht möglich Rückschlüsse auf die Daten zu ziehen. Es ist mit vertretbarem technischem Aufwand auch nicht möglich, Datensätze zu konstrurieren, die den gleichen Hashcode ergeben.

[13] *Software-/Firmwareverifikation*: Verfahren mit dem sichergestellt werden kann, dass das ausführbare Programm von einer berechtigten Stelle erstellt wurde und auf dem Übertragungsweg nicht verändert wurde.

[14] *Secure Boot*: Verfahren zur Software Verifikation bei dem die Gültigkeit und Modifikationsfreiheit bei jedem einzelnen Programmstart überprüft wird. Bei diesem Verfahren würden auch Datenfehler beispielsweise als Folge von Speicherfehler erkannt werden.

[15] *Update, Upgrade, Aufspielen, Flashen*: Laden von neuen Funktionen oder neuen Programmen auf ein mikrokontroller- oder rechnerbasiertes System.

[16] *Firewalls*: Programme, die bei Rechnersystemen und Clouddiensten zum Einsatz kommen. Das Ziel besteht darin, unberechtigte Zugänge von außen zu unterbinden. Firewalls werden von spezialisierten Firmen angeboten.

[17] *Virenscanner*: Programme, die bei Rechnersystemen und Clouddiensten zum Einsatz kommen. Das Ziel besteht darin, ungewünschte Software zu erkennen und zu löschen, die die Date- oder Betriebssicherheit untergraben. Virenscanner werden von spezialisierten Firmen angeboten und müssen ständig aktualisert werden, um rasch auf neu Bedrohungen reagieren zu können.

[18] *Flash-Files*: Ausführbare Programme für Mikrocontroler-basierte Systeme. Können über Schnittstellen eingelesen werden, um die Funktion eines Gerätes zu ändern oder erweitern.

[19] *Schnittstellen:* Datenverbindungen eines Gerätes nach außen. Verbreitete Schnittstellen sind: Feldbusse, Ethernet, WLAN, Bluetooth, USB und NFC.

[20] *NFC-Karten, RFID-Karten:* Datenkarten für Kontaktlose Übertragung. Sobald die Karten in die Nähe des Lesegerätes gebracht werden, wird eine Verbindung aufgebaut und der Dateninhalt ausgelesen. Das Sicherheitskonzept beruht auf dem Prinzip der Nähe. NFC Karten werden oft für Autorisierung verwendet oder tragen Daten anhand derer ein Paket oder Produkte im logistischen Fluss identifiziert und verfolgt werden können.

8. Literatur

[1] Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0. Abschlussbericht des Arbeitskreises Industrie 4.0. Acatech, Deutsche Akademie der Technikwissenschaften. April 2013.

[2] Umsetzungsstrategie Industrie 4.0. Ergebnisbericht der Plattform Industrie 4.0. VDMA, ZVEI, April 2015.

[3] http://www.plattform-i40.de

[4] IUNO – Das Nationale Referenzprojekt für IT-Sicherheit in der Industrie 4.0. Gefördert vom Bundesministerium für Bildung und Forschung. http://www.iuno-projekt.de/

[5] J. Göppert, W. Bockting und F.-J. Gesthuysen. Aufbau eines einfach handhabbaren Systems zur Absicherung von Stromquellen-Parameterbereichen in einem nicht vernetzten Umfeld. EVS-Berichte Band 315, ISBN 978-3-945023-46-4, DVS Media GmbH. Düsseldorf, 2105.