Ein Stück mehr Sicherheit – Die Datensicherung als Teil der Cybersecurity-Strategie

Dr. Thorsten Sögding, Stefan Schnackertz

Wo früher Computerprogramme mit wenigen Kilobytes in speicherprogrammierbaren Steuerungen auskamen, erzeugen die Editoren von heute umfangreiche Datenpakete. Ein Grund dafür ist die rasante Entwicklung der höheren Programmiersprachen, die für Anwender verständlicher sind. Aber auch die fortschreitende Digitalisierung und Weiterentwicklung der Automatisierung fordert einen höheren Programmieraufwand. Steuerungen werden vernetzt, sollen zusätzlich geschützt werden, müssen immer umfangreichere Aufgaben übernehmen und es lässt sich bisher nicht vermeiden, dass das Datenvolumen in den Produktionshallen ins Unendliche wächst. Die Übersetzung der geschriebenen Programme in Maschinensprache wird durch die schnelleren Prozessoren gemeistert. Diese arbeiten visuelle Programmiersprachen in Maschinencodes ab und erleichtern dem Menschen viel Arbeit, nicht aber die Aufgabe, die Daten ordentlich und in Versionen sortiert, zu verwalten.

Mit unterschiedlichen Softwareversionen sollte man bereits in der Phase der Inbetriebnahme einer Produktions anlage rechnen. Hier entstehen die meisten Daten, die von den Automatisierungstechnikern aufeinander abgestimmt werden, bis die Produktionsanlage nach den Wünschen der Betreiber läuft. Je mehr Daten entstehen, desto größer ist das Risiko, dass sich Fehler einschleichen. Datenbestände können verwechselt werden oder fehlerhafte Bausteine enthalten. Dies kann ungewollt geschehen, etwa durch Fehleinschätzungen, oder aber es wird mit falschen Datensätzen gearbeitet. Das Programm kann aber auch von außen manipuliert werden und gefälschte Ergebnisse liefern. Einer der Gründe hierfür ist die zunehmende Anbindung der Automatisierungssysteme mit dem Internet und auf einmal öffnen sich Türen für unerwünschte Netzwerkzugriffe.

Einige Computerviren warten nur darauf, dass eine IP-Adresse einer Automatisierungssteuerung im Netz auftaucht, so wie es bei Stuxnet der Fall war. Der Computerwurm wurde speziell so entwickelt, dass er gezielt nach Automatisierungsgeräten, wie Human Machine Interfaces (HMI) und Speicherprogrammierbaren Steuerungen (SPS) in einer speziellen Anordnung suchte und als er sie endlich fand, begann der zerstörerische Angriff. Da die Urheber sich bisher auch noch nicht dazu bekannt haben, bleiben die Hintergründe im Unklaren. Deutlich wird jedoch, dass die Entwickler keine Skrupel hatten, Mensch, Natur und Umwelt zu gefährden.

Die Datensicherung als Teil der Cybersecurity-Strategie

Aus diesem Grund ist es notwendig geworden, die Produktion mit einer Cybersecurity Strategie zu schützen. Dieses Vorgehen, bei dem diverse Verteidigungslinien durch die IT-Abteilungen aufgebaut werden, wird Defence-in-Depth-Strategie genannt. Die unterschiedlichen Systeme sollen die Cybersicherheit erhöhen, eine ganzheitliche Lösung gibt es jedoch noch nicht. Bekannte und erfolgreiche Defence-in-Depth-Strategien sind beispielsweise:

▸ Die klassische Firewall schützt Rechnernetze vor unerlaubten Netzwerkzugriffen.

▸ Ein SIEM (Security Information and Event Management) überwacht in Echtzeit Ereignisse sowie Meldungen und berücksichtigt dabei auch Langzeitdaten.

▸ Ein *Intrusion Detection System* erkennt Angriffe.

▸ Ein *Intrusion Prevention System* verhindert Angriffe.

▸ Der *Honey Pot* ist eine Ablenkungsmaßnahme, um Angreifer in die Irre zu führen.

▸ Das Awareness-Training dient der Schaffung eines ausreichenden Sicherheitsbewusstseins.

Es gibt noch weitere Abwehrmaßnahmen, doch vorrangig gilt es, das Bewusstsein der eigenen Mitarbeiter zu schärfen. Noch macht der Mensch die meisten Fehler - durch Unachtsamkeit oder Unwissenheit.

Die Sicherung und Dokumentation der Daten

Was ist die beste Strategie bei einem Cyberangriff? Wenn alle Verteidigungslinien durchbrochen sind, hilft nur noch eine Datensicherung, ein Backup auf den letzten Stand der Daten, die in Ordnung waren (Disaster Recovery). Kritische Programme müssen geschützt werden und ganz konkret die Daten aus den Automatisierungsgeräten. Seit Beginn der Datenaufzeichnungen werden Schutzmaßnahmen entwickelt, um sicherzustellen, dass die Daten unverändert bleiben. Die Datensicherung (Backup) ist eine häufig verwendete Möglichkeit.

Die Datensicherung eines Automatisierungsgerätes aus der Produktion (z. B. eines Roboter, einer SPS oder einer HMI-Bedienstation) ist manuell nur mit großem Aufwand zu bewerkstelligen. Wenn das Gerät vernetzt wird, kann sie automatisch und zeitgesteuert durchgeführt werden. Dabei ist zu beachten, dass die verschiedenen Daten innerhalb einer Steuerung vollständig und konsistent gesichert werden.

Die konsistente Datensicherung

Man unterscheidet bei einer Datensicherung eines Automatisierungsgerätes zwischen vier verschiedenen Datentypen (s. Bild 1), die alle gemeinsam in einer konsistenten Form abgespeichert werden:

1. Zuerst wird das Programm einer Steuerung gesichert, das für den Ablauf der Produktionsschritte zuständig ist. Es wird mit einem Editor erzeugt, der die Programmiersprachen von Maschinen beherrscht (z. B. KOP, AWL, GRAPH)

2. Die Sollwerte und Parameter (wie zum Beispiel Temperaturen oder Füllstände) werden gesondert betrachtet, in manchen Sicherungen werden diese Daten bewusst ausgeschlossen. Es handelt sich um Zustände, die im Condition Monitoring weiterverarbeitet werden. Für ein konsistentes Backup ist es wichtig, dass die Sollwerte und Parameter zum Zeitpunkt der Sicherung genau definiert sind (Initialwerte).

3. Die Konfigurationsdaten haben die Aufgabe, Zustände zu erreichen und sie sind wichtig für die individuelle Produktion. Hier kann es sich um Rezepturen handeln oder Energiewerte. Es können kundenindividuelle Daten sein.

4. Letztendlich gehört auch die Gerätelogik der Automatisierungskomponente zur Datensicherung, denn auf einem älteren Betriebssystem läuft ein modernes Programm nicht rund oder entscheidende Konfigurationsdateien werden nicht korrekt abgespielt (z. B. die Firmware).

Die Klassifizierung einer Datensicherung ist wichtig für die Dokumentation. Generell sollte jede Datensicherung bei jedem Datentransport auf Vollständigkeit und Richtigkeit überprüft werden. Will man ganz sicher sein, vergleicht man bei jeder Datensicherung die Checksumme eines Programmes. Die Prüfsumme (Checksumme) ist ein Wert, der aus den Ausgangsdaten berechnet wird und in

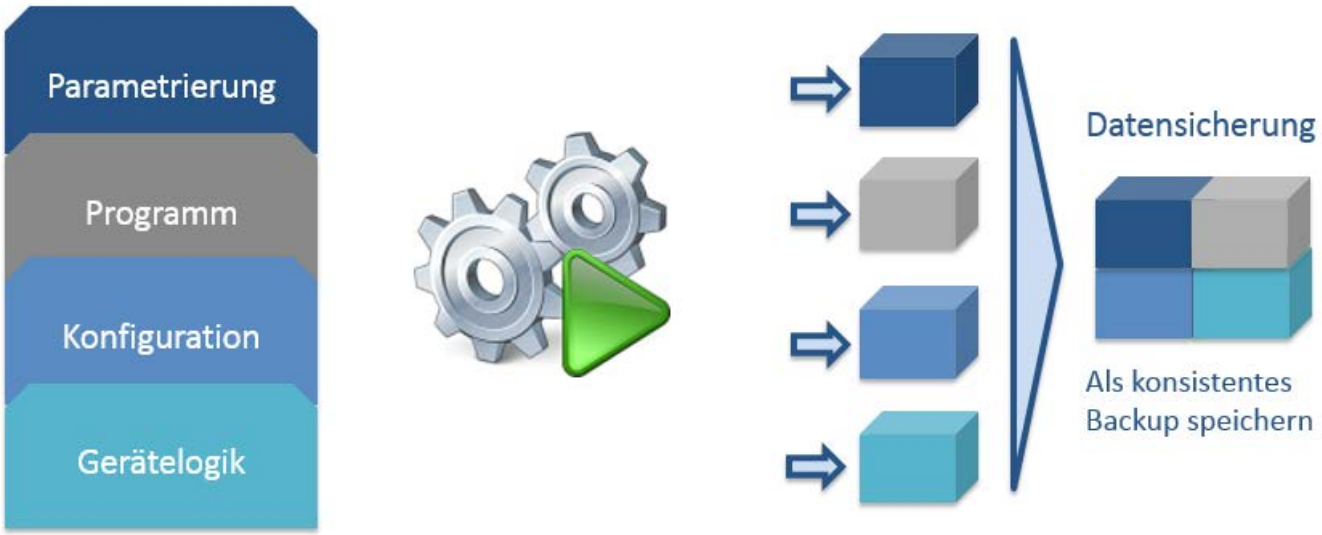

Bild 1: Eine Datensicherung aus der Produktion ist dann vollständig, wenn sie für ein Disaster Recovery (die Wiederherstellung auf einen älteren Stand) genutzt werden kann.

der Lage ist, mindestens einen Bitfehler in den Daten zu erkennen. Je nachdem wie komplex die Berechnungsvorschrift für die Prüfsumme ist, können mehrere Fehler erkannt oder auch korrigiert werden [1]. Bei gleicher Checksumme ist das Programm unverändert. Bei Änderungen vergibt man eine Versionsnummer mit Datum und Uhrzeit und hält fest, wer die Version wann und aus welchem Grund erstellt hat.

Auch ohne ein Datenmanagementsystem ist dies die gängige Praxis in der Produktion. Der Vorgang wird häufig durch den Automatisierungstechniker per Hand durchgeführt, indem er von Maschine zu Maschine geht und Daten sichert, vergleicht und dokumentiert. Wer hat was, wann, wo und warum geändert? Es sind die täglichen Fragen in der Instandhaltung, sei es von einer Schicht zur nächsten, bei der Inbetriebnahme einer neuen Maschine oder bei der Abstimmung einer Steuerung auf eine neue Produktionslinie. Jede Änderung, die in der Produktion nicht dokumentiert wurde, führt zu einer Unsicherheit, ob sie gewollt oder ungewollt durchgeführt wurde. Wichtiger ist, dass die verschiedenen Daten innerhalb einer Steuerung vollständig und konsistent gesichert werden, sonst kann der Datenstand häufig nicht für ein Disaster Recovery genutzt werden.

Wie funktioniert ein Disaster Recovery?

Werfen wir einen Blick in die Produktionshallen und auf die Herausforderungen für ein Disaster Recovery. Fast immer ist die Instandhaltungsabteilung zuständig. Das Thema wird oft getrennt von der Office-IT behandelt, weil das Wissen um den Maschinencode vom Maschinenbauer kommt. Der Instandhalter hat ein Programmiernotebook, mit dem er sich mit den unterschiedlichen Komponenten in der Produktion verbindet. Die Daten der letzten Datensicherung sind in der Regel auf einem virtuellen Server im Netzwerk gespeichert und je nach Berechtigungsstufen erreichbar.

Im Falle eines Disaster Recoverys kopiert der Instandhalter die letzte bekannte Version auf sein Notebook und prüft sie auf Konsistenz, Vollständigkeit und Dokumentation (s. Bild 2). Dann vernetzt er sich mit dem Automatisierungsgerät und spielt die Version auf. Jetzt vergleicht er den Stand (online im Gerät) mit der letzten Sicherung auf dem Server. Sind beide Versionen bis auf das letzte Bit gleich, dann weiß der Instandhalter, dass alles in Ordnung ist und er dokumentiert dies. Sind beide Versionen nicht gleich, kommt es auf die Unterschiede an und welche Auswirkungen diese auf die Produktion haben (s. Bild 3). Es gibt Unterschiede, die trotz aller Sorgfalt und Vorsicht erklärbar sind wie beispielsweise ein physikalischer Fehler oder der Ausfall einer Batterie. Nicht dokumentierte Unterschiede können aber auch auf menschliche Fehler oder im schlimmsten Fall auf manipulierte Daten hinweisen.

Wenn alle Verteidigungslinien fallen, hilft die Wiederherstellung aus einer Datensicherung

Alle Systeme im Detail zu beherrschen ist eine herausfordernde Aufgabe. Auch weil Hacker jeden Tag neue Ideen haben und nicht zögern, diese auszuprobieren. Es werden zudem immer mehr Angriffe registriert, gegen die eine Verteidigung unmöglich ist (Zero-Day-Attacken). Durch Cyber-Angriffe auf Produktionsanlagen haben wir gelernt, dass Angriffe auf automatisierte Steuerungen sehr

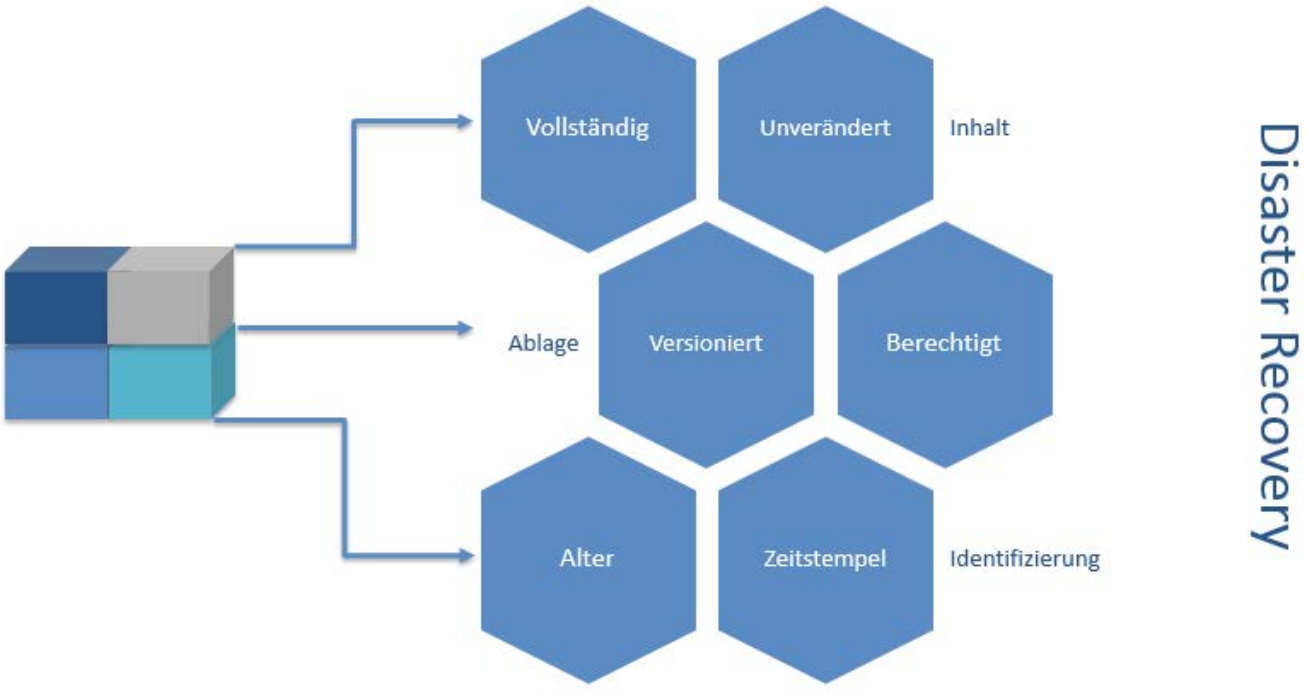

Bild 2: Darstellung der Klassifizierung einer Datensicherung in der Produktion nach Inhalt, Ablage und Identifizierung für ein Disaster Recovery.

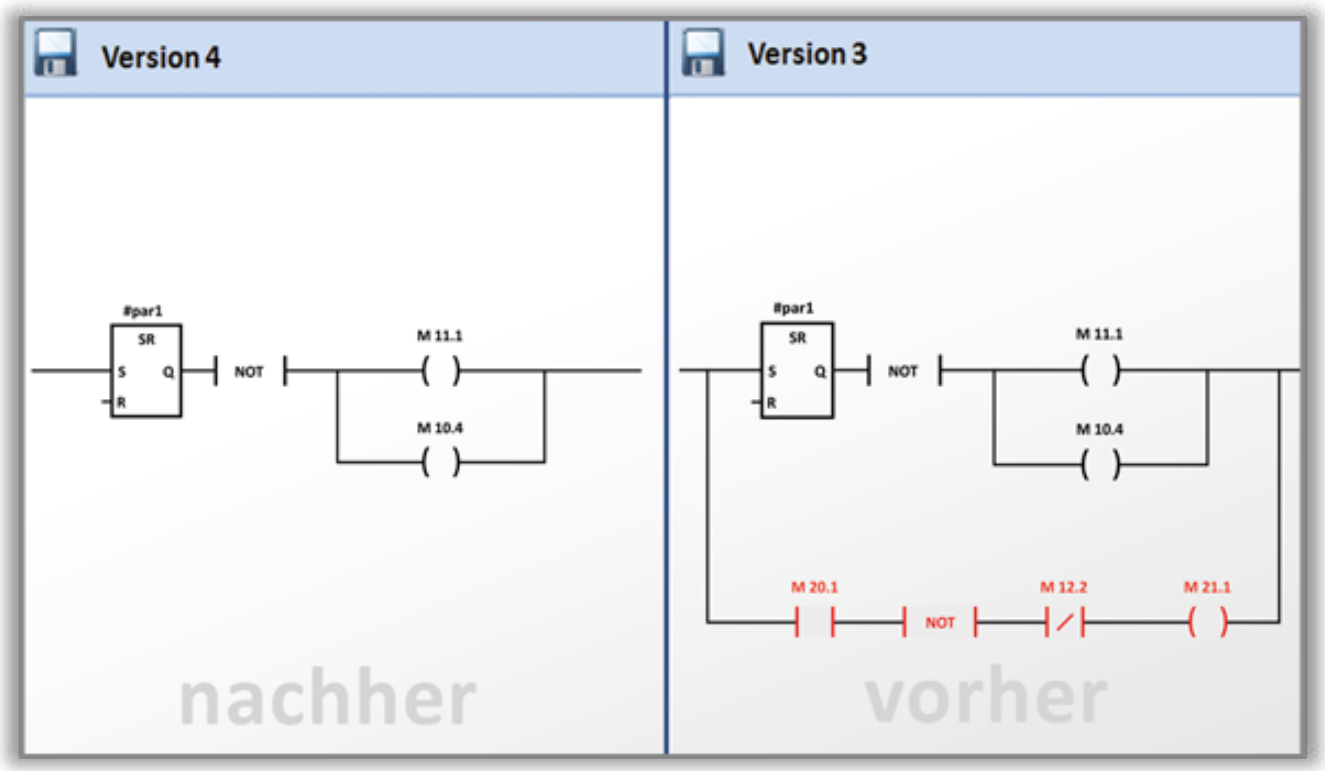

Bild 3: Unterschiedsanalyse zwischen zwei Softwareprojekten. Änderungen werden in Rot hervorgehoben.

gefährlich sein können. Es erfordert eine umfangreiche Verteidigungsstrategie, um Produktionsdaten zu schützen, und keine hat sich bisher als alleiniges Allheilmittel erwiesen. Kein Virenscanner schützt die Produktion in Echtzeit (Real-Time-Class), kein Softwareupdate kann durchgeführt werden, ohne dass nicht die Gefahr besteht, dass Daten manipuliert werden.

Seither werden die Verteidigungslinien mit aller Macht verstärkt und Sicherheitslücken geschlossen. Doch jedes Jahr tauchen neue Cyberangriffe auf und wenn diese dann einmal durchkommen, hilft die Wiederherstellung des Systems mit dem letzten „sauberen“ Backup [2]. Kein Wunder also, dass Cybersecurity das Top-Thema der Digitalisierung ist. Bis ein konkretes und wirksames Mittel gegen die Angriffe gefunden wird, sollten wir für den Notfall gewappnet sein.

Eine Datensicherung ist ein guter Anfang.

Referenzen:

[1] https://de.wikipedia.org/wiki/Pr%C3%BCfsumme

[2] In 2016 Deutsche Wasserwerke, http://www.spiegel.de/netzwelt/web/deutschland-sicherheitsluecke-wasserwerke-ungeschuetzt-im-internet-a-1103147.html In 2017 Ausnutzen einer Sicherheitslücke bei Windows-XP-Rechnern durch Wannacry-Virus, http://www.spiegel.de/wirtschaft/unternehmen/cyberangriffe-auf-deutsche-firmen-verursachen-milliardenschaeden-a-1158975.html

Dr. Thorsten Sögding
Head of Business Development
AUVESY GmbH & Co. KG
76829 Landau in der Pfalz
Tel. +49 6341 6810-560
Thorsten.Soegding@auvesy.de

Stefan Schnackertz
Business Development
AUVESY GmbH & Co. KG
76829 Landau in der Pfalz
Tel. +49 6341 6810-561
Stefan.Schnackertz@auvesy.de