

## Passivierungsverfahren

## Edelstahl mit verbessertem Korrosionsschutz versehen

Produktion Nr. 10, 2009

TÜBINGEN (ba). Rostflecken am Auto sind ein ärgerlicher Anblick. An Maschinen in der Chemie- oder Pharmaindustrie oder an chirurgischen Instrumenten können sie jedoch die Sicherheit von Anwender oder Patient gefährden. Daher findet hier besonders korrosionsbeständiger Edelstahl Verwendung.

Doch ist Edelstahl nicht gleich Edelstahl. Man zählt über 100 Sorten, die

sich in ihrer Legierung unterscheiden. Die Ansprüche an diese sind hoch, mitunter sogar gegensätzlich. So wird neben der Korrosionsbeständigkeit in vielen Fällen auch die Härtebarkeit gefordert. „Dann geht das eine auf Kosten des anderen“, sagt Dr. Rudolf Reichl vom Naturwissenschaftlichen und Medizinischen Institut in Reutlingen (NMI). „Die Härtebarkeit wird nämlich mit einer geringeren Korrosionsbeständigkeit erkauft. Aber das soll sich jetzt ändern.“ Reichl ist Leiter eines Projektes, zu dem sich neunzehn

Firmen aus dem Maschinenbau, der Chemie- und Pharmaindustrie und der Medizintechnik zusammengefunden haben. Sie wollen die Korrosionsbeständigkeit von Edelstählen deutlich erhöhen. Kein leichtes Unterfangen: Da ist zunächst einmal die chemische Zusammensetzung des Werkstoffes an seiner Oberfläche zu berücksichtigen. Je nachdem, wie er behandelt wird, sind die Auswirkungen auf seine Oberfläche und damit auf seine Korrosionsbeständigkeit verschieden. Natürlich spielen auch die

Passivierungsverfahren, also wie der Werkstoff mit Korrosionsschutz versehen wird, eine Rolle. „Da kann man nicht einfach irgendwo ansetzen“, so Reichl, „sondern man muss einem ganzheitlichen Ansatz folgen, der alles im Blick hat.“

Darauf ist auch die wissenschaftliche und technische Zielstellung des Projektes ausgerichtet. Bereits knapp neun Monate nach Projektbeginn können die Wissenschaftler des NMI mit Ergebnissen aufwarten. „Der erste Meilenstein ist erreicht“, sagt Reichl.

„Unsere Erwartungen haben sich ganz und gar erfüllt. Hinsichtlich einer höheren Produktsicherheit sind wir wirklich sehr gut vorwärts gekommen: Wir haben die Korrosionsbeständigkeit verbessern können und das bei nachgewiesener Bioverträglichkeit der korrosionsgeschützten Werkstoffoberflächen. Damit wurden Qualitätssprünge erreicht, die für unsere Partner zu entscheidenden Wettbewerbsvorteilen werden.“ Und das ist in diesen Zeiten eine gute Nachricht.

**Überformate bis zu 6.000 x 2.000 mm<sup>2</sup>**

Laserschneiden

- bis 40 mm Edelstahl oxidfrei
- bis 25 mm Baustahl & 12 mm Alu
- Materiallager bis 6.000 x 2.000 mm<sup>2</sup>

Laserschweißen

- bis 12 mm Einschweisstiefe
- 2 und 2½ D-Bearbeitung

Anwendungstechnik

- Abkanten 3000 mm
- Anarbeitung - Schweißen - Montage

**PS LASER** PS Laser GmbH & Co. KG  
Fon 0 42 04 - 99 86 - 0 Bahnhofstraße 56  
Fax 0 42 04 - 99 86 - 99 27321 Thedinghausen

Info@ps-laser.de  
www.ps-laser.de

## Produktionsnetze

## Sicherheit ist machbar

von Robert Wouters  
Produktion Nr. 10, 2009

MÜNCHEN (Iz). Am Industrial Ethernet kommt man nicht mehr vorbei. Ein Verzicht wegen potenzieller Sicherheitsprobleme ist keine Alternative. Denn Sicherheit ist machbar. Experten wissen, wie das geht.

Auf Basis von Ethernet sind auch in der Welt der Produktion die einfache und schnelle Vernetzung, hohe Bandbreiten zu geringen Kosten sowie Flexibilität und unbeschränkter Datenzugriff möglich. Diese Vorteile wollten viele Unternehmen nutzen. In den vergangenen Jahren wurden immer mehr Feldbusssysteme dadurch ersetzt.

Allerdings wird diese Entwicklung immer noch kontrovers diskutiert. Neben der stabilen Verfügbarkeit ist die Sicherheit ein zu hinterfragendes Problem. Aus der Offenheit und Transparenz des Internet Protokolls ergeben sich die aus der Office-Welt bekannten Sicherheitsrisiken auch für das Produktionsnetz. Sie reichen von Angriffen auf Betriebsgeheimnisse, über das wissentliche oder unwissentliche Verändern von Produktionsdaten, bis hin zur Sabotage. Dabei werden Security-Lösungen oft vor dem Hintergrund der Echtzeitproblematik diskutiert. Jeder Security-Mechanismus muss anhand von Regeln oder Konfigurationen überprüfen, ob Verbindungswünsche erlaubt sind. Das kostet Zeit und auch Performance.

#### Böse Hacker sind die Ausnahme bei Störungen

Doch es gibt mittlerweile praktikable Lösungen. Einen guten Schritt weiter kommen Betroffene mit den Ergebnissen, die der Fachausschuss ‚Security‘ in der VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) erarbeitet hat. Sie liegen seit August 2007 in Form der Richtlinie VDI/VDE 2182 Blatt 1 vor. Die Blätter 2, 3 und 4 werden im Sommer 2009 publiziert. Dipl.-Ing. Klaus Koch gehört dem Fachausschuss an und sagt: „Wir haben einen prozessorientierten Ansatz für die Entwicklung von Security-Maßnahmen erarbeitet, der alle wesentlichen Aspekte der eingesetzten Geräte, Systeme und Anlagen berücksichtigt.“ Koch, der auch Geschäftsführer bei der CAT-Consulting für Automatisierungstechnik ist, hebt hervor, dass „mit der Richtlinie die Sichtweisen von Herstellern, Systemintegratoren, Maschinenherstellern und Betreibern gleichermaßen berücksichtigt wurden.“ Die Richtlinie unterstützt den Anwender mit einem Vorgehensmodell für eine angemessene und wirtschaftliche Sicherheitslösung. Das greift bei existierenden und neu geplanten Anlagen. Die wenigen veröffentlichten Berichte über Störungen zeigen, dass bei den Auslö-



mGuard industrial RS von Innominate für die ‚Stealth Mode‘-Firewall zur autarken Integration in Produktionsnetz und Schutz jeder Steuerung vor unerlaubtem Zugriff.

Torsten Rössel, Leiter Geschäftsentwicklung der Innominate Security Technologies AG, plädiert für ‚Industrie-Firewalls‘. Sie werden als eigenständige, autarke Systeme ins Produktionsnetz integriert. Entscheidend ist dabei ihre rückwirkungsfreie und unabhängige Arbeitsweise. Eine solche ‚Stealth Mode‘-Firewall von Innominate z.B. wird transparent der Maschine vorgeschaltet. Sie bleibt so für Angreifer ‚unsichtbar‘. Alternativ kann sie als Router mit der sogenannten 1:1 Network Address Translation identische, interne Maschinennetze auf eindeutige virtuelle Adressen abbilden. Eingriffe in das Betriebssystem oder Konfigurationen an der Maschine sind auch bei Sicherheitsupdates nicht notwendig. Trotzdem können die Maschinen über einen sicheren ‚Tunnel‘ via Internet erreicht und ferngesteuert werden. Ein Zugriff auf das übrige Firmennetz ist nicht möglich. Ein industrielles Anlagennetz kann man sicherheitstechnisch nicht so verwalten wie ein Office-Netz.

#### „Sicherheit ist ein permanenter Prozess.“

Ralph Langner,  
Vorstandsvorsitzender der Langner Communications AG

Ralph Langner meint: „Sicherheit wird nicht einmal geschaffen, sondern ist ein permanenter Prozess.“ Dafür ist auch die Trennung der Fertigungsebene vom restlichen Firmennetzwerk nötig. Torsten Rössel kennt dafür eine brauchbare Regel: „Wenn man anfängt, Sicherheit zu implementieren, ist das Produktionsnetz in sich zunächst meist völlig offen. Dann werden nach und nach die tatsächlich notwendigen Verbindungen identifiziert und die zulässige Kommunikation auf diese eingeschränkt. Nach der Devise: Was nicht explizit erlaubt ist, ist verboten.“ Und damit ist eigentlich schon das größte Bedrohungspotenzial weg.

**HBS**

**Die bestefeste Verbindung\***

\* in Millisekunden

Bolzenschweißen

- Handgeräte
- Stationäre Anlagen
- CNC-Vollautomaten
- Schweißbolzen

[www.hbs-info.de](http://www.hbs-info.de)

**Wer hilft Ihnen wirklich?**

**Entfettung & Reinigung von Neu- und Reparaturteilen ... BvL!**

**BvL**

OBERFLÄCHENTECHNIK

Grenzstraße 16  
D-48488 Emsbüren  
Tel (0 59 03) 951-60  
Fax (0 59 03) 951-90  
[www.BvL-Group.de](http://www.BvL-Group.de)

Fachbetrieb nach § 19 (I) WHG  
Zertifiziert DIN ISO 9001:2000