

UPDATE

Das Innovationsmagazin
von Phoenix Contact



Sicherheit

Cyber Security

Der fortwährende Kampf um die Sicherheit der Netze

Sensible Türsteher

Wie konfektionierbare Steuerungen automatischen
Rolltoren die technischen Manieren beibringen

Mit Blitz und Donner

Warum Blitze im niedersächsischen Großenmeer
höchst willkommen sind

Tödliche Unfälle

9.815
 tödliche Haushaltsunfälle
 in Deutschland pro Jahr
 (davon 4.000 Treppenunfälle)

3.500
 tödliche Verkehrsunfälle
 in Deutschland pro Jahr
 (in Thailand 22.000)

Funktionale Sicherheit

43.791
 Arbeitsunfälle an Maschinen
 in Deutschland im Jahr 2015

37%
 illegale Manipulationen im
 Jahr 2017 an allen Maschinen-
 Schutzeinrichtungen

Cyber-Kriminalität

33%
 Anstieg von Schad-Software
 auf mobilen Endgeräten

? 175 Tage
 durchschnittlich bleibt
 ein Angriff unentdeckt

82.600
 Hackerangriffe in
 Deutschland (2016)



83%
 deutscher Unter-
 nehmen registrierten
 Phishing-Angriffe
 (2016)

1 Cyber-Angriff
 alle 3 Minuten
 in Deutschland (2018)

Datendiebstahl
 Verteilung der erbeuteten
 Daten in Prozent (2018)



Blitzschutz

4,4
 Blitze pro Jahr auf 1 km² im
 Landkreis Garmisch-Partenkirchen
 (Ort mit den häufigsten
 Blitzen in Deutschland)

44 ⚡
 Blitze durchschnittlich
 weltweit pro Sekunde

232
 Blitze pro Jahr auf 1 km²
 auf dem Maracaibo-See,
 Venezuela (Ort mit den
 häufigsten Blitzen weltweit)



Torsten Gast,
Director Competence Center Services
für Safety & Industrial Security

Gallier und der Cyberspace

Liebe Leserinnen, liebe Leser,

„Auf dass uns der Himmel nicht auf den Kopf falle.“ Die Welt hat sich seit den Zeiten von Asterix, Obelix und ihrem gallischen Chef Majestix zwar deutlich geändert. Doch der Wunsch nach Sicherheit ist nach wie vor allgegenwärtig. Dem stellen wir uns bei Phoenix Contact.

Zunächst einmal geht es natürlich um den Schutz von Leib und Leben. Was passiert, wenn der Blitz einschlägt? Wie sichern wir Maschinen? Und wie halten wir unerwünschte Eindringlinge fern? Wir lösen solche Herausforderungen heute etwas weniger handfest als die Gallier, etwa durch auslesbare RFID-Markierungen an unseren Blitzschutzanlagen (ab Seite 40). Und vor einer vernünftigen Videoüberwachung hätten auch die alten Römer Respekt (ab Seite 44).

Ähnlich umweltverträglich wie antike Streitwagen sind heute wohl nur E-Autos. Wir haben nachgeschaut, wie deren Batterien auf Zuverlässigkeit getestet werden (ab Seite 34). Wind und Sonne kannten auch schon gottesfürchtige Gallier. Die Einspeisung dieser Energien stellt unsere heutigen Verteilnetze aber vor neue Herausforderungen. Wie die Stadtwerke Kempen dies sicher bewerkstelligen, verraten sie ab Seite 30.

Mit ganz neuen Bedrohungen hat der moderne Mensch in seiner vernetzten Welt zu tun. Wir stellen uns den Herausforderungen aus dem Cyberspace mit einem ganzen Strauss von Massnahmen, von Hardware über Software-Entwicklung bis hin zu ganzheitlichen Beratungsdiensten. Ein 360°-Rundumschutz für unsere Kunden.

Derart geschützt hätte auch der Chef des kleinen gallischen Dorfs keine Bange, dass ihm nicht doch noch der Himmel auf den hörnerbewehrten Kopf falle!

Torsten Gast



Die Wabe gilt als die stabilste aller Geometrien im Tierreich. Sie schafft durch ihre Struktur Sicherheit für einen ganzen Staat



Was macht Computernetze wirklich sicher? Ein Interview mit Dr. Lutz Jänicke

10

Cyber Security

Der Hüter der Netze

Was für eine Motivation steckt eigentlich hinter den Angreifern auf Computernetze? Und wie kommt man den Finsterlingen bei? | 10

IRMA passt auf

Und das, ohne dass man es merkt. Was man sich davon bei den Stadtwerken von Bad Pyrmont verspricht | 14

Die Daten-Bodyguards

Du kommst hier nicht rein. Eigentlich sind die Kollegen von Cyber Security Berlin aber sehr sympathisch. Und ausserdem echte „Kundenverstehere“ ... | 18



Damit Windrotoren nicht zu Eis-Weitwurfmaschinen werden

22



Sicherheit bei Tür und Tor hat sich die ASO Safety GmbH auf die Fahnen geschrieben

26



Eine Reportage über einen Betrieb, für den Blitze Grund zur Freude sind

34



Unerkannt kommt an seiner Lösung für Videoüberwachung niemand vorbei

44

SICHERE WINDTURBINEN

Pflaster für die Flügel

Wenn Blattläuse in schwindelerregenden Höhen Eisdetektoren installieren | 22

SICHERE ANLAGEN

Sensible Türsteher

Wer sagt, dass Leiterplatten-Anschlusstechnik langweilig sein muss? Auf das Produkt kommt es an! | 26

SICHERE NETZE

Wer hat's erfunden?

Die Schweizer NSE macht mit ihrem Schutzgerät KOMBISAVE intelligente Stromnetze noch sicherer | 30

SICHERE BATTERIEN

Höllenfahrt für Lilon-Akkus

Hochleistungsbelastung für die Antriebsmittel der Zukunft - unter kontrollierten Bedingungen | 34

BLITZSCHUTZ

Blitz und Donner digital

Wie behält man den Überblick, wenn Klima und Wetter die Ableiter strapazieren? | 40

SICHERER RAUM

Eierlegende Video-Wollmilch-Box

Sie ist das Universalgenie zwischen Kamera und Zentrale | 44

Editorial | 03

Aus der Branche | 06

Hinter den Kulissen | 48

Impressum | 51

Vorschau | 51



Offshore-Windparks sollen in einem Verbund Energie liefern, die auf einer künstlichen Insel umgewandelt wird

Klimaschutzfaktor 50

Dänemark überrascht mit kühnem Plan für eine radikale Energiewende

So richtig erfolgreich war die Klimakonferenz in Madrid nicht, denn die meisten Industrieländer, mit Ausnahme der EU, mochten sich an konkreten weiteren Schritten auf dem Weg zu einer echten Energiewende nicht beteiligen.

Ganz anders Dänemark, das auf der UNO-Konferenz ein deutliches Statement abgab.

Und zwar mit einem Plan, wie man ihn sonst nur von arabischen Öl-Potentaten kennt: Mittels einer künstlichen Insel, die als Hub für umliegende Offshore-Windparks errichtet werden soll, will das nordische Land einen wesentlichen Beitrag zur Klimasanierung leisten. Während die Windräder erneuerbare Energie in

einer Größenordnung von 10 GW erzeugen, sollen auf der Insel Power-to-X-Technologien in speicherbare Energieträger wie Wasserstoff, synthetische Kraftstoffe oder Gas umgewandelt und dann per Tankschiff an Land gebracht werden. Zur Einordnung: Dafür benötigt man rund 1.000 Hochleistungs-Wind-

räder. Die gewonnene Energie würde mehr als 10 Millionen Haushalte versorgen, also mehr, als Dänemark Einwohner hat. Standortsuche und Genehmigung sollen bereits 2021 abgeschlossen sein, danach wird der konkrete Baubeginn geplant.

energinet.dk

Bugatti unter den Rechenkünstlern

Der teuerste Serien-Mac

Wenn es um die Anschaffung neuer Office-PC geht, wacht das Auge des Controlling argwöhnisch über die Nutzer von Mac-Computern. Das Lifestyle-Image begleitet eben auch das eigentliche Kerngeschäft des Unternehmens aus Cupertino. Sind die teuren Kisten wirklich erforderlich?

Doch Mac's sind das Handwerkszeug von Medientreibenden. Einem Rembrandt hätte man ja auch nicht den Pinsel weggenommen und ihn mit einem Stück Kreide an die Leinwand geschickt. Allerdings sind die rekordverdächtigen 52.000 Dollar, mit denen man das neue Spitzenmodell Mac Pro zur Highend-Rechenrennmaschine am Arbeitsplatz machen kann, schon eine sehr selbstbewusste Ansage.

apple.com



Wenn Brillen schlau machen

Neue Miniaturisierung blendet Daten in normale Sehhilfen ein

Sie werden „Smartglasses“ genannt: Brillen, die mittels Projektortechnologie Zusatzinformationen ins Sichtfeld einblenden. Bisher waren sie allerdings umständlich und zu klobig.

Bosch Sensortec hat jetzt eine neue Generation von schlaun Brillen entwickelt. Mittels eines gebündelten Lichtscanners wird ein holografisches Element gescannt, das in die Linse der Brille integriert ist. Dieses Element lenkt den Strahl direkt auf die Netzhaut, wo ein hochauflösendes Bild erzeugt wird – scharf, hell und auch bei direkter Sonneneinstrahlung gut erkennbar.

Das „Light Drive System“ selber ist so klein, dass es in nahezu jede moderne Brille integriert werden kann. Die Daten, etwa Navigationsinfos, liefert ein verbundenes Smartphone. Zur Bedienung hat Bosch Sensortec

auch noch passende Sensoren im Paket, die in den Brillenbügel eingesetzt werden können.

Das System wird erstmalig auf der Consumer Electronics Show CES Anfang Januar 2020 in Las Vegas vorgestellt.

bosch-sensortec.com



5G lernt laufen

Forschungsprojekt 5G Industry Campus Europe

Auf dem Campus der RWTH Aachen startet das grösste industrielle Forschungsprojekt Europas in Sachen 5G. Unter der Leitung des Fraunhofer Instituts für Produktionstechnologie (IPT) sollen Möglichkeiten der Nutzung der superschnellen Mobilfunknetze entwickelt und erprobt werden.

Ziel ist es, z. B. den Einsatz mobiler Robotik steuern zu können. Die Überwachung grösserer Fertigungsprozesse oder von ganzen Produktionsketten steht ebenfalls auf dem Plan.

ipt.fraunhofer.de



Energiewettlauf

Der Osten wird Hightech-Zone

Lange galt das Thema Batterie als verloren für westliche Industrien. Zu weit schien der Technologievorsprung asiatischer Marktführer zu sein.

Doch seit Tesla seine Gigafactory-Pläne nahe des Berliner Flughafens verkündete, scheint ein Bann gebrochen. Jetzt zieht BASF mit der Planung einer Batteriefabrik am Traditionsstandort Schwarzheide nach.

Das Ziel sei es, Batteriekathoden für etwa 300.000 Elektroautos pro Jahr herzustellen, teilt BASF mit. Die Basismaterialien wie Nickel-Kobalt-Aluminiumoxid oder Nickel-Kobalt-Manganoxid kommen aus der finnischen Fabrik in Harjavalta. An eine Endfertigung von Batterien oder Batteriezellen denke man allerdings nicht, so BASF.

Die Entscheidung für den Einstieg in die mobilen Energiespeicher wird laut Unternehmensleitung im Frühjahr 2020 erwartet.

basf.com



Mit dem Server heizen

Green IT – überflüssige Abwärme clever genutzt

Der grösste Einsparfaktor in Rechenzentren liegt bei der Klima- und Lüftungstechnik. Diese macht bis zu 60 Prozent der Energiekosten aus. Denn mit den Prozessoren von Computern kann man im Betrieb locker auch Spiegeleier braten, so heiss werden die digitalen Kraftmeier. „Eine Herdplatte gibt eine Wärme von etwa acht Watt pro Quadratmeter ab“, führt Nicolas Röhrs aus. „Die neueste Generation an Server-Prozessoren kommt locker auf 31 Watt pro Quadratmeter“, erklärt der Start-up-Gründer.

In Serverräumen wird es schnell unerträglich warm, wenn die Wärme nicht abgeführt, sprich die Räume aufwändig klimatisiert werden. In Zeiten von Klimaschutz und CO2-Effizienz ein sprichwört-

lich heisses Thema. Das Start-up Cloud&Heat hat dazu eine pfiffige Lösung entwickelt. Die Dresdner setzen eine innovative Heisswasser-Direktkühlung ein, die eine Nachnutzung der Abwärme zum Heizen von Gebäuden oder die Anbindung an Fern- und Nahwärmenetze ermöglicht. Diese kann ohne den Einsatz von Wärmepumpen das Temperaturniveau konstant auf 60 Grad halten.

Green IT nennt das Start-up seine Vision. Und versteht darunter viel mehr als nur ein Heizsystem. Um die Klimabelastung von Rechenjobs transparent zu gestalten, hat Cloud&Heat etwa eine neue Software entwickelt, die die CO2-Bilanz von Rechenjobs in Echtzeit ermittelt.

cloudandheat.com



Statt energieintensiv zu kühlen, wird mit diesen Serverschränken geheizt





SICHERHEIT

NACHGEFRAGT



Der Hüter der Netze



Wenn Daten sicher werden sollen, schlägt seine grosse Stunde. Dr. Lutz Jänicke hat die Verantwortung für die Sicherheit von Produkten und Lösungen bei Phoenix Contact. Ein Interview über Burgen, Schlapphüte, Mafia und Motivation.

Von Hause aus ist Dr. Lutz Jänicke eigentlich Elektrotechniker. Aber im Zuge seiner Promotion und nachfolgender Aufgaben ist er „irgendwie ins Thema reingerutscht“. Mittlerweile ist er ein international bekannter Experte für das Thema Datensicherheit. Und allererste Adresse bei Phoenix Contact, wenn es um den systemischen Schutz von Netzwerken geht. Das Interview fand passenderweise in der alten Burg- und Schlossanlage von Bad Pyrmont statt.

→ Herr Dr. Jänicke, sind wir hier sicher?

(schmunzelt) Naja, vor 1000 Jahren vielleicht. Aber wie hat man früher Burgenanlagen angegriffen? Man hat geschossen, gestürmt, belagert und schliesslich Tunnel gegraben, die die Mauern zu Fall bringen sollten. Also nach Schwachstellen gesucht. Das ist heute nicht anders als vor 1000 Jahren.

Security war und ist kein technisches, sondern ein Prozess-thema. Es kommt darauf an, dass keine Lücke auftaucht.

→ Einmal Security aufgesetzt, dauerhaft sicher?

Nein, das ist ein kontinuierlicher Prozess. Man muss sich vorher überlegen, wie man seine Abwehr so organisiert, dass man

auf möglichst alle Eventualitäten vorbereitet ist. Und dann muss die Abwehr dem Angreifer möglichst einen Schritt voraus sein. Im Mittelalter hatte man dafür Jahre Zeit, heute muss das flotter gehen.

Fehler entstehen häufig in klassischen Mustern. Man verlässt sich auch beim Programmieren darauf, dass die Kollegen ihren Job gut gemacht haben. Schleichen sich in einer Arbeits-teilung Fehler ein, sind das die offenen Tore für einen Angriff. Dagegen hilft das Vier-Augen-Prinzip. Wie beim klassischen Burgbau muss schon am Anfang das Verteidigungskonzept stehen. Das meinen wir mit Security by Design.

Das ist arbeitsintensiv, für kreative Köpfe lästig und auch teuer. Am Ende hat man dann ein Produkt, das noch nicht einmal anders aussieht als ein unsicheres Produkt, nur teurer ist. Das muss man erst mal argumentieren. Helfen tut der Gesetzgeber bei der kritischen Infrastruktur. Oder die eigene bittere Erfahrung durch Produktionsausfälle. Das kostet schnell mehrere Millionen Euro bis hin zum massiven Kundenverlust durch Lieferunfähigkeit oder dem unternehmerischen Kollaps. Das nennt man dann Sparen am falschen Ende.





→ **Nimmt die Bedrohungslage insgesamt zu?**

Definitiv. Statistiken unserer Branche sind schwierig zu bekommen, aber die beim FBI gemeldeten Schäden durch Cyber-Security-Vorfälle in den USA haben sich in den letzten zehn Jahren verzehnfacht, von 2008 auf 2018, von 200 Mio. auf 2 Mrd. Dollar. Das sind absolut realistische Zahlen.

→ **Wer sind die bösen Jungs? Und was sind die Motive?**

Es gibt ganz unterschiedliche Angreifer. Es gibt die Einzelperson, die agiert, da ist der Schaden meist aber nicht so hoch. Das kann aus anarchischen Motiven sein, aber eben auch ganz handfeste wirtschaftliche Gründe haben. Häufig wird Schad-Software benutzt, die tatsächlich gekauft werden kann, wie man das von Apps kennt.

Dann gibt es kommerzielle Organisationen, wo man hochwertige Angriffe gegen Geld kaufen kann, etwa Dienstleister der organisierten Kriminalität in Russland. Und man hört von chinesischen Gruppen, die dann allerdings im Staatsauftrag handeln. Das ist dann schon halbstaatlich.

Und dann gibt es noch die staatlichen Akteure, also NSA, chinesische Volksarmee oder die heimische Bundeswehr, die ja auch aufrüstet. Man kommt den vermeintlichen Akteuren auf die Schliche, wenn man etwa die Zeitstempel der Serveraktivitäten ausliest. Da findet man dann auffallend oft übereinstimmende Zeiten aus einer ganz bestimmten Zeitzone. Denn auch bei Cyber-Piraten gibt es übliche Office-Zeiten.

→ **Wie trainiert man seine Cyber-Abwehrkräfte, wenn man selber „zu den Guten“ gehört? Wie kommt man an die erforderlichen Tools, wenn man selber nicht angreift?** Man muss nicht mal ins Darknet gehen. Selbst die NSA veröffentlicht ab und an Tools, die kann man sich einfach runter-

laden. Oder bei eBay für 10 Dollar erwerben. Für Laborzwecke im eigenen Umfeld darf man die auch in Deutschland verwenden, nur nicht zu Angriffszwecken im freien Feld.

Doch man braucht auch die echte Umgebung, um seine Werkzeuge zu testen, und damit auch die Abwehr. Wenn man solche Tools durchs Haus geistern lässt, können aber in unserer vernetzten Umgebung Dinge passieren, die wir eben nicht mehr im Griff haben. Daher sind wir da sehr vorsichtig. Ziel muss es aber sein, dass unsere Netze das aushalten.

→ **Wir leben in einer immer vernetzteren Welt. An die Sicherheit denkt man aber immer erst nach Vorfällen. Eine Wahrnehmung, die real ist?**

Viele kleinere Unternehmen agieren tatsächlich so. Das ist wirklich kritisch. Größere Unternehmen sind meist deutlich vorsichtiger. Die IT von Phoenix Contact etwa ist sehr wachsam. So ist die Produktion z. B. komplett abgekoppelt vom normalen Office-Netzwerk.

→ **Wie fing das Thema bei Phoenix Contact an?**

Beim Berliner Start-up Innominate sind wir 2002 mit dem Thema mobile Firewalls gestartet, sind aber schnell in den Bereich Industrieautomation vorgestossen. 2008 hat Phoenix Contact dann Innominate übernommen.

Die Phoenix Contact-Gruppe kann aber nicht nur auf Firewalls setzen, sondern muss Datensicherheit in all ihren Prozessen berücksichtigen. Meine Aufgabe ist es, das Thema Security ein Stück weit zu demokratisieren. Wir machen Trainingsprogramme, bilden Leute aus, entwickeln Tools. Jeder, der Software schreibt, muss sich dem Thema Security stellen und sich an bestimmte Guidelines halten.



→ **Wie harmoniert Cyber Security mit klassischer Industrie und herkömmlicher IT?**

Eigentlich gut. Wir sind die Fachleute für unseren speziellen Bereich. Das wird im Allgemeinen in der IT gewürdigt.

Ganz anders sieht das oft in der Produktion aus. Da ist in der Regel keiner für die Security zuständig. Wird eine Maschine aufgestellt, denkt niemand an deren saubere Integration ins Netzwerk. Dann wird ganz zuletzt gemotzt, warum denn die Steuerung nicht angeschlossen sei. Da müsse noch „ne Strippe gezogen“ werden.

Für Controller sind wir allerdings häufig nur ein Kostenfaktor. An dem kann man doch sparen. Läuft doch auch ohne. Wir haben häufig sehr grosse Schäden, die aber ziemlich selten sind. Daher glaubt jeder, dass es sein Unternehmen nicht trifft.

→ **Auf welchen Feldern ist Phoenix Contact in Sachen Cyber Security aktiv?**

Wir sind sowohl im eigenen Unternehmen als auch bei Kunden aktiv. Das hilft in beiden Richtungen, denn so wächst auch unser Beratungsverständnis in den Produktionsbereichen. Und unsere neuen Zertifizierungen zeigen, dass wir von Bestandsaufnahme bis Installation, Inbetriebnahme sowie Schulung alle Prozesse auch kompetent abbilden und anbieten können. Das ist TÜV-geprüft, ganz sprichwörtlich.

Wir haben gerade ein sehr aufwändiges mehrstufiges Zertifizierungsprozedere mit dem TÜV Süd hinter uns und erfolgreich bestanden. Das zeigt, wie ernst wir das Thema wirklich nehmen.

→ **Was kommt in Sachen Security in Zukunft aus Ihrer Sicht auf die Unternehmen zu?**

Grundsätzlich ist davon auszugehen, dass die massiv wachsende Bedrohung Geschäftsführungen unter Druck setzen wird. In der Lieferkette steigt der Kundendruck dadurch, dass Security immer mehr ein Thema in der Lieferantenbewertung wird. Auch der Gesetzgeber wird neue Regeln setzen.

→ **Offenheit und Verschwiegenheit – ist sich die Branche der Netzwerkschützer nicht durch übertriebene Geheimhaltung bei Cyber-Angriffen selbst im Wege?**

Das ist eine Frage der Kultur. Es ist richtig, dass ein Austausch über Bedrohung und erfolgte Angriffe für alle wichtig ist. Unternehmen, die nicht börsennotiert sind, kommunizieren hier auch schon recht offen. Ein Verschweigen ist geradezu schädlich.

Aber vermeldet etwa ein DAX-Konzern einen erfolgreichen Angriff, dann sinken auch die Aktienwerte. Doch auch hier gibt es ein langsames Umdenken. Alle werden angegriffen. Das ist kein Zeichen von Schwäche. Nur der, der nicht handelt, agiert fahrlässig. Und der, der behauptet, nicht angegriffen zu werden, merkt wahrscheinlich nur den Angriff nicht.

→ **Trifft das auch für Phoenix Contact zu?**

Natürlich. Wenn wir mit unserer Bedeutung am Markt NICHT zum Zwecke der Industriespionage von bestimmten Staaten aus Südostasien heraus angegriffen werden, dann hätten wir etwas falsch gemacht. Auch wir bilden uns im täglichen Abwehrkampf immer weiter, trainieren also sowohl für uns selber als auch für unsere Kunden. ■

phoenixcontact.de/services



„Angegriffen werden ist kein schlechter Job. Nicht abzuwehren ist ein schlechter Job.“

Dr. Lutz Jänicke

IRMA passt auf

Big Brother is watching you. Das ist umso besser, wenn es tatsächlich ein Mitglied der eigenen Familie ist und kein unbekannter Eindringling. Die Stadtwerke von Bad Pyrmont setzen daher eher auf eine „grosse Schwester“, nämlich auf IRMA.

Mittels der beiden Pumpen wird ein Hochwasserbehälter versorgt





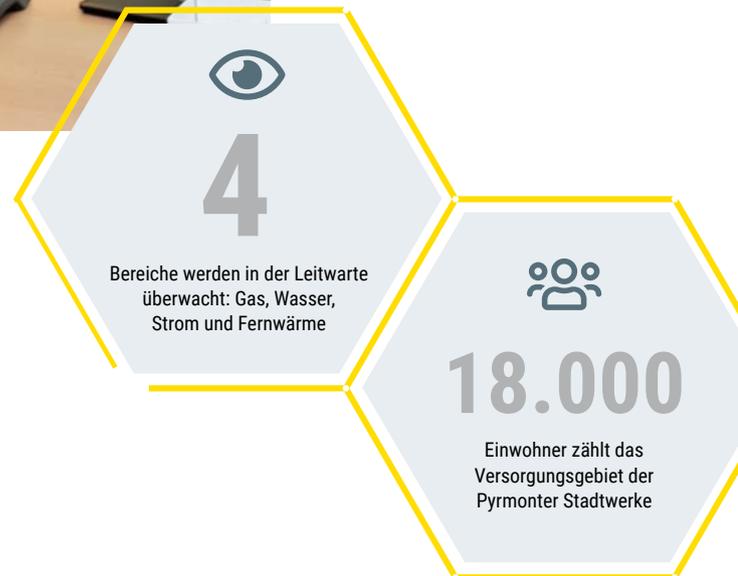
Thorsten Hamann hat in der Leitwarte die Versorgung „seines“ Bad Pyrmonts stets im Blick

An Frank Jakob und Thorsten Hamann kommt man nur heran, wenn die Herren es wollen. Denn ihr Reich ist durch eine Sicherheitstür vom Rest der Stadtwerke Bad Pyrmont abgetrennt. Was seinen guten Grund hat, denn die beiden arbeiten in der Leittechnik der Stadtwerke. Hier laufen Informationen über die Versorgungsleitungen von Strom, Wasser, Abwasser und Gas zusammen, werden kontrolliert und bei Bedarf Reparatur- oder Servicearbeiten angestoßen. Kein Bereich, in dem Besucher unkontrolliert ein- und ausgehen sollten. „Schon das gehört zur ersten Stufe unseres Sicherheitskonzepts.“

Kurort mit Tradition

„Wir überwachen in dieser Leitwarte die Versorgung von rund 18.000 Einwohnern in unserem Stadtgebiet“, berichtet Frank Jakob, der Abteilungsleiter der Leittechnik ist. „Neben dem Strom-, Wasser- und Gasnetz überwachen wir auch die Versorgung von Grosskunden mit Fernwärme. Dazu zählen u. a. das hiesige Staatsbad mit dem Steigenberger Hotel, das Konzerthaus und die Wandelhalle.“ Bad Pyrmont ist ein traditionsreicher Kurort mit zahlreichen öffentlichen Einrichtungen und reichlich Historie.

„Die Sensorik, mit der wir die Versorgung überwachen, ist fast komplett per Kupferkabel angeschlossen“, erläutert Thorsten Hamann. „Natürlich setzen auch wir auf immer mehr



Digitalisierung unserer Systeme, um schneller und zuverlässiger zu agieren. Dabei installieren wir nicht nur, sondern bauen z. B. unsere Schaltschränke selber auf und programmieren auch unsere Steuerungen, die vor Ort die Fernwartung realisieren, selber.“ Der Techniker ist nicht nur versiert, wenn es um die zahlreichen Spezialfälle geht, die der Themenmix von Gas, Wasser und Strom mit sich bringt. Hamann ist auch zuständig für die Überwachung der Überwachung, nämlich für IRMA. „Als Energieversorger unterliegen wir den Auflagen zur sogenannten kritischen Infrastruktur. Der Gesetzgeber verlangt von uns besonders strenge Massnahmen zum Schutz und zur Absicherung der Systeme.“

Diese Massnahmen werden fortlaufend durch Experten überwacht, die bei den Stadtwerken Bad Pyrmont bei regel-





Die teils historische
Infrastruktur täuscht:
Die Technik ist auf
neuestem Stand

Bild unten:
Frank Jakob ist
Chef der Leittechnik
und zeigt hier den
„Wohnort“ von IRMA

„Man merkt uns nur, wenn
etwas passiert und danach
nichts mehr klappt.“

Thorsten Hamann,
Stadtwerke Bad Pyrmont



mässigen Besuchen die Anlagen und ihre Strukturen genau analysieren. Diese Besuche werden Audits genannt. Besteht ein Versorger dieses Audit, erhält er die erforderliche Zertifizierung nach DIN 27001 für den weiteren Betrieb. „Beim letzten Audit wurde festgestellt, dass unsere zentrale Firewall den Anforderungen an die Cyber-Sicherheit nicht mehr genügt“, berichtet Frank Jakob.

Überwachung im Hintergrund

„Es wurde also dringend Zeit, sich dem Thema intensiv zu widmen. Und zwar so, dass wir in Zukunft auch hier selber administrierend tätig sein können. Und da sind wir auf IRMA aufmerksam geworden.“ Was versteckt sich hinter der russisch klingenden Abkürzung? Hauke Kästing, einer der Experten von Phoenix Contact für den Bereich Security, erklärt: „IRMA steht für Industrie Risiko Management Automation und basiert auf einer gehärteten Linux-Anwendung, die auf einem Industrie-PC von Phoenix Contact installiert ist. Das System arbeitet im Hintergrund und überwacht selbstständig sämtliche Teilnehmer und Kommunikationsverbindungen.“

Dabei wird nicht der Inhalt der Kommunikation überwacht, sondern der Datenverkehr. Ständig sausen im Netzwerk der Stadtwerke Pymont Daten hin und her, übertragen Steuerungen Messwerte, melden etwa Smart Meter Stromverbräuche, senden Sensoren Wasserstände. Diese Datenkommunikation wird zunächst von IRMA erfasst und „gelernt“. „Das ist für uns die eigentliche Arbeit“, schildert Thorsten Hamann. „Wir müssen IRMA die einzelnen Kommunikationspartner „beibringen“, sie quasi anmelden.“ Sobald IRMA schlau genug ist, weiss das System, welche Aktivitäten normal sind. Und vor allem merkt sie, wenn Anomalien auftauchen. Wenn etwa eine Steuerung anfängt, nicht nur mit der Leitwarte zu kommunizieren, sondern mit anderen Steuerungen im Netzwerk. Oder ein Netzwerk-Teilnehmer eine Verbindung ins Internet aufbaut, die nicht zu seinen Aufgaben gehört. „Dann schlägt IRMA Alarm und macht uns auf eventuelle Störungen aufmerksam. Aber IRMA bleibt stets im Hintergrund, ist ein reines Monitoring-System und hat damit auch keine Rückwirkungen in unsere aktiven Systeme.“

Wir lernen unser Netzwerk kennen

Für Frank Jakob und seine Kollegen ist dies einer der wesentlichen Vorteile des Systems. Dazu kommt aber noch ein sehr erfreulicher Nebeneffekt, wie Thorsten Hamann schildert: „Mit IRMA haben wir unser eigenes Netz noch einmal ganz neu kennengelernt. Erst IRMA hat uns gezeigt, wer eigentlich mit wem kommuniziert. Und aus diesem Wissen zaubert uns IRMA einen stets aktuellen Netzwerkplan, der für die nächste Zertifizierungsrunde wichtig ist. Auf Knopfdruck.“ (lo) ■

stadtwerke-bad-pymont.de

Bild Mitte:
Haben alles im Blick
und alarmieren bei
Bedarf die Techniker:
Thorsten Hamann
und Frank Jakob

Diese Pumpe ist
wirklich noch in Betrieb.
Und fernüberwacht!



Cyber-Attacken

Stadtwerke im Visier

Oktober	2018 mehr als
2019	150
Attake Stadtwerke Langenfeld	Cyber-Attacken auf kritische Infrastruktur gemeldet
September	Bis
2019	2032
Attake Stadtwerke Stuttgart	mehr als 40 Mio. Smart Meter Gateways in Deutschland verbaut



mGuard

Guard variants



CYBER SECURITY



Die beiden verstehen
beim Thema Daten-
sicherheit keinen Spass:
Martin Dickopp
und Kilian Golm

Die Daten- Bodyguards

Wenn es ernst wird mit der Datensicherheit, dann schlägt ihre grosse Stunde. Die Phoenix Contact Cyber Security in Berlin geht mit jedem Hacker in den Nahkampf. Ein Besuch bei den Datenwächtern in der Hauptstadt.

Sie waren ein Start-up. Jung, frech, erfolgreich. Und irgendwie sind sie immer noch ein Start-up. Wenn auch als Teil der Phoenix Contact-Gruppe. Die Cyber Security Berlin hat sich ihre Eigenständigkeit bewahrt. Das merkt man sofort, wenn man in Berlin-Adlershof an ihre Pforte klopft. Oder besser klingelt. Moderne Fassade, cooler Empfang. Und dann ist erst mal Schluss. Wer hier weiter will, der bekommt Begleitung.

Denn lässig ist man in der Richard-Willstätter-Strasse nicht. Wenn es um Datensicherheit und Cyber-Kriminalität geht, dann besteht dazu auch kein Anlass. „Wir verfolgen die jeweils neuesten Cyber-Attacken natürlich genau“, verrät Kilian Golm im Gespräch. Jüngstes Opfer ist ein Unternehmen, welches selber im Bereich Datensicherheit aktiv ist. „Aber da gibt es keine Schadenfreude“, betont der Geschäftsführer der Berliner Phoenix Contact-Tochter. „Der Vorgang zeigt uns deutlich, wie stark die Bedrohung durch Cyber-Kriminalität mittlerweile angestiegen ist.“

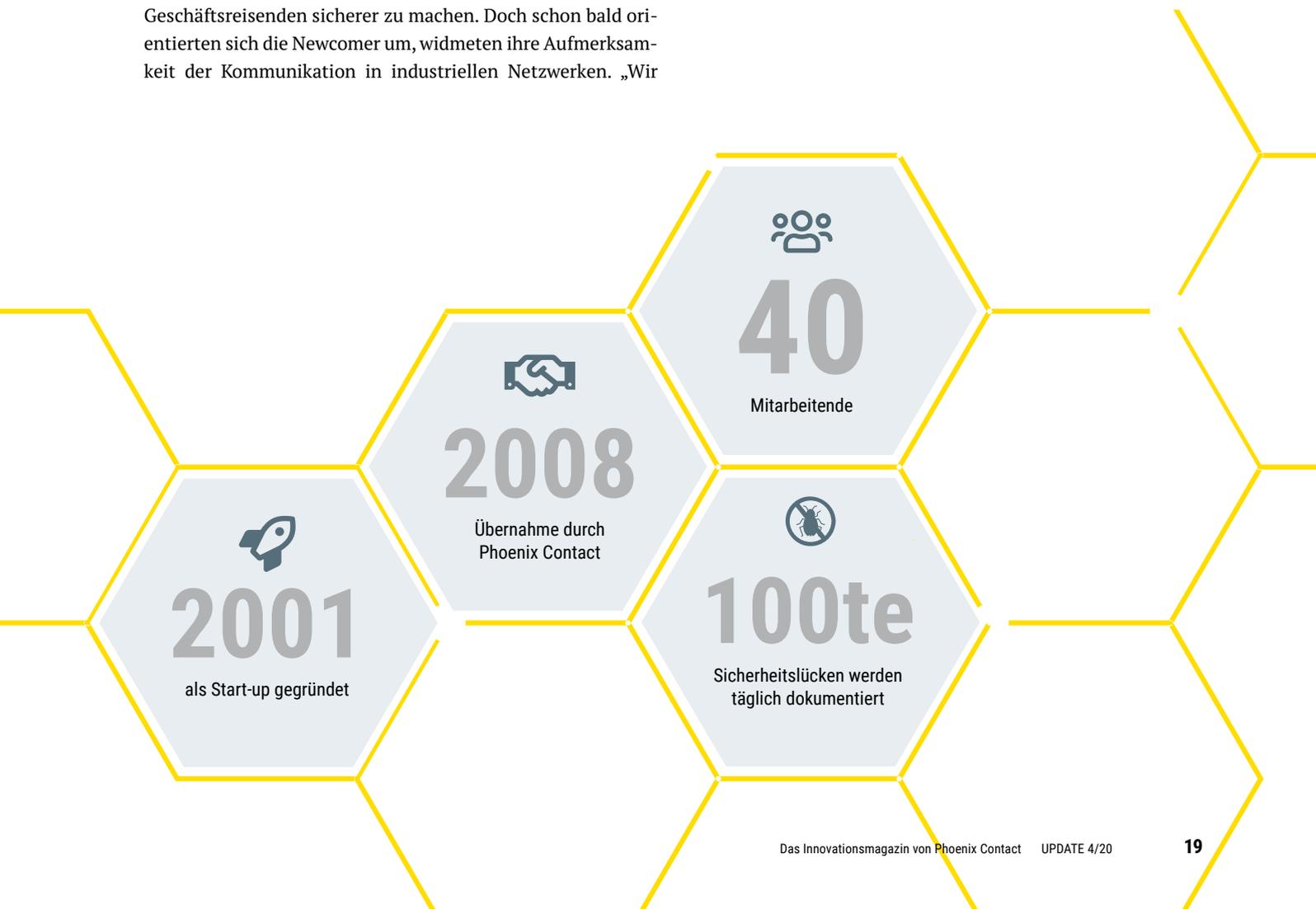
Mit m zum Durchbruch

Begonnen haben die Berliner im Jahre 2001 als ein typisches Start-up mit vier Mitarbeitern, von Beginn an am Innovationsstandort Adlershof. Anfangs mit der Idee, Daten von Geschäftsreisenden sicherer zu machen. Doch schon bald orientierten sich die Newcomer um, widmeten ihre Aufmerksamkeit der Kommunikation in industriellen Netzwerken. „Wir

haben industrielle Security entwickelt, als die noch niemand auf dem Schirm hatte“, schildert Geschäftsführer Kilian Golm. „Das hat uns Kundenbeziehungen beschert, die teils noch bis heute halten. Vertrauen ist im Sicherheitsgeschäft ein existenzieller Faktor.“

Einer, der fast von Beginn an dabei war, ist Martin Dickopp: „Eine Basis unseres Erfolgs war die Entwicklung der mGuard-Produkte und -Lösungen“, schildert der Security-Experte. „Diese Hardware- und Software-Komponenten sind quasi eine mobile Firewall. Daher auch das m für mobil. Die allerdings nicht in Systeme eingreifen und eine aktive Rolle spielen, sondern quasi als unsichtbares Device im Hintergrund über die Sicherheit wachen, also stets im Stealth Mode agieren.“

Die Idee wurde eine Erfolgsgeschichte, die Technologie zum Patent angemeldet und der ehemalige Kunde Phoenix Contact übernahm 2008 das Start-up. 2016 wurde das Berliner Unternehmen dann in Phoenix Contact Cyber Security umbenannt. Heute zählt die Phoenix Contact-Tochter gut 40 Mitarbeitende. Am Berliner Standort wird Sicherheits-Software entwickelt und verbessert sowie bei der Kundenberatung an



Arbeiten am Ring

Jede Software hat Sicherheitslücken. Das lässt sich bei der Komplexität heutiger Systeme nicht mehr verhindern. Entscheidend ist, dass diese Lücken beim Bekanntwerden möglichst schnell wieder verschlossen werden. Hier arbeitet das eigene „Product Security Incident Response Team“, kurz PSIRT, exklusiv für die Produkte der mGuard-Familie. Diese schnelle Eingreiftruppe sichtet und analysiert täglich mögliche Sicherheitslücken. Und wer glaubt, dass dabei Langeweile aufkommt: Pro Tag werden hunderte Sicherheitslücken bekannt und dokumentiert!

Nachdem gefiltert wurde, welche Meldungen die eigenen Produkte betreffen, analysieren die Experten teils bis auf Quellcodeebene, welche Auswirkungen die Lücke haben kann. Wird die Meldung als starke Bedrohung erkannt, dann wird mit höchster Priorität und mit allen Kräften an der sofortigen Behebung der Lücke gearbeitet. Ist die Bedrohung dagegen nicht zeitkritisch, ist also quasi nur eine der vielen Sicherheitsmauern gefallen, dann wird beim nächsten regulären Update ein Sicherheitspatch aufgespielt, der diese Lücke wieder schliesst. „Diese Arbeit im Hintergrund macht die eigentliche Qualität in unserem Sicherheitsmanagement aus“, beschreibt Martin Dickopp. „Die Netzwerke unserer Kunden bleiben sicher, ohne dass sie sich kümmern müssen, denn wir arbeiten ja diskret im Hintergrund.“ Cyber-Kämpfer im Verborgenen ...

**Wettrüsten**

Wer Daten schützen will, muss international denken. Nach Land, Luft, See und Weltraum wird nun der Cyber Space zum Battleground



ganzheitlichen Lösungen inklusive Trainings gearbeitet, während die mGuard-Hardware in Bad Pyrmont montiert wird.

„Cyber Security sollte nicht am Ende einer Entwicklung, sondern an ihrem Anfang stehen.“

Kilian Golm

Jeder ist verwundbar

Die „mGuard“ Netzwerksicherheitsgeräte besitzen Funktionalitäten, die Router, Firewall, VPN (Virtual Private Network), QoS (Quality-of-Service) und Angriffserkennung (Intrusion Detection) unterstützen. Ergänzt wird der Leistungsumfang durch eine hoch skalierbare Device-Management-Software. „mGuard hat mehr als 1000 Konfigurationsmöglichkeiten, ist daher eines der komplexesten Produkte im gesamten Portfolio von Phoenix Contact“, erklärt Martin Dickopp selbstbewusst.

„Einen absoluten Schutz“, so führt Dickopp aus, „gibt es trotzdem nicht. Jeder ist verwundbar. Wir versuchen, das Niveau des Eindringens aber so hoch zu machen, dass der Aufwand für einen Angreifer zu gross wird.“

Dabei unterscheiden die Cyber Bodyguards grundsätzlich zwischen zwei Angriffsarten. Die einen sind ungezielt, verbreiten sich ungerichtet und attackieren jedes Netzwerk, auf

das sie treffen. Die anderen sind gezielte Cyber-Attacken. Die werden entweder durch private Hacker inszeniert, die sich mit sportlichem Ehrgeiz auf Firewalls und Sicherheitskonzepte stürzen, um die eigene Finesse zu demonstrieren. Oder es stecken organisierte Gruppen mit kriminellen Absichten bis hin zu staatlichen Akteuren dahinter. „In unseren Bedrohungsanalysen, die wir für unsere Kunden erstellen, betrachten wir Angreifer mit unterschiedlichen Ressourcen“, beschreibt Kilian Golm das Dienstleistungskonzept von Cyber Security, dass sich in das umfassende Security-Dienstleistungsportfolio der Unternehmensgruppe eingliedert.



Die bekanntesten

Cyber Attacken

Die Liste von Security-Zwischenfällen in der Industrie wird immer länger.

Eines der bekanntesten war die

Stuxnet

Attacke 2010, die speziell SCADA-Systeme befallen hatte.

Der Virus

Industroyer

hat 2016 für Aufsehen gesorgt, ein Jahr später stürzte sich

Triton

speziell auf Sicherheitssteuerungen.

WannaCry

war eine Erpresser-Software, die 2017 über 230.000 Systeme befallen hatte.

URGENT/11

ist eine im Sommer 2019 bekanntgewordene Sicherheitslücke, die über 2 Milliarden industrielle Geräte weltweit betrifft. Und vor der Kunden sich mit Hilfe der mGuard-Produktfamilie schützen können.



mGuard

Die Hardware wird am Standort Bad Pymont montiert

Recherche im Zwielficht

Wer richtig kämpfen will, muss seine Gegner kennen. Gehen also in der Richard-Willstätter-Strasse Gangster und Schlapphüte ein und aus? Martin Dickopp muss schmunzeln: „Nein, so dramatisch läuft das nicht ab. Aber es ist richtig, wir besuchen auch Hacker-Konferenzen, recherchieren in schwieriger zugänglichen Bereichen des Internet und tauschen uns in Foren und Communities aus.“ Wer will, lässt die Berliner Experten auch mal einen Scheinangriff auf das vermeintlich sichere Firmennetzwerk durchführen. „Finde die Lücke“ ist hier das Motto.

Wer braucht den Schutz der professionellen Daten-Sicherer? „Eigentlich jeder Betrieb. Unsere Kunden reichen vom kleinen Maschinenbauer im Familienbetrieb bis hin zur Grossindustrie weltweit. Und natürlich auch das eigene Unternehmen. Cyber-Kriminalität kennt keine Grenzen.“ Dabei betont Kilian Golm: „Cyber-Sicherheit ist ein steter Prozess, kein einmaliger Vorgang. Man muss Sicherheit als System denken – Security by Design. Heutige Betriebe und Technologien sollten Security sowohl in ihren Produkten als auch in ihren Produktionsanlagen von Beginn an mitberücksichtigen und nicht als letzten Sicherheitsgurt am Ende der Entstehung begreifen und dem System aufpfropfen.“ (lo) ■

phoenixcontact.com

EISERKENNUNG



Pflaster für die Flügel



Ein wirklich lauschiges Plätzchen hat sich die Blattlaus da ausgesucht. In mehr als 100 Metern Höhe, über dem schwäbischen Wald, im Schein der Abendsonne. Die Aufgabe des professionellen Industriekletterers: die Montage eines innovativen Eiserkennungssystems. Das soll alle schützen, die unten bleiben müssen.

Blattläuse – so nennen sich die Kletterer selber, die sich in die luftigen Höhen von Windkraftanlagen wagen. Und die Anlage hier im schwäbischen Lauterstein ist eines der grössten Exemplare, die onshore aufgestellt werden: 140 Meter Nabenhöhe. Doch Höhenangst kennen Industriekletterer natürlich nicht. Und so lässt sich auch Tommy Liebmann nicht von seiner luftigen Lage in mehr als 100 Metern Höhe erschüttern. Seelenruhig raut er die Oberfläche des Rotorblatts auf und klebt mit gekonnten Handgriffen ein ganz besonderes Pflaster auf.

„Es geht darum, dem Windrad ein neues Gespür zu verschaffen“, erklärt Karl-Heinz Meiners. Der Projektmanager von Phoenix Contact steht am Fuss des imposanten Bauwerks und ergänzt: „Nämlich dem Erkennen von Eis an der Oberfläche. Ziel ist es, eine bestehende Windkraftanlage mit einem Eisdetektionssystem nachzurüsten, das wirklich das Entstehen und die Dicke von Eis messen kann.“

Ein unerwartet laues Lüftchen sorgt dafür, dass das Sensorpflaster noch so spät im Jahr montiert werden kann. Den Standort auf der schwäbischen Alb wählte der Projektpartner

und Betriebsführer, die Firma wpd windmanager, aus. Hier ist bereits ein alternatives System im Einsatz. Ziel ist es, noch genauere Ergebnisse über die Eisbildung zu erhalten.

Unerwünschte Eismaschine

Eis ist für Windkraftanlagen ein echter Spassverderber. In kalten Regionen, bei kühler Witterung oder in Höhenlagen kann sich nämlich an den Blättern der Anlagen Feuchtigkeit niederschlagen und zu Eis gefrieren. Aus einzelnen Kristallen werden dabei Eisschichten. Die können schnell zentimeterdick werden.

Problem: Das geschieht nicht gleichmässig. Aus einem aerodynamisch geformten glatten Rotorblatt wird eine runzelige Eislandschaft. Die bremst den Schwung und damit den Ertrag an Windenergie. Und zwar drastisch.

Ausserdem verändert sich das fein austarierte System durch Unwuchten. Alle sich drehenden Einheiten werden einer deutlich höheren Last ausgesetzt, die Lebensdauer der Anlage reduziert sich so drastisch. Teure Schäden an der Anlage drohen.

Und wenn es zu Tauwetter kommt oder die elastischen Flügel durch die ungleichmässige Last in unerwünschte Schwingungen geraten, können kiloschwere Eisplatten ihren Halt verlieren und in Drehrichtung abgeworfen werden. An den

Lukas Christ und Karl-Heinz Meiners mit einem der insgesamt 24 Sensorpflaster, die ihre Signale an die Steuerungselektronik senden





Durch das Blade-Intelligence-System wird Eiswurf verhindert und die Verfügbarkeit erhöht



Safety first: Die Industriekletterer erklimmen den Windturm von aussen. Die Arbeiten am Schaltschrank in der Gondel führen dann die Experten von Phoenix Contact durch

„Wir wissen,
dass Eis vorhanden ist.
Andere vermuten nur,
dass es sich gebildet hat.“

Karl-Heinz Meiners,
Senior Project Manager Phoenix Contact

Türmen in Lauterstein ist zwar bereits ein Eiserkennungssystem im Einsatz, es muss also niemand den Kopf einziehen. Warnschilder stehen aber auch in diesem schwäbischen Windpark und warnen vor Eiswurf.

Dem Kristall auf der Spur

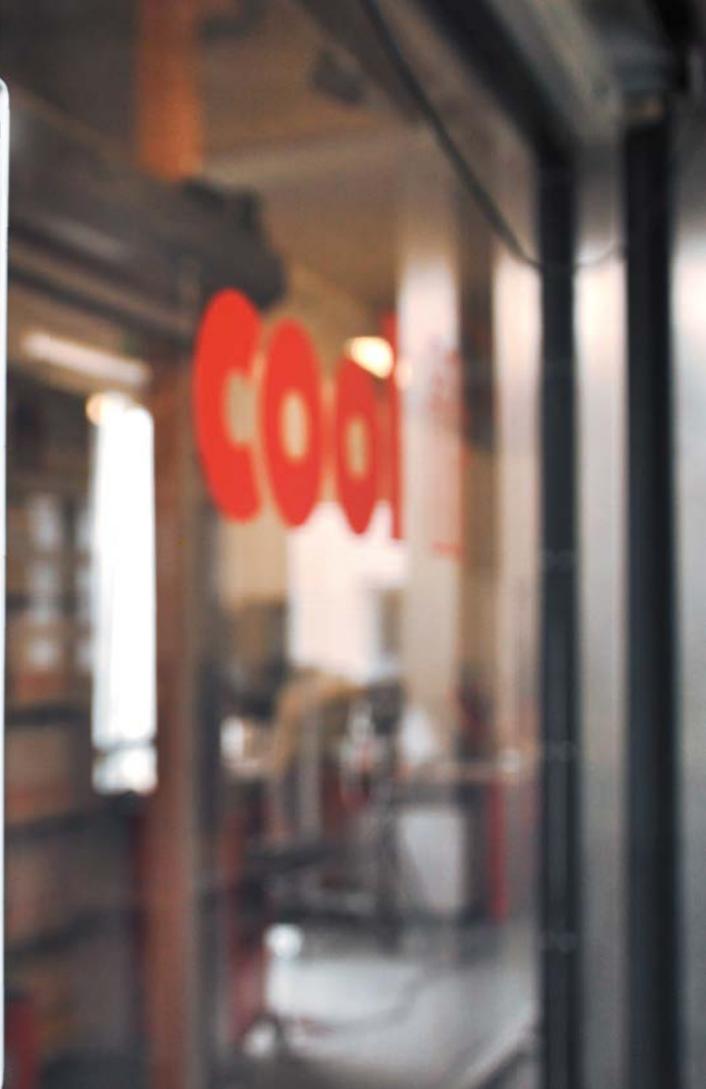
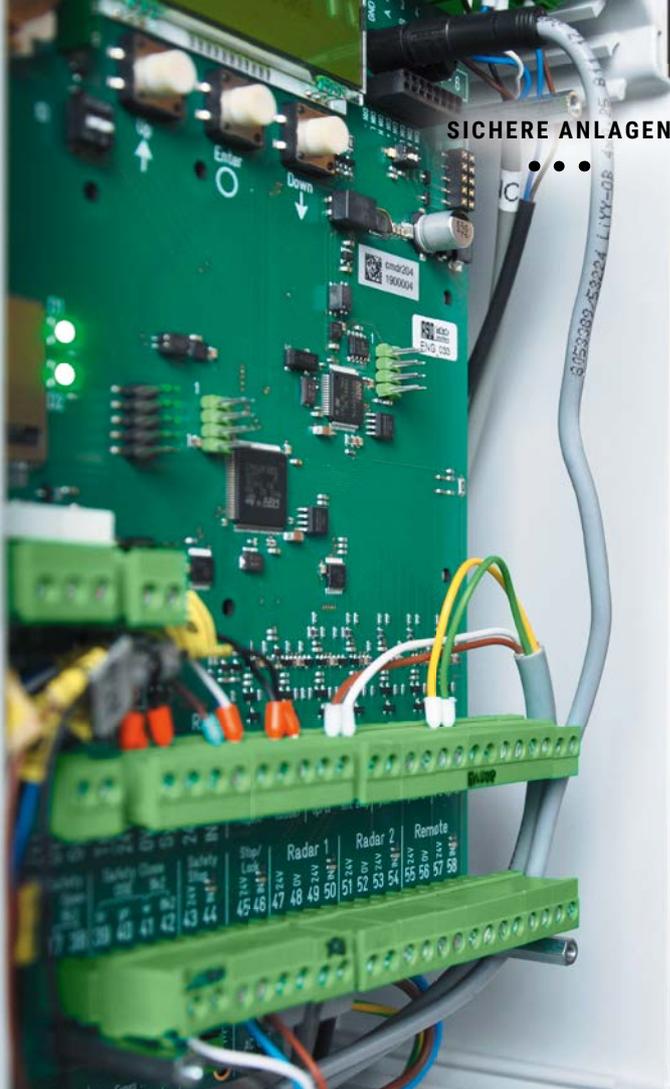
Abhilfe schafft nur der Stillstand der Anlage. Oder eine Heizung. „Die ist aber sehr teuer, da enorm aufwendig in Herstellung oder Nachrüstung“, erklärt Experte Meiners. „Das lohnt sich nur, wenn die Anlagen in wirklich dauerhaft kalten Umgebungen stehen.“ Der gelernte Industrieelektroniker und studierte Feinwerk- und Medizintechniker weiss, wovon er spricht, denn seit zehn Jahren ist er ein weltbummelnder Teil des Windteams von Phoenix Contact und war schon überall auf Windkraftanlagen im Einsatz. „Das Innovative an unserem System, das wir Blade Intelligence nennen, ist

die tatsächliche Messung von Eis und seiner Dicke. Das kann nämlich kein anderes am Markt befindliches System.“ Ein derartiges Eiserkennungssystem ist auch bereits im ausgewählten Windpark des Projektpartners wpd windmanager im Einsatz. Parallel dazu wird nun die Blade Intelligence getestet. wpd windmanager erhofft sich von der neuen Sensorik noch genauere Ergebnisse.

Der Marathon-Sensor

Das unterarmgrosse Pflaster, das die Blattläuse auf die Oberfläche der Windflügel kleben, erkennt dagegen mittels induktiver Messung einen tatsächlichen Eisbefall und auch seine Dicke. Ausserdem misst es die Temperatur. „Diese Daten werden dann an den Schaltschrank in der Gondel gefunkt und dort von einer Steuerung ausgewertet“, erklärt Karl-Heinz Meiners. „Und da so die tatsächliche Eisbildung festgestellt wird, kann die Anlage auch automatisch wieder anfahren, wenn keine Eisbildung mehr droht.“ Der aufwendige Einsatz von Serviceteams wird deutlich verringert, die Verfügbarkeit der Anlage drastisch erhöht.

In der flachen Apparatur verstecken sich aber nicht nur induktive Sensoren und Temperaturfühler, sondern auch ein kleines Solarpanel, eine Antenne und eine Batterie. „Das System ist viele Jahre wartungsfrei aktiv“, beantwortet Meiners die Frage nach der Dauerhaftigkeit des Einsatzes. Kein Wunder, dass sich die freischaffende Blattlaus in 100 Metern Höhe besondere Mühe gibt, die Hightech-Pflaster penibel sauber zu verkleben. (10) ■

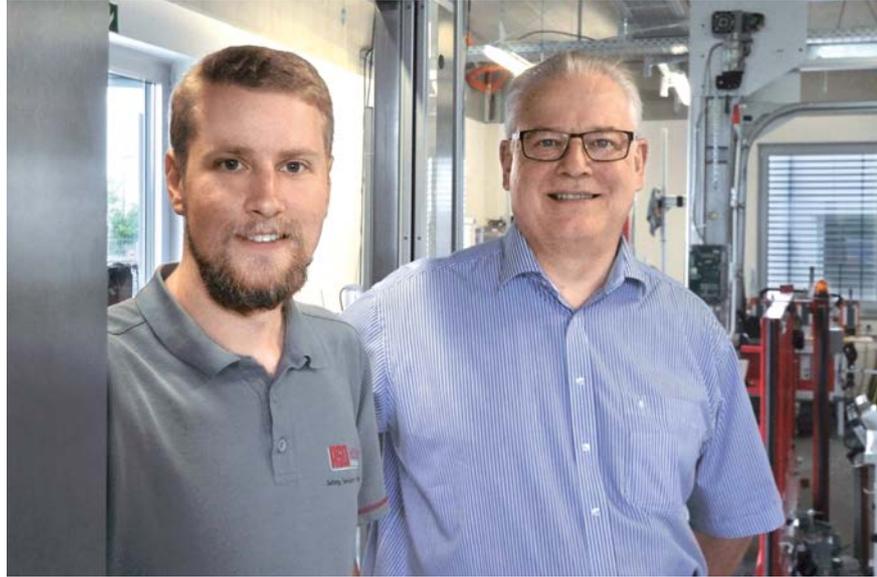


Sensible Türsteher

Je sensibler der Türsteher, desto angenehmer der Eintritt. Warum das nicht nur für den Einlass in begehrte Locations geht, zeigt ein Besuch im westfälischen Lippstadt. Dort residiert die ASO Safety Solutions GmbH. Und die wissen, wie man mechanischen Eintrittsregulierern die richtigen Manieren beibringt.



Die SKEDD-Anschlusstechnik ermöglicht lötfreie Anschlüsse



Norbert Pewny und Dennis Mettner betreuen die neue Torsteuerung

Schliessen gehört zu ihrem Job, doch Projektmanager Norbert Pewny und Hardware-Entwickler Dennis Mettner sind gar nicht verschlossen, wenn es um das neueste Produkt aus ihren Reihen geht: „Mit der Drico 2.0 haben wir eine Flexibilität erreicht, die so am Markt noch nicht existiert“, fasst Pewny die Vorzüge der neuen Torsteuerung zusammen.“ Die beiden Experten arbeiten bei der Firma ASO Safety Solutions in Lippstadt. Das Unternehmen ist einer der führenden Entwickler, Hersteller und Distributoren von Sicherheitslösungen rund um Türen, Tore und Maschinenbau. Rund 170 Beschäftigte arbeiten hier und an Standorten in den USA und China an Lösungen für die Fördertechnik, die Hub- und Steigtechnik, die Flurförderzeugtechnik und den Bereich Safety, Sensors & Controls.

Das Tor ist eine Maschine

In letzterem Bereich stellt ASO drei grosse Produktgruppen her, die dafür sorgen, dass bewegliche Tür- und Torelemente nicht ausser Rand und Band geraten: Sicherheitskontaktleisten, Sicherheitskontaktpuffer und Sicherheitskontaktmatten. Allen gemein ist eine Steuerungseinheit, die die Daten der Sensorik erfasst und erforderliche Befehle an die Anlagen- oder Fahrzeugsteuerung weiterleitet.

Hört sich simpel an, ist aber im Detail gespickt mit technologischen Herausforderungen. Denn wichtig ist vor allem eine zuverlässige und möglichst schnelle Signalerfassung und -bearbeitung. Wer will schon, dass sich ein schnellaufendes Rolltor beim Schliessen in eine Guillotine verwandelt? Dennis Mettner zeigt, worauf es bei den hier eingesetzten Sicherheits-

„Wir betrachten ein Tor wie eine Maschine. Mit den gleichen strengen Sicherheitsvorschriften.“

Norbert Pewny,
Hardware-Entwickler ASO Safety

kontaktleisten an der Unterkante der Tore ankommt: „In den flexiblen Gummielementen sind Kontaktleisten angebracht. Berühren die sich, etwa wenn das Tor auf einen Widerstand trifft, dann schaltet die Anlagensteuerung blitzschnell den Vortrieb ab, der Motor stoppt und das Tor hält an.“ Projektmanager und Elektroingenieur Norbert Pewny ergänzt: „Wir betrachten ein Tor wie eine Maschine. Und daher gelten hier die gleichen strengen Sicherheitsvorschriften.“

Maschinenstopper

Damit kennt sich ASO bestens aus, denn ihre Kontaktmatten und Bumper sorgen dafür, dass auch im Betrieb befindliche Maschinen die richtigen Manieren an den Tag legen, wenn sie mit ihrem menschlichen Bedienpersonal auf Tuchfühlung gehen. Anschaulich wird dies etwa bei den Kontaktpuffern, →



Dennis Mettner
ist Entwickler
bei ASO Safety

den Bumpnern, die z. B. an den beweglichen Portalen grosser CNC-Fräsen befestigt sind. Diese Portale sind auf einem Maschinentisch gelagert, auf dem das Werkstück, etwa eine Holzplatte, fixiert ist. Am auf Schienen fahrenden Portal sind die Werkzeuge zur Bearbeitung angebracht. Gesteuert durch ein Bearbeitungsprogramm verfährt das Portal so, dass die beweglichen Werkzeuge, etwa Bohrer oder Fräsen, auf der Platte an den richtigen Stellen aktiv werden können.

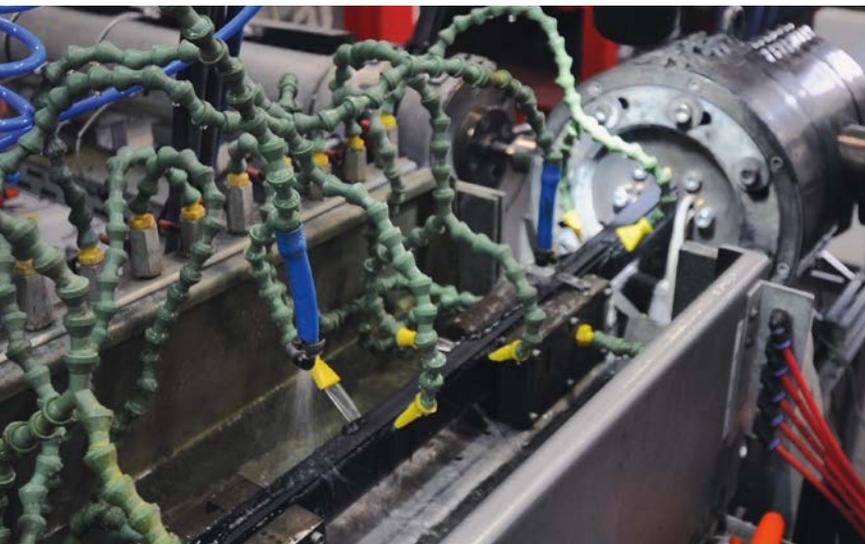
Wenn jetzt ein Bediener dem schweren Portal in die Quere gerät, drohen Unfälle. Grossflächige Absperrungen würden aber dem Platzbedarf einer Produktion oder Werkstatt im Weg stehen. Durch den Einsatz von Bumpnern reagiert die Steuerung aber blitzschnell auf ungeplanten Kontakt und hält die schwere Maschine an.

Heimische Fertigung

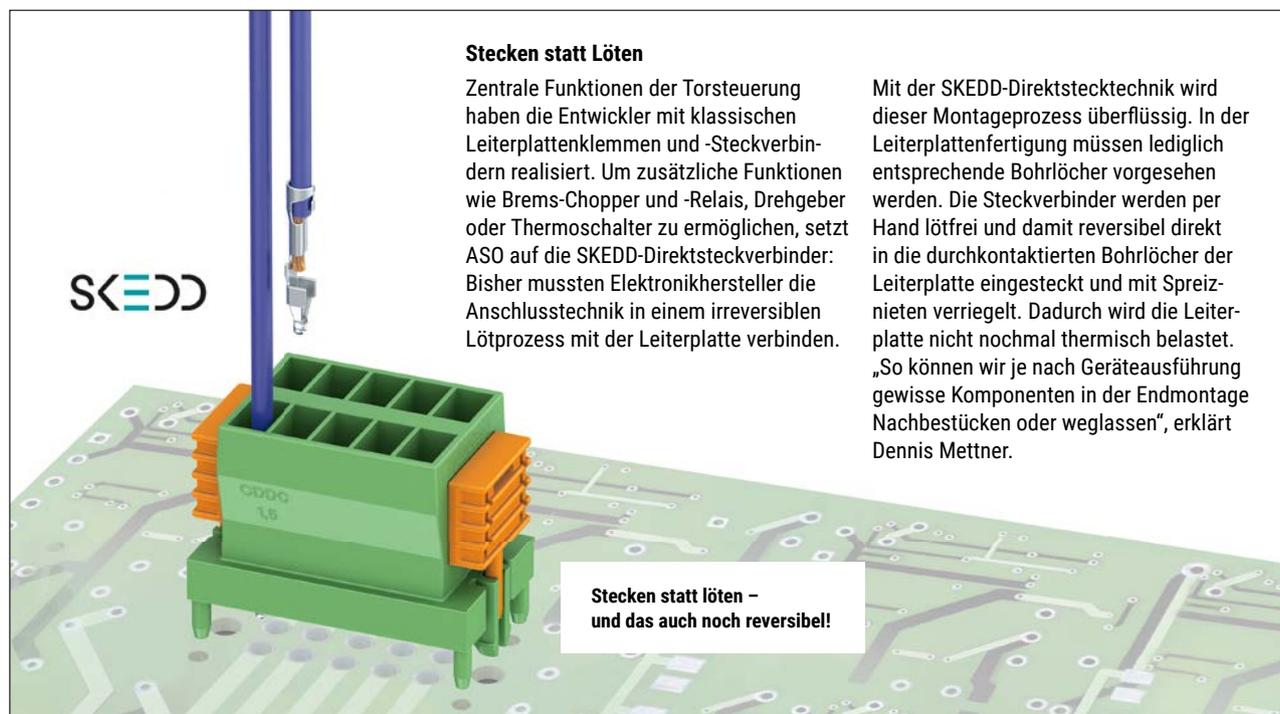
Beim Gang durch die Produktion überrascht, dass ASO den Grossteil der Elemente selber herstellt. Lange Förderstrecken ziehen sich durch die Fertigung, auch die Gummielemente werden hier produziert und in ihrer Entstehung genau kontrolliert.

„Unsere Fertigungstiefe ist eines unserer Argumente beim Kunden“, berichtet Mettner. „Gerade dadurch wird es uns

Hochwertige Profilverfertigung
im heimischen Lippstadt



Berühren sich die
Kontaktleisten, wird
blitzschnell geschaltet



Stecken statt Löten

Zentrale Funktionen der Torsteuerung haben die Entwickler mit klassischen Leiterplattenklemmen und -Steckverbindern realisiert. Um zusätzliche Funktionen wie Brems-Chopper und -Relais, Drehgeber oder Thermo-Schalter zu ermöglichen, setzt ASO auf die SKEDD-Direktsteckverbinder: Bisher mussten Elektronikhersteller die Anschlusstechnik in einem irreversiblen Lötprozess mit der Leiterplatte verbinden.

Mit der SKEDD-Direktstecktechnik wird dieser Montageprozess überflüssig. In der Leiterplattenfertigung müssen lediglich entsprechende Bohrlöcher vorgesehen werden. Die Steckverbinder werden per Hand lötfrei und damit reversibel direkt in die durchkontaktierten Bohrlöcher der Leiterplatte eingesteckt und mit Spreiznieten verriegelt. Dadurch wird die Leiterplatte nicht nochmal thermisch belastet. „So können wir je nach Geräteausführung gewisse Komponenten in der Endmontage Nachbestücken oder weglassen“, erklärt Dennis Mettner.

Stecken statt löten -
und das auch noch reversibel!

480



Varianten der Torsteuerung
sind mit den SKEDD-
Direktverbindern möglich.

möglich, auf jeden Kundenwunsch individuell einzugehen. Unsere Kunden kommen vor allem aus der Industrie und dem produzierenden Gewerbe, da sind Sonderanfertigungen ganz alltäglich.“

Genau um diese Flexibilität geht es auch beim Austausch der beiden Fachleute mit den Phoenix Contact-Experten. Die Torsteuerungen werden nämlich in unterschiedlichen Leistungsklassen mit entsprechend skalierten Funktionsausstattung angeboten. „Das obere Leistungsspektrum unseres Angebots bilden hochfrequent genutzte Tore, etwa mit mehreren Antrieben, Induktionsschleifen zur Steuerung beim Anfahren von Förderfahrzeugen oder mit eigenem Ampelsystem“, schildert Pewny. „Je komplexer das Gesamtsystem ist, desto wichtiger werden sicherheitsgerechte Funktionen. Entsprechend muss die Funktionalität der Steuerung mitwachsen.“

Der Grundgedanke bei der Entwicklung der neuen Steuerung war eine möglichst transparente Hardware-Skalierung, dessen Nutzen unsere Kunden unmittelbar nachvollziehen können.“ Die jeweilige Hardware-Ausstattung führt – je nach Ausstattungsmerkmalen – zentrale Funktionen horizontal oder vertikal öffnender Tore aus. Dazu gehören die Ansteuerung von Frequenzumrichtern und Drehstrommotoren zum Öffnen und Schließen der Tore, Sicherheitsfunktionen wie Lichtschranken oder Totmannschalter sowie zusätzliche Features wie Thermo-Schalter, Funkempfänger, Weggeber oder LC-Displays. Und natürlich fällt in diesen Bereich auch die mögliche elektronische Zutrittskontrolle in zahlreichen Varianten.

Sensibel dank Modulumöglichkeit

Je mehr Sensorik einer Torsteuerung zur Verfügung steht, desto feinfühler reagiert sie auf Signale der Bediener. Beim Anschluss der antriebsrelevanten Funktionen nutzen Mettner und sein Entwicklerteam die SKEDD-Direktsteckverbinder von Phoenix Contact. Der modulare Baukasten umfasst insgesamt neun unterschiedliche Leiterplatten-Layouts, über die die Entwickler den Funktionsumfang ihrer Torsteuerung passgenau skalieren können. Möglich sind so hunderte von Kombinationen, die die automatisierten Türsteher aus Lippestadt immer genauer machen sollen. Je sensibler der Einlass, desto sicherer und komfortabler fühlen sich die Benutzer. (10) ■

asosafety.de



Wer hat's erfunden?

Mit dem kombinierten Schutz- und Feldsteuergerät KOMBISAVE haben die Entwickler der Schweizer Phoenix Contact-Tochter NSE einen Volltreffer gelandet. Auch wenn dieser tunlichst zu vermeiden ist, wenn es um die Stromnetze und ihre Sicherheit geht.

Fahren Sie einfach der 110-kV-Leitung bis zum Ende nach, Nummern gibt's da nicht.“ Schon bei der Wegbeschreibung war klar, dass der Besuch des Umspannwerks im niederrheinischen Kempen ein besonderer wird. Also Blick nach oben, die Hochspannungsleitung fest im Blick, langsam der Strasse nach.

Kempen ist eine 36.000 Einwohner zählende Stadt am Niederrhein. Schön gelegen, traditionsreiche Vergangenheit, prosperierende Gegenwart. Im Gewerbegebiet am Industriering Ost warten Reinhard Bretzke und Michael Kairies auf uns. Die beiden sind Angestellte der hiesigen Stadtwerke, zuständig für die Energieversorgung ihrer Heimatstadt. Und führen uns zunächst in die Zentrale ihres Schaffens – ihre Netzleitstelle.

Houston – wir sind gelandet

Ein wenig erinnert die Wand aus Monitoren an die berühmte NASA-Leitwarte der Raumfahrer in Cape Kennedy. Dabei geht es hier ganz irdisch zu. „Wir sind zuständig für die Energieversorgung unserer Stadt“, beschreibt Reinhard Bretzke knapp. Hört sich zunächst ganz bodenständig an, ist jedoch ein Job mit direkter Anbindung an die Zukunft. „Wir stellen gerade unsere Netze komplett um auf einen zentralen Betrieb mit digitaler Netzleittechnik.“ Also doch ein wenig NASA!

Die Energienetze zählen zur sogenannten kritischen Infrastruktur, unterliegen also besonders strengen Normen und Anforderungen an Sicherheit und Verlässlichkeit. Kein Wunder, denn ohne Strom läuft in der modernen Zivilisation nicht einmal mehr die Wasserversorgung. Bretzke ist ein alter Hase, wenn es um Energie geht. Seit gut 45 Jahren ist er dem Thema

treu, war lange im niedersächsischen Hildesheim für die Energieversorgung zuständig. Seit fünf Jahren ist er verantwortlich für die Stromversorgung in Kempen.

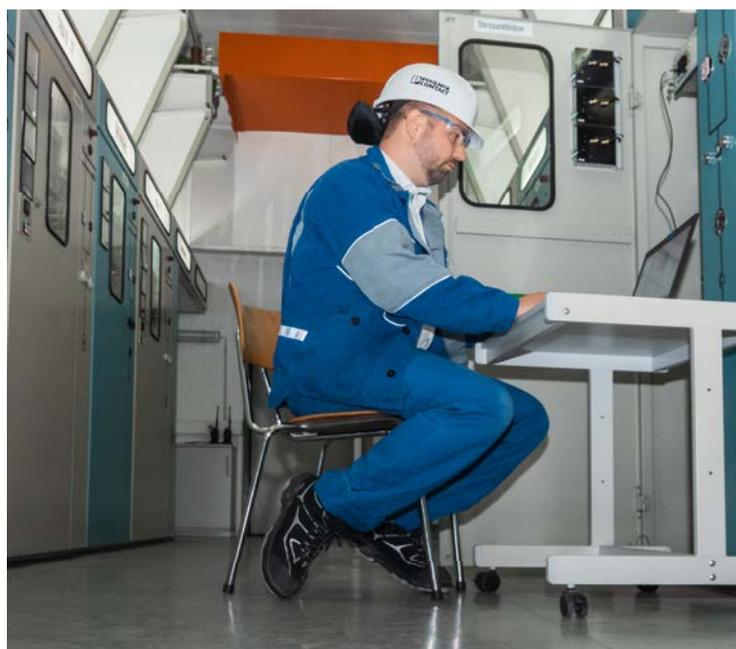
„Mich hat in der schönsten Stadt am Niederrhein die grüne Wiese für den Bereich Netz-Monitoring gereizt. Zusammen mit meinen zwölf Mitarbeitern kümmere ich mich hier um das Mittelspannungs- und Niederspannungsnetz sowie die zugehörige Kommunikationstechnik für das Netz-Monitoring. Die Aufgaben sind wirklich vielfältig, daher ist die Spannweite der Anforderungen auch extrem.“

Einer, der damit locker umgeht, ist Michael Kairies. Der 38-jährige Energieelektroniker ist u. a. zuständig für die Netz-



„Wir brauchen in Zukunft intelligente Energienetze.“

Reinhard Bretzke,
Leiter Energieversorgung Stadtwerke Kempen



„Wir haben keine Stunde gebraucht, um das Gerät in Betrieb zu nehmen.“

Das Schutzgerät lässt sich einfach parametrieren und in Betrieb nehmen



Vertrauen einander: Timo Beuth (Phoenix Contact) und Reinhard Bretzke (Stadtwerke Kempen)



In der Leitwarte haben die Energieversorger ihre Netze stets im Blick

leitstelle. Und damit ein Experte, wenn es um die Einbindung von Schutz- und Leittechnik ins Kempener System geht. Mit flinken Fingern ruft er die passende Darstellung auf einem der Monitore auf, zeigt die Verteilung des lokalen niederrheinischen Stromnetzes und sowohl die Einspeiser als auch die abnehmenden Grosskunden. Währenddessen erklärt Reinhard Bretzke, warum wir eigentlich hier sind.

Herausforderung Energiewende

„Auf unsere Energienetze kommen immer mehr Herausforderungen zu. Durch den Umbau der Energieversorgung hin zu Erneuerbaren Energien verändert sich die Einspeisung total. Jahrzehntelang haben wir mit konstanten Einspeisungen durch Grosskraftwerke gearbeitet. Jetzt kommen immer neue Energiequellen hinzu, die auch noch ungleichmässig einspeisen und dezentral verteilt sind. Gleichzeitig brauchen wir aber auf der Abnehmerseite nach wie vor hohe Versorgungssicherheiten. Das bedeutet, dass wir die Energieverteilung ebenfalls neu denken müssen. Wir brauchen in Zukunft intelligente Netze.“

Wenn rohe Ströme gefahrlos walten

Timo Beuth, Field Application Engineer Phoenix Contact, erklärt: „In der Energietechnik soll neben der hohen Versor-

gungssicherheit auch kein Personen- oder Anlagenschaden bei einem Fehler entstehen.“ Im Stromnetz treten Erdfehler am häufigsten auf. Im privaten Umfeld ist es z. B. eine defekte Kabelisolierung am Bügeleisen, im Mittelspannungs-Verteilnetz ein Bagger, der die Kabelisolierung beschädigt oder ein Ast, der die Freileitung bei starkem Wind berührt.

Beim Beispiel des Bügeleisens fliesst ein Erdfehlerstrom bei Berührung der defekten Leitungsstelle über den Körper des Menschen und über den Boden ab. Ein Fehlerstrom-Schutzschalter (FI) erkennt, dass ein Fehlerstrom fliesst und schaltet sofort ab. So schnell, dass man den Strom gar nicht merkt. Die elektrische Versorgung kann durch Einschalten des FI-Schutzschalters schnell wiederhergestellt werden, die Person hat überlebt und die elektrische Anlage wurde geschützt.

Wenn ein Ast eine Mittelspannungs-Freileitung durch eine Windböe berührt, sieht die Sache anders aus. Der Energieversorger möchte nicht gleich den Strom eines ganzen Versorgungsgebiets abschalten, jedoch auch keine Personen und Anlagen aufgrund eines Erdfehlerstroms gefährden. Denn die Kräfte, die hier agieren, sind ungleich grösser. Schon eine Annäherung an die Fehlerquelle kann zu einem zerstörerischen Lichtbogen führen. Also wird der Fehlstrom quasi an der „Sicherung“ vorbeigeleitet. Mittels des Schutz- und Feldsteuergeräts „KOMBISAVE“ der Phoenix Contact-Tochter NSE

gelingt das Kunststück, den Erdfehlerstrom sicher orten zu können und das Stromnetz nur lokal abzuschalten. Die niederohmige Sternpunktterdung des Mittelspannungstransformators reduziert gefährliche einpolige Erdkurzschlussströme und verhindert eine unzulässige Spannungserhöhung im unmittelbaren Bereich der Fehlerstelle. Durch Umschaltungen auf weitere vorhandene Reserveeinspeisungen lässt sich die Versorgungssicherheit binnen weniger Minuten dank der digitalen Netzleittechnik schnell wiederherstellen.

Lasst die Hände in den Taschen

Im Umspannwerk, an dem die 110-kV-Hochspannung aus dem Transportnetz in die 10-kV-Mittelspannung des Verteilnetzes transformiert und verteilt wird, öffnet Reinhard Bretzke die Türen. „Lassen Sie ihre Hände besser in den Hosentaschen“, warnt er vor allzu forschen Kameraperspektiven mit fatalen Folgen. Hier besteht bei Unachtsamkeit Lebensgefahr.

Hinter einer Schaltschranktür mit der Aufschrift „Sternpunktbildner“ leuchtet uns schon das NSE KOMBISAVE an. „Wir konnten das Schutzgerät wirklich nahezu sofort anpassen und bedienen und sind nach wie vor begeistert von der einfachen Montagemöglichkeit. Die Einbindung in unsere Leittechnik war problemlos und die erforderlichen Parameter im Schutzgerät schnell eingestellt. Letztendlich haben wir keine Stunde gebraucht, um aus der Verpackung heraus ein einsatzbereites und parametrieres Schutzgerät für eine spezielle Anwendung zu haben – und das ohne uns einzulesen. Bei ein oder zwei Details standen uns dann noch die Experten von Phoenix Contact ruckzuck zur Seite,“ zeigt sich Michael Kairies über das Teamwork sichtlich zufrieden. „Und die Parametrier-Software Digicom der NSE-Geräte ist nicht nur kostenfrei, sondern auch intuitiv zu bedienen.“

Damit sparen die Stadtwerke Kempen nicht nur Zeit und Aufwand beim Erneuern ihrer Energienetze. Sie investieren auch in die Versorgungssicherheit ihrer Betriebe und Bürger in der „schönsten Stadt am Niederrhein“. (lo) ■

nse.ch

Da, wo die 110-kV-Leitung endet –
Umspannwerk in Kempen



Höllen- fahrt für Lilon-Akkus

Die Welle der E-Mobilität rollt. Und zwar gewaltig. Damit verbunden sind die Entwicklung und Erprobung neuer Technologien in bisher ungeahnten Dimensionen. Bei Phoenix Testlab in Blomberg werden bis zu 800 kg schwere LiIon-Akkupakete getestet. Ein Blick hinter die Kulissen einer modernen Folterkammer.



SICHERE BATTERIEN



Das Thema ist sprichwörtlich heiss: Immer wieder geistern Nachrichten von brennenden E-Autos durch die Nachrichten. Das Thema Akkumulator bekommt durch die geforderte enorme Energiedichte und ihren Einsatz im rollenden Alltag eine ganz neue Brisanz. Und damit auch Dinge wie Haltbarkeit, Dauerbelastung und Sicherheit. Daher ist Phoenix Testlab in Blomberg bei der Automobilindustrie eine allererste Adresse.

„Wir machen Akkus alt. Und das ganz schnell.“ Der das sagt, trägt keinen Zauberhut oder ist im Besitz einer Zeitmaschine. Michael Jonca leitet das Batterielabor bei Phoenix Testlab. Und wirkt nicht nur ausgesprochen sympathisch, sondern auch sehr seriös. Also kein Hokuspokus, sondern echte technologische Pionierleistung, mit der den Energiespendern von E-Fahrzeugen hier zu Leibe gerückt wird.

Die Herren der Zeitreise

„Unsere Aufgabe ist es, Lithium-Ionen-Akkus im Prototypenstadium künstlich altern zu lassen. Durch unsere ausgeklügelten Testverfahren stressen wir die empfindlichen Energieträger derart, dass dies weit mehr als einem Autoleben entspricht.“ Eine virtuelle Zeitmaschine. Also doch ein wenig

„Wir machen Lithium-Ionen-Akkus alt. Weit mehr als ein Autoleben dauert. Und das ganz schnell.“

Michael Jonca,
Leiter Prüflabor Batterietechnik



Im T-Schocker werden Temperaturstürze simuliert – in ständigem Wechsel von -40 °C bis +75 °C

Blick in den Zwischenboden eines modernen E-Lieferwagens mit Batteriezellen





Michael Jonca in einem Teil der Batterielabore, der modular aufgebaut ist

Zauberei! „Dabei richten wir uns streng nach den Vorgaben der Hersteller“, erklärt Michael Jonca seine Aufgaben.

Phoenix Testlab ist ein unabhängiges Prüfinstitut, welches 1994 von Phoenix Contact gegründet wurde – noch unter dem Namen Phoenix EMV-Test GmbH. Der damalige Anlass war die seit dieser Zeit vorgeschriebene Elektromagnetische-Verträglichkeits-Prüfung (kurz EMV). Von Beginn an war die Unabhängigkeit des Instituts trotz der räumlichen Nähe zum gründenden Unternehmen ein wichtiges Merkmal des Testlabors. Diese Unabhängigkeit ist einer der Eckpfeiler für den raschen Erfolg des Hightech-Unternehmens. Ein anderer: Der Kunde ist König.

Daher gelten in den heiligen Hallen am Königswinkel 10 auch oftmals strenge Vorgaben der Kunden. „Sorry, aber diese Geräte und Prüflinge sind für Fotografen tabu.“ Das betrifft insbesondere die Automobilbranche. Für die und ihre bis zu 800 Kilogramm schweren Energiespeicher ist Phoenix Testlab seit 2011 ein nahezu unverzichtbarer Partner. Im Frühjahr dieses Jahrs begann der Betrieb eines der modernsten Labore

der gesamten Branche für die Prüfung von Lithium-Ionen-Batterien und -Modulen auf einer Fläche von ca. 950 Quadratmetern.

„Der Aufbau dieses Testcenters begann mit diesen Containern.“ Zusammen mit Thomas Worsch, dem Marketingexperten von Phoenix Testlab, starten wir einen Rundgang durch das Prüfinstitut. „Container sind ideal, weil wir die jeweiligen Testkomplexe und die Prüflinge aus Sicherheitsgründen einzeln handhaben können.“ Michael Jonca führt aus: „Zwar testen wir hier keine Zerstörungsszenarien, setzen also den Prüfling nicht absichtlich der Zerstörung aus. Aber auch unsere Haltbarkeits- und Lebensdauertests stressen die grossen Batterien erheblich. Daher gibt es auch eine ganz enge Zusammenarbeit mit der ansässigen Feuerwehr, die einen potenziellen Brand ohne Gefährdung des restlichen Testlabs und der Mitarbeiter und umliegender Anwohner schnell unter Kontrolle bringen muss.“

In der Folterkammer

Die grossen Batterieblöcke werden über Monate hart ran- genommen. Erste Station ist die elektrische Prüfanlage. „Wir laden hier mit richtig Energie, boosten in ein bis zwei Stunden



auf Vollladung. Und das viele tausend Male. Unser Stromverbrauch ist daher ähnlich hoch wie der der gesamten Fertigung von Phoenix Contact in der Nachbarschaft.“

Kein Wunder, dass am Ende dieses Testlaufs die Prüflinge ein bis zwei Wochen liegen gelassen werden, bis sie wieder an den Auftraggeber zurückgesandt werden. „Die chemischen Reaktionen im Akku sind ja nicht abrupt beendet, das klingt noch eine Weile nach“, erklärt der Chef des Batterielabors. „Die Gefahr einer Entzündung auf dem Transportweg wäre zu hoch für eine sofortige Rücksendung.“

Schütteln für die Schifffahrt

Es wird mechanisch. Wir marschieren zur nächsten Folterkammer. Die hört sich nach Jahrmarkt an: „Das ist unser Shaker, unsere Rüttelkammer. Hier schütteln wir den Batteriepack rund zwei Wochen lang ununterbrochen, und das kombiniert mit einer Klimakammer, sodass wir hier Hitze und Kälte simulieren können.“ Die Ausmasse des haushohen Prüfstands sind enorm. „Wir heben den Prüfling mitsamt seinem von uns angefertigten Aggregatrahmen mit einem 5-Tonnen-Kran auf seinen Platz.“ Die stählerne Schüttelplatte wiegt allein 35 Tonnen. Sie ist im Fundament federnd gelagert, sonst würde im weiten Umkreis die Erde beben“, berichtet Thomas Worsch. Jonca ergänzt: „Hier testen wir auch Komponenten aus der Schifffahrt und der Industrie, nicht nur Batterien, sondern auch ganze Schaltschränke.“ Der Prüfstand rüttelt im „einaxialen Schwingungsverfahren“. Um einen Prüfling in allen drei Dimensionen durchzuschütteln, wird seine Lage auf der Prüfanlage verändert. Eine Gemeinheit hat der Prüfstand auch noch drauf: „Wir simulieren hier auch einen mechanischen Schock, also etwa die Fahrt über einen Bordstein. Da lasten dann bis zu 50g auf dem Prüfling.“

Die Batterien sind je nach Kundenwunsch mal sechs Monate, mal fast anderthalb Jahre im Phoenix Testlab. Nicht drumherum kommen die bemitleidenswerten Dauerläufer um das nächste

18



Monate dauern die längsten Testreihen mit Prototyp-Akkupaketen

2



Wochen Ruhephase erhalten die strapazierten Energieträger, bevor sie zurückgesandt werden

Testmartyrium: den T-Schocker. „Zehn bis dreissig Tage lang muss der Batteriepack einen Temperatursturz von -40 °C bis +75 °C aushalten. Das sind ganz typische Anforderungen aus der Automobilindustrie“, lässt uns Michael Jonca staunen. „Hier wird die Dichtigkeit der Aussenhülle strapaziert.“

Letzte Hürde Schwimmbad

Ist der Prüfling bis hierhin noch immer bei guter Laune, droht ihm im Tauchbecken die nächste Tortur. „Dieses grosse Becken ist ganz neu“, schallt Joncas Stimme durch das spezielle Schwimmbad. An der Decke der grosse Kran, der die Batterien ins kalte oder warme Wasser hebt. „Wir können das Wasser auch beheizen.“

Für jedes Akkupaket ist ein Team an Ingenieuren und Mitarbeitern zuständig, denn die jeweiligen Testprozeduren sind komplett unterschiedlich. „Momentan befinden sich zwölf verschiedene Prüflinge, und damit auch zwölf verschiedene Energieträger für ihre jeweiligen E-Fahrzeuge, bei uns im Test.“ Wer den netten Herrn Jonca durch seine Folterkammern begleitet, der kann sich mit Sicherheit darauf verlassen, dass die Prüflinge, die hier heil entkommen, nahezu jede Tortur mit Leichtigkeit ertragen. (lo) ■

phoenix-testlab.de





Der Shaker kann Prüflinge bis zu einem Gewicht von vier Tonnen durchrütteln



Geschüttelt, gerüttelt, geschockt und zum Abschluss noch baden geschickt

Die Module erleichtern die Trennung von eventuellen Havaristen vom übrigen Testprogramm

BLITZSCHUTZ



30.000

Grad Celsius wird die Luft im
Entladungskanal heiss



300

Millionen Euro beträgt die
durchschnittliche Summe an
Schäden durch Blitze pro Jahr in D
(Gesamtverband der Deutschen
Versicherungswirtschaft)



Blitz und Donner digital

Wenn Reyno Thormählen nach oben schaut und Gewitterwolken sieht, dann hellt sich seine Miene auf. Gewitter sind gut. Wenn es ordentlich blitzt und donnert, dann können seine Anlagen ihre Schutzfunktion unter Beweis stellen. Denn Reyno Thormählen ist Chef eines Blitzschutzunternehmens.

Mitten in der niedersächsischen Provinz, in Großenmeer bei Oldenburg, befindet sich eines der innovativsten Handwerksunternehmen Deutschlands. „Wir sind Marktführer beim Thema Blitzschutz“, gibt sich Thormählen selbstbewusst.

120 Mitarbeiter arbeiten an sieben Standorten im Norden der Republik an Anlagen, die Gebäude sicherer machen. Wobei „Norden“ weit gesteckt ist. „Wir sind bis Köln und Leipzig aktiv“, erklärt der Geschäftsführer. „Unsere Kunden kommen zu etwa 80 Prozent aus dem industriellen Umfeld, zehn Prozent aus dem öffentlichen Bereich und ebenso viele aus dem privaten Sektor.“

Kasernen, Flughäfen, Industrieanlagen, Windparks – für die Teams von Thormählen geht es oft hoch hinaus. Kein Wunder, dass die Niedersachsen sogar eigene Industriekletterer in ihren Reihen haben. „Wir installieren Blitzschutz etwa bei North

→



Reyno Thormählen ist einer der Geschäftsführer von Blitzschutz Thormählen



Thormählen kann auch privat, die meisten Kunden stammen aber aus der Industrie

Stream 1 und 2 oder sind beim Lärmschutzdeckel der A7 bei Hamburg dabei“, beschreibt Thormählen seine aktuellsten Projekte. Der studierte E-Techniker kümmert sich vor allem um Strategie und Marketing im Großenmeerer Handwerksunternehmen.

Thormählen ist ein Vorzeigeunternehmen, wenn es um Digitalisierung im Handwerk geht. „Wir sind stets interessiert, unsere Abläufe zu verbessern, die Prozesse zu verschlanken und Papier zu vermeiden. Wir wollen die Möglichkeiten der heutigen Zeit nutzen und unsere Dienstleistung verbessern, indem wir unsere Produkte intelligenter machen.“ Neben den Grossprojekten glänzen die Norddeutschen auch mit Innovationen wie dem Unterdach-Blitzschutz bei Reetdächern („Wir waren die ersten, die das entwickelt haben“) oder Details wie

RFID

Die Radiofrequenzidentifikation (RFID) dient der berührungslosen Identifikation, dem Datenaustausch und der Lokalisierung von Transpondern/Tags ohne Sichtkontakt. Mit Hilfe eines RFID-Handhelds, das als Sende- und Empfangseinheit fungiert, werden Daten durch elektromagnetische Wellen (UHF) oder durch ein magnetisches Feld (HF) an einen Transponder/Tag gesendet und empfangen. Thormählen setzt einen BLUE-MARK ID COLOR-Drucker von Phoenix Contact ein, mit dem sich das Markierungsmaterial individuell und farbig gestalten lässt.

dem Einsatz eines speziellen Drehmomentschlüssels, um das materialbestimmte Anzugsmoment zu erzeugen. „Ist in explosionsgefährdeten Anlagen vorgeschrieben, hat aber niemand benutzt. In Industrieanlagen ist das kritisch.“

Allen Blitzschutzanlagen gemein ist, dass sie meist nichts tun. Und wenn sie aktiv werden, dann merkt es niemand. Für jeden Verrieb ein Graus. Die Wirkungsweise einer Blitzschutzanlage erfährt eigentlich nur jemand, der keine hat. Wenn es also zu spät ist.

Die Auftragslage ist trotzdem gut: „Wir haben mehr als genug zu tun. Je mehr Anlagen vernetzt werden und IoT-Einzug in die Welt von Produktion und Kommunikation hält, desto empfindlicher reagieren diese Sensibelchen auf die rohen Kräfte der Natur“, erklärt Jens Barghorn, zweiter Geschäftsführer und als gelernter Elektromeister ein Mann der Praxis.

Die intelligente Trennstelle

Blitzanlagen wollen gewartet werden. Denn sie unterliegen der Witterung, können durch bauliche Veränderungen in ihrer Schutzfunktion beeinträchtigt oder tatsächlich vom Blitz getroffen werden. Damit der Monteur vor Ort schnell weiss, welchen Stand die Anlage hat, muss er auf die jeweils vorhandene Dokumentation zurückgreifen. Thormählen setzt an den Trennstellen der Blitzschutzanlage, also dort, wo der Zustand per Messung kontrolliert wird, spezielle RFID-Kennungen von Phoenix Contact ein. Die sind in einer wetterbeständigen Plakette untergebracht, die Thormählen per NFC-Schnittstelle und mit einem speziellen Industriedrucker von Phoenix Contact selber mit Informationen anreichert.

„Unser Kunde soll eine sprechende Messstelle bekommen, die ihm per Smartphone und passender App direkt Auskunft über seine Blitzschutzanlage gibt“, beschreibt Reyno Thormählen den Grund für den Einzug der „schlauhen Plaketten“. „Wir haben gemeinsam mit Phoenix Contact richtige Grundlagenforschung betrieben. Zunächst ging es darum, RFID-Chips

und deren Antennen auf ihre Blitzverträglichkeit zu testen. Niemand wusste etwa, wie die Datenspeicher auf den Plaketten reagieren, wenn durch einen Blitzschlag hohe Impulsströme durch die Ableitungen fließen. Welches Material müssen wir verwenden?“

„Der Blitzschutz wird durch den Klimawandel und den erhöhten Einsatz von Niederspannung im IoT-Bereich immer wichtiger.“

Jens Barghorn,
Geschäftsführer Blitzschutz Thormählen

Blitzschutz mit Vision

Auch eine eigene Anlagenwartungs-App wurde gemeinsam mit Phoenix Contact entwickelt, mit der das Auslesen dank der RFID-Technologie berührungslos möglich wird. Spielerei? „Auf keinen Fall. Mit dieser Technologie kann das Facility Management die Anlage in ihr Wartungskonzept einbinden, also von sich aus tätig werden und nicht nur unserer Wartungsroutine folgen“, beschreibt Jens Barghorn die Vorteile der Trennstellenmarkierung.

„Wir rüsten momentan jeden neuen Auftrag mit individuell bedruckten RFID-Plaketten aus, aktuell sind das rund 2000 Aufträge.“ „Das ist für uns ein Invest in die Beziehung zu unseren Kunden“, ergänzt Reyno Thormählen. „Blitzschutz ist ein langfristiges Thema. Wir wollen keine Blitzschutzanlagen liefern, wir wollen dauerhafte Sicherheit anbieten.“ (lo) ■

thormaehlen.de



Individuell bedruckbare
RFID-Plaketten erleichtern
die Wartung

Mit den Informationen
des Chips erkennt der
Monteur sofort die
wichtigsten Details der
zu prüfenden Anlage

Eierlegende Video- Wollmilch- Box

Bei Sport und Spass ist ein Erfolg, der schon von vornherein feststeht, langweilig. Geht es aber um industrielle Sicherheitsanwendungen, schlägt der Puls für eine sichere Sache schneller. Ist die neue Smart Camera Box solch ein Gewinnertyp?

Das Telefon in der Redaktion läutete vor einigen Wochen Sturm. Am anderen Ende eine Kollegin, die fragte: „Im nächsten Heft geht es doch um das Thema Sicherheit, oder? Wir haben da was ganz Tolles.“ *Aha, was ganz Tolles*, denkt der Schreiber dieser Zeilen. „Ja, eine Videobox für bildgestützte Überwachungsanlagen.“ *Werte Kollegin, was ist denn an einer Anschlussbox für Video spannend? Bei Amazon gibt's Wildüberwachungskameras für unter 50 Euro. Die können sogar WLAN.* „Das ist doch ganz was anderes. Treffen Sie sich doch einmal mit einem der Kollegen, die die Box entwickelt haben!“

→

VIDEOÜBERWACHUNG





Die Spleissbox (oben) basiert auf einer Neuentwicklung, die 2018 vorgestellt wurde

Industrie braucht es handfest

Gefragt, getan – wenige Tage später treffen wir uns zu einem Vor-Ort-Termin mit Produktmanager Tommy Göring. Doch bevor wir die Vorzüge der handlichen grauen Kiste in der Aussenwelt demonstriert bekommen, muss der Experte kurz erläutern, wie Phoenix Contact auf das Thema Video kommt. „Das ist gar nicht schwer. Wir sind in der Ausstattung von Ethernet-Netzen schon lange aktiv. Und bekamen immer mal wieder Anfragen, ob unsere Medienkonverter sich nicht auch für Gigabit-Datenübertragungen eignen würden. Doch das braucht der Automatisierer mit seinen wenigen Daten eigentlich gar nicht. Also haben wir geschaut, was da eigentlich übertragen werden soll. Und festgestellt: hochwertige

„60 bis 80 Prozent aller Anwendungen werden mit dieser Box abgedeckt.“

Tommy Göring

Videokameras besitzen auch eine RJ45-Buchse für Standard-Ethernet. Und daher kamen die Anfragen.“

Die Recherche ergab schnell, dass Videokameras selber kein Feld für Phoenix Contact sind, denn die Technologie ist extrem schnelllebig. „Wir stellen aber mit unserer Smart Camera Box eine Verbindung zwischen Kamera und Videozentrale her. Und das zukunftssicher und komplett.“ Der Experte für den Bereich Industrial Communication Interface betont, dass für die Kameras einer Videoüberwachung normalerweise extra Schaltschränke gefertigt, mit Einzellösungen diverser Hersteller bestückt und dann mit oftmals zwei Monteuren installiert werden müssten.

„Das können wir besser. Also haben wir vor etwa anderthalb Jahren angefangen, unsere Lösung zu entwickeln.“ Tommy Göring öffnet die Box. „Die ist zunächst einmal nach IP65 und IP67 geschützt, hält also auch jahrelang dicht. Und das zwischen -40 °C bis +70 °C, also fast überall.“ Energie bekommt der smarte Kasten mittels 230-V-Anschluss, die dann mittels Power-over-Ethernet, also eines kombinierten Strom- und Datenkabels, an die Kameras weitergeleitet wird.

Anschlüsse in Hülle und Fülle

Das elektronische Innenleben und die angeschlossene Kamera werden mittels steck- und austauschbarer Blitzschutzelemente aus dem unternehmenseigenen Überspannungsschutzprogramm TRABTECH vor spontanen Überraschungen aus dem Stromnetz geschützt. „Die setzen bei Auslösung durch Blitzschlag oder Überspannung auch eine sogenannte SNMP-Meldung an die Videozentrale ab.“ Sollten Bösewichte sich an dem Gehäuse zu schaffen machen, dann sorgen spezielle Näherungssensoren für einen weiteren Alarm in der Zentrale. Die smarte Box kommuniziert also.

Die Daten gelangen im Regelfall per Glasfaser an ihren Abnehmer in der Zentrale, gerade bei grossen Distanzen. „Dafür

besitzt die Box eine eigene Lichtwellen-Spleisscassette. Hier können Glasfasern angeschlossen und mit einem Stecker versehen werden, sodass das Kabel der Kamera nur noch eingesteckt werden muss.“

Sitzt die Videokamera dagegen in der Nähe der Zentrale, findet auch ein Standard-Ethernetkabel seinen Anschluss. Und soll die Smart Camera Box in ein bestehendes älteres Netz eingebunden werden, dann ist auch an eine Möglichkeit gedacht, eine Zweidrahtleitung, etwa ein Koaxkabel, mit der modernen Ethernet-Welt zu verbinden.

Apropos moderne Welt: „Wir sprechen hier von High-End-Videokameras. Da ist viel mehr drin als nur eine optische Baugruppe. Mittlerweile sind das selber Computer, die die Bilder schon in der Kamera auswerten, also etwa erkennen, wenn es ein Mensch ist, der sich dem Zaun nähert.“

Eigentlich ist es keine Box, sondern ein Gerät

„Bis zu vier Kameras können an die Box angeschlossen werden. Die erforderliche Energie liefern wir mit dem neuen Power-over-Ethernet-Standard IEEE 802.3bt, der deutlich höhere Stromstärken zulässt. Damit lassen sich auch motorgetriebene Kameras antreiben.“ Für den Blick in jede Ecke also.

Der kann bei Bedarf sogar ausgeleuchtet werden. „Wir haben auch eine Hutschiene untergebracht. Hier finden etwa unsere WLAN-Accesspoints oder Mobilfunk-Router ihren Platz. Dazu steht ein 24-V-Ausgang für die erforderliche Energie parat.“

Den letzten und entscheidenden Trumpf spielt die Wunderwaffe in Sachen Videokommunikation dann vor Ort aus. Tommy Göring schnappt sich eine Leiter, klemmt sich seine Box unter den Arm und flitzt die Sprossen hoch. Oben demonstriert er, wie einfach sich Box und Kamera verbinden sowie installieren lassen. „Durch unsere Entwicklung eines speziellen Mastadapters reicht ein Monteur für die Installation. Das ist normalerweise eine Arbeit für zwei Mitarbeiter.“

Vorgestellt wird die Smart Camera Box, so ihr offizieller Name, auf der Hannover Messe 2020. Und wer immer sich mit dem Thema Videoüberwachung auseinandersetzen muss, sollte die Geduld aufbringen und auf den knackigen Gewinertyp und seine Auslieferung warten.

Und vielen Dank an die Kollegin und ihre Überzeugungskraft. Da kommt meine Wildüberwachungskamera dann doch nicht mit! (lo) ■

update.phoenixcontact.com



Die Videobeleuchtung lässt sich natürlich ebenfalls über die Box steuern

Grüsse aus Casablanca

Neue Vertriebsniederlassung betreut Maghreb-Staaten

In der westmarokkanischen Hafen- und Handelsstadt am Mittelmeer hat Phoenix Contact eine neue Vertriebsgesellschaft gegründet. Die Geschicke in der nordafrikanischen Metropole leitet Youssef Asmi, der bereits seit vielen Jahren im Unternehmen ist. Er hat zuvor zwölf Jahre für Phoenix Contact Kanada gearbeitet.

Jetzt hat er sich entschlossen, zurück in sein ursprüngliches Heimatland zu gehen.

Youssef Asmi als Country Manager und die neue Niederlassung werden damit die Ansprechpartner für Kunden aller drei Maghreb-Staaten, also sowohl von Marokko als auch von Algerien und Tunesien.



Casablanca ist das Tor zu den drei Maghreb-Staaten Tunesien, Algerien und Marokko



Roland Bent in neuer Funktion

Vorsitz Fachbereich Industriesteuerungen

Der ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V. vertritt die wirtschafts-, technologie- und umweltpolitischen Interessen der deutschen Elektroindustrie. Der Fachverband Automation hat Ende 2019 eine neue Führung gewählt. An der Spitze steht zukünftig Dr. Jan Mrosik, Chief Operating Officer Digital Industries bei Siemens. Und ihm zur Seite steht u. a. der CTO von Phoenix Contact, Roland Bent. Er ist jetzt Vorsitzender für den Fachbereich Schaltgeräte, Schaltanlagen und Industriesteuerungen.

zvei.org

Offen wie ein Scheunentor

Zwei Milliarden Geräte sind von entdeckten Schwachstellen bedroht

Im Juli 2019 wurde die Entdeckung von elf Zero-Day-Sicherheitschwachstellen bekannt gegeben, die das Echtzeitsystem Wind River VxWorks betreffen.

VxWorks wird in über zwei Milliarden Geräten genutzt, vor allem in wichtigen Industrie-, Medizin- und Unternehmensgeräten. Die elf Sicherheitsschwachstellen werden unter dem Namen Urgent/11 zusammengefasst und ermöglichen es Angreifern, aus der Ferne und ohne jede Nutzerinteraktion Kontrolle über Geräte zu erlangen. Dabei werden Sicherheitssysteme wie

Firewalls umgangen. Aufgrund der enormen Verbreitung alle Geräte zu aktualisieren, auf denen VxWorks läuft, ist nicht einfach oder überhaupt nicht möglich. Deswegen bietet Phoenix Contact mit den mGuard-Security-Routern eine einfachere und nachrüstbare Lösung: Die Security-Appliances werden einfach ins Netzwerk integriert und schützen die VxWorks-Geräte vollständig vor Angriffen über alle kritischen Urgent/11-Sicherheitslücken.

twitter.com/mguardcom



mGuard-Produkte sichern auch auf der Hutschiene

Wissenschaftliche Hochkaräter zu Gast in Bad Pyrmont

Professor Suzanne D. Berger vom MIT auf Recherche-Tour durch Deutschland

Gleich mit vier WissenschaftlerInnen reiste eine Delegation des renommierten Massachusetts Institute of Technology nach Bad Pyrmont, um sich den Phoenix Contact-Standort und die hier ansässige Smart Factory anzuschauen.

Prof. Suzanne D. Berger, besuchte Deutschland, um für ein neues Buch zu recherchieren. 2013 wurde die Studie „Making in America: From Innovation to Market“ veröffentlicht, in der Prof. Berger der Frage nachgeht, ob die USA die Leistungsfähigkeit des Produktionsbereichs stärken müssen, um aus Innovationen Wert zu schöpfen.

Jetzt startete ein neues Projekt: In der Task Force „Work of the Future“ beschäftigen sich Mitarbeitende verschiedener MIT-Fakultäten gemeinsam mit der Frage, welchen Einfluss neue Technologien auf die Beschäftigten haben.

Bei der Suche nach Unternehmen, die auf dem neuesten Stand hinsichtlich moderner Technologien sind, war das MIT-Team auf Phoenix Contact aufmerksam geworden. Während des Jahrestreffens des World Economic Forums Ende 2018 in Tianjing (China) wurde Phoenix Contact als eine

der neun weltweit führenden Smart Factories ausgezeichnet, die IIoT-Technologien bereits in der Praxis einsetzen.

Eine Führung durch den Produktionsbereich zeigte, dass sich Maschinen und Anlagen innerhalb kurzer Zeit auf die Fertigung neuer Produkte umrüsten lassen.

Die herzustellenden Produkte sind aufgrund eines digitalen Zwillings so smart, dass sie sich ihren Weg durch die Bearbeitungsstationen selbst suchen. So lassen sich auch Kleinserien und Sonderfertigungen realisieren, die in einer reinen Massenfertigung unwirtschaftlich wären.



Prof. D. Berger (Mitte) mit ihrem Team und Produktionsleiter Dr. Tilman Potente (re.)

Neuer GM in Südafrika

Der Neue setzt auf Teamwork

Kurz vor Jahresende 2019 hat der Springbock-Staat am Kap von Afrika mit Carl Kleynhans einen neuen General Manager bekommen. Mehr als 18 Jahre Berufserfahrung in der IT- und Elektronikbranche bringt der studierte Business Manager mit, u. a. auch in deutschen Elektronikunternehmen.

Teamwork ist nach eigenen Angaben sein Mittel auf dem Weg zu weiteren Erfolgen.



phoenixcontact.com

Innovation aus dem Drucker

Protiq druckt reines Kupfer

Mit dem 3-D-Druck von reinem Kupfer hat Protiq einen Durchbruch im Bereich der Additiven Fertigung erreicht. Auf der Spezialmesse formnext Ende November 2019 in Frankfurt präsentierte das Team um Geschäftsführer Dr. Ralf Gärtner das weltweit einzigartige Verfahren.

Der Druck von reinem Kupfer galt bisher als nicht möglich, denn das Metall reflektiert die Strahlen des schmelzenden Lasers bis hin zu seiner Zerstörung.

Aufgrund seiner hervorragenden elektrischen Leitfähigkeit werden aus Kupfer u. a. Induktoren für die partielle Härtung von Bauteilen hergestellt. Die Herstellung ist aufwändig und zeitintensiv, dauert normalerweise Wochen.

Mit dem neuen Verfahren ist es möglich, die herkömmliche Bearbeitungszeit auf wenige Stunden zu reduzieren. Ausserdem lassen sich die Herstellungsdaten des Bauteils direkt auf die Online-Plattform von Protiq hochladen, konfigurieren und bestellen.

protiq.com



Termine/Orte 2020

Messe	Datum	Ort
SIAMS	21. – 24. April	Forum de L'arc, Moutier
SINDEX	22. – 24. Sept.	BERNEXPO, Bern

Forum	Datum	Ort
Communication Conference 2020	18. März	Fachhochschule Nordwestschweiz, Windisch
Tunnel-Forum 2020	28. April	Tagelswangen

Seminare	Datum	Ort
Praxisseminar maschinenbau.next	24. März	Tagelswangen
Industrielle Cybersicherheit – Grundlagen IEC 62443	19. Mai	Tagelswangen
Seminar für Gebäudemanagementsystem Emalytics	25. – 29. Mai	Tagelswangen
Praxisseminar ADVANCED-TRABTECH	10. September	Tagelswangen

Workshop	Datum	Ort
Zertifizierter Überspannungsschutz-Experte	25. Juni	Tagelswangen

Agenda Webinare: phoenixcontact.direct

Innovator des Jahres

Stecken statt Löten überzeugt Jury

Mit der ScaleX-Technologie der FINEPITCH Board-to-Board-Steckverbinder wurde Phoenix Contact als „Innovator des Jahres 2019“ ausgezeichnet. Leser des Magazins Design & Elektronik wählten die Innovation auf Platz eins in der Kategorie Elektromechanik. Torsten Janwlecke, Präsident der Business Area Device Connectors und Markus Sonderer, Senior Director of Product Marketing and Product Development, nahmen den Preis bei der Preisverleihung des Weka-Verlags in München entgegen.

Die FINEPITCH-Serie dient der Verbindung von Leiterplatten miteinander, möglichst schnell, möglichst zuverlässig und möglichst sicher: Mit den Board-to-Board-Steckverbindern bietet Phoenix Contact erstmals geschirmte und ungeschirmte Lösungen für die Signal- und Datenübertragung.

Von der Telekommunikation über die Gebäude- und Industrieautomation bis hin zu IoT-Anwendungen – Board-to-Board-Steckverbinder ermöglichen platzsparende Lösungen für die Signal- und Datenübertragung. Und das auch in industriellen Umgebungen, die rau und herausfordernd sind. Möglich sind individuelle Leiterplattenausrichtungen mit unterschiedlichen Bauformen, Stapelhöhen und Polzahlen in den Rastern 0,8 mm und 1,27 mm.

Sicherheit, wenn es knallt

Award für ImpulseCheck

Mit ImpulseCheck, dem Assistenzsystem für Überspannungsschutz, hat Phoenix Contact den GIT Sicherheit Award 2020 in der Kategorie gewonnen. Dr. Martin Wetter, Geschäftsbereichsleiter Überspannungsschutz, nahm den Preis im Rahmen der Messe SPS in Nürnberg entgegen.

Mit dem intelligenten Assistenzsystem ist der State-of-health, also der aktuelle Zustand des Überspannungsschutzes, jederzeit online abrufbar. ImpulseCheck bietet neben der Überwachung der Überspannungsschutzgeräte zusätzlich eine einfache und umfassende Analyse der Anlagen-EMV. Mögliche Störgrößen werden erkannt, bevor es zu einem Ausfall in der Anlage kommt. Dadurch werden Service- und Wartungseinsätze besser planbar.



Kostensenker Facility

Auszeichnung für Gebäudemanagementsystem

Mit dem eigenen Gebäudemanagementsystem „Emalytics“ im Einsatz am Standort Bad Pyrmont senkt Phoenix Contact die dortigen Betriebskosten erheblich. Und das mit so innovativen Methoden, dass das System den Preis des „Produkt des Jahres“ in der Kategorie Smart Building gewonnen hat. Der Preis wurde vom Weka-Verlag ausgelobt.

Gesteuert und überwacht wird das hochautomatisierte Gebäude über das IoT-basierte Gebäudemanagementsystem. Unter anderem sind der Energieverbrauch des Gebäudes, die Belegung der Besprechungsräume und der Zustand der Heizungsanlage per Mobilfon aktuell abrufbar.

weka.de



Die nächste Ausgabe erscheint im Mai 2020:

Handwerk

Die aktuelle Berichterstattung wird häufig von den faszinierenden Themen rund um Industrie 4.0 und dem Internet der Dinge dominiert. Doch die Basis allen Tuns liegt in der Hände Arbeit. Die kommende Ausgabe beschäftigt sich mit der manuellen Grundlage von Industrie und Handwerk.

SMART HOME IM HANDWERK

Gebäudeautomation

Von Frankfurt bis Mallorca – Stephan Christmann und sein Team machen das Leben leichter und Gebäude sicherer.

WERKZEUGFERTIGUNG

Schweden-Power

Wer weiss denn sowas?
Im Land von Elch und Wikinger entstehen hochwertige Handwerkzeuge für die Kunden von Phoenix Contact.

WERDEGANG

Industriekarriere

Ein Besuch in der eigenen Ausbildungswerkstatt. Warum Phoenix Contact ein Herz für das Handwerk hat.

Impressum

Phoenix Contact GmbH & Co. KG
Corporate Communications
Lutz Odewald (Chefredakteur)
Telefon: +49 5235 3-42153
E-Mail: lodewald@phoenixcontact.com

Gestaltung und Umsetzung:
Ralf Tegtmeyer, Christian Brill

Bildnachweise:
Titelbild: © S_D_Brath/Shutterstock
© Shutterstock: 2, 5, 6, 7, 8, 20, 40, 48, 51
Andre Köller: 3, 4, 5, 10 ff, 34 ff, 44 ff, 49
Thomas Franz: 22 ff
Lutz Odewald: 5, 14 ff, 18 ff, 26 ff, 30 ff, 36, 40 ff
Aus der Branche: Bosch Sensortec, Cloud & Heat

Copyright © 2020 by Phoenix Contact
Alle Rechte vorbehalten.

Sicher ist, dass nichts sicher ist.
Selbst das nicht.

Joachim Ringelnatz,
deutscher Schriftsteller (1883 – 1934)

phoenixcontact.ch

