Fraunhofer

FORSCHUNG KOMPAKT

09 | 2014 ||

1 Auf dem Weg zum sicheren Smart Home

Immer mehr Funktionen in Häusern lassen sich über das Internet steuern. Das »Smart Home« verspricht effizientes Gebäudemanagement. Doch die Systeme sind in vielen Fällen nicht sicher und lassen sich nur mit großem Aufwand erneuern. Forscher arbeiten an einer Software, die Hackerangriffe abwehrt, bevor sie die Gebäude erreichen.

2 Ethanolfeuerstellen – die unterschätzte Gefahr

Ethanolkamine werden immer beliebter. Dabei sind sie nicht nur brandgefährlich – in der Vergangenheit ist es wiederholt zu schweren Unfällen mit den Deko-Feuerstellen gekommen. Die Geräte verunreinigen auch die Luft in Räumen. Dies belegt eine neue Fraunhofer-Studie. Ebenfalls auf dem Prüfstand sind Holzkaminöfen.

3 Zentrale Biobank für die Medikamentenforschung

Die Arbeit mit Stammzellen ist wichtig bei der Entwicklung von neuen Medikamenten. Wissenschaftler können an ihnen testen, wie Wirkstoffe reagieren. Bisher stehen die Stammzellen jedoch nicht schnell genug sowie in ausreichender Qualität und Menge zur Verfügung. Eine zentrale Biobank soll diese Lücke jetzt schließen.

4 Mehr Sicherheit auf europäischen Bahnhöfen

Flieht eine verdächtige Person mit Bus und Bahn, wird es für die Polizei oft schwierig. Denn die Sicherheitssysteme der verschiedenen Verkehrsbetriebe und Sicherheitsorganisationen sind meist nicht kompatibel. Das EU-Projekt Secur-ED soll Abhilfe schaffen und eine bessere Zusammenarbeit innerhalb einer Stadt ermöglichen.

5 Simulationen für bessere transparente Oxidschichten

Touchscreens und Solarzellen basieren auf transparenten leitfähigen Sauerstoffverbindungen. Treten jedoch Fehler in der atomaren Struktur dieser Schichten auf, sinken ihre Transparenz und Leitfähigkeit. Anhand von atomaren Modellen konnten Forscher Fehler in den Schichten identifizieren und Lösungen einwickeln, um sie zu beheben.

6 Fingerabdruck für Frachtstücke

Sicherheit hat in der Luftfrachtlogistik oberste Priorität – doch die Prüfverfahren sind zum Teil sehr zeit- und kostenaufwändig. Fraunhofer-Forscher wollen nun mit einem neuen Ansatz für digitale Logistik für mehr Effizienz sorgen, ohne dass die Sicherheit der Luftfrachtprozesse leidet.

Fraunhofer-Presse | Telefon +49 89 1205-1302 | presse@zv.fraunhofer.de | www.fraunhofer.de/presse

Die Fraunhofer-Gesellschaft ist die führende Organisation für angewandte Forschung in Europa. Unter ihrem Dach arbeiten 67 Institute und Forschungseinrichtungen an Standorten in ganz Deutschland. Rund 23 000 Mitarbeiterinnen und Mitarbeiter bearbeiten das jährliche Forschungsvolumen von zwei Milliarden Euro. Davon erwirtschaftet die Fraunhofer-Gesellschaft etwa 70 Prozent aus Aufträgen der Industrie und öffentlich finanzierten Forschungsprojekten. Die internationale Zusammenarbeit wird durch Niederlassungen in Europa, Nord- und Südamerika sowie Asien gefördert.

Impressum

FORSCHUNG KOMPAKT der Fraunhofer-Gesellschaft | Erscheinungsweise: monatlich | ISSN 0948-8375 | Herausgeber und Redaktionsanschrift: Fraunhofer-Gesellschaft | Kommunikation | Hansastraße 27c | 80686 München | Telefon +49 89 1205-1302 | presse@zv.fraunhofer.de | Redaktion: Beate Koch, Britta Widmann, Tobias Steinhäußer, Janine van Ackeren | Abdruck honorarfrei, Belegexemplar erbeten. Alle Pressepublikationen und Newsletter im Internet auf: www.fraunhofer.de/presse. FORSCHUNG KOMPAKT erscheint in einer englischen Ausgabe als RESEARCH NEWS.

Fraunhofer

Auf dem Weg zum sicheren Smart Home

FORSCHUNG KOMPAKT
09 | 2014 || Thema 1

Botnet. Ein Begriff aus der Computerwelt schleicht sich langsam in die Welt der Gebäudeautomation. Mit diesem Angriffsszenario ist laut Dr. Steffen Wendzel von der Bonner Abteilung »Cyber Defense« des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie FKIE in Wachtberg zu rechnen. Der Forscher aus der ist Experte für die Hackermethode und hat sie zusammen mit Viviane Zwanger und Prof. Dr. Michael Meier unter die Lupe genommen. Angreifer infiltrieren dabei mehrere Rechner – Bots (von engl. robots) – ohne die Kenntnis ihrer Eigentümer, schließen sie zu Netzen (engl. nets) zusammen und missbrauchen sie für Computerattacken. Die Forscher untersuchten, was es aktuell noch gar nicht gibt: Angriffe durch Botnets auf »Smart Homes«, mit dem Internet vernetzte Gebäude bzw. Gebäudefunktionen. Das Ergebnis: Die Bedrohung ist real, über das Internet gesteuerte Rollläden, Heizungen oder Schließsysteme können für derartige Attacken genutzt werden. »Unsere Experimente im Labor zeigten, dass Gebäude-IT nicht ausreichend gegenüber Angriffen aus dem Internet geschützt ist. Ihre Netzwerkkomponenten können als Botnet missbraucht werden«, so Wendzel. Der Hacker hat es dabei nicht wie bisher auf PCs abgesehen, sondern auf diejenigen Komponenten der Gebäudeautomation, die Häuser mit dem Internet verbinden. Das sind im Gebäude verbaute, kleine Kästchen, die ähnlich wie Router für den Heimcomputer aussehen und funktionieren. »Sie sind jedoch sehr einfach aufgebaut, können nur schwer aktualisiert werden und weisen Sicherheitslücken auf. Die Kommunikationsprotokolle, die sie nutzen, sind veraltet«, so Wendzel.

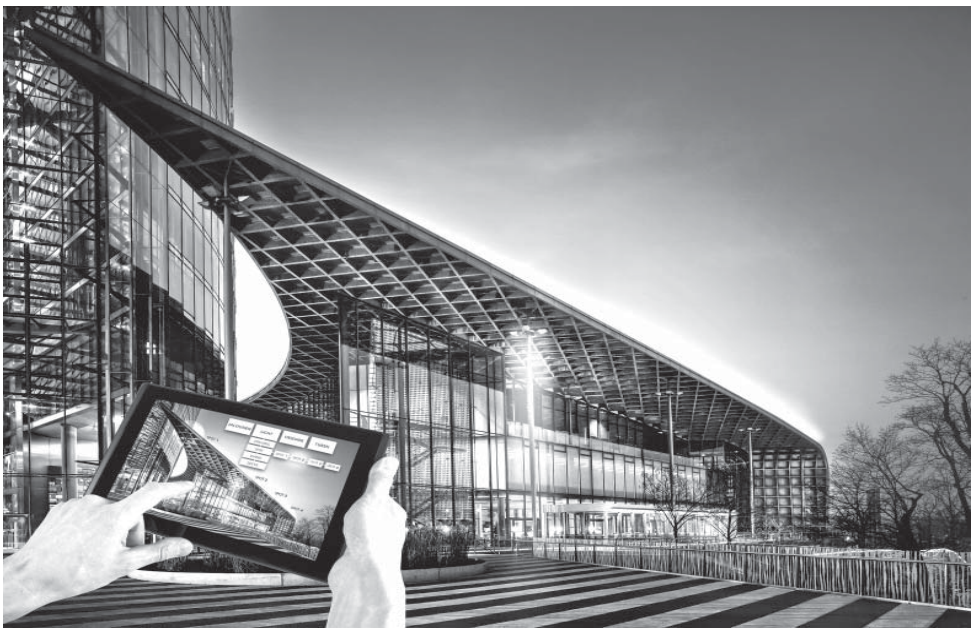
Schutzsoftware schaltet sich zwischen Internet und Gebäude-IT

Damit die Heizung, die Beleuchtung oder die Lüftung von Gebäuden über das Internet gesteuert werden können, ist es notwendig, spezielle Technik zu installieren: Es handelt sich dabei um kleine Minicomputer, die Temperaturen, Licht oder Luftfeuchtigkeit messen und in Netzwerken zusammengeschlossen sind. »Sie sicherheitstechnisch auf dem neuesten Standard zu halten, ist teuer«, sagt Wendzel. Am FKIE entwickelte das Team eine Schutzsoftware, die sich einfach zwischen Internet und Gebäude-IT schalten lässt. Die Technologie filtert potentielle Angriffe aus den Kommunikationsprotokollen heraus, noch bevor sie die eigenen vier Wände oder das Bürohaus erreichen. Ganz egal, welche Technik innerhalb der Gebäude verwendet wird: Sie muss bei dieser Herangehensweise nicht ausgetauscht werden.

Die Forscher nahmen dazu den gängigen Kommunikationsstandard der Gebäudeautomation unter die Lupe und entwickelten darauf aufbauend Regeln für den Datenverkehr. Halten eintreffende Daten diese nicht ein, wird der Kommunikationsfluss angepasst. »Die Software funktioniert wie eine Firewall mit Normalisierungskomponente«, sagt Wendzel. Ein »Analyzer« prüft sämtliche Ereignisse auf Plausibilität, die auf den Weg zu den Systemen geschickt werden. Schlägt er Alarm, geht der Vorfall unmittelbar an den »Normalizer«. Dieser blockiert das Ereignis entweder ganz oder wandelt es

passend um. »Die Grundlagenforschung ist erfolgreich abgeschlossen. Im nächsten Schritt wollen wir die Technologie zusammen mit einem Industrieunternehmen zur Produktreife bringen. In spätestens zwei Jahren sollte ein Produkt auf dem Markt sein«, sagt Wendzel.

Bei ihrer Analyse der Botnet-Angriffe skizzierten die Forscher konkrete Bedrohungsszenarien für Smart Homes. »Aus meiner Sicht ist das Thema ›Überwachung‹ das drängendste«, sagt der Cyber Defense-Forscher. Indem der Angreifer sich in die IT von Gebäudefunktionen hackt, erfährt er im schlimmsten Fall wo die Insassen sind und was sie machen. Das reicht dann bis zum Gang auf die Toilette. Einbrecher, zum Beispiel, könnten die Daten nutzen, um ihre Raubzüge vorzubereiten. Hier agiert der Hacker passiv, zapft Informationen an. Er wäre aber genauso gut in der Lage, aktiv in die Systeme einzugreifen. Zum Beispiel für einen Auftraggeber aus der Energiebranche. Der könnte von mehr verkauftem Öl oder Gas profitieren, wenn der Verbrauch mehrerer Heizungen künstlich erhöht wird. Wie real dieses Szenario ist, zeigt ein aktuelles Beispiel: Im vergangenen Jahr gab es eine Lücke im Sicherheitssystem einer an das Internet angeschlossenen Heizung. Angreifer hatten die Möglichkeit, die Heizkörper auszustellen oder zu beschädigen. Momentan rät Sicherheitsexperte Wendzel deshalb davon ab, Gebäudefunktionen in Eigenheimen allzu sorglos mit dem Internet zu verbinden.



Gebäudemanagement mit dem Tablet: In vielen modernen Bürohäusern lassen sich Licht, Jalousien oder Türen zentral über das Internet steuern. Das bringt Effizienzgewinne, birgt aber auch Gefahren. (© Fraunhofer FKIE) | Bild in Farbe und Druckqualität: www.fraunhofer.de/presse

Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE | Fraunhoferstraße 20 | 53343 Wachtberg | www.fkie.fraunhofer.de
Kontakt: Dr. Steffen Wendzel | Telefon +49 228 7360-555 | steffen.wendzel@fkie.fraunhofer.de
Presse: Herrad Schmidt | Telefon +49 228 9435-103 | herrad.schmidt@fkie.fraunhofer.de

Fraunhofer

Ethanolfeuerstellen – die unterschätzte Gefahr

FORSCHUNG KOMPAKT
09 | 2014 || Thema 2

Am Vormittag den Kamin im Baumarkt kaufen und am Abend bereits die heimelige Atmosphäre des Deko-Feuers genießen. Die Anbieter von Ethanolfeuerstellen werben mit dem leichten und schnellen Aufbau der dekorativen Öfen ohne Schornstein. Doch beim Betrieb der Feuerstellen ist Vorsicht geboten. Denn Ethanol ist ein Brennstoff, der zusammen mit Luft ein explosionsfähiges Gemisch bildet. Läuft Ethanol beim Befüllen der Brennkammern aus und entzündet sich, steht schnell der ganze Raum in Flammen.

Darüber hinaus bergen die Deko-Objekte ein weiteres Gefährdungspotenzial: Glaubt man den Herstellern, sondern die Geräte keine schädlichen Verbrennungsrückstände in die Raumluft ab. Eine Studie des Fraunhofer-Instituts für Holzforschung, Wilhelm-Klauditz-Institut WKI in Braunschweig belegt das Gegenteil. »Die Öfen besitzen keinerlei geführte Abluft, daher werden alle Verbrennungsprodukte direkt an die Umgebung abgegeben. Das sind beispielsweise sehr feine Verbrennungspartikel und gasförmige Verbindungen wie Formaldehyd und Benzol. Daten über die Auswirkung von Ethanolöfen auf die Luftqualität im Innenraum gibt es bislang kaum«, sagt Dr. Michael Wensing, Chemiker am WKI. Der Forscher und seine Kollegen haben die Höhe und Art der freigesetzten Emissionen untersucht. Ebenfalls auf dem Prüfstand der Wissenschaftler waren Holzkaminöfen.

Tests in der Prüfkammer

Die Ethanolfeuerstellen wurden in einer 48-m^3-Prüfkammer aus Edelstahl getestet. Dabei haben die Forscher die DIN 4734-1 berücksichtigt, die technische Mindeststandards für Ethanolkamine definiert, und die Prüfkammer entsprechend den Herstellerangaben gelüftet. Das Team von Dr. Wensing untersuchte vier Öfen und insgesamt acht flüssige und gelförmige Brennstoffe. »Rein theoretisch verbrennt Ethanol oder Bioethanol beim Verbrennungsprozess vollständig zu Kohlendioxid (CO_2) und Wasser. In der Praxis sieht das anders aus. Wie die Verbrennung im Einzelfall abläuft, hängt von der Qualität des Brennstoffs und anderen Faktoren ab – etwa von der Art des Brennstoffs oder der Verbrennungstemperatur. Das Ethanol verbrennt in der Regel nicht vollständig. Vielmehr entstehen neben CO_2 giftige Verbrennungsgase wie das Atemgift Kohlenmonoxid, organische Verbindungen wie die krebserregende Substanz Benzol, aber auch die Reizgase Stickstoffdioxid und Formaldehyd sowie ultrafeine Verbrennungspartikel«, sagt Wensing. In den meisten Fällen konnten die Wissenschaftler hohe Schadstoffkonzentrationen messen, Richtwerte wurden häufig überschritten. Beispielsweise überstiegen alle Geräte den Innenluftrichtwert von 0,35 mg/m^3 für Stickstoffdioxid, in einem Fall mit 2,7 mg/m^3 sogar erheblich. Bei Formaldehyd wurde der Richtwert von 0,1 ppm (parts per million) ebenfalls nicht eingehalten. Bei 0,45 ppm lag hier der höchste gemessene Wert. Ein Ofen erzielte beim freigesetzten Kohlendioxid eine Spitzenkonzentration von circa 6000 ppm – und lag damit deutlich über dem hygienisch unbedenklichen Wert von 1000 ppm. Entscheidend ist dabei auch der Brennstoffverbrauch.

Dies bedeutet: Je mehr Ethanol in einer bestimmten Zeit verbrennt, desto mehr Schadstoffe werden freigesetzt. Ebenfalls abgegeben wurden ultrafeine Verbrennungspartikel, deren Durchmesser 10.000-mal kleiner ist als die Dicke eines menschlichen Haares und die tief in die Lunge eindringen können. »Deko-Öfen mit Ethanolfeuerung sind eine Quelle für gesundheitsgefährdende Verunreinigungen der Innenraumluft. Um eine gesundheitlich unbedenkliche Luftqualität zu gewährleisten, raten wir dazu, auf den Einsatz dieser Geräte im Innenraum von Wohnungen zu verzichten. Sie sollten nur in großen und sehr gut gelüfteten Räumen betrieben werden«, resümiert Wensing.

Ein anderes Bild ergab sich bei den Tests der Holzkaminöfen, die als zusätzliche Heizung immer populärer werden. In Deutschland unterliegen die Emissionen dieser Heizquellen in die Außenluft strengen gesetzlichen Regelungen. Die Belastungen bewohnter Innenräume – etwa durch undichte Ofentüren – wurden bisher vernachlässigt. Daher haben die Forscher vom WKI sieben Öfen vor Ort in Wohnungen unter realen Bedingungen untersucht. Im Fokus standen auch hier flüchtige organische Verbindungen, Fein- und Ultrafeinpartikel sowie Verbrennungsprodukte wie Kohlendioxid, Kohlenmonoxid, Formaldehyd und Stickstoffdioxid. Das Ergebnis: Solange die Ofentür geschlossen ist, beeinflussen die Öfen die Luftqualität im Innenraum nur geringfügig. Lediglich beim Nachlegen von Feuerholz und beim Anzünden gelangen Emissionen in die Raumluft. Dann konnten die Forscher einen kurzfristigen Anstieg der Konzentrationen messen. »Im geschlossenen Betrieb werden Substanzen nicht in nennenswerter Höhe freigesetzt. Beispielsweise sind die Werte für Formaldehyd unbedenklich«, sagt Wensing. Einzige Ausnahme: Bei einem der Öfen haben die Forscher sehr hohe Konzentrationen von 72 Mikrogramm/m³ von Benzol festgestellt. Den Anstieg führen sie jedoch auf den Gebrauch des paraffinhaltigen Anzünders zurück. Zum Vergleich: Beim Anzünden dieses Ofens mit Papier lag der Wert nur bei 8 Mikrogramm/m³. »Solange die Ofentür und der Aschekasten gut abgedichtet sind, ist nicht mit gesundheitlichen Beeinträchtigungen zu rechnen. Die Lüftungsklappen sollten so eingestellt sein, dass der Ofen gut zieht und auf paraffinhaltige Anzünder sollte man verzichten«, so Wensing.

Ethanolkamine verbreiten eine behagliche Atmosphäre. Doch ihre Schadstoffemissionen sind erheblich. (© Fraunhofer WKI/Manuela Lingnau) | Bild in Farbe und Druckqualität: www.fraunhofer.de/presse

Fraunhofer-Institut für Holzforschung WKI, Wilhelm-Klauditz-Institut | Bienroder Weg 54E | 38108 Braunschweig | www.wki.fraunhofer.de
Kontakt: Dr. Michael Wensing | Telefon +49 531 2155-331 | michael.wensing@wki.fraunhofer.de
Presse: Simone Peist | Telefon +49 531 2155-208 | simone.peist@wki.fraunhofer.de

Fraunhofer

Zentrale Biobank für die Medikamentenforschung

Mit Hilfe von menschlichen Stammzellen bewerten Wissenschaftler, wie Patienten auf neue Medikamente reagieren und untersuchen, wie Krankheiten entstehen. Seit ein paar Jahren ist es möglich, durch Rückprogammierung Stammzellen, die noch alle Zelltypen des menschlichen Körpers bilden können, aus Gewebeproben erwachsener Menschen künstlich zu erzeugen. Davor war die Pharmaforschung auf adulte Stammzellen oder Primärzellen mit einem eingeschränkten Potential angewiesen. Eine andere Möglichkeit wäre die Verwendung von humanen embryonalen Stammzellen. Neben den moralischen Bedenken stehen diese allerdings nur in begrenzter Vielfalt zur Verfügung. Das neue Verfahren erlaubt zum Beispiel Haut- oder Blutzellen von erwachsenen Menschen biologisch so umzuprogrammieren, dass sie sich ähnlich verhalten, wie embryonale Stammzellen und sich in jeden beliebigen Zelltyp umwandeln lassen. »Man spricht von induzierten pluripotenten Stammzellen, abgekürzt iPS-Zellen«, sagt Dr. Julia Neubauer vom Fraunhofer-Institut für Biomedizinische Technik IBMT in St. Ingbert. »In den letzten Jahren sind immer mehr lokale Biobanken entstanden. Keine davon erfüllt jedoch die Anforderungen von Pharmaindustrie und Forschungseinrichtungen: Diese benötigen die Stammzellen ›Ready-to-use‹. Das bedeutet in großer Zahl, konsistent charakterisiert, in ausreichender Qualität und systematisch katalogisiert.«

Zusammen mit 26 Partnern aus Wirtschaft und Forschung hat das IBMT Anfang des Jahres ein Projekt zum Aufbau einer zentralen »European Bank for induced pluripotent Stem Cells (EBiSC)« gestartet, einer Biobank für iPS-Zellen von Patienten mit spezifischen Krankheitsbildern (http://ebisc.org). Bereits nach sechs Monaten Projektlaufzeit stehen erste Zellen zur Verfügung, die zur Entwicklung neuer Medikamente genutzt werden können. Ziel ist es, nach drei Jahren über 1.000 definierte und charakterisierte Zelllinien mit hundert Millionen Zellen anzubieten. Diese Größe ist nötig, da für ein einzelnes Wirkstoffscreening bereits mehrere Millionen Zellen getestet werden müssen. Die Biobank entsteht vor den Toren Londons, ein identisches – »gespiegeltes« – Pendant zum IBMT-Standort in Sulzbach/Saar.

Zellen werden schonend eingefroren

Das IBMT wurde aufgrund seiner umfassenden Expertise in den EU-Projekten »Hyperlab« und »CRYSTAL« für EBiSC engagiert. Die Wissenschaftler kümmern sich um das Einfrieren der Zellen und die Automatisierung der Zellkultivierung und Biobank. Stammzellen müssen auf unter minus 130 Grad Celsius abgekühlt werden, damit sie über einen längeren Zeitraum überleben. Um den Kälteschock im gasförmigen Stickstoff zu überstehen, präparieren sie die Wissenschaftler entsprechend. Das IBMT hat beispielsweise Technologien entwickelt, die es erlauben, die Zellen extrem schonend einzufrieren. »Zellen mögen es nicht, wenn sie von der Oberfläche entfernt werden, auf der sie wachsen. Bisher war das für das Einfrieren jedoch nötig. Bei unserer Methode können die Zellen auf der Kulturoberfläche haften bleiben«, schildert Neubauer.

Genau wie bei Lebensmitteln ist auch bei Stammzellen eine geschlossene Kühlkette besonders wichtig für deren Funktion und Haltbarkeit. Die Wissenschaftler bewahren Zellen in etwa 2x1 Meter großen Behältern, sogenannten Kryotanks, auf. Diese müssen die Wissenschaftler öffnen, wenn sie eine Probe entnehmen wollen. Das Problem: Bei offenem Behälter kommen auch die anderen Röhrchen mit der wärmeren Raumluft in Kontakt und tauen auf. »Das ist genau wie daheim im Kühlschrank. Auch dessen Tür sollte nicht zu lange offen stehen«, sagt Neubauer. Zusammen mit ihren Kollegen am IBMT und dem Industriepartner Askion GmbH hat sie eine Stammzell-Biobank mit Schutzhauben entwickelt, die andere Proben schützt, wenn der Behälter geöffnet wird. So bleibt die Temperatur und auch die Luftfeuchtigkeit – ein weiteres wichtiges Haltbarkeitskriterium – konstant.

Ähnlich wichtig wie das einwandfreie Einfrieren ist, dass die Prozesse automatisch ablaufen. »Das sichert die Konsistenz und macht es erst möglich, große Zellmengen in angeforderter Qualität bereit zu stellen«, so Neubauer. Bei der Kühlung können die Wissenschaftler bereits eine fertige Technologie vorweisen: In ihrer automatischen Biobank ist jedes Zellröhrchen mit Barcodes versehen, um sie nachverfolgen zu können. Die Proben werden auf einem Laufband zu den einzelnen Kühlbehältern transportiert. Ein Computer überwacht den gesamten Einfrier- und Lagerprozess.

An der Automatisierung der Zellkultivierung, dem Vermehren der Zellen, arbeiten die Wissenschaftler gerade. Hier gibt es grundsätzlich zwei Ansätze: mit Robotern, die jede manuelle Bewegung in maschinelle umsetzen oder in gerührten Bioreaktoren, in denen die Zellen frei beweglich optimal mit Nährstoffen und Sauerstoff versorgt werden. Das IBMT hat beide Technologien im Portfolio. »Bis zum Ende des Projekts werden wir wissen, welche Methode sich am besten für unsere Zwecke eignet«, sagt Neubauer.

Die Biobank besteht aus drei Kryotanks mit gekühlten Schutzhauben und einer Transferstation, von der aus die Probenbehälter über ein Schienensystem transportiert werden. Insgesamt haben ungefähr 60.000 Proben Platz. (© Fraunhofer IBMT) | Bild in Farbe und Druckqualität: www.fraunhofer.de/presse

Fraunhofer-Institut für Biomedizinische Technik IBMT | Ensheimer Straße 48 | 66386 St. Ingbert | www.ibmt.fraunhofer.de
Kontakt: Dr. Julia Neubauer | Telefon +49 6894 980-258 | julia.neubauer@ibmt.fraunhofer.de
Presse: Dipl.-Phys. Annette Maurer | Telefon +49 6894 980-102 | annette.maurer@ibmt.fraunhofer.de

Fraunhofer

Mehr Sicherheit auf europäischen Bahnhöfen

Der Zug fährt in wenigen Minuten. Doch in dem Gewimmel des Bahnhofs ist es alles andere als leicht, schnell zum richtigen Gleis zu gelangen. Es ist unübersichtlich und die vollen Bahnsteige machen den Reisenden zu schaffen. Aber auch Sicherheitsexperten, Bahnmitarbeiter sowie Polizei und Feuerwehr kommen ins Schwitzen. Zum Beispiel, wenn sie eine gesuchte Person verfolgen oder ein Verdächtiger einen Koffer unbewacht stehen gelassen hat. Die Bahnhöfe setzen IT-Systeme ein, die ihre Kunden vor Gefahren schützen sollen. Allerdings gibt es dabei ein Problem: Oft ist nicht nur ein Bahnhof oder ein einziger Nahverkehrsbetreiber bedroht. Da der Einsatz dieser IT nicht zentral koordiniert wird, sind die Systeme innerhalb einer Stadt meist nicht kompatibel zueinander. Sich in kritischen Situationen auszutauschen und Hand in Hand zu reagieren, ist schwierig.

Technologien, die sich »verstehen«

Das Projekt Secur-ED soll aufzeigen, wie die organisatorische und informationstechnische Zusammenarbeit innerhalb von europäischen Großstädten verbessert werden kann – und das bei verschiedenen Bedrohungen und unterschiedlichen Randbedingungen. Das Kürzel steht für Secure Urban Mass Transportation – European Demonstrator. Mit 39 Partnern und einem Budget von 40,2 Millionen Euro ist es eines der größten Demonstrationsprojekte der europäischen Sicherheitsforschung. »Da es in den meisten Großstädten bereits viele Sensoren – etwa Videokameras – und Leitstellen für Sicherheit im Nahverkehr gibt, haben wir zunächst analysiert, worin die Aufgaben der beteiligten Partner sowie der vorhandenen IT-Systeme liegen«, sagt Dr. Wolf Engelbach, Projektleiter am Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO. »Dazu haben wir ein Interoperabilitätskonzept entwickelt: Es beschreibt, wie die Beteiligten ihre Informationen in kritischen Situationen bestmöglich austauschen können. Darauf aufbauend lassen sich dann konkrete Formate, die den Austausch regeln, ausarbeiten und implementieren.« Damit die Sicherheitsbehörden ihre Informationen besser miteinander teilen und Vorgehensweisen besprechen können, haben die Forscher zusätzlich einen Multitouch-Tisch gebaut: Nach außergewöhnlichen Ereignissen können die Beteiligten Daten auswählen, den Partnern bereitstellen und die Lage gemeinsam auswerten.

Testläufe in Berlin, Madrid, Mailand und Paris

Die neuen Lösungen von Secur-ED haben die Forscher mit den Partnern zu integrierten Lösungen verbunden – abgestimmt auf die Bahnhöfe und Schienennetze in Berlin, Madrid, Mailand und Paris – und sie dort in Testläufen erprobt. So schlich sich in Mailand ein »Unbefugter« auf ein Bahndepot, was die Mitarbeiter in der »Leitstelle« mit Hilfe einer Wärmekamera sowie einer Zoom-Kamera sofort erkennen konnten. In einem anderen Szenario wurde ein Fahrgast von einem Busfahrer als verdächtig eingestuft und der Zentrale gemeldet. Obwohl er am Bahnhof ausstieg, konnten die Ange-

stellten in der Leitstelle ihn im Auge behalten – dank einer neuen Software. Sie mussten die verdächtige Person lediglich auf einem Kamerabild markieren. Die Software errechnet dann automatisch, wohin der Gesuchte sich bewegen dürfte und schlägt dem Mitarbeiter von den insgesamt 300 Kameras diejenige vor, die die Person im Anschluss erfasst.

Auch bei der Fahndung nach Personen könnte die Polizei künftig auf die Ergebnisse des Projekts setzen: So haben die Forscher in Madrid das Bild einer gesuchten Person via LTE, also über das Mobilfunknetz, an die städtischen Busse übertragen. Kameras in den Bussen verglichen die Gesichter der einsteigenden Fahrgäste mit dem der gesuchten Person. Stimmte das Gesicht überein, gab das System eine automatische Nachricht an den Busfahrer sowie an die Leitstelle aus.

So zahlreich die Übungen auch waren – die Projektpartner können nicht alle Entwicklungen in allen Varianten durchspielen. Daher haben die Forscher am IAO in Stuttgart zusätzlich Vorschläge entwickelt, wie verschiedene Szenarien ergänzend nachgestellt werden können. Dazu gehören beispielsweise agentenbasierte Simulationen und Berechnungen zur Gasausbreitung, um Evakuierungen zu planen sowie Kameras und Sensoren zu platzieren.

Die Abschlusskonferenz von SECUR-ED (www.secur-ed.eu) findet am 17. September in Brüssel statt. Zudem wird das Projekt vom 16. bis 18. September auf der Sicherheitsforschungskonferenz Future Security 2014 (www.future-security2014.de) in Berlin präsentiert.

Das EU-Forschungsprojekt Secur-ED soll für mehr Sicherheit auf europäischen Bahnhöfen sorgen. Hier sind Feuerwehrleute bei einem Testlauf in Madrid zu sehen. (© Secur-ED) | Bild in Farbe und Druckqualität: www.fraunhofer.de/presse

Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO | Nobelstr. 12 | 70569 Stuttgart | www.iao.fraunhofer.de
Kontakt: Dr. Wolf Engelbach | Telefon +49 711 970-2128 | wolf.engelbach@iao.fraunhofer.de
Presse: Juliane Segedi | Telefon +49 711 970-2124 | juliane.segedi@iao.fraunhofer.de

Fraunhofer

FORSCHUNG KOMPAKT
09 | 2014 || Thema 5

Simulationen für bessere transparente Oxidschichten

Sei es beim Smartphone, dem Tablet-PC oder dem Fahrkartenautomaten – viele Geräte werden heutzutage per Touchscreen bedient. Basis dieser Bildschirme sind spezielle Oxidschichten: Sie sind transparent und leiten elektrischen Strom. Experten sprechen auch von TCO-Schichten, kurz für transparent conducting oxides. Auch auf Solarzellen und in beheizbaren Fenstern leisten diese TCOs gute Dienste. Um mit neuen Produkten und Anwendungen Schritt halten zu können, entwickeln die Hersteller die Schichten ständig weiter: Sie sollen elektrischen Strom gut leiten und möglichst durchsichtig sein – schließlich sollen die Nutzer beim Display eines Tablet-PCs oder Smartphones durch die Schicht hindurch erkennen, was der Bildschirm anzeigt. Ein zusätzlicher Schimmer durch das Oxid würde dabei stören. Auch bei Solarzellen darf die Oxidschicht das Sonnenlicht nicht abschirmen, sondern muss es ungehindert in die Zelle lassen. Für neu entwickelte Oxidschichten sind somit Transparenz und Leitfähigkeit der Dreh- und Angelpunkt. Aber auch die Herstellungstemperatur und die Verformbarkeit der Schichten spielen eine Rolle.

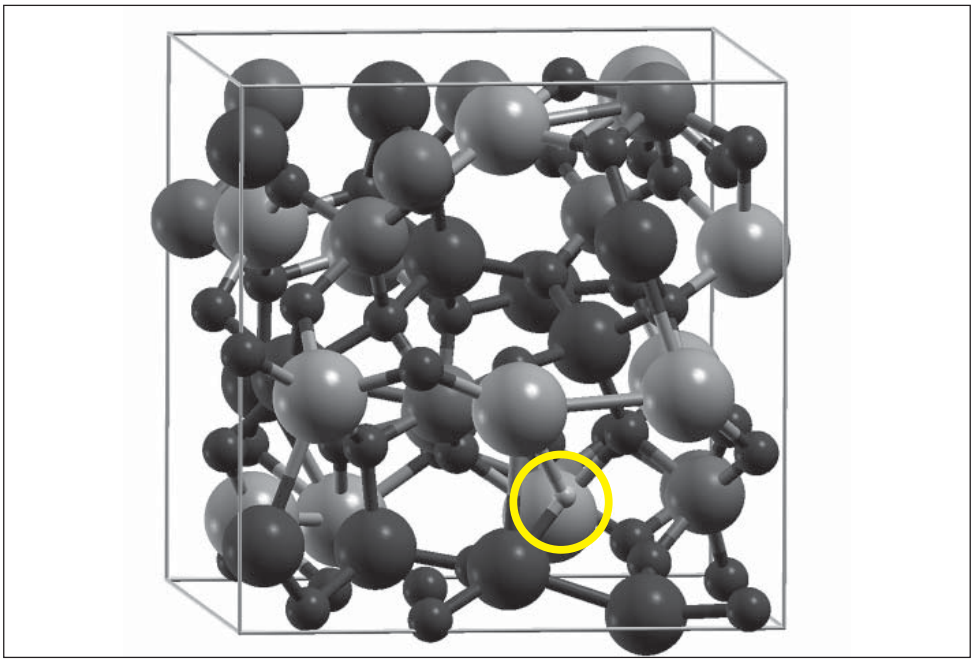
Die Atomstruktur realitätsnah simulieren

Forscher am Fraunhofer-Institut für Werkstoffmechanik IWM in Freiburg unterstützen die Hersteller beim Optimieren der Oxidschichten. »Wir haben eine effektive und anwendungsorientierte Methode entwickelt, um die Eigenschaften von TCO-Schichten zu simulieren«, sagt Dr. Wolfgang Körner, Wissenschaftler am IWM. Der Clou: Die Wissenschaftler simulieren die Atomstruktur der Schichten besonders realitätsnah und unter Berücksichtigung von allen möglichen atomaren Fehlern – egal ob es sich dabei um ungeordnete amorphe oder kristalline, sehr geordnete Strukturen handelt. Anhand dieser Simulationen untersuchen sie, wie gut sich die Elektronen in der Schicht bewegen können, also wie gut das Oxid elektrischen Strom leitet. »Wir können gezielt nachverfolgen, wie sich die elektronische Zustandsdichte verändert, wenn wir die atomare Struktur der Schicht ändern«, erläutert Körner. Die Forscher können ebenfalls beantworten, ob das Licht absorbiert wird, oder ob es die Schicht ungehindert passiert und sie durchsichtig erscheinen lässt. »Wir verlagern die Trial-and-Error-Materialversuche in den Computer und können so viel schneller und kostengünstiger die Eigenschaften abschätzen, die die jeweilige Stoffzusammensetzung des betrachteten TCOs hat«, sagt Wolfgang Körner. In seinen Projekten vergrößert er das Verständnis dafür, wie die jeweiligen Eigenschaften der Oxidschichten entstehen. Dieses Verständnis hilft seinen Industriepartnern, ihre Produktionen zu verbessern oder gewünschte Oxidschicht-Eigenschaften zu erhalten.

Die wesentlichen Defekte, die in solchen Schichten auftreten, konnten die Forscher bereits finden. Die Strukturen lassen sich nie ganz fehlerfrei fertigen: Zwar sollten sie nur aus bestimmten Atomen bestehen, beispielsweise aus Zink, Zinn und Sauerstoff. Doch mogeln sich immer mal wieder auch andere Atome mit hinein, etwa Wasserstoff-

atome – und verändern somit die Leitfähigkeit und die Transparenz der Schicht. Doch welche Defekte im atomaren Aufbau mindern die Transparenz? Und wie kann man diese Defekte beseitigen und den Oxiden somit zu mehr Durchsichtigkeit verhelfen? Die Forscher fanden unter anderem heraus, dass es bei bestimmten Oxiden hilft, sie einmal zu geeignet hohen Temperaturen aufzuheizen oder in sauerstoffreicher Umgebung zu erwärmen.

In einem zweiten Ansatz drehen die Wissenschaftler den Spieß um: Sie fügen verschiedene Atome gezielt in die Struktur ein und simulieren, welche Auswirkungen das auf die Eigenschaften hat. Hierbei ist das Ziel, die Leitfähigkeit und die Transparenz mit den passenden »Verunreinigungen« noch weiter in die Höhe zu treiben und so ein Material im Computer designen zu können.



Modell-Ausschnitt einer amorphen Oxidschicht, in die gezielt Wasserstoff-Atome eingebracht wurden. Wasserstoff ist unten rechts als kleinste, eingekreiste Kugel zu sehen; der Sauerstoff ist durch kleine Kugeln repräsentiert; die großen Kugeln stehen für Indium, Zinn und Gallium. (© Fraunhofer IWM) | Bild in Farbe und Druckqualität: www.fraunhofer.de/presse

Fraunhofer-Institut für Werkstoffmechanik IWM | Wöhlerstraße 11 | 79108 Freiburg | www.iwm.fraunhofer.de
Kontakt: Dr. Wolfgang Körner | Telefon +49 761 5142-374 | wolfgang.koerner@iwm.fraunhofer.de
Presse: Katharina Hien | Telefon +49 761 5142-154 | katharina.hien@iwm.fraunhofer.de

Fraunhofer

Fingerabdruck für Frachtstücke

Tausende Frachtstücke werden täglich mit dem Flugzeug transportiert – rund 70 Prozent davon in Passagiermaschinen. Strengste Kontrollen sollen verhindern, dass gefährliche Substanzen wie Sprengstoff an Bord geschmuggelt werden. Prüfverfahren, etwa das Röntgen der Fracht, sind aber zeit- und kostenaufwändig und müssen wiederholt werden, wenn Verdachtsmomente aufkommen. Bisher fehlen einfach überprüfbare Merkmale, um den »sicheren« Status eines Frachtstücks nachzuweisen.

Forscher des Fraunhofer-Instituts für Fabrikbetrieb und -automatisierung IFF in Magdeburg arbeiten im Verbundprojekt ESecLog mit Entwicklungspartnern und Anwendern wie Panalpina und Lufthansa Cargo daran, das Dilemma zwischen Sicherheit und Effizienz zu lösen: Mit Hilfe einfacher Prüfverfahren fassen sie für jedes Frachtstück Merkmale wie 3D-Kontur oder RFID-Kennung zu einem zentralen Sendungsprofil zusammen. »Der Clou ist, dass wir diese Merkmale dokumentieren und zu einem digitalen Gesamtbild zusammenfügen. Jedes Frachtstück verfügt damit über einen digitalen Fingerabdruck. Dieser lässt während der gesamten Transportkette prozessübergreifend und jederzeit genaue Aussagen über den Sicherheitsstatus der Fracht zu«, erläutert Olaf Poenicke, Projektleiter am IFF.

Sicherungsdraht verhindert nachträgliche Manipulationen

So arbeiten die Partner etwa an einem Marker, mit dem sich überprüfen lässt, ob ein Frachtstück bereits geröntgt wurde – bislang ist das nicht nachvollziehbar. Die Forscher entwickeln zudem ein RFID-Siegel, um nachträgliche Manipulationen an einer Sendung zu erkennen. Dazu positionieren sie einen Transponder mit einem hauchdünnen Sicherungsdraht an den Sollbruchkanten eines Pakets. Wird es geöffnet, zerreißt der Draht. Die Sendung ist dann zwar weiterhin identifizierbar, zusätzlich erhält der Kontrolleur aber die Information, dass der Draht beschädigt ist. »Mit dieser Technologie lassen sich auch ganze Paletten prüfen. Befindet sich ein Frachtstück mit gebrochenem Draht darunter, lässt sich die betroffene Sendung über die ID genau identifizieren«, so Poenicke. Zusätzlich kann mittels 3D-Scan die Kontur der Palette erfasst werden. Wird nachträglich ein Packstück auf die Palette gelegt, ändert sich die Kontur.

All diese Informationen sollen in einer Art Sendungshistorie zusammengefasst werden. Im zentralen Fingerprint-Informationssystem wird den Kontrolleuren diese Dokumentation als Zeitstrahl auf einem Tablet zur Verfügung gestellt. Bei Bedarf können sie zusätzliche Informationen zu den einzelnen Stationen abrufen und sich etwa nochmals alle Röntgenbilder anzeigen lassen. Mit dieser Technik soll der Aufwand bei Nachkontrollen drastisch reduziert werden. Bislang muss bei einem Manipulationsverdacht jedes Frachtstück nochmals einzeln geprüft oder gar geöffnet werden. Poenicke erläutert, wie das im ungünstigsten Fall aussehen kann: »Oft erfolgt die Zulieferung auf dem Landweg. Gilt die Ladung bereits als sicher, wird der LKW vor dem Transport versiegelt.

Stellt man dann am Flughafen fest, dass das Siegel gebrochen wurde, muss der gesamte Inhalt nochmal kontrolliert werden«. Mit den ESecLog-Lösungen ließe sich in einem solchen Fall schnell überprüfen, ob einzelne Packstücke manipuliert worden sind.

Bis die Verfahren zum Einsatz kommen, wird es indes noch dauern: Nachdem das Konsortium die einzelnen Lösungen konzipiert hat, befinden sich die Technologien nun in der Entwicklungsphase und sollen bis Ende des Jahres einsatzbereit sein. Im kommenden Jahr soll dann eine Testumgebung entstehen, um das Zusammenspiel der Verfahren zu optimieren. Die Forscher des Fraunhofer IFF stellen das Projekt auf dem Deutschen Logistik-Kongress vom 22. bis 24. Oktober in Berlin vor. ESecLog wird vom Bundesministerium für Bildung und Forschung (BMBF) gefördert.

Verladen von Luftfracht. Im Projekt ESecLog arbeiten Forscher des Fraunhofer IFF mit weiteren Partnern an einem digitalen Fingerabdruck für die sicherheitssensible Luftfracht. So sollen künftig Manipulationen an den Sendungen leicht erkennbar sein. (© Fraunhofer IFF/Anna Mahler) | Bild in Farbe und Druckqualität: www.fraunhofer.de/presse

Fraunhofer-Institut für Fabrikbetrieb und -automatisierung IFF | Sandtorstraße 32 | 39106 Magdeburg | www.iff.fraunhofer.de
Kontakt: Olaf Poenicke | Telefon 49 391 4090-337| olaf.poenicke@iff.fraunhofer.de
Presse: Anna-Kristina Mahler | Telefon +49 391 4090-446 | anna-kristina.mahler@iff.fraunhofer.de