U.S.-GERMAN STANDARDS PANEL 2018

Securing Future Technologies – Cybersecurity and Other Challenges and Solutions for Smart Manufacturing, Mobility and Agriculture

U.S.-GERMAN STANDARDS PANEL 2018

Securing Future Technologies – Cybersecurity and Other Challenges and Solutions for Smart Manufacturing, Mobility and Agriculture

→ For presentations, please refer to:
www.din.de/de/din-und-seine-partner/public-affairs/aktuelles/u-s-german-standards-panel-agenda-und-praesentationen-271682

PROGRAM

APRIL 09th

RESTAURANT: Darlington House,
1610 20th St NW, Washington, DC

WELCOME DINNER

8 _ ***Address:***
Dr. Thomas Zielke, *Head of Division Responsible for Technology Transfer via Standardization and Patents, General Issues of Standardization and Patent Policy,* ***Federal Ministry*** *for Economic Affairs and Energy (BMWi)*

APRIL 10th

VENUE: FHI 360 Conference Center,
Academy Hall, 1825 Connecticut Avenue
NW, Washington, DC

WELCOME ADDRESS

10 _ ***Joe Bhatia,*** *President and CEO, ANSI*

WELCOME ADDRESS

11 _ ***Christoph Winterhalter,*** *Chairman of the Executive Board, DIN*

WELCOME ADDRESS

12 _ ***Thomas Sentko,*** *Standards Manager International, DKE*

KEYNOTE SPEECH

13 _ **Deloitte Technology Trend Study**
Scott Buchholz, *Chief Technology Officer for the Deloitte Federal Division of Deloitte Consulting, LLP*

1. SHORT PRESENTATIONS AND Q&A

Moderator:
Sibylle Gabler, *Head of Government Relations, DIN*

APPROACHES TO CYBERSECURITY

14 _ **The NIST Cybersecurity Framework**
Adam Sedgewick, *Senior IT Policy Advisor, Information Technology Laboratory, NIST*

15 _ **European Regulation on Cybersecurity and Data Protection**
Peter Fatelnig, *Minister-Counsellor for Digital Economy Policy, Trade & Agriculture Section, Delegation of the European Union to the United States of America*

15 _ **International Legal Regulation of Cybersecurity**
Dr. Dennis-Kenji Kipker, *Scientific Managing Director, University of Bremen, Project Manager at CERT@VDE*

2. BREAKOUT SESSIONS
2.1 SMART MANUFACTURING

Moderator:
Alec McMillan, *IEC SEG 7 on Smart Manufacturing Co-Convenor*

2.2 SMART MOBILITY

Moderator:
Steven Sill, *Intelligent Transportation Systems (ITS) Architecture and Standards Program Manager, ITS Joint Program Office (JPO), U.S. Department of Transportation*

2.3 SMART AGRICULTURE

Moderator:
Dorothee Töreki, *Digitization Advisor, IBM Cognitive Collaboration and Talent Solutions*

28 _ **Farming 4.0 Delivers Basic Data for the Future Transport Food Chain – 365FarmNet Concept, a European Example**
Klaus-Herbert Rolf, *Governmental Affairs Manager, 365FarmNet Group*

29 _ **The Role of Standards in Smart Farming**
Timothy West, *Manager, Enterprise Engineering Standards, Deere & Co.*

RECEPTION AND DINNER

Teddy & The Bully Bar
1200 19th Street NW,
Washington, DC

30 _ ***Address:***
Otto Graf, *Counselor for Development, World Bank, IDB, Embassy of the Federal Republic of Germany*

APRIL 11th

REPORTS FROM THE BREAKOUT SESSIONS

CYBERSECURITY IN SMART MANUFACTURING, SMART MOBILITY AND SMART AGRICULTURE

21 _ Smart Manufacturing: ***Alec McMillan***
25 _ Smart Mobility: ***Steven Sill***
29 _ Smart Agriculture: ***Dorothee Töreki***

OPEN DISCUSSION

Moderator:
Joseph Tretler, *Vice President for International Policy, ANSI*

NEXT STEPS AND TRANSATLANTIC COOPERATION IN THE STANDARDIZATION OF SMART MANUFACTURING, SMART MOBILITY AND SMART AGRICULTURE

PRESENTATION AND PANEL DISCUSSION

Moderator:
Gordon Gillerman, *Director Standards Coordination Office, NIST*

STANDARD DEVELOPMENT ORGANIZATIONS AND CONFORMITY ASSESSMENT IN CYBERSECURITY

32 _ **Cybersecurity and Standards: A Safe Connected World**
Miguel Bañón, *Managing Director, Epoche & Espri – a DEKRA company, DEKRA e. V.*

33 _ **Security Is the New Safety**
Ingo M. Rübenach, *Vice President, Central, East & South Europe, Underwriters Laboratories (UL)*
Sonya Bird, *International Standards Manager, Underwriters Laboratories (UL)*

PANELIST: Christoph Winterhalter, *Chairman of the Executive Board, DIN*
PANELIST: Dr. Jens Gayko, *Head of Standardization Council Industrie 4.0*

CLOSING REMARKS

34 _ ***Joe Bhatia,*** *President and CEO, ANSI*
34 _ ***Christoph Winterhalter,*** *Chairman of the Executive Board, DIN*
34 _ ***Thomas Sentko,*** *Standards Manager International, DKE*

WELCOME DINNER

APRIL 09th

Dr. Thomas Zielke, Thomas Sentko, Joe Bhatia, Christoph Winterhalter

Dr. Anne Kleinschrodt, Peter Fatelnig

Dorothee Töreki, Stephan Voit

Dr. Jens Gayko

Prof. Dr. Volker Skwarek, Alec McMillan, Thomas Sentko

Rüdiger Marquardt

Volker Jacumeit, Klaus-Herbert Rolf, Tom Lusco

Allison Barnard Feeney, Dr. Bradley D. Taylor

Mario Beier

Timothy West, Klaus-Herbert Rolf

Peter Fatelnig, Sibylle Gabler

Matthias Kuom, Dr. Dennis-Kenji Kipker

Dr. Thomas Zielke, Joseph Tretler

Craig Rodine

Steven Cornish, Klaus-Herbert Rolf

OPENING REMARKS

Dr. Thomas Zielke
Head of Division Responsible for Technology Transfer via Standardization and Patents, General Issues of Standardization and Patent Policy, Federal Ministry for Economic Affairs and Energy (BMWi)

→ I am happy to be back in Washington today. Thank you for the invitation! I already had the honor of contributing to the last U.S.-German Standards Panel in 2016. Same occasion, same place, same speaker: it seems that the standards community favors continuity.

But there have been differences and changes since 2016. One of them is my new perspective. At that time, I was appointed as Representative of the German and Transatlantic Businesses, the Federation of German Industry and the German Chambers of Commerce and Industry here in Washington. I returned to Berlin in July 2016 after more than seven wonderful years in DC. I did not know at the time that I would be responsible for standardization, technology transfer and patents in the Federal Ministry for Economic Affairs and Energy.

I am happy to build up on the old connections to this conference format today and I would therefore like to greet you now on behalf of the German Government. The Federal Government takes your topics very seriously.

You know that it took Germany longer than usual to form a new administration after the election in September 2017. The parties involved are the same, but the ministers have changed. The coalition agreement, which is politically binding among ruling parties, sets the political framework for the next four years, and it also explicitly emphasizes standardization. This is unusual, but not too much, since standards have increasingly become a part of trade policy in a positive but sometimes also in a negative sense. The latter becomes evident when they are used to build up walls. In particular, the new Federal Government, collaborating with the German and European standardization organizations, intends to strengthen and to promote international cooperation in standardization. At the same time, small and medium-sized enterprises should also be equipped with better opportunities to participate.

This idea of international cooperation in standardization is essential for us. After all, cooperation in the removal of technical barriers to trade, the harmonization of standards and recognition of test procedures are aspects of trade policy that have become much more important. The general situation tells us as much: we witness some major shifts in international trade relations, and this should not affect the world of standards or technical rules.

We have not come to a Transatlantic Trade and Investment Partnership (TTIP) agreement, at least not for the time being. The Trans-Pacific Partnership (TPP) will likely come, but in a different setting. Peter Altmaier, the German Minister for Economic Affairs, came to Washington on March 19th and 20th. He met with Secretary of Commerce Wilbur Ross and Unites States Trade Representative Robert Lighthizer. Furthermore, in a coordinated effort with EU Commissioner for Trade Cecilia Malmström, he accomplished that the EU would be – at least for a certain timeframe – exempted from the imposed higher duties on steel and aluminum. Additionally, a constructive dialogue between the United States and the EU on even more relevant trade questions and problems has been agreed upon. Minister Altmaier has also pointed out publicly that the bilateral relations with the U.S. are of the most importance to Germany and that common interests outweigh current problems.

Yet the businesses and all stakeholders involved in standardization will have to find solutions for the ongoing changes in technology, digitization, and industry 4.0. In these respective fields, the United States and Germany will have not only the possibility but rather the obligation to shape conditions. We must not just react to current challenges or even refuse to shape tomorrow's world, but act.

It is good to see that the International Organization for Standardization (ISO) has adopted its willingness to be "open-minded and open for change," as was the motto of ISO's last General Assembly hosted by the German national standardization body DIN in Germany in September 2017. We have every reason to look not only to ourselves, but to be outgoing instead: technological changes that require common standards happen likewise in our home countries as they do in other countries. We therefore have intensified our efforts to help advise and collaborate with partners all over the world accordingly. Existing projects have been expanded and new ones we have established or are currently being established. The German Government supports the national standardizations bodies DIN and DKE in that respect and works hard in strengthening the European standardization scheme as well as contributing to it.

But there are other parts of the world. In China, new standardization and cybersecurity laws have been adopted. Many international stakeholders have previously acknowledged that progress has been made. However, the bill leaves many questions unanswered, and in some areas, e.g. concerning the definition of legal terms, it is still unclear whether the overall impact of the law will be positive or negative. The German-Chinese Commission for Standardization (DCKN), a joint initiative of DIN and the Standardization Administration of the People's Republic of China (SAC), has been working on several topics for many years, including industry 4.0 and electromobility. We want to build trust here, but also to convey our idea of fair treatment in matters of technology transfer and in the development and implementation of standards.

With regards to the collaboration on international standards with India, we contributed by submitting a collective statement to the Indian Standards Conclave. The Conclave's goal is to develop a new standardization strategy for India. As a part of our project "Quality Infrastructure Global," we have been working with India at governmental level and in cooperation with standardization organizations, business associations and companies for many years.

This week, we are traveling to Mexico in order to exchange views on how to intensify the bilateral cooperation in the standardization sector by setting up a newly formed working group. But also issues such as accreditation, certification and market surveillance will be tackled. Mexico is the partner country of this year's International Industrial Fair in Hannover – following the U.S., which was the partner country in 2016.

The Federal Government of Germany also wants to substantiate the new Comprehensive Economic and Trade Agreement (CETA) between the EU and Canada, which from now on will be implemented step by step. CETA expressively calls for coordination and intensified collaboration as well as joined actions in the development and application of standards. Again, the aim is to facilitate the flow of trade and to provide as few obstacles as possible for companies involved in international trade or at least to reduce existing problems.

Of course, the approaching BREXIT also raises concerns with regard to standardization since we do not know whether and – if yes – in what way, the British national standardization body BSI will or will not continue to participate in European standardization cooperation under the EU standardization regulation. We will discuss this informally during the next regular meeting of the joint working group "Tripartite" with our British and French colleagues in June. There is a strong effort from the business community, in particular in the U.K., to keep as many advantages of the single market as possible.

The agenda of this year's U.S.-German Standards Panel clearly indicates where potential fields of cooperation between our institutions lie. Digitization and cybersecurity, in particular the newly enforced EU regulation on data privacy, play an important role as well as the NIST cybersecurity framework. The agenda additionally features a number of related questions concerning cybersecurity and smart manufacturing, smart mobility and smart agriculture. The breakout session on smart mobility for example will tackle questions concerning blockchain technology, charging networks and data privacy – all respective fields in which common standards are needed. In the smart agriculture session, you will focus on an important sector that is set out to improve the efficiency of food production through digitization. There is much to learn here from approaches to modern agriculture. I am excited about every one of these topics and I wish you a great conference that takes us all to where we want to be: to the top of the movement.

WELCOME ADDRESS

Joe Bhatia
President and CEO, ANSI

→ A few years ago, our U.S. Department of Commerce's International Trade Administration, or ITA, issued a report with some really staggering statistics. The report says, as we all know, that standards and conformance play a critical role in the economy. But what they discovered in their analysis is that standards and technical regulations impact a tremendous 93% of global exports.

This "93%" statistic has been an important one for us at ANSI. It has been a powerful tool as we look to get more attention paid to the importance of standardization by U.S. industry and government leaders. Such an impressive figure helps make it crystal clear that globally relevant standards and conformance make a big difference – to market access, the competitiveness, and to companies' bottom lines.

So what do I mean when I say "globally relevant standards?"

The U.S. endorses the globally accepted standardization principles of the World Trade Organization's Technical Barriers to Trade Agreement, which include openness, balance, consensus, and transparency, among many others. We believe that – as long as these principles are followed – a high-quality, globally relevant standard will emerge, regardless of which standards developing organization – or which nation – produced it. We see this global success in a multitude of industry sectors: automotive, aerospace, oil and gas, to name a few.

ISO and IEC are some of the most recognized names in standards development, but it is important to note that other standard developing organizations are also developing high-quality, globally relevant standards, and in some cases, have been doing so for well over a century. And speaking of that, I want to announce that 2018 is ANSI's 100th anniversary. We are thrilled to celebrate this huge milestone: a century of service to the industry, workers, businesses, and the government agencies of the United States.

I want to conclude with a few statistics about why standards and conformance are so important to the continued health of the excellent trade relationship between the U.S. and Germany[1]. In 2017 alone, the U.S. exported nearly 53 billion dollars in goods to Germany, and in turn, imported over 117 billion dollars in goods from them.

Compare these to figures from fifteen years ago, when exports to Germany totaled 28 billion dollars, and imports from Germany were valued at about 68 billion dollars. These figures demonstrate that our German friends started with an advantage and have been able to maintain that edge. Still, I believe we have come a long way in this key trade relationship. And the importance of our relationship is only going to continue to grow.

We are so pleased to have a terrific turn out for today's discussion. We have chosen some very forward-looking topics, including cybersecurity, smart manufacturing, mobility, and agriculture. And we are delighted to have a keynote address from Scott Buchholz of Deloitte, who will be looking at some of these macro tech trends. Scott has been with us before, and I am sure we all will enjoy his comments. Throughout our discussions today I look forward to hearing from all of you, and to continuing to work together in the future. Thank you for your attention.

[1] https://www.census.gov/foreign-trade/balance/c4280.html

WELCOME ADDRESS

Christoph Winterhalter
Chairman of the Executive Board, DIN

→ During our first Standards Panel in 2013, we asked how standards can support the Transatlantic Trade and Investment Partnership (TTIP). We would never have expected that five years later there would be no TTIP and that free trade faces increasing political challenges. In this political environment it is very important and very re-assuring that ANSI and DIN are continuing their tradition of the U.S.-German Standards Panel in bringing together our expert communities. After all, in standardization we are not talking politics, in standardization we are talking technology and business.

So the question from five years ago is still up-to-date – if slightly modified: how can standards best support businesses in international trade? The answer is rather simple: facilitate the making of the best standards and do it internationally. International standards are continuously becoming more important and are being used more intensively around the world. They are our common language of technology. The digitalization of our economies and societies is – for better or worse – international by design. Digitalization can only be successful, secure and beneficial for all with the help of international standards. We are well under way in many areas to set standards that make the cyberspace more secure, facilitate the digital factory and support technology development for smart homes and cars, just to name a few examples. However, a lot of work remains to be done, a lot of good ideas need to be listened to and put into standardization action.

Standardization itself needs to adapt to the challenges and opportunities of increasing digitalization. The German Standardization Strategy, which has been comprised by our stakeholders in 2016, gives us guidance:
"New types of organizational and operational structures with the associated innovative processes for coordination and moderation are necessary to address far-reaching changes [like digital transformation]. Even in a multifaceted standardization landscape with new actors and dynamic processes, established and proven values such as neutrality and the coherence of the body of German standards still remain of central importance. The policy of cooperation and coordination will also be continued in order to maintain the coherence and consistency of the body of German standards (including adopted European and International Standards) with other collections of technical rules (such as those drafted by fora and consortia) but also with those issued by American standards development organizations (SDOs)." DIN and DKE have been given the mandate *"to organize standardization topics and coordinate teamwork beyond the borders of their own organizations, including for fora and consortia and other standards development organizations."* I therefore regard the U.S.-German Standards Panel, besides our engagement in ISO and IEC, as one key element in implementing the goals of our German Standardization Strategy.

I am very much looking forward to listening to you, the expert community in smart manufacturing, smart mobility and smart agriculture, as you gather ideas for possible new projects. Let's seize the opportunity to continue making the best standards for our business communities and our societies on both sides of the Atlantic Ocean!

WELCOME ADDRESS

Thomas Sentko
Standards Manager International, DKE

→ As Joe Bhatia and Christoph Winterhalter have pointed out, we are already working together internationally as standardization organizations and will continue to do so – on both sides of the pond and with other regions around the world, but furthermore beyond the known borders of ISO, IEC and other standards development organizations.

As a member of DKE, the German Commission for Electrical, Electronic and Information Technologies, I am here to represent the German view on electrotechnical standardization. DKE is a part of DIN and focusses on the electrical, electronic and IT-related elements in the sectors already mentioned by Joe Bhatia and Christoph Winterhalter.
We are also part of the VDE, the Association for Electrical, Electronic and Information Technologies, and therefore strongly connected to industry and academia.

Physics, mathematics and the technical foundations of energy and communications technology are the same around the world – it is only regulation, usage and historical developments that differ from region to region. These variating framework conditions may result in distinguished approaches to standardization, especially in cybersecurity, that we want to discuss during this conference. More importantly, we will also address regulatory aspects of standardization. We will focus on IT security aspects of electromobility, industry 4.0 and agriculture. The examples, however, will show that the same aspects are at stake in each of these sectors:

- privacy,
- ownership of data and
- trust in technology, manufacturers and service providers.

With the advancement of the digital transformation and increasing "smartness" in traditional and electrotechnical sectors alike, the importance of these aspects will further increase. To take up Christoph Winterhalter's remarks: standardization, its processes and deliverables will need to change as a result of digitization.

This process will require changes within the industry – standardization's key stakeholder – but also in standardization organizations and the usage of standards. As standardization organizations, we are called upon to accompany and shape these developments in a constructive way and to transform our organizations accordingly. In the future, we will be challenged to deliver our products in machine-readable formats, design a more agile development process for standards and adapt it in accordance to the conditions of the modern job market.

I am happy to be here to join you in the upcoming discussions, the world cafe-style brainstormings and other interesting formats that we have prepared for this U.S.-German Standards Panel. I am looking forward to learning more about your view on the cybersecurity aspects of our future world.

KEYNOTE SPEECH

Deloitte Technology Trend Study

Scott Buchholz
Chief Technology Officer for the Deloitte Federal Division of Deloitte Consulting, LLP

→ Deloitte invites you to read our 2018 Tech Trends, The Symphonic Enterprise. As digital reality, cognitive, and blockchain continue to redefine IT and business, organizations should look to move beyond vertical or horizontal approaches to new technology. Ideally, strategy, technology, and operations should work together, in harmony, across domains and boundaries.

Many companies competing in markets that are being turned upside down by technology innovation are no strangers to discord. Today, digital reality, cognitive, and blockchain – stars of the enterprise technology realm – are redefining IT, business, and society in general. In the past, organizations typically responded to such disruptive opportunities by launching transformation initiatives within technology domains. For example, domain-specific cloud, analytics, and big data projects represented bold, if single-minded, embraces of the future. Likewise, C-suite positions such as "chief digital officer" or "chief analytics officer" reinforced the primacy of domain thinking.

But it did not take long for companies to realize that treating some systems as independent domains is suboptimal at best. Complex predictive analytics capabilities delivered little value without big data. In turn, big data was costly and inefficient without cloud. Everything required mobile capabilities. After a decade of domain-specific transformation, one question remains unanswered: how can disruptive technologies work together to achieve larger strategic and operational goals?

We are now seeing some forward-thinking organizations approach change more broadly. They are not returning to "sins of the past" by launching separate, domain-specific initiatives. Instead, they are thinking about exploration, use cases, and deployment more holistically, focusing on how disruptive technologies can complement each other to drive greater value. For example, blockchain can serve as a new foundational protocol for trust throughout the enterprise and beyond. Cognitive technologies make automated response possible across all enterprise domains. Digital reality breaks down geographic barriers between people, and systemic barriers between humans and data. Together, these technologies can fundamentally reshape how work gets done, or set the stage for new products and business models.

This year, we invite you to look at emerging technology trends from a different angle. When technologies act in unison, we no longer see the enterprise vertically (focused on line of business or isolated industries) or horizontally (focused on business processes or enabling technologies). In the symphonic enterprise, the old lines become blurred, thus creating a diagonal view that illuminates new business opportunities and creative ways of solving problems. For example, in the new core chapter, we discuss how, in the near future, digitized finance and supply chain organizations could blur the lines between the two functions. Sound unlikely? Consider this scenario:

IoT sensors on the factory floor generate data that supply chain managers use to optimize shipping and inventory processes. When supply chain operations become more efficient and predictable, finance can perform more accurate forecasting and planning. This, in turn, allows dynamic pricing or adjustments to cash positions based on real-time visibility of operations. Indeed, the two functions begin sharing investments in next-generation ERP, the Internet of Things, machine learning, and RPA. Together, finance and supply chain functions shift from projects to platforms, which expands the potential frame of impact. Meanwhile, business leaders and the C-suite are increasingly interested only in strategy and outcomes, not the individual technologies that drive them. Does the convergence of finance and supply chain really seem so unlikely?

Of course, some domain-specific approaches remain valuable. Core assets still underpin the IT ecosystem. Cyber and risk protocols are as critical as ever. CIO strategies for running "the business of IT" are valuable and timeless. Yet we also recognize a larger trend at work, one that emphasizes the unified "orchestra" over individual advances in technology.

SHORT PRESENTATIONS AND Q&A:

Approaches to Cybersecurity

MODERATOR: **Sibylle Gabler**, Head of Government Relations, DIN

Adam Sedgewick
Senior IT Policy Advisor,
Information Technology
Laboratory, NIST

The NIST Cybersecurity Framework

→ Adam Sedgewick gave an introduction to the NIST Cybersecurity Framework that was developed to give the industry guidance through standards, guidelines and best practices on how to promote the protection of critical infrastructure. It consists of three main components: the Core, Implementation Tiers, and Profiles.

The Framework Core provides a set of desired cybersecurity activities and informative references organized around particular outcomes. It guides organizations in managing and reducing their cybersecurity risks in a way that complements an organization's existing cybersecurity and risk management processes.

The Framework Implementation Tier describes how cybersecurity risk is managed by an organization. It guides organizations to consider the appropriate level of rigor for their cybersecurity programs, and is often used as a communication tool to discuss risk appetite, mission priority, and budget.

The Framework Profile aligns industry standards and best practices to the Framework Core in an implementation scenario. It supports prioritization and measurement while factoring in business needs.

Using a common and accessible language, the NIST Cybersecurity Framework is understandable by many professionals and adaptable to many sectors and uses. The risk-based approach is enabling best practices to become standard practices and evolves faster than regulation and legislation since it can be updated as stakeholders learn from its implementation.

The feedback from the first few years of implicating the Framework is currently being transferred into an update. Amongst other things, version 1.1 will enhance guidance in applying the Framework to manage cybersecurity within supply chains and for acquisition decisions.

Peter Fatelnig
Minister-Counsellor for Digital Economy Policy, Trade & Agriculture Section,
Delegation of the European Union to the United States of America

European Regulation on Cybersecurity and Data Protection

→ Since the adoption of its cyberstrategy in 2013, the European Commission undertook a number of actions to build a European cybersecurity policy and operational capacity with EU member states, business, civil society and the citizens. Today's cybersecurity package is complemented by regulations for data protection (GDPR), privacy in digital communications (ePrivacy), better global law enforcement schemes and the cooperation across Europe for a single cybersecurity market.

This conversation focusses on two strands which have a bearing on the event topic: a single cybersecurity market through a certification framework for cybersecurity products and the Network and Information Security Directive.

A new mandate for ENISA will turn it into an independent body advising and organizing the strategic coordination and operational cooperation in case of incidents. ENISA will be the central actor in the new cybersecurity certification framework. Europe needs a competitive market for cybersecurity products. Users want to buy cybersecurity products which fit their needs and come from a competitive market place. Certification will give this to users. The certification framework is voluntary, schemes are specific to certain products and certificates are valid across the EU. The process to adopt new certification schemes is transparent, involving standardization organizations, business and member states.

The Directive on Network and Information Security (NIS) will be transposed into national law by May 2018. It builds up member states' cybersecurity capabilities and EU-wide cooperation.

These measures have two effects: rebuild the trust of users and businesses, and increase their readiness to invest in the digitization of society and economy; create a market place for cybersecurity products, a competitive space for certified quality products "made in Europe" or anywhere else, as this certification framework is open to the world. Europe believes in the value of free trade, free digital trade and the free flow of data.

Dr. Dennis-Kenji Kipker
Scientific Managing Director,
University of Bremen,
Project Manager at CERT@VDE

International Legal Regulation of Cybersecurity

→ During the last years, several countries worldwide have started to address cybersecurity issues in their legislation, including Germany, Russia, China, the United States and the European Union as a community of states. I would like to introduce some of the most important cybersecurity regulations which have been adopted in recent years or which will be adopted soon.

In Germany, the IT Security Act (IT-SiG) came into force in 2015. As an amending act, the law changed various existing laws, including the Act on the Federal Office for Information Security (BSIG), as well as the national Telecommunications Act (TKG) and the Act on the Federal Criminal Police Office (BKAG). With the German regulation, new duties, especially for the operators of critical infrastructures, have been established, including technical and organizational measures as well as duties to report IT security incidents to competent authorities. Based on the German legislative act, the European Union (EU) has introduced its Network and Information Security Directive (EU NIS) in 2016 with similar obligations, but now also including digital service providers such as online marketplaces or cloud computing service providers. The NIS Directive will be followed by the EU Cybersecurity Act in 2018, which will establish a new kind of EU-wide cybersecurity certification.

Russia introduced its first Cybersecurity Doctrine in 2000, which was revised in 2016. This directive has formed the legal basis for the new Russian Cybersecurity Law, which came into force in the beginning of 2018. The Russian legal provisions are similar to the European regulation in this

field, but the main goal of the Russian cybersecurity regulation is not focused on economic, but mostly on political and military interests.

The Chinese Cybersecurity Law of 2016 is also relatively new, as well as the "Measures on Security Review of Network Products and Services" catalogue, which is based on this regulation. Chinese cybersecurity legislation addresses two topics: network security as well as data protection. Several measures are taken into account to reach this goal, but the Chinese data protection level is still beyond GDPR in the EU. For foreign companies exporting IT products to China, the cybersecurity review is of high importance, because IT security-certified products will be given priority in the Chinese market.

U.S. regulation for cybersecurity is spread among different branches of industry and levels of legislation; possibilities of self-regulation are also taken into account. Examples in this field are the Health Insurance Portability and Accountability Act (HIPAA, 1996), the Federal Information Security Management Act (FISMA, 2002) or the Cybersecurity Information Sharing Act (CISA, 2015). Insufficient IT security measures of companies in the U.S. may be sanctioned by the FTC.

All in all, there are many different approaches to a regulation of cybersecurity on the international level – it has become a "hot topic" in recent years. While Germany and Europe are trying to address cybersecurity issues as a uniform approach, there are countries like Japan which only focus on specific challenges like IoT security. Nonetheless, the legal development of cybersecurity always has to take into account the international standardization to reach the maximum level of legal certainty through a technical concretization of legal cybersecurity requirements.

Abdourahmane Ndione, Leslie McDermott

Fran Schrotter

John Kulick

Britt Kritzler, Sibylle Gabler

Megan Hayes

Sibylle Gabler, Peter Fatelnig, Dr. Dennis-Kenji Kipker, Adam Sedgewick

Christoph Winterhalter, Joe Bhatia, Thomas Sentko

Diane Haithcock

Dr. Gerhard Steiger, Fred Hayes

Eric Moughler

Alec McMillan, Dr. Jens Gayko, Volker Jacumeit

Dorothee Töreki

BREAKOUT SESSION
SMART MANUFACTURING

MODERATOR: **Alec McMillan**
IEC SEG 7 on Smart Manufacturing Co-Convenor

Prof. Dr. Volker Skwarek
Professor for Technical Computer Science at the Hamburg University of Applied Sciences (HAW)

The Role of Smart Contracts in Smart Production Blockchains for Mass Transactions: Standardization of Interfaces for Blockchain-like Sensor Networks Within (I)IoT Systems

→ Industry 4.0 is the paradigm for future production, fully flexible with the lot size "one." This long-term target requires many changes as well in the production technology itself as in the way of cooperation between manufacturers: the high flexibility also requires information exchange and interaction between suppliers, contractors and competitors. Only this openness enables a company-overarching production chain to deliver each part and semi individually.

Blockchain and distributed ledger systems offer state-of-the-art protocols for this kind of open and secured information exchange: without hierarchy, peer-to-peer, with a minimum of interfaces, immutably distributed over all participants. In blockchains of the second evolution step, distributed applications, also called "smart contracts," enable transaction-based automation of processes, as these smart contracts may start new transactions and smart contracts again.

If now products and semis – communicating IoT devices themselves – initiate and control their own production process, they can start smart contracts within the distributed production network, moving between the machines, carrying production plans and transporting the products to other plants or customers. Many use cases for smart production, such as intra- and inter-factory supply chain management, license management and transfer, delivery monitoring and security, are possible.

This information exchange not only enables but also requires standardization of interfaces: blockchain itself only carries data and automates processes, e.g. with smart contracts. To become interoperable between different products, machine types and brands, the interfaces have to be the same or at least similar for all participants. ISO TC 307 WG 3 "Smart Contracts" and Platform Industrie 4.0 "RAMI" have already started standardization on the meta level. But for concrete production and delivery chains, the standardization of communication for dedicated environments and use cases has to be started.

Tony Zertuche, Jeff Grove

Dr. Jens Gayko
Head of the Standardization Council Industrie 4.0

The Reference Architectural Model RAMI 4.0 and the Standardization Council as an Element of Success for Industry 4.0

→ The technical and economic trend behind the concepts called fourth industrial revolution or smart manufacturing is expected to become a game changer in many ways. We expect tremendous changes in value-added chains, innovation processes and development processes but also the role of standardization. First of all, smart manufacturing is a so-called convergent technology which combines several known technologies. This implies the need for collaboration between experts of traditionally different sectors. Typically these different sectors have established their own language, models and rules for defining standards. During the ramp up of a convergent technology, it is important to moderate between these different groups to find common languages, models and rules for defining standards. The Standardization Council Industrie 4.0 (SCI 4.0) sees this as one of its roles.

Another characteristic of smart manufacturing is the very conceptional approach of system of systems. In order to handle and visualize this complexity, typically three-dimensional models are used. These models serve as a tool but they are no design guide for specific products. The SCI 4.0 coordinates several activities based on the structure of the Reference Architectural Model RAMI 4.0. These activities include, for example, the concept of the I4.0 component.

As a third aspect, the fourth industrial revolution will also affect the process of developing standards. A trend from "writing standards" to "engineering standards" is visible and demanded by the experts. This implies a close interaction with reference implementation and test-bed activities. Together with the Labs Network Industrie 4.0 (LNI 4.0) initiative, the SCI 4.0 proposes an agile approach for engineering standards in the 21st century.

Keith A. Stouffer
Cybersecurity for Smart Manufacturing Systems, Project Leader, NIST

Cybersecurity in Smart Manufacturing

→ Keith Stouffer presented the NIST Cybersecurity for Industrial Control Systems (ICS) work including the Cybersecurity for Smart Manufacturing Systems project, NIST SP 800-82, Guide to Industrial Control System (ICS) Security, the Cybersecurity Framework Manufacturing Profile and the Cybersecurity for Smart Manufacturing Test-bed.

Dr. Bradley D. Taylor
Visiting Assistant Professor, Electrical Engineering and Computer Science Department, School of Engineering, The Catholic University of America

Smart Manufacturing & Cybersecurity: Foundational ISA/IEC 62443 Standards Evolving with Learning Machines

→ Looking forward, our world is getting smaller, more interconnected. This presents us with great opportunities and challenges. Interoperability in sharing work, particularly when new technological resources are expensive but often underutilized by a single organization, promises improved efficiencies through the discovery and integration of resources available remotely. In an environment where

organizations vary widely (e.g. companies, professional societies, universities, legislatures), their rational perspective varies by their size, mission, technologies, and other factors. Further, exposure of resources potentially invites bad cyber actors. This requires not only protective standards, but also assurance that derived tools are ready on a moment's notice – for use only when needed.

Industrial Automation & Control Systems (IACS) protection from cyber attacks has inspired the term *Operational Technology*, as opposed to the more familiar *Information Technology*, to express the quantitative and qualitative differences in threats and consequences. We review the ISA/IEC 62443 series of standards background, developed through the efforts of 900 people on the ISA 99 Committee, over the past 16 years. Standards evolution continues as we discover new attack vectors. Given the potential speed of attacks launched and a preference to avoid preemptive attacks, employing learning machines intelligently provides a possible solution: a means for discovering appropriate partners, ensuring benevolent interaction (even though new to each other), allowing successful accomplishment of shared goals securely.

Ingo M. Rübenach, Alec McMillan, Dr. Gerhard Steiger

Dr. Bradley D. Taylor, John Kulick, Allison Barnard Feeney

Volker Jacumeit

Dr. Jens Gayko, John Kulick

1. Specific requirements of smart manufacturing for smart contracts:

- → Defined reaction times
- → Timed criticality
- → Business-to-business requirements
- → Ability to upgrade/flexibility
- → Ability for interaction between smart contracts

Action Items in connection with ISO TC 307 on blockchains:

- → Submit this report for information
- → Highlight the specific smart manufacturing smart contracts requirements to the attention of the USNC TAG and DKE mirror committee
- → Ask TC to find out what's already available in industry
- → Develop blockchain use cases using invited industry manufacturing experts to participate within ISO TC 307

2. How can we combine safety and security? Is safety exterminating security? How can we align the shop floor with the office floor?

- → The key element is risk assessment; the processes for safety apply also for security. In smart manufacturing both have to be taken into account simultaneously. Safety is static and security is dynamic.
- → Control access into the machine; access is not always necessary. What is needed for predictive maintenance is the data from the machine. If access is needed, it must be restricted and monitored.
- → Build the digital twin and test the overall package (safety and security)
- → More cooperation between ISO and IEC and other SDOs is required
- → The dialogue will lead to an evolution of the roles within an organization
- → In standardization we have to implement a matrix organization and put the system into focus
- → Complement the existing work in silos of today
- → Building resiliency into the design of the smart manufacture/plant

Action Item:
Have ISO & IEC groups work together in a more collaborative way.

3. Is the German model of the Standardization Council adoptable for the USA? How important is transatlantic cooperation, and do we need an International Standardization Council?

- → The German model of a Standardization Council was established initially by large German industrial companies. There are strong antitrust rules in place.
- → Some two years later, government became involved, reached out to SMEs and extended the stakeholder interest
- → The Standardization Council promotes a top-down RAMI model picture
- → Trade associations (VDMA, ZVEI, BITKOM) are looking at bottom-up education for limited-resource SMEs with focus on specific areas
- → Government funding is limited to international outreach and local market activities
- → Standardization council faces challenges in industry funding

General consensus: the USA needs a focal point to

- → provide education and training on what research, standards and industry programs exist in the U.S. today
- → provide assistance to U.S. industry in identifying which activities and organizations are relevant to their individual goals
- → promote links and action plans to bridge the gap from R&D implementation pilots to standards development activities
- → engage large U.S. manufacturing businesses in setting a U.S. strategy
- → engage government recognition and support of the initiative
- → engage trade associations (SMEs), regulators, system integrators

In the USA there is no central coordination entity

- → Possible structures include:
- → An independent industry-funded consortium
- → A government-sponsored initiative akin to "Smart Grid" at NIST. Could this be a component of U.S. infrastructure investment?
- → Expansion of NIST smart manufacturing program office currently administrator of 14 independent U.S.-focused innovation institutes
- → ANSI company member forum – strong U.S. manufacturing company initiative and support required with government recognition

Action Items:

- → Explore ANSI taking an initial role utilizing the resources of the Company Member Forum with support of Government and Organization Member Forums to communicate U.S. smart manufacturing technology and standards programs
- → Convene initial bilateral industry-led meetings with DKE/DIN industry 4.0 organizations, and expand to other global leaders in smart manufacturing technology and standards to identify areas of interest
- → Innovation institutes
  - – Encourage the innovation institutes and other U.S.-based research activities to participate in the ANSI Company Member Forum program, provide presentations on their activities and identify standardization opportunities
- → Communication
  - – There should be some kind of communication of all U.S. and international smart manufacturing implementations to all stakeholders on a regular basis with a view to coordinating U.S. participation efforts and leveraging available resources to maximum effect

BREAKOUT SESSION
SMART MOBILITY

MODERATOR: **Steven Sill**
Intelligent Transportation Systems (ITS) Architecture and Standards Program Manager,
ITS Joint Program Office (JPO), U.S. Department of Transportation

Steven Sill
Intelligent Transportation Systems (ITS) Architecture and Standards Program Manager,
ITS Joint Program Office (JPO), U.S. Department of Transportation

Interoperable Integration of ADS and Smart Mobility into the Transportation System

→ Technologies for Automated Driving Systems (ADS) and smart mobility are evolving rapidly and are often capable of operating in compliance with laws and regulations without communicating with the infrastructure or other mobile users of transportation systems. However, operating independently without coordination with the operator of the roadway system – the Infrastructure Owner Operators (IOO) – and other mobile participants will forego potential safety and efficiency benefits of coordinated operation. Further, assuring interoperability across the multiple regions will require agreements on standardized means of cooperation. Steven Still discussed the challenges to achieving interoperable integration and a candidate approach to achieve this goal. He provided information on the existing U.S. ITS national reference architecture and ITS standards currently available to support deployment.

Stephan Voit
Senior Manager eMobility,
Innogy SE

Cybersecurity for E-Mobility Systems in Worldwide Standardization

→ Cybersecurity and e-mobility should work together hand in hand. To design and operate a secure e-mobility environment, a lot of effort is necessary. Stephan Voit gave an overview on the hurdles which have to be mastered. Challenges, naming conventions, typical attack vectors and (best) practices of e-mobility's stakeholders are shown. He specially analyzed smart charging with ISO 15118.

Tom Lusco
Senior Systems Engineer,
Iteris, Inc.

The U.S. Intelligent Transportation Systems (ITS)

→ The Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) provides the framework – the reference architecture for intelligent transportation system deployments in the United States. Organized according to well-known systems engineering principles embodied in ISO 42010, ARC-IT's structure enables planners and engineers to spend more time

developing content and deploying systems rather than organizing and researching.

ARC-IT's models address the primary concerns voiced by ITS stakeholders: issues related to functionality, performance, security, organization, feasibility and more are framed within its four viewpoints. In particular, ARC-IT provides the basis for deployers to embark on products with "the ilities" in mind: extensibility, scalability, affordability and, especially in the world of cooperative ITS, interoperability. Communications, data and security requirements are defined across the breadth of the architecture, and traced to architecture artifacts. Architecture content is manipulated by companion tools that enable customization and application of the architecture to conceiving, developing and deploying ITS.

Ellen Nadeau
Privacy Risk Strategist, NIST

Privacy in Connected Vehicle Environments

→ As we increasingly develop and deploy connected, cooperative, and automated transportation technologies (including vehicle, infrastructure, and portable devices), protecting people's privacy is important to the adoption of these new technologies, and our ability to reap their full benefits. Developing new cooperative Intelligent Transportation Systems (ITS) environments leads to a variety of new privacy risks; meanwhile, there is minimal guidance on how to bring typical IT-focused risk management processes into the Internet of Things (IoT) space, and to connected and automated vehicles specifically.

The National Institute of Standards and Technology (NIST) has worked on implementing a privacy risk assessment methodology with the Department of Transportation's pilot sites – which demonstrates one approach to identifying and managing privacy risks in a cooperative ITS environment, and has highlighted a few privacy risks that are particularly prevalent in this space. The development of risk-based, outcomes-focused, voluntary standards can contribute to this gap in guidance for privacy risk management in the connected vehicles cooperative ITS space.

Matthias Kuom
Program Manager,
German Aerospace Center
(DLR)

Blockchain in Smart Mobility

→ Blockchain is currently being discussed as disruptive technology for a wide range of applications. It is appraised as a technology for everyone who wants to spontaneously and straightforwardly form a group, build up and use infrastructure together (e.g. energy, parking spaces or vehicles).

What role can blockchain play in mobility, can it trigger radical innovations? The potential benefits of blockchain in mobility and transport are just as compelling as they are in other industries – immutability, elimination of non-value-added intermediaries, traceability, etc.

By that, blockchain may not trigger radical innovation, but can reinforce and accelerate the following trends, as well as changing value chains:

- Autonomous vehicles can play an important role both in inner-city traffic and on long distances (e.g. robotaxis, automated ridesharing).
- Automated driving will further increase the requirements for short-term payment transactions. For efficiency gains in traffic flow, a kind of operating program for road traffic is necessary, which can be implemented by micro-payment between vehicles.
- Passenger transport will in future be more characterized by intermodality. In conjunction with "sharing" models, in which the user no longer owns a means of transport, new billing and access authorization mechanisms are developed.

Blockchain, or distributed ledger technology in general, is particularly suitable for this.

The German Federal Ministry for Economic Affairs and Energy has started a bunch of projects exploring the potential of the technology, e.g. within the project SAMPL, a safety solution ("Chain of Trust") for additive manufacturing processes will be developed. The entire process from the creation of the digital 3D print data to the identification of the printed components is considered. This solution can significantly change logistics processes. The projects Pebbles, BloGPV and SMECS deal with the use of blockchains in marketplaces between producers of renewable

energy and consumers. These are building blocks for the widespread use of electric vehicles. The goal of Charge4C is the creation of an innovative sharing platform, which enables a dynamic pricing of parking and charging and can organize communities and corresponding services around charging points in the private and public sector.

The initial experience from the projects shows that there is enormous potential in technology, but that there are still some steps to go before it is ready for real productive operations. In general I can conclude that mobility will change away from ownership-based models towards service models – and blockchain/DLT is the right technology to support this trend.

When designing blockchains, safety aspects and technical standards must be taken into account at an early stage. And we need interoperability standards between different blockchains to ensure technological openness. And most important: development and testing of DLT must be carried out before a maybe too early regulation.

Holger Zeltwanger
Technical Manager,
CAN in Automation (CiA)

Commercial Vehicles, Telemation & Additional Mobile Machinery – Security Threats

→ Connecting vehicles to the cloud is nothing new. For many years, data has been sent from vehicles to the internet or proprietary servers via different remote and wireless networks. However, these existing links are not made to be shared by different parties. In the example of "machines on wheels" (this includes vehicles for agriculture, forestry, road construction, etc.), Holger Zeltwanger addressed challenges and solutions that have already been discussed in standardization committees. This includes ISO 16844 (tachograph), ISO 15765 (on-board diagnostics), ISO 11992 (automatic steering and on-board weighing), DIN 4630 (body application), etc. In addition, he reported about European Committee requirements for secure access to commercial vehicles and discussed general requirements on secure systems with respect to CAN-based networks (major communication technology in commercial vehicles). This includes latest developments on the CAN physical layer (smart transceivers), which may be standardized in the ISO 11898 series.

Craig Rodine
Director of Standards,
ChargePoint, Inc.

Charging Network Cybersecurity: Status Quo and Future Challenges

→ Today's Electric Vehicle Charging Networks (EVCN) exhibit varying levels of cybersecurity, depending on their origins and evolutionary paths. Proprietary networks built to meet the business goals of the charging station vendor/network operator and their customers (site owners) incorporate commercial-grade cybersecurity as an essential foundation of the service platform. Networks deployed to meet primarily social, rather than business, goals may be not at all cybersecure – as was dramatically revealed in a presentation and demonstration by Matthias Dahlheimer (34C3, December 2017, Berlin).

A state-of-the-art, CPI DSS 3.2-certified EVCN incorporates more than 47,000 charging ports (>25,000 stations) and has delivered over 35 million charging sessions without any known security breaches. The IEC Technical Committee (TC) 69 is currently working on developing comprehensive cybersecurity requirements for open EVCN standards supporting a wide range of charging use cases and services. German and U.S. IEC TC 69 mirror committees should coordinate their work so our combined talents and resources can be applied most efficiently to bring about the critically needed enhancement of cybersecurity support for EV charging networks worldwide.

Thomas Sentko, Holger Zeltwanger, Matthias Kuom

Diane Haithcock

↘ REPORT
BREAKOUT SESSION SMART MOBILITY

1. How can mobility standardization serve a global marketplace, meet local needs and foster innovation?

→ Scope: what can standardization resolve?

→ Many "clean sheet" opportunities

→ Pilots before large-scale implementation

→ Commercial and public sector, multi-SDO cooperation
- Balance public and private interests

→ Certification and testability are paramount

2. What is the role of individual and private transport in future mobility?

→ Definition:
- Private: under control of an operator
- Public: shared, scheduled, funded (individually, collectively)

→ Answer depends on:
- Geography (living in cities, suburbs, rural areas)
- Economics (income)
- Environmental situation (pollution)
- Personal needs and abilities
- Nature of the family unit
- Dis/Connected to digital world

→ Use cases can be derived from the circumstances and conditions mentioned

→ The regulator has the chance to influence the transition process

→ Fee on access to cities

→ Fee on emissions

→ Different speed of transition:
- Cities, metropolitan areas, rural areas (differs in time, need for funding)

3. How can we effectively manage cybersecurity in a rapidly evolving mobility environment?

→ Continuous monitoring of risks

→ Implementing the standards that already exist

→ Setting the proper, effective incentives or penalties

→ Formal compliance and certification

→ Peer pressure and public shaming

→ Larger credentialed cybersecurity workforce

→ Learn from other industries

→ Develop a quick way to share cybersecurity information

→ Available repository of R&D results

Action Items:

→ Multi-SDO, stakeholder cooperation in mobility:
- Facilitate pilot cooperation? Workshops?
- Cooperation among traditional competitors – SDOs and businesses

→ Near term:
- Hold a workshop to develop a mechanism regarding cybersecurity information sharing

→ Long term:
- Develop cybersecurity educational programs for current practitioners

→ Stakeholders need to cooperate on consensus on how to manage the integration of new transportation options for the public benefit
- E.g. public transport funding can be re-thought

→ "De-emphasize private – promote public!"

BREAKOUT SESSION

SMART AGRICULTURE

MODERATOR: **Dorothee Töreki**
Digitization Advisor, IBM Cognitive Collaboration and Talent Solutions

Dorothee Töreki
Digitization Advisor, IBM Cognitive Collaboration and Talent Solutions

Smart Agriculture – A Brief Outlook into the Future

→ The following quote from Klaus Schwalb, the Founder and CEO of the World Economic Forum, points out in a nutshell how deep the change due to digitization will be: "This Fourth Industrial Revolution is, however, fundamentally different. It is characterized by a range of new technologies that are fusing the physical, digital and biological worlds, impacting all disciplines, economies and industries, and even challenging ideas about what it means to be human." As we all live in a digitalized world for decades, the question about the difference between the years behind us and the future comes up. Several technologies are currently building a perfect storm of disruptive change:

- **Internet of Things:** It is not only ourselves creating a lot of data by tracking our movements and vital data but also more and more things – from the refrigerator to the smart home to agricultural fields – are equipped with sensors creating a huge amount of data every second.
- **Artificial Intelligence:** Nowadays we have the technology to open the treasure chest and get new insights out of this data. Machine learning algorithms are capable of finding patterns and getting new insights from various data sources. Furthermore, computers become more and more human, as they are now able to interpret pictures and understand human language.
- **Cloud Services:** To make use of artificial intelligence it is no longer necessary to invest a huge amount of money, it can just be implemented by using cloud-based services. That gives artificial intelligence an even more disruptive power, as not only large companies but also small start-ups can use it with a relatively small amount of money in the beginning.
- **Blockchain:** Blockchain technology dispenses with the need for middlemen. Several parties who do not trust each other are now able to interact safely. Blockchain is

a ledger, where any kind of information can be stored safely in a decentralized database. This means that no single instance can modify data or store un-validated information.

These information technologies together build a perfect storm. We are coming from the era of industrialization, where revenue was generated by producing and selling goods. Nowadays we are entering an era where more and more revenue will be generated by offering flexible data-based services. Looking a few years into the future when autonomous cars will be standard might illustrate this. A family planning a trip to the sea over the weekend will probably no longer use its own car but order a mobility service just with a fingertip on a smartphone. This car no longer has a steering wheel and requires no attention to driving from any of the passengers. They will have time to consume data-based services. This mobility service might provide tailored offerings based on the information that is available about you: if you prefer Italian middle-class restaurants, the screens in the car could show a special offer from a restaurant which you will arrive at around dinner time. When you order now, you will perhaps receive a 10% discount. And by the increasing availability of autonomous car services with easy handling at the same time, the ownership of cars will decrease significantly – because the second most expensive item in every household is a car. And this in return has a huge impact on urban design. This small example shows an attribute of digitalization in a nutshell: the change of technology in one industry (automotive) will transform other industries and societies as well. Digitalization has always been considered holistically.

The same applies to agriculture. Already now the manufacturing companies of agricultural machines offer data services to farmers or other players in the industry: from advice about what to sow, when, where and to what extent to irrigate up to a recommendation about the best time to sell the goods.

But this is just the beginning. Blockchain can offer a complete new level of transparency into the food industry. Today Walmart and IBM run a project about food safety with blockchain technology. The goal is to offer consumers a 360-degree view of the food product: on which farm it was produced, how the soil composition is, whether pesticides were applied and if yes, what kind of pesticides, etc. This might lead to a higher appreciation of organic farming or animal-appropriate production.

But let's go a step further to the project from Caleb Harper from MIT. He founded the OpenAgricultureLab and his project is about food computers. These food computers can provide the perfect environment for almost any given plant based on big data analytics – perfect light, temperature, humidity, nutrient input, etc.

Combine this with the major shift in urban design caused by a reduced number of cars due to autonomous driving – why not reuse a former parking garage for a food computer? Or bring food computers into offices and private homes. This can be an option for a radical shift in food production: the conditions for cultivation of food today are that it can be cultivated for mass production and the food can be moveable across long distances easily. The food computers may initiate a mind shift – from mass production to high quality at lower scale on a local basis.

I highly recommend viewing the TED Talk from Caleb Harper[1]. And by the way, his project is completely open – everybody can download the construction manual and can contribute his experiences in an open community.

The examples described before should show the potential of a radical mind change in food production. This future outlook is just a vague forecast, but we all should keep in mind that we are just at the beginning. Technology and nature will merge together more and more – be it sensors in fields, computers that act like humans or many other things to come. The most important factor is to face these challenges with an open mind.

[1] https://www.youtube.com/watch?v=cn5hnzwHUJY&t=299s

Rüdiger Marquardt
Member of the Executive Board, DIN

Standardization in Smart Agriculture – The Process Already Started

→ The agricultural sector is facing enormous challenges to feed the 9.6 billion people by 2050. ISO standards help deliver a more profitable and sustainable agricultural production by equipping farmers with new technologies, the right knowledge and information, and mechanisms to gain fair access to markets. Worldwide accepted international standards will contribute to a sustainable, cost-effective and environmentally friendly production of agricultural products. Governments can reference an international standard rather than developing their own laws and regulations. This avoids a situation in which various standards are being developed.

Britt Kritzler
Digital Transformation & Open Innovation Consultant, Kritzler Consulting Ltd.

Cybersecurity in Smart Agriculture

→ Blockchain has the potential to disrupt a range of industries. We have all heard of, if not personally known, a cryptocurrency millionaire and are aware of the large investments pouring into FinTech start-ups with a reference to blockchain in their name. The advantages for the food system are real. And large food operators are trialing blockchain pilots in various supply chains worldwide to address different business problems. From provenance over improved hygiene protocols to identifying the source of contaminated foods in seconds, as opposed to weeks, blockchain technologies suit a range of applications. In her presentation, Britt Kritzler explored some of these applications in lieu of expected risk benefits, with the aim to offer a starting point to regulators for prioritizing open innovation projects they might wish to participate in.

Nick Tindall
Senior Director of Government and Industry Affairs for the Association of Equipment Manufacturers (AEM)

Connected Farm = Smart Farm

→ Nick Tindall talked about the impact connected farms have on food production. Sensors on corn and soybean harvesting equipment for example already generate up to seven gigabits of data per acre. The evaluation of this data allows for increased precision in the production cycle which can lead to a 15% production increase and raise the profitability of one acre of land by up to $100. The challenge in implementing the concept of connected farms in the agricultural sector lies in providing the framework conditions for the use of broad amounts of data, e.g. regarding the access to broadband internet in remote areas.

Klaus-Herbert Rolf
Governmental Affairs Manager,
365FarmNet Group

Farming 4.0 Delivers Basic Data for the Future Transport Food Chain – 365FarmNet Concept, a European Example

→ Farming is becoming increasingly complex, also due to growing regulatory requirements and obligations to provide proof to the legislators. The farmer as an entrepreneur is hardly able to meet the requirements using conventional methods.

This is where 365FarmNet comes in. This comprehensive yard management software for agricultural holdings enables multi-vendor and cross-segmental management of the entire farm with a single software solution. The existing individual solutions for a clearly defined production sector are now being replaced by a modern, extensive cloud-based system solution that intelligently and closely links individual operation areas and improves processes through the use of intelligent data analysis.

365FarmNet is Europe's renowned and multiple award-winning software for managing the entire farm, independent of size and type of farm. 365FarmNet develops innovative applications for users from more than 25 countries.

We set international standards for digital yard management and show potentials for more efficient, future-proof and sustainable farming and food.

With modern technology and open interfaces, we foster innovation and accessibility.

Thus, the economic and ecological potentials in agriculture can be raised. At the same time the database for the future food chain is being created. This also calls for uniform digital industry standards.

Timothy West
Manager, Enterprise Engineering Standards, Deere & Co.

The Role of Standards in Smart Farming

→ Taking a look at smart agriculture from the point of view of standards, not smart agriculture technology, we need to consider three essential aspects: precision, connected and sustainability.

The benefits are better decisions in all aspects of the agriculture industry, using fewer resources and minimizing the impact on the environment to feed the world. Everyone can agree these are good things. The technology is available to all – not just large farms – and it will be adopted in all markets of the world.

Standards are already written in the three areas of precision, connected and sustainability. This work continues today. It needs to include not just equipment but stakeholders from up and down the supply chain.

There is a link between standards and regulations, but standards do not equal regulation. The use and creation of voluntary consensus standards is encouraged. Regulations are not. Let the market and the customers drive the direction.

Standards are essential. They are inevitable and it is the stakeholders' responsibility to create these standards.

↘ REPORT
BREAKOUT SESSION SMART AGRICULTURE

1. Why do we need standards to support the realization of smart agriculture? How important is transatlantic cooperation (U.S.-Europe and/or U.S.-Germany) for the successful development of smart agriculture standards?

→ The problems:
- an increasing population to feed
- a limited amount of farmland
- a decreasing farming workforce

→ Nature hates a vacuum – there will be standards, either consensus industry-driven or government-directed – standards are not the same as regulation

→ Individual company or national solutions will arise if global or transatlantic solutions do not – this may not lead to sustainable solutions

→ Consensus standards are a proven means to provide the process and platform to bring together or integrate diverse players for transatlantic or global solutions and be responsive to customer needs

→ USA and Germany should join forces to lead directions for smart agriculture standardization as our approaches to agriculture are similar – if we don't do it, it won't get done in the near term

2. Without standardization, what would smart agriculture look like, and how would it succeed?

→ Without standards, realization of smart agriculture will take longer and be more fragmented by competitive solutions

→ Solutions may not be sustainable or responsive to customer needs

→ Interoperability of equipment will not be optimized

→ A common language will be lacking for collaboration between agriculture and other disciplines such as the finance community

→ Agriculture will not be sustainable for some farmers over time

→ Without standards, agriculture may face greater regulation

3. What standards may be missing and are needed for smart agriculture to succeed? By what target dates should such standards be developed and by whom?

Action Item:

→ ANSI, DIN and DKE should establish a joint strategic-level study group on smart agriculture in order to understand:
- the needs of farmers, parties that require data from farmers and consumers of agricultural products;
- the possible future directions of regulations related to agriculture;
- the range of existing standards available from ISO, IEC, ITU-T, other SDOs and consortia that may contribute to smart agriculture

→ This joint strategic study group should develop a coordinated vision/roadmap/gap analysis with recommendations for possible new standards initiatives

→ Consideration should be given to making this a broader initiative – in Europe and North America

→ Target date: mid-2019 for results

RECEPTION AND DINNER

APRIL 10th

Otto Graf
Counselor for Development,
World Bank, IDB, Embassy of the Federal Republic of Germany

"Free trade is of major importance to Germany and a key issue in the transatlantic dialogue. It does, however, not come naturally. Rules under which goods can be exchanged have to be created. These rules include standards. If we want to have functioning cooperation and exchange of goods in central areas such as autonomous driving or digital security, common standards are essential and needed. The U.S.-German Standards Panel is laying the groundwork for these standards. Therefore, the significance of the Panel reaches far beyond actual standard setting."

Joe Bhatia, Christoph Winterhalter

Britt Kritzler, Craig Rodine

John Kulick, Holger Zeltwanger

Thomas Sentko, Tony Zertuche

Christoph Winterhalter

Ingo M. Rübenach, Matthias Kuom

Dr. Dennis-Kenji Kipker, Dr. Jens Gayko, Dr. Anne Kleinschrodt,
Rüdiger Marquardt, Dr. Bradley D. Taylor

PRESENTATION AND PANEL DISCUSSION:

Standard Development Organizations and Conformity Assessment in Cybersecurity

MODERATOR: **Gordon Gillerman**, Director Standards Coordination Office, NIST

APRIL 11th

Ingo M. Rübenach

Timothy West

Miguel Bañón
Managing Director,
Epoche & Espri – a DEKRA company, DEKRA e. V.

Cybersecurity and Standards: A Safe Connected World

→ Miguel Bañón talked about the ever-increasing need for product vendors and service providers to show transparency and trustworthiness from product vendors and service providers. He outlined how standards and third-party certification play a critical role in the provision of this trust.

Security Is the New Safety

→ "Safety" used to refer to physical safety attributes – electric shock, mechanical hazards, risk of fire. A manufacturer could address these risks and feel that a safe product was being provided. In today's time, though, products are connected to the internet and to each other, introducing an additional risk to be considered. A house thermostat is no longer just a simple controller for the air system, but an access to devices in the house. Cybersecurity therefore cannot be ignored – it is the new safety. In their presentation, Ingo M. Rübenach and Sonya Bird addressed UL's approach to cybersecurity through standards development and through testing programs.

Ingo M. Rübenach
Vice President, Central, East & South Europe,
Underwriters Laboratories (UL)
Sonya Bird
International Standards Manager,
Underwriters Laboratories (UL)

PANELIST:
Christoph Winterhalter
Chairman of the Executive Board, DIN

"Structuring standardization work in silos requires a lot of horizontal coordination. That is slowing us down. We will need to develop a much more dynamic organization in which we have the right expertise for every single product in a virtual committee. This entails tremendous challenges and changes to standardization: coordination is a first step, but the next step is a network that constantly connects experts in new, project-oriented ways."

PANELIST:
Dr. Jens Gayko
Head of the Standardization Council Industrie 4.0

"The digital transformation community learns very dynamically. In addition to the Standardization Council Industrie 4.0, there is also the Labs Network Industrie 4.0. At some point during writing a specification you have to pause and go ahead and do some prototyping. Do prototyping, learn from the experience of implementing it and then come back and improve the standard!"

Timothy West, Dr. Gerhard Steiger

Dr. Ulrike Bohnsack, Mario Beier

Tony Zertuche

CLOSING REMARKS

Joe Bhatia
President and CEO, ANSI

"The sessions certainly shed light upon the various challenges the standards and conformance community is facing in leading technology areas, and how we are all working to identify solutions and action items to address these challenges together as we move forward."

Christoph Winterhalter
Chairman of the Executive Board, DIN

"With cybersecurity we picked the right topic for this year's U.S.-German Standards Panel. And it was very helpful to concentrate on three vertical areas of application. That helped us to better understand the challenges and learn from each other by using ideas from one sector and apply them to another sector."

Thomas Sentko
Standards Manager International, DKE

*"As so often education is the key.
It is our task to educate our experts in the traditional standardization committees to reflect security and transparency aspects in their area of expertise.
We succeeded in safety – let's do it in security!"*

List of participants

Naimah Alemmrani
The Catholic University of America

Abdullah Almalki
The Catholic University of America

Ibrahim Almubark
The Catholic University of America

Mofaq Alotaibi
The Catholic University of America

Mohammed Alqahtani
The Catholic University of America

Miguel Bañón
Epoche & Espri, a DEKRA company

Allison Barnard Feeney
NIST

Jaron Bass
International Trade Administration

Mario Beier
DIN e. V.

David Bergman
IPC

Joe Bhatia
ANSI

Sonya Bird
UL

Dr. Ulrike Bohnsack
DIN e. V.

Christine Brown
USTR

Scott Buchholz
Deloitte

Stephanie Carroll
ANSI

Steven Cornish
ANSI

Peter Fatelnig
Delegation of the European Union to the United States of America

Sibylle Gabler
DIN e. V.

Dr. Jens Gayko
Standardization Council Industrie 4.0

Gordon Gillerman
NIST

Otto Graf
Embassy of the Federal Republic of Germany

Jeff Grove
ASTM International

Diane Haithcock
Underwriters Laboratories Inc.

Dennis Haub
DKE

Fred Hayes
PMMI

Megan Hayes
PLASTICS

Karan Hofmann
RTCA

Zack Hornberger
MITA

Volker Jacumeit
DIN e. V.

Ajit Jillavenkatesa
NIST, U.S. Dept. of Commerce

Kyle Johnson
U.S. Department of Commerce

Dr. Dennis-Kenji Kipker
University of Bremen

Dr. Anne Kleinschrodt
Federal Ministry for Economic Affairs and Energy

Britt Kritzler
Kritzler Consulting Ltd.

John Kulick
Siemens

Matthias Kuom
DLR e. V.

Tom Lusco
Iteris, Inc.

Rüdiger Marquardt
DIN e. V.

Leslie McDermott
ANSI

Alec McMillan
IEC SEG 7 on Smart Manufacturing Co-Convenor

Brian Meincke
ASTM International

Eric Moughler
Caterpillar

Ellen Nadeau
NIST

Abdourahmane Ndione
ASN

Mike Nelson
DigiCert

Elaine Newton
Oracle

Sharon Okello
ANSI

Michael Palm
Underwriters Laboratories Inc.

Jorge Pardo
U.S. Department of Commerce

Erik Puskar
NIST

Anthony Quinn
Department of Commerce

James Rentsch
Aerospace Industries Association

Sam Rizzo
USTR

Charles Robinson
International Society of Automation

Craig Rodine
ChargePoint, Inc.

Klaus-Herbert Rolf
365FarmNet Group

Jessica Roop
ANSI

Ingo M. Rübenach
Underwriters Laboratories Germany GmbH

Fran Schrotter
ANSI

Adam Sedgewick
NIST

Thomas Sentko
DKE

Steven Sill
U.S. Department of Transportation

Prof. Dr. Volker Skwarek
HAW Hamburg

Annie Sokol
NIST

Joel Solis
NEMA

Anish Srivastava
TÜV Rheinland OpenSky

Dr. Gerhard Steiger
VDMA

Keith A. Stouffer
NIST

Dr. Bradley D. Taylor
The Catholic University of America

John Thompson
Underwriters Laboratories Inc.

Nick Tindall
Association of Equipment Manufacturers

Dorothee Töreki
IBM Deutschland GmbH

Joseph Tretler
ANSI

Hiroshi Tsuchiya
NEDO

Wil Vargas
AAMI

Stephan Voit
Innogy SE

Timothy West
Deere & Co.

Christoph Winterhalter
DIN e. V.

Holger Zeltwanger
CAN in Automation (CiA)

Tony Zertuche
ANSI

Dr. Thomas Zielke
German Ministry of Economics and Energy

Imprint
DIN German Institute for Standardization
Am DIN-Platz, Burggrafenstraße 6, 10787 Berlin, Germany
Phone +49 30 2601-1112, Fax +49 30 2601-1115
E-mail: presse@din.de, www.din.de
Editor: Sibylle Gabler
Designed and set by: ergo Industriewerbung GmbH, Berlin
Photos: Charlie Archambault
Printed by: PieReg Druckcenter Berlin GmbH, Berlin
94714/2018-05

ANSI American National
Standards Institute
1899 L Street, NW, 11th Floor
Washington, DC 20036
USA
Phone +1 202 293 8020
Fax +1 202 293 9287
E-mail: pr@ansi.org
www.ansi.org

DIN German Institute for Standardization
Am DIN-Platz
Burggrafenstraße 6
10787 Berlin
Germany
Phone +49 30 2601-1112
Fax +49 30 2601-1115
E-mail: presse@din.de
www.din.de

DKE Deutsche Kommission
Elektrotechnik Elektronik Informationstechnik
in DIN und VDE
Stresemannallee 15
60596 Frankfurt am Main
Germany
Phone +49 69 6308-0
Fax +49 69 6308-9863
E-mail: dke@vde.com
www.dke.de