WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Center for the Fourth Industrial Revolution

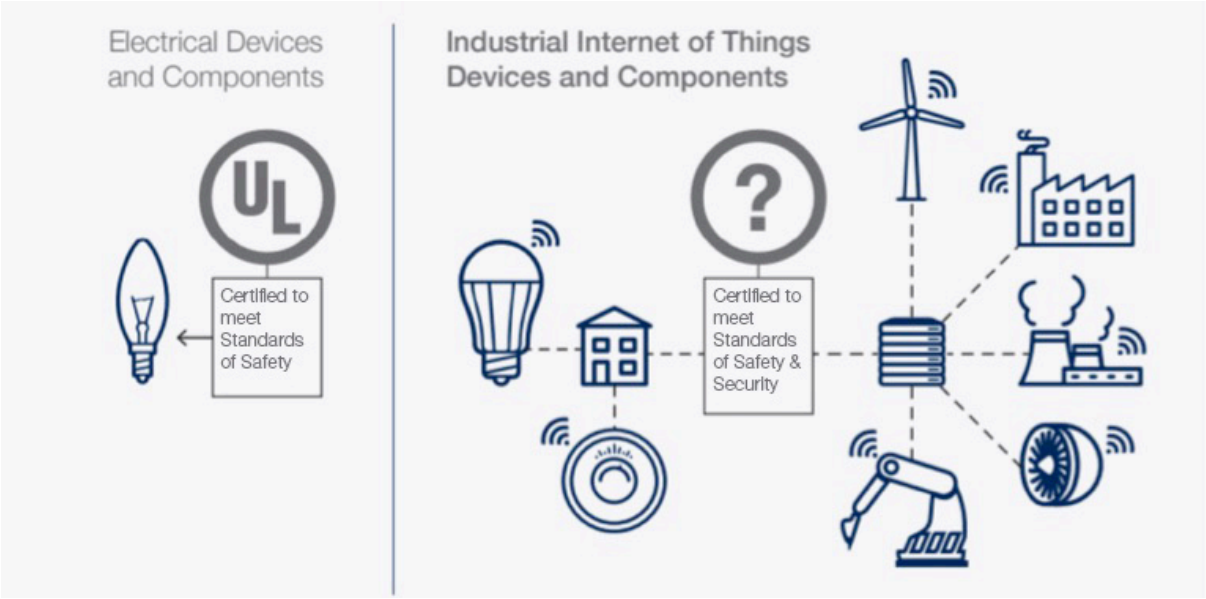
Digital Protocol Network on Industrial Internet of Things Safety and Security

The challenge

The Fourth Industrial Revolution is transforming all aspects of the economy and society. New technologies enabled by the internet are disrupting businesses, governments and society through new business models, and also changing social norms, resulting in significant and growing governance gaps on a variety of critical issues. Current governance models are struggling to address the rapid and transnational nature of these gaps. Digital Protocol Networks are new, informal, agile and multistakeholder-driven mechanisms, which develop actionable solutions at “internet speed” to address these technology governance gaps. The purpose of each Digital Protocol Network is to develop actionable protocols, i.e. practical solutions that address a specific governance gap in the form of an informal framework or standard. These include detailed specifications, operational processes, implementation guidelines, verification instruments, maintenance procedures and/or conflict/dispute resolution mechanisms.

Digital Protocol Network on Industrial Internet of Things Safety and Security

Technologists have forecast the growth of billions of internet-enabled and connected devices. Although this will facilitate improved industrial and economic productivity and efficiency, there are also significant concerns about the increased safety and security risks to business, governments and society at large. This is already partly reflected in the increasing number of widely publicized hacks in industries as diverse as nuclear power, retail and healthcare. The current industrial internet of things (IIoT) marketplace does not incentivize producers to build preventative security features or processes into production, nor is there sufficient public awareness to drive this type of demand.



The purpose of the IIoT Safety and Security Network is to optimize security in IIoT platforms and help direct stakeholders to design and develop these platforms in a way that ensures public safety and security. The network's goal is to activate existing incentives typically associated with the insurance industry, combining supply-side and demand-side strategies to reinforce the marketplace for IIoT safety and security. This network can augment the work to which organizations like UL and IEEE have committed in other industrial and consumer sectors, and will focus its initial outreach on core constituencies not typically represented in IIoT safety and security policy discussions, including manufacturers, the insurance industry and security researchers. The multinational nature of the threat models necessitates taking both global and regional views that reflect economic and social differences relative to the IIoT ecosystem.

Network output: Incentive framework for IIoT safety and security

These protocols will raise the norm-setting opportunities of risk mitigation strategies. The framework is designed to overcome market failure by developing a set of criteria for what constitutes "safe" IIoT endpoints and the systems with which they connect within an IIoT network. This work includes the identification and incorporation of existing standards and the actors necessary to ensure IIoT safety and security. By focusing on implementation, assessment and maintenance best practices, the incentives for adoption of security by design are better aligned. Once the protocols have been developed, the network, in collaboration with the Center for the Fourth Industrial Revolution, will integrate the operation of these consensus-driven norms through the engagement of government, industry, civil society, standard-setting organizations and decision-making bodies.

The Digital Protocol Network on Industrial Internet of Things Safety and Security is one of multiple projects at the Forum's Center for the Fourth Industrial Revolution. The center was established in 2017 to partner with forward-leaning governments, and leading companies, civil society and experts from around the world. Its aim is to co-design and pilot approaches to policy and governance for emerging technologies.

Getting involved

Network chair – helps the group understand its objectives and makes sure it is functioning effectively.

Network experts – have acquired significant knowledge relating to the network's focus area through research and practice. They contribute this knowledge to the development of solutions to the issues the community has identified.

Network community – comprising individuals who work in the field of the network's focus area, are interested in the subject matter and/or would like to participate in discussions without making the time commitment required of other network constituents. The Forum's 5,000+ Expert Network and TopLink platform are leveraged to enable this.

Facilitator – responsible for overseeing all logistical aspects of the network, along with guiding the collaboration of consensus norm-setting agreements.

The Center for the Fourth Industrial Revolution welcomes suggestions from its members and constituents on new Digital Protocol Network ideas that address governance gaps in the IoT domain. Please send your suggestions as per the contact details listed at the end of this document.

Network Co-Chairs and Network Experts

Network Co-Chairs

David Scharia, Director and Chief of Branch, Counter Terrorism Executive Directorate (CTED), United Nations, New York

Michael McNeil, Global Product Security and Services Officer, Royal Philips, USA

Network Experts

Aaron Kleiner, Director, Industry Assurance and Policy Advocacy, Microsoft Corporation, USA
Benedikt Abendroth, Cybersecurity Strategist, Microsoft Netherlands, Netherlands
Chris Harrison, Assistant Professor of Human-Computer Interaction, Carnegie Mellon University, USA
David O'Brien, Senior Researcher, Berkman Center for Internet and Society, USA
Edy Liongosari, Managing Director, Accenture, USA
Hamed Soroush, Senior Research Security Engineer, Real-Time Innovations (RTI), USA
Jesus Molina, Co-Chair, Security Working Group, Industrial Internet Consortium, USA
Lori Bailey, Global Head of Cyber Risk, Commercial Insurance, Zurich Insurance Group, Switzerland
Michael Tennefoss, Vice-President of Strategic Partnerships, Aruba Networks, USA
Ryan Gillis, Vice-President, Cybersecurity Strategy and Global Policy, Palo Alto Networks, USA
Siby Abraham, Chief Technologist and Vice-President, Wipro, India
Sukamal Banerjee, Senior Vice-President and Global Head, Engineering Services, HCL Technologies, USA
Urs Gasser, Executive Director, Harvard Berkman Center for Internet and Society, USA
Andrew Hall, Client Relationship Director, Willis Towers Watson, UK

Contact

For more information about our Digital Protocol Network on Industrial IoT Safety and Security, email:

Eddan Katz, Project Lead, Digital Protocol Networks, Eddan.Katz@weforum.org
Daniel Dobrygowski, Project Lead, Information Technology Industry, Daniel.Dobrygowski@weforum.org

Key dates

28-29 September: MIT IoT Workshop, Boston, USA

30 November: Partner Leadership Workshop at the Center for the Fourth Industrial Revolution, San Francisco, USA

12 December: Finalization of Draft Protocols, New York, USA

19 December: Review at Internet Governance Forum, Geneva, Switzerland

23-26 January: Review at the Annual Meeting 2018, Davos-Klosters, Switzerland

24-25 January: United Nations Counter Terrorism Committee Executive Directorate (CTED) Asia ICT and Counter-Terrorism Dialogue, Bangkok, Thailand