WORLD ECONOMIC FORUM

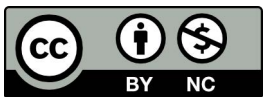
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Center for the Fourth Industrial Revolution Protocol Design Networks

Industrial Internet of Things
Safety and Security Protocol

April 2018

Contents



REF 160418

Protocols are defined as informal norm-setting frameworks that are accompanied over time by (1) detailed specifications, (2) operational processes, (3) implementation guidelines, (4) verification instruments, (5) maintenance procedures, and/or (6) conflict/dispute resolution mechanisms.

The implementation and success of this Protocol will require the active participation of key stakeholders across the IIoT ecosystem.

Executive Summary

The World Economic Forum has convened a network of experts to support the growth of a secure and reliable industrial internet of things (IIoT). These experts (the Network) are drawn from the business strategy, critical infrastructure, insurance, manufacturing, policy, security research and the technology communities. The Network recognizes that the vulnerable state of safety and security within this exponentially growing sector is untenable and has identified a number of challenges in the development of an optimally secure IIoT. It has focused on actionable solutions to those challenges.

The Network has developed a protocol framework through which actors can be aligned on the shared responsibility that ensures the security of IIoT products, practices and infrastructure. The IIoT ecosystem is not controlled by any particular stakeholder, neither is there a single discernible category of actors encharged with primary responsibility for its governance. When the risk of harm is so widely spread, public safety and preventive security can only be meaningfully addressed with a collective commitment to the mutual obligations of confronting the challenges of a complex interconnected environment.

The IIoT Safety and Security Protocol (the Protocol) generates an understanding of how insurance, which plays an integral part in the incentive structures of cybersecurity norm-setting and governance, can facilitate the improvement of IIoT security design, implementation and maintenance practices. The framework is intended to strengthen security IIoT services using active hardening processes that can be validated through proven penetration, configuration and compliance techniques.

Background

The internet of things (IoT) presents new opportunities for societal transformation through technology, especially for enterprises that harness the promise of IoT to improve business processes and for governments that look to IoT to improve infrastructure and the provision of vital services. Indeed, IoT has been heralded as the harbinger of the Fourth Industrial Revolution (a digital revolution characterized by the fusion of technologies, blurring the lines between the physical, digital and biological spheres), with the potential to impact industries at a scale equal to prior advancements in steam, electrical, nuclear and computing power.

The impressive growth of connected devices and IoT operates within a continuously evolving cyber-physical environment, with innovators and entrepreneurs pushing the boundaries of IoT's potential. This dynamic rate of change, however, also emboldens malicious actors to develop new and increasingly sophisticated mechanisms to exploit vulnerabilities that are both unique to IoT systems, or are imported with the vulnerable components, devices, or systems that are used as part of IoT services. The sheer scale and inextricable interconnectedness of IoT further compound the safety and security risks into actual physical threats, exposing the potential for catastrophic harm.

The industrial internet represents one of the most promising and transformative applications of IoT. The Industrial Internet Consortium defines the industrial internet as an "internet of things, machines, computers and people, enabling intelligent industrial operations using advanced data analytics for transformational business outcomes." IIoT is broad in focus but can perhaps most easily be understood as the application of IoT technologies in an industrial or business environment, as opposed to individual consumer setting.

As documented in the Forum's publication, Industrial Internet of Things: Unleashing the Potential of Connected Products and Services, IIoT is expected to dramatically alter manufacturing, energy, agriculture, transport and other industrial sectors of the economy which, together, account for nearly two-thirds of the global gross domestic product (GDP).

Whereas IIoT shares many characteristics with consumer IoT, it is notable both in its potential for economic impact as well as in its inherent complexity and system design across the supply chain. Accenture estimates that IIoT could add $14.2 trillion to the global economy by 2030, arguably making IIoT one of the biggest drivers of productivity and growth in the next decade. Unlike consumer IoT solutions, such as a wearable fitness tracker, which may be purchased by an individual with a single purpose (e.g., recording and encouraging healthy activity), IIoT solutions tend to be integrated into larger operational systems, creating significant interdependencies among various IIoT components. As a result, IIoT solutions can require additional planning and awareness to ensure adequate interoperability, scalability, precision and accuracy, programmability, latency levels, reliability, resilience, automation and serviceability.

As IIoT transforms previously isolated systems to a connected network that is intertwined with our day-to-day lives and businesses, it creates new critical dependencies on the robust functionality of that infrastructure. IIoT brings the familiar and ever-increasing digital risks associated with cybersecurity into physical spaces, creating a vast array of new vulnerabilities including threats to public safety, physical harm and catastrophic systemic attacks on commonly shared public infrastructure. Known IoT security vulnerabilities are widespread, spanning from low-end consumer devices to large-scale industrial systems. The attack surface for bad actors willing to exploit the digitally networked environment now penetrates not only the home with the popularity of consumer devices but also spreads across the transport and other municipal systems of our smart cities and permeates the increasingly connected manufacturing floor in core production processes. The potential impact of an attack on critical infrastructure would be far-reaching, extending deeper into more and more vital aspects of our economy, health, safety, public services and national security. Security, therefore, looms as the critical challenge for the products, systems and services that are dependent on IIoT, if not the viability of IIoT itself.

The time when decisions about cybersecurity risk exposure can be postponed has already passed. The Mirai botnet virus, which targeted "zombie" legacy IoT devices which were not being updated regularly, enabled the mounting of massive distributed denial of service (DDoS) attacks using an army of IoT devices to take down internet access across multiple ISPs and websites. The potential risk of harm, which now extends beyond information interruption to cyber-physical critical infrastructure, has already demonstrated the exponential impact on mass populations in multiple cyberattacks over the past several years in Ukraine. In the summer of 2017, a cyberattack that started on Ukrainian government and business computer systems, utilizing ransomware for owners to regain access to their computers, cascaded on to impact energy companies, gas stations, railroads, the airport and other critical infrastructure. Previously, in late December 2015, a multipronged attack on the Ukrainian electrical utility control system brought down the power grid in three provinces in Ukraine, resulting in power outages that lasted up to six hours and affected 225,00 customers.

The exposure to liability for the private sector for the insecurity of IoT devices is also now evident, as suggested by the lawsuit filed by the Federal Trade Commission (FTC) against D-Link Corporation for the misleading advertising of its security and the company's failure to address security flaws. Government agencies, IoT companies, and security-focused interest groups – including the Network – are all working to identify the full breadth of IoT security challenges and define frameworks and principles to address them.

Requirements and Opportunities for the Network

Network members were recruited from across industry, international organizations, civil society and academia to review and investigate the governance structure, IIoT security gaps and incentives/penalties/regulation that would drive improved IIoT security practices. The Protocol outlined in this document follows the agile governance model of policy development enabled by this type of multistakeholder collaboration. A list of Network members and contributors can be found in the appendix to this document. To maximize the success and impact of ongoing work, the Network will be guided by the following requirements and opportunities:

1. **The Network should have broad stakeholder representation.** Discussions about IIoT security typically involve technology companies and recognized academics. Only with recent, highly publicized IIoT security breaches have public policy experts joined the discussion and become aware of the depth and scope of the problem. The IIoT user community is much less well informed; it comprises organizations and individuals that lack expertise or even awareness about IIoT security and/or experience in implementing policy guidelines established for the public interest. Addressing IIoT security issues requires informed decision making by all of these constituencies.

2. **The Network should increase awareness about IIoT security concerns and their consequences.** User awareness about IIoT security issues, and even less so expertise in remediating IIoT security gaps, is low across all user communities and across vertical markets – from small business start-ups to sophisticated enterprise technologists. There is particular concern about security awareness at the IIoT device level, where connected devices and sensors typically lack security capabilities that are de rigueur in information technology systems; e.g., password change functionality and over-the-air updates. In addition to low awareness, entities deploying IIoT systems tend to attribute less weight to the future consequences of security breaches than would be expected based on standard models of time discounting. Without countervailing stakeholders that are biased towards future consequences, the direct and collateral damage to third parties would constitute a significant market failure. The insurance industry constitutes such a stakeholder and its engagement will propel behavioural changes by entities deploying IIoT systems, to whom underwriting services could be impacted by non-compliance with security standards.

3. **The Network should help entities deploying IIoT services to understand security issues.** Cybersecurity expertise is not typically the province of either vendors or users of IIoT systems. Many of the companies increasingly deploying and implementing IIoT have neither the capacity nor the long-term business strategy motivation to systematically address their cybersecurity vulnerabilities. Akin to the cognitive limitations that consumers experience with the consequence of major financial decisions, entities deploying IIoT services may be incapable of reconciling the asymmetry between multi-variable system design implementation decisions and the associated repercussions. Offsetting this asymmetry using mandatory information disclosure as a policy tool will have limited usefulness if the disclosure itself cannot be comprehended or easily implemented. Supplementing mandatory disclosure with a financial incentive to act efficaciously, and a financial disincentive to do otherwise – whether as a policy tool or by interested parties in the private sector – will lead to far higher levels of compliance than would the policy tool alone.

4. **The Network should help establish new incentive structures for IIoT security.** Achieving IIoT security requires a broad education outreach about IIoT security risks, definition of steps necessary to address security gaps and incentives/penalties to facilitate corrected behaviour. IIoT security has to be designed into products, systems and solutions during the design and implementation stages. Today, there are no governance structures in place to adequately incentivize IIoT security best practices. Market forces alone are insufficient to drive security best practices – today's economy incentivizes time-to-market and profitability and does not disincentivize bad behaviour since the consequences of a security breach often impact a diffuse group of third parties. The Network has identified a critical need to address IIoT user behaviour, product design and system implementation. Key elements include:

   - Education and awareness
   - Use of secure design principles
   - Insurance and risk mitigation
   - Data security
   - Legacy IIoT devices and implementations
   - Vertical market-specific extensions for highly regulated industries that also handle personally identifiable information; e.g., healthcare, finance, banking
   - Minimizing citizen impact of both IIoT security solutions and the consequences of security breaches
   - Agile regulatory structures

5. **The Network should encourage national governments to engage in public-private partnerships.** Taking into account the potential risk of terrorist attacks on critical infrastructure, including through the use of communications technologies, the UN Security Council has endorsed resolution 2341. Under this resolution, member states are called on to share knowledge and experience to protect critical infrastructure from terrorist attacks through cooperation domestically and across borders with governmental authorities, foreign partners and private-sector owners and operators. Resolution 2341 calls on member states to establish and strengthen public-private partnerships to protect, mitigate, investigate, respond to and recover from damage from terrorist attacks on critical infrastructure facilities, including through joint training, and the use or establishment of relevant communication or emergency warning networks. It also calls on member states to identify and share good practices in the protection of critical infrastructure.

6. **The Network should assist the insurance industry as it seeks to manage IIoT risks.** The Network should provide guidance in the development of metrics, materials and new tools that mitigate the IIoT risk and encourage the active hardening of systems and devices. Insurance is not an alternative to risk but rather one tool in the risk management strategy. Given the exponential hazards of both an interconnected environment and the extension into the physical environment to cause harm, the actuarial predictive models continue to be developed. Additionally, the few publicized instances of hacking or security breaches in IIoT and the levels of vulnerability of IIoT as part of the broader digitally networked environment have yet to be fully appreciated. There is a need to develop the sense of shared responsibility towards IIoT and to understand how, alongside all other measures, the insurance industry can assist to prevent, respond and recover from the hazards and threats. This modification of incentives is an integral part in the maintenance of respective levels of business confidence, continuity and reputation in the development of IIoT.

7. **The Network should leverage learnings from the historical role of insurance in confronting new risk scenarios.** Insurance schemes give incentives to actors to reduce risks by using, for example, differentiated premiums, deductions, exclusions and experience-rating. The insurance industry also plays a crucial role in the research and development of safety methods, the implementation of private safety codes, and the tailored coaching of safer conduct. Two examples of successful outreaches on technical issues with broad societal impacts both include well-defined incentives/penalties: (a) the electrical safety initiative launched in the 20th century by product manufacturers and insurance companies to ensure safer electrical products for business and home included incentives by insurance companies; and (b) the payment card industry initiative to entice merchants to implement best practices to protect financial transactions includes significant financial penalties for non-compliance.

Protocol Objective and Key Drivers for Impact

The objective of this Protocol is to improve the security of IIoT devices and systems, and align user, manufacturer and implementer behaviour with the broader public-interest goals of safety and security. The potential for harm from IIoT is spread across a vast multitude of organizations – each with minimal risk exposure but collectively with the possibility of a great magnitude of damage. Therefore, the policy solutions for IIoT safety and security must overcome the collective action challenges, utilizing mechanisms that have historically been instituted to manage widely distributed risk. The Protocol aims to leverage insurance programmes, standards and governance structures to create incentives – and realign demand/supply-side economics – to advance best practices in IIoT security design, implementation and maintenance. This framework is intended to strengthen security in IIoT systems using active hardening processes that can be validated with proven penetration, configuration and compliance techniques.

The IIoT ecosystem includes a variety of types of entities, each of whom has a collective interest in strengthening safety and security. These primary stakeholder groups include the following:

a) **Hardware makers**, who manufacture or assemble individual components or parts (e.g., sensors or microprocessors) that may be incorporated into IIoT devices or directly connected into a larger IIoT system architecture

b) **Device manufacturers**, who manufacture or assemble IIoT devices (e.g., factory equipment) included within a larger IIoT system architecture

c) **Network service providers**, who provide the connectivity required to establish a network of devices within the IIoT environment and manage corresponding device communications

d) **Data centre or cloud service providers**, who provide the storage and processing services related to IIoT device communications and data flows

e) **Middleware vendors**, who enable the integration and management of diverse IIoT devices and systems

f) **Software vendors**, who provide the platforms and tools for analysis, business intelligence and automation tied to IIoT data and devices

g) **IT service providers**, who provide a range of professional services to help plan, customize, roll out and operate IIoT systems

h) **Governments**, who regulate business and consumer environments and in many cases also manage or operate critical infrastructure related to IIoT

i) **Standards bodies**, who develop, coordinate, promulgate, interpret or otherwise engage in the distribution of technical standards to advance interoperability and other needs related to IIoT

j) **Industry groups**, who encourage collaboration among companies in the IIoT ecosystem and promote the advancement of shared interests

k) **Consumers**, who purchase and deploy IIoT systems and represent a broad range of industry verticals such as manufacturing, transport, logistics, agriculture, oil, gas and mining, food services, hospitality, energy and other utilities, health and real estate

l) **Civil society**, who represent and facilitate dialogue, and/or advocate on behalf of communities who are directly or indirectly impacted by IIoT

Whereas each of the above referenced stakeholder groups will have an interest in seeing this Protocol advanced, there are three distinct communities that are the target audience for this Protocol: (1) the financial sector, including the insurance industry community; (2) companies, governments and other entities who operate IIoT systems as end-users and may currently or in the future seek insurance policies to protect their firms against security risks associated with IIoT; and (3) national governments and international governance bodies focused on protection of critical infrastructure.

Insurance is an important market-based incentive mechanism, especially for fostering security-enhancing behaviour. Lower insurance premiums have prompted millions of business and consumers to install fire and security systems, and good driver discount programmes create tangible economic incentives to engage in safer and less risky behaviour. The same incentive structure can be applied to a Protocol for insuring IIoT systems. Insurance providers may use this Protocol not only to evaluate whether baseline requirements for insurability and/or conditions for differentiated premiums programmes have been met but also to differentiate between the strength and reliability of the implementation to inform the underwriting decision process. Whereas there is not a one-size-fits-all approach to implementing this Protocol, a breakdown of incident exposures and common insurance types has been included in the appendices as a framework for understanding the types of policies that may be most relevant to the management of IIoT security risks.

For companies, governments and other entities who operate IIoT systems as end-users, this document provides guidance on how to go about securing their IIoT operations according to increasingly accepted industry-wide standards. It aims to create new incentives for self-regulation of security concerns and encourages a preventive approach to cybersecurity rather than waiting for government regulation to define the terms and obligations. The improvement of safety and security practices in IIoT system deployments should serve as a benchmark of expectations for other deployments across the supply chain, and have a positive influence on consumer IoT security practices.

For national governments and international governance bodies, the Protocol provides a means of initiating a dialogue with domestic industries and its relation to concerns over the safety and security of critical infrastructure in the interconnected IoT environment. The Protocol supports mechanisms by which IIoT system providers can share information about their vulnerabilities in a way that maximizes safety and security in the public interest.

Additional opportunities to enhance the preventive measures surrounding IIoT include greater open-source intelligence; increased risk assessment; greater levels of scenario building and testing; access to risk-management platforms; incident response planning exercises; and specialist risk engineering. In response to an IIoT incident, there is also the opportunity to enhance loss investigation; implementation of response strategy; emergency support; IT forensics; specialist legal and public relations support; and funding support.

IIoT Safety and Security Protocol

Requirements for Insurability and/or Participation in Differentiated Premiums Programmes

As part of a broader risk mitigation strategy to improve the safety and security of IIoT systems and operations, insurers shall establish clear requirements for insurability and/or participation in differentiated premiums programmes. These foundational requirements guide participating entities to take specific steps based on best practices to integrate cybersecurity and resilience against attack into its operations, processes and work product.

IIoT security should be infused throughout an entity deploying IIoT systems overall strategy, culture, information technology (IT) and operational technology (OT). It should then be verified through corporate governance and risk management mechanisms. Entities deploying IIoT systems should also have procedures in place to detect, mitigate, verify and manage IIoT security risks and vulnerabilities throughout the entire life cycle of the IIoT system.

Towards this goal, the Protocol sets forth baseline conditions that shall be required for insurability and/or participation in pricing discount programmes in three areas: Line of Business IIoT Device Safeguards; Internal Governance and Risk Management; and Record-Keeping and Metrics.

A. Line of Business IIoT Device Safeguards

An entity deploying IIoT systems must demonstrate that the following safeguards are implemented for the IIoT devices or systems it designs, builds, installs, maintains, monitors, interacts with and/or controls. The adoption and implementation of appropriate, existing and recognized IIoT security standards is a critical component of effective risk management.

1. **Risk-assessment models.** Entities installing and operating IIoT systems must employ a risk-assessment model that first identifies all of the digital and physical assets that need to be protected. The risk assessment model should identify the risk factors that affect the IIoT system processes and the possible threat agents as well as the inclusion of a thorough vulnerability assessment. The risk-assessment model should be based on risk factors that are defined as acceptable or not acceptable, and provide scoring in a vulnerability assessment on identified risks. There should be executive management responsibility and adjudication of risk assessments with an annual review and audit of said risks.

2. **Segmentation.** Entities deploying IIoT systems must correctly segment the assets into logically isolated sub-systems that share common security requirements based upon risk assessment models. Information flow and access within and between subsystems must be restricted utilizing network mechanisms such as identity, context, role- and policy-based access, next-generation firewalls and gateways.

3. **Device integrity and availability.** Devices, components and endpoints of a system that have been defined as critical assets should use a model for defining the endpoints' value in the system. If the device's value is tied to data and system integrity, mechanisms should be in place to protect it. If the device's value is tied to availability and reliability, mechanisms should be in place to provide uptime. If the device's value is tied to confidentiality, the same applies. Using a CIA model for devices' risk to the system should be declared as part of the risk assessment.

4. **Encryption.** Entities deploying IIoT systems must ensure that new devices and associated applications support current, generally accepted security and cryptography protocols and best practices, where applicable. Data both at rest and in transit, that is scored in the risk assessment to be protected, should include sufficient industry accepted practices to secure the data. Many industrial protocols currently in use were not designed with security in mind and lack basic authorization and encryption features. Entities deploying IIoT systems should properly address these challenges utilizing additional security controls and upgrade to systems supporting encryption whenever possible.

5. **Patches and updating.** Entities deploying IIoT systems must have mechanism-updating software on the devices, components and software to validate that the software has been delivered from a trusted source and has not been tampered with. Delivery mechanisms can be automated and/or manual depending on the environment and should allow for the ability to roll back easily. System installers and operators should have proficiency in delivering the updates, and designers and manufacturers should develop mechanisms to deliver those changes.

6. **Privacy.** All personally identifiable data in transit and in storage must be encrypted using current and generally accepted security standards.

7. **Interoperability.** IIoT devices and services must be able to communicate with one another using standard protocols – not only with a base station. Devices should use standard ports for network traffic.

8. **Software development lifecycle.** Entities deploying IIoT systems must ensure all IIoT devices, services and associated software have been subjected to a rigorous, standardized software development lifecycle process and methodologies including unit, system, acceptance, regression testing and threat modelling, along with maintaining an inventory of the source for any third-party/open-source code and/or components utilized. These entities should employ generally accepted code and system-hardening techniques across a range of typical use case scenarios and configurations, including preventing any data leaks between the device, apps and cloud services. Manufacturers should use a secure development lifecycle process that is tied into threat modelling and the risk assessment identified. Those processes should demonstrate industry best practices on securing code base, using threat modelling and risk assessment, supply chain management of software contents and sources, and penetration testing based on the risk assessment of the products and software.

9. **Root of trust.** Entities installing and operating systems should create trusted networks with trust zones that define the communication paths within a system. The trust zones can define how data and endpoints are protected within the trust zones.

10. **Vulnerability disclosures.** Entities deploying IIoT systems must establish coordinated vulnerability disclosure, including processes and systems to receive, track and promptly respond to external vulnerabilities' reports from third parties.

B. Internal Governance and Risk Management

An entity deploying IIoT systems must demonstrate adequate internal governance and risk-management mechanisms for the IIoT devices or systems it designs, builds, installs, maintains, monitors, interacts with, and/or controls. The Forum's Advancing Cyber Resilience: Principles and Tools for Boards, from which the list below is adapted, provides a business model and best practices for such mechanisms at the board level.

1. **Board oversight.** The entities deploying IIoT system's board and senior leadership must formally review the organization's IIoT cyber strategy (prevention, transfer and response) as part of the firm's risk-management strategy (avoidance, reduction, sharing and retention) and business continuity plans, and engage in governance and oversight of this strategy.

2. **Top-level accountability.** Entities deploying IIoT systems must identify a "responsible officer" for cybersecurity/resilience and ensure that business and IT personnel have appropriate command of the subject. In addition to, or as part of this role, entities deploying IIoT systems must also have an officer accountable for organizational security/resilience and implementation of a responsibility assignment matrix (RAM). There should also be mechanisms put in place to ensure that information flows from individual roles back up to management. See appendix for further explanation of the RAM, as well as multiple alternative participation types.

3. **Cyber-resilience.** Entities deploying IIoT systems must demonstrate that cyber-resilience is integrated into business strategy; and quantify and determine organizational cyber risk strategy and assessment, with a combined approach towards people, capital and technology.

4. **Ongoing assessment.** Entities deploying IIoT systems must conduct frequent and thorough assessments of assets throughout the service and endpoint ecosystems.

5. **Ongoing testing.** Entities deploying IIoT systems must prepare and adhere to IIoT security best practices throughout its distribution, installation, service and maintenance channels; and, throughout the life-cycle of the IIoT service, periodically test IIoT cybersecurity and resiliency using penetration testing and other proven security techniques.

6. **Track and address legacy systems.** Entities deploying IIoT systems must initiate processes to track and address legacy and obsolete solutions and ensure adequate maintenance.

7. **Information sharing.** Entities deploying IIoT systems must operationalize the sharing of information about threats and vulnerabilities with recognized intermediaries from the private sector or government agencies.

8. **Incident response.** Cyber-event handling procedures should be developed on how to respond, triage and publicly react to a potential event. Forensic plans to identify the level of an event and its impact should be planned and audited annually. This should involve senior and board level engagement.

C. Record-Keeping and Metrics

Business decision-makers should monitor reports on the security of their IIoT systems from the moment the systems are conceived, through their design and creation and throughout their operation. The correct measures and metrics inform decision-makers, operators and other stakeholders. While some of the metrics and measures will vary according to the distinctive contextual considerations of the vertical industry of its application, some security metrics are common across industries, such as: the number of detected attack attempts and the breakdown of those attempts; as well as characterizing successful attacks, incidents, close calls, policy violations and anomalies that have merited investigations.

1. **Performance indicators.** Entities deploying IIoT systems must establish clear and accurate representations (dashboards and other visualizations) of security metrics, including data sources, communications and system capabilities, as well as key performance identifiers that would allow operational and business personnel to make improved business decisions. Security then becomes a valuable part of the operational process and its value can be quantified in terms of the costs by averting wrong decisions.

2. **Metrics.** Entities deploying IIoT systems must establish security metrics to ensure a continuous feedback loop to identify areas of risk, increase accountability, improve security effectiveness, demonstrate compliance with laws and regulations and provide quantifiable inputs for effective decision-making. Such metrics help identify security problems early and assist in faster and more efficient management and governance.

Implementation of Protocol

The implementation and success of this Protocol will require on the active participation of key stakeholders across the IIoT ecosystem. The Protocol is rooted in a model of incentive-based self-regulation by entities who are deploying IIoT systems. As such, it assumes that governments will either not actively or will inconsistently regulate these areas. The support of governments will also be critical in the creation of mechanisms by which IIoT system providers can share information about their vulnerabilities in a way that maximizes safety and security in the public interest.

Implementation of the Protocol will occur at or before the determination of insurability or consideration for differentiated premiums. It is assumed that legacy IIoT devices or systems will not be grandfathered in; rather, implementation of the Protocol must occur prior to issuing new insurance or renewing existing insurance. IIoT insurers will assess applicants by using the above referenced requirements to determine insurability or acceptance into differentiated premiums programmes and provide guidance to applicants based on this review.

To assess whether or not entities deploying IIoT systems meet these requirements, insurers are likely to expect the following indicators of compliance:

1. Appropriate internal security safeguards to ensure that the entity deploying IIoT systems complies with Protocol requirements and regards security as a vital component of its overall business strategy.

2. Certification or assurance that the IIoT Firm has adopted the Protocol requirements including appropriate IIoT standards. The IIoT insurer is likely to determine the applicable standard(s) pertinent to each use.

3. IIoT insurers may contribute to the indicators and data consortium relevant information and analysis to ensure a better overall understanding of IIoT security.

4. Proof of assets sufficient to maintain and update already deployed (also known as “legacy”) IIoT systems in compliance with Protocol requirements to ensure security in the face of evolving IIoT security threats throughout the life cycle of the IIoT systems.

Information related to security breaches and incidents implicating IIoT devices or implementations is critical to determinations of the insurability. To ensure the availability of these indicators and data, this Protocol recommends the creation of a consortium of entities deploying IIoT systems and IIoT insurers to pool these data and establish insurability indicators and risk assessments. This consortium will be furnished with data and indicators by entities deploying IIoT systems and IIoT insurers. A Protocol for the development of the consortium and its operation may be the subject of a future expert network.

Entities deploying IIoT systems, IIoT insurers, and interested third parties (e.g., security providers, consultants, and regulatory bodies) should provide relevant data and indicators (or results of analysis or proprietary data) to the indicators and data consortium. This consortium can be a vital source of the information necessary to assess insurability of the IIoT ecosystem.

Verification mechanisms for this Protocol relate to entities deploying IIoT systems and IIoT insurers. These entities and IIoT insurers need to verify the operation of this framework in incentivizing security through insurability as well as the efficacy of the Protocol components. Verification procedures should be determined by the IIoT community and regularly exercised and reviewed.

To maintain the applicability of this Protocol in the face of evolving IIoT security risks – from time to time new findings, security standards, cybersecurity principles and best practices will need to be incorporated into the Protocol. IIoT insurers should regularly survey and monitor the IIoT security standards ecosystem to ensure that applicable standards listed in the appendix are up-to-date and that entities deploying IIoT systems continue to apply appropriate standards to legacy and new IIoT devices and systems. Further maintenance measures will need to be determined as this Protocol is applied to IIoT system deployments and insurers.

IIoT should be viewed as a property of digitization and cyber infrastructure, the means and medium through which computing devices and systems will connect, and should be studied and governed under this overall framework. Emerging technology, such as quantum computing and developments in space, machine learning and automation, should be closely monitored by the Network to ensure the Protocol remains effective and up-to-date.

Conflicts relating to this Protocol should be resolved in a manner to be determined by the affected community. Any conflict-resolution mechanism must be transparent and provide an opportunity for all interested parties to submit the basis for their dispute to a neutral third party.

Appendices

A. Network of Experts

Protocol Design Network for Industrial Internet Safety and Security

Co-Chairs:
Michael McNeil – Head of Product Security & Services, Royal Phillips
David Scharia – Director, Chief of Branch, United Nations Security Council Counter-Terrorism Executive Directorate (UN CTED)

Members:
Benedikt Abendroth – Cybersecurity Strategy, Microsoft
Siby Abraham – Vice-President, Chief Technologist, Wipro
Lori Bailey – Global Head of Cyber Risk, Zurich Insurance Company
Sukamal Banerjee – Corporate Vice-President, Hi-Tech & Communications, BU Head IoT Works, HCL Technologies
Urs Gasser – Professor of Practice, Harvard Law School
Ryan Gillis – Vice-President, Cybersecurity Strategy & Global Policy, Palo Alto Networks
Haizhou Gu – Office of the CITO, UN CTED
Chris Harrison – Assistant Professor of Human-Computer Interaction, Carnegie Mellon University
Vijayakumar Kabbin – General Manager, Wipro
Isha Kharbanda – Group Manager, Corporate Marketing, HCL Technologies
Aaron Kleiner – Director, Industry Assurance and Policy Advocacy, Microsoft
Edy Liongosari – Chief Research Scientist, Accenture Labs
Jesus Molina – Director of Business Development, Waterfall Security Solutions
David O'Brien – Senior Reseearcher, Berkman Klein Center for Internet & Society, Harvard University
Gil Perez – Senior Vice-President, IoT & Digital Supply Chain, SAP
Marc Porret – ICT Coordinator, UN CTED
Tony Shakib – IoT & Intelligent Cloud BD, Microsoft
Hamed Soroush – Senior Member, Research Staff, PARC/Xerox
Michael Tennefoss – Vice-President of Strategic Partnerships, Aruba, a Hewlett Packard Enterprise company
William Westerlund – Talent Acquisition, Accenture

Industrial Internet Safety and Security Experts Community

Maarten Botterman – Chair, Dynamic Coalition on Internet of Things, Internet Governance Forum
Maya Bundt – Head of Cyber & Digital Solutions, Swiss Reinsurance Company
Leslie Chacko – Director & Head, Emerging Technologies, Global Risk Center, Marsh & McLennan Companies
Anupam Chander – Professor of Law, University of California, Davis School of Law
Andrew Hall – Client Relationship Director, Willis Towers Watson
Ajit Jillavenkatesa – Senior Policy Advisor, Standards and Digitization, National Institute of Standards and Technology (NIST), United States Department of Commerce
Karen McCabe – Senior Director, Technology Policy and international Affairs, Institute of Electrical and Electronics Engineers (IEEE)
Ken Modeste – Principal Engineer, Security and Global Communications, Underwriters Laboratory
Jayraj Nair – Vice-President, Global Head of IoT, Wipro
Caio Mario da Silva Pereira Neto – Professor, Fundação Getulio Vargas (FGV) São Paulo
Ian Smith – Technical Lead, IoT Programme, GSM Association (GSMA)
Rachna Stegall – Global Director, Connected Technologies, UL

World Economic Forum Contributors

Daniel Dobrygowski – Lead, IT Industry
Eddan Katz – Lead, Digital Protocol Networks
Jeff Merritt – Head, Internet of Things
Anne Toth – Head, Data Policy
Alex Wong – Head, Global Challenge Partnerships
Melody Chang – Community Specialist, IoT and Blockchain

B. Incident Exposures and Insurance Types

Incident Type Group	Coverage Scope
Business interruption; interruption of operations	Reimbursement of lost profits caused by a production interruption not originating from physical damage
Contingent business interruption (CBI) for non-physical damage	Reimbursement of the lost profits for the observed company caused by related third parties (supplier, partner, provider, customer) production interruption not originating from physical damage
Data and software loss	Costs of reconstitution and/or replacement and/or restoration and/or reproduction of data and/or software which have been lost, corrupted, stolen, deleted or encrypted
Financial theft and/or fraud	Pure financial losses arising from cyber internal or external malicious activity designed to commit fraud, theft of money or theft of other financial assets (e.g., shares); it covers both pure financial losses suffered by the observed company or by related third parties as a result of proven wrong-doing by the observed company
Cyber ransom and extortion	Costs of expert handling for a ransom and/or extortion incident combined with the amount of the ransom payment (e.g., access to data is locked until ransom is paid)
Intellectual property theft	Loss of value of an intellectual property asset, resulting in pure financial loss
Incident response costs	Compensation for crisis management/remediation actions requiring internal or external expert costs, but excluding regulatory and legal defence costs Coverage includes: - IT investigation and forensic analysis, excluding those directly related to regulatory and legal defences costs - Public relations, communication costs - Remediation costs (e.g., costs to delete or cost to activate a "flooding" of the harmful contents published against an insured) - Notification costs
Breach of privacy	Compensation costs after leakage of private and/or sensitive data, including credit-watch services, but excluding incidents response costs
Network security/ security failure	Compensation costs for damages caused to third parties (supplier, partner, provider, customer) through the policyholder/observed company's IT network, but excluding incident response costs; the policyholder/observed company may not have any damage but has not been used as a vector or channel to reach the third party
Reputational damage (excluding legal protection)	Compensation for loss of profits due to a reduction of trade/clients because they lost confidence in the impacted company
Regulatory and legal defence costs (excluding fines and penalties)	A: Regulatory costs – compensation for costs incurred to the observed company or related third parties when responding to governmental or regulatory inquiries relating to a cyberattack (covers the legal, technical or IT forensic services directly related to regulatory inquiries but excludes fines and penalties) B: Legal defence costs – coverage for own defence costs incurred to the observed company or related third parties facing legal action in courts following a cyberattack
Fine and penalties	Compensations for fines and penalties imposed on the observed company; insurance recoveries for these costs are provided only in jurisdictions where it is allowed.
Communication and media	Compensation costs due to misuse of communication media at the observed company resulting in defamation, libel or slander of third parties, including web-page defacement, as well as patent/copyright infringement and trade secret misappropriation
Legal protection – lawyer fees	Costs of legal action brought by or against the policyholder, including lawyer fees costs in case of trial; e.g., identity theft, lawyer costs to prove the misuse of victim's identity
Assistance coverage – psychological support	Assistance and psychological support to the victim after a cyber-event leading to the circulation of prejudicial information on the policyholder without his/her consent
Products	Compensation costs in case delivered products or operations by the observed company are defective or harmful resulting from a cyber-event, excluding technical products or operations (tech errors and omissions, E&O) and excluding professional services E&O
Directors and officers (D&O)	Compensation costs in case of claims made by a third party against the observed company directors and officers, including breach of trust or breach of duty resulting from cyber-event

Tech E&O	Compensation costs related to failure in providing adequate technical service or technical products resulting from a cyber-event
Professional services E&O, professional indemnity	Compensation costs related to the failure in providing adequate professional services or products resulting from a cyber-event, excluding technical services and products (tech E&O)
Environmental damage	Coverage scope: compensation costs after leakage of toxic and/or polluting products consecutive to a cyber-event
Physical asset damage	Losses (including business interruption and contingent business interruption) related to the destruction of physical property of the observed company due to a cyber-event at this company
Bodily injury and death	Compensation costs for bodily injury or consecutive death through the wrong-doing or negligence of the observed company or related third parties (e.g., sensible data leakage leading to suicide)

Appendix C. Relevant Definitions

Term	Definition	Source
Access control	Means to ensure that access to assets is authorized and restricted based on business and security requirements; note: access control requires both authentication and authorization	ISO/IEC 27000:2016
Data integrity	Property that data has not been altered or destroyed in an unauthorized manner	ISO/IEC 27040:2015
Industrial internet	Internet of things, machines, computers and people, enabling intelligent industrial operations using advanced data analytics for transformational business outcomes	IIC
Industrial internet of things (IIoT) system	System that connects and integrates industrial control systems with enterprise systems, business processes and analytics	IIC
IoT device	Endpoint component of an IIoT system that interacts with the physical world through sensing or actuating	IIC
IoT sensor	Component of an IoT device that observes properties of the physical world and converts them into a digital form	IIC
Reliability	Ability of a system or system component to perform its required functions under stated conditions for a specified period of time	ISO/IEC 27040:2015
Resilience	Ability of a system or system component to maintain an acceptable level of service in the face of disruption	IIC
Safety	The condition of the system operating without causing unacceptable risk of physical injury or damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment	ISO/IEC Guide 55:1999(1)
Security	Property of being protected from unintended or unauthorized access, change or destruction ensuring availability, integrity and confidentiality	IIC
Trustworthiness	Degree of confidence one has that the system performs as expected with characteristics including safety, security, privacy, reliability and resilience in the face of environmental disruptions, human errors, system faults and attacks	IIC
Vulnerability	Weakness of an asset or security controls that can be exploited by one or more threats	ISO/IEC 27000:2016(1)

D. Responsibility Assignment Matrix

Security touches every element of an IIoT device and system lifecycle, and consequently IIoT safeguards require cross-functional, cross-departmental and cross-company collaboration.

A responsibility assignment matrix (RAM) is a charting system that describes the participation by various roles in completing tasks or deliverables for a project or business process. It is especially useful in clarifying roles and responsibilities in complex projects and processes. It is intended to reduce confusion and increase project efficiency, while placing a focus on accountability and making sure that the workload is evenly distributed. It is often referred to by the acronym RACI (R = responsible, A = accountable, C = consulted, I = informed) and multiple alternative variations on the process include: PARIS (participant, accountable, review required, input required, sign-off required); PACSI (perform, accountable, control, suggest, informed); RASI (responsible, accountable, support, informed); DAVI (driver, approver, contributors, informed); RAPID (responsibility, authority, task, support, informed).

The following are considered important insurance considerations for the design, manufacturing, service, distribution, integration and other uses of IIoT, creating a RAM for personnel to implement active security hardening:

1. Identifying the devices, processes and systems that comprise its IIoT exposure
2. Security vulnerability assessment and gap-remediation plan
3. Secure configuration assessment and gap-remediation plan
4. Secure application assessment and gap-remediation plan
5. Secure management and patch assessments and gap-remediation plan
6. Secure data transport and storage assessment and gap-remediation plan
7. Secure firmware, software, hardware and application upgrades and end-of-life assessments and remediation plan
8. Secure integration testing, penetration testing and compliance testing during the design, commissioning, and run stages and gap-remediation plan

E. Indicative Chart of IoT Resources

The following collection of resources is intended to provide a summary of some commonly cited standards and guidelines related to IoT. It should not be viewed as a comprehensive or exhaustive list.

Organization	Publication	Abstract	Publication Date	Ecosystem Approaches	Domain Covered
NIST (National Institute of Standards and Technology)	Special Publication 800-160 (Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems)	a) Breaks down processes into four categories: 1. Agreement processes 2. Organization-project enabling processes 3. Technical management processes 4. Technical processes b) Focuses on system-security engineering c) From stakeholders' perspective d) Uses international standards	11/15/2016	Manufacturer and consumer perspective	Generic
IIC (Industrial Internet Consortium)	Industrial Internet of Things Volume G4: Security Framework	a) Breaks down industrial space into three roles: 1. Component builders 2. system builders 3. Operational users b) Separates security evaluation into: 1. Endpoint 2. Communications and connectivity 3. Monitoring and analysis 4. Configuration and management c) Focuses on five specific IIoT characteristics: safety, security, privacy, reliability and resilience d) Delivers security from business, functional and implementation perspectives e) Well-designed risk assessments	09/19/2016	Technological perspective	Industrial IoT

DHS (Department of Homeland Security)	Strategic Principles for Securing the Internet of Things (IoT)	a) Highlights approaches and suggested practices to fortify the security of the IoT b) Provides stakeholders with tools to comprehensively account for security as they develop, manufacture, implement, or use network-connected devices c) Focuses on the following key areas: 1. Incorporating security at the design phase 2. Advancing security updates and vulnerability management 3. Building on proven security practices 4. Prioritizing security based on potential impacts 5. Promoting transparency across the IoT ecosystem 6. Connecting carefully and deliberately	11/16/2016	Manufacturer and consumer perspective	Generic
GSM Association	IoT Security Guidelines	The GSMA IoT Security Guidelines provide best practice for the secure design, development and deployment of IoT solutions across industries and services. Addressing typical cybersecurity and data privacy issues associated with IoT services, the guidelines outline a step-by-step process to securely launch IoT solutions to market and keep them secure through their lifecycles.	10/31/2017	Technological perspective	Generic
GSM Association	IoT Security Assessment Scheme	The purpose of this document is to enable the suppliers of IoT products, services and components to self-assess the conformance of their products, services and components to the GSMA IoT Security Guidelines. Completing a GSMA Security Assessment will allow an entity to demonstrate the security measures it has taken to protect its products, services and components from cybersecurity risks.	09/29/2017	Technological perspective	Generic
IoTAA (IoT Alliance Australia)	Internet of Things Security Guideline	a) Promotes a 'security by design' approach to the IoT b) Assisting businesses, carriers and digital service providers (who use IoT systems or devices) in various industries to better understand the practical application of security and privacy for IoT device use c) Promoting awareness of the relevant legislative framework d) Assists industry to understand some of the relevant legislation on privacy and security	02/23/2017	Technological perspective	Generic
OWASP (Open Web Application Security Project)	IoT Security Guidance	a) Manufacturer IoT security guidance b) Developer IoT security guidance c) Consumer IoT security guidance	02/14/2017	Technological perspective	Generic
OTA (Online Trust Alliance)	IoT Trust Framework	a) Includes a set of strategic principles to help secure IoT devices b) Key principles have been identified for different areas c) Outlines mandatory requirements, including comprehensive and security patching post-warrant	01/05/2017	Technological perspective	Generic

IoTSF (IoT Security Foundation)	IoT Security Compliance Framework	a) Provides a comprehensive and practical checklist to guide organizations through a security-assuring process b) Offers a methodical approach to determining an organization's unique security posture for both business processes and technical requirements c) Designed to be generally applicable and extendable	12/06/2016	Technological perspective	Generic
UL (Underwriters Laboratory)	UL 2900-1: Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	a) Requirements regarding the software developer (vendor or other supply chain member) risk-management process for its product b) Methods by which a product shall be evaluated and tested for vulnerabilities, software weaknesses and malware c) Requirements regarding the presence of security-risk controls in the architecture of a product	07/05/2017	Technological perspective	Generic
UL (Underwriters Laboratory)	UL 2900-2-2: Particular Requirements for Industrial Control Systems	This security evaluation outline applies to industrial control system components, including: a) Programmable logic controllers (PLC) b) Distributed control systems (DCS) c) Process control systems d) Data acquisition systems e) Historians, data loggers and data storage systems f) Control servers g) SCADA servers h) Remote terminal units (RTU) i) Intelligent electronic devices (IED) j) Human-machine interfaces (HMI) k) Input/output (IO) servers l) Fieldbuses m) Networking equipment for ICS systems n) Data radios o) Smart sensors p) Controllers q) Embedded system/controllers	03/20/2016	Technological perspective	Industrial IoT

Endnotes

1 Discussion of the Shared Responsibility framework for Internet Governance in the context of IoT further articulated in: Cerf, Vinton G. and Ryan, Patrick S. and Senges, Max and Whitt, Richard S., IoT Safety and Security as Shared Responsibility (February 21, 2016). Journal of Business Informatics, Number 1, Issue 35 (2016), pp 7-19, https://ssrn.com/abstract=2735642.

2 Klaus Schwab, "The Fourth Industrial Revolution: What it means and how to respond," (14 Janury 2016), https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

3 For a discussion of security within the context of public policy issues concerning cyber physical systems, see Laura DeNardis and Mark Raymond, "The Internet of Things as a Global Policy Frontier," 51:2 UC Davis L. Rev, 475 (December 2017), https://lawreview.law.ucdavis.edu/issues/51/2/Symposium/51-2_DeNardis_Raymond.pdf.

4 The Industrial Internet Consortium, "The Industrial Internet Vocabulary Technical Report V 2.0," (July 2017), http://www.iiconsortium.org/vocab/index.htm

5 World Economic Forum, "Industrial Internet of Things: Unleashing the Potential of Connected Products and Services," (January 2015), http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf.

6 See World Economic Forum, "Impact of the Fourth Industrial Revolution on Supply Chains," (October 2017), http://www3.weforum.org/docs/WEF_Impact_of_the_Fourth_Industrial_Revolution_on_Supply_Chains_.pdf

7 Accenture Technology, "Winning With the Internet of Things," (January 2015), https://www.accenture.com/us-en/insight-industrial-internet-of-things.

8 Benson Chan, "IoT vs. Industrial IoT: 10 Differences That Matter," IoT for All, (14 December 2017), https://www.iotforall.com/iot-vs-industrial-iot-differences-that-matter/.

9 Bruce Schneier, "Click Here to Kill Everyone: With the Internet of Things, we're building a world size robot. How are we going to control it?"," New York Magazine, 27 January 2017, http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html/.

10 Lily Hay Newman, "The Botnet that Broke the Internet Isn't Going Away," Wired Magazine (9 December 2016). https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/

11 Nicole Perlroth, Mark Scott, and Sheera Frankel, "Cyberattack Hits Ukraine Then Spreads Internationally," New York Times (27 June 2017), https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

12 For a technical analysis, see E-ISAC, SANS ICS. "Analysis of the Cyber Attack on the Ukrainian Power Grid" (18 March 2016), http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

13 Lesley Fair, "D-Link Case Alleges Inadequate Internet of Things Security," Federal Trade Commission (5 January 2017) https://www.ftc.gov/news-events/blogs/business-blog/2017/01/d-link-case-alleges-inadequate-internet-things-security

14 For a survey of regulatory issues and relevant ICT governance bodies, see Ian Brown, "Regulation and the Internet of Things," in Trends in Telecommunication Reform 2016: Regulatory Incentives to Achieve Digital Opportunities, International Telecommunications Union (ITU) 2016, http://www.itu.int/pub/D-PREF-TTR.17-2016.

15 For an articulation of agile governance and the conditions of dynamic policy development, see World Economic Forum, "Agile Governance: Reimagining Policy-making in the Fourth Industrial Revolution," (January 2018)

16 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4076052/

17 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4265800/

18 UN Security Council, Security Council resolution 2341 (2017) [on threats to international peace and security caused by terrorist acts], 13 February 2017, S/RES/2341 (2017), available at: http://www.refworld.org/docid/58b40b6310.html

19 For a broad discussion of the relationship between private insurance and government in the regulation of behavior, see Kyle D. Logue & Omri Ben-Shahar, "Outsourcing Regulation: How Insurance Reduces Moral Hazard" 111 Mich. L. Rev. 197 (2012), http://repository.law.umich.edu/mlr/vol111/iss2/2.

20 For a list of definitions related to specific terms referenced herein, please see the appendices.

21 World Economic Forum, "Advancing Cyber Resilience: Principles and Tools for Boards," (January 2017), http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf

22 Source: CRO Forum Concept Paper on a proposed categorization methodology for cyber risk. (June 2016) Available at https://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web-2.pdf.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org