WORLD ECONOMIC FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

Center for the Fourth Industrial Revolution

Industrial Internet of Things Safety and Security Digital Protocol Network

Digital Protocols are defined as informal norm-setting frameworks that are accompanied over time by (i) detailed specifications, (ii) operational processes, (iii) implementation guidelines, (iv) verification instruments, (v) maintenance procedures, and/or (vi) conflict/dispute resolution mechanisms.

Contents

Executive Summary 2
Background and Need 2
Definitions 3
Focus of the Network 4
IIOT SAFETY AND SECURITY DIGITAL PROTOCOL 7
I. Requirements for Insurability of IIoT Services 7
A. Line of Business IIoT Device Safeguards 7
B. Internal Governance and Risk Management 8
II. Operation of Protocol 10
A. Assessment mechanisms 10
B. Insurability requirements 10
III. Implementation of Protocol 10
A. Safeguards Assurance 10
B. Indicators & Data Clearinghouse 11
IV. Verification of Protocol 11
V. Maintenance of Protocol 11
Network & Community Comments 12
Recommendations and Next Steps 14
Conclusion 14

[INSERT DISCLAIMER (attn.: legal) e.g. “The World Economic Forum disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the publication, use of, or reliance on Digital Network Protocols or the IIoT Protocols. The World Economic Forum also makes no guaranty or warranty as to the accuracy or completeness of any information published herein.]

Executive Summary

The World Economic Forum (the 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 the existing challenges to the development of an optimally secure IIoT and focused on actionable solutions to those challenges.

The Network is developing a protocol framework through which actors can be aligned around incentives that ensure the security of IIoT products, practices, and infrastructure that abide by the obligations of shared responsibility[1] for the safety and security of critical infrastructure. The IIoT ecosystem has no single stakeholder, and no single category of actors who bear the primary responsibility for its governance. When the risk of harm is so widely spread, public safety and preventative 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 Digital Protocol (the Protocol) aims to develop an understanding of how insurance, as a key part of the incentive structures of cybersecurity norm-setting and governance, can facilitate the improvement of IIoT security design, implementation, and maintenance practices. The developing frameworks are intended to increase the security IIoT services using active hardening processes that can be validated using proven penetration, configuration, and compliance techniques.

Background and Need

IIoT presents new opportunities for societal transformation through technology, especially for enterprises that harness the promise of IIoT to improve business processes and for governments that look to IIoT to improve infrastructure and the provision of vital services. Indeed, IIoT 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.[2]

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

[1] Discussion of Shared Responsibility in this context further articulated in:
Internet Governance Is Our Shared Responsibility. Vint Cerf, Patrick Ryan, Max Senges
I/S: A Journal of Law and Policy for the Information Society, 10 ISJLP 1 (2014).
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309772;
IoT Safety and Security as Shared Responsibility. Vint Cerf, Patrick Ryan, Max Senges, Richard Whitt
Journal of Business Informatics, Number 1, Issue 35 (2016), pp 7-19
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2735642

[2] https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

As IIoT transforms previously isolated systems to a connectivity that is more intertwined with our day-to-day lives and businesses, it creates dependencies on the robust functionality of that infrastructure undermined by security breaches. The IoT's extension into physical spaces combines the familiar digital risks within the policy realms of cybersecurity into real-world effects with substantial vulnerability to public safety, physical harm, and catastrophic systemic attacks on commonly shared public infrastructure. The very nature of the vulnerabilities have therefore changed. The attack surface for bad actors willing to exploit the digitally networked environment now penetrates into the home with the popularity consumer devices, spreads across the transportation 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 our critical infrastructure would be far reaching, reaching further 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.

Known IIoT security vulnerabilities are widespread, spanning from low-end consumer devices, increasingly being used in manufacturing processes, through to large scale industrial systems.[3] The time when decisions about cybersecurity risk exposure can be postponed has already passed. The Mirai botnet virus, which targeted "zombie" legacy IoT devices that were not regularly being updated, 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.[4] The exposure to liability 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 Corp. for the misleading advertising of their security and the company's failure to address security flaws.[5] Government agencies, IIoT firms, and security-focused interest groups—including the Network—are all working to identify the full breadth of IIoT security challenges and define frameworks and principles to address them.

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 of Things (IIoT)	Machines, computers, networks, 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

[3] J.M. Porup, "'Internet of Things' Security is Hilariously Broken and Getting Worse," *Ars* Technica, January 23, 2016, https://arstechnica.com/information-technology/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/

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

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

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)

Focus of the Network

Network members were recruited from across industry, International organisations, 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. To maximize the success and impact of this work, the Network shall be guided by the following observations which surfaced during scoping discussions in October 2016.

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 is comprised of organizations and individuals that lack expertise or even awareness about IIoT security and/or experience with implementing public policy guidelines established for the common good. 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, much less 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 rigeur in information technology systems, e.g., password change functionality and over-the-air updates. In addition to low awareness, IIoT suffers from present bias by firms and users who 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 their engagement will propel behavioral changes by firms and users to whom underwriting services could be impacted by non-compliance with security standards.

3. The Network should help IIoT Firms and users 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,[6] IIoT Firms and users 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.[7] 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 behavior. 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 incentivize IIoT security best practices. Market forces alone are insufficient to drive security best practices: in today's economy they incentivize time-to-market and profitability, and do not disincentivize bad behavior since the consequences of a security breach often impact a diffuse group of third parties. The Network has identified an incentive framework and Protocol for IIoT security to address IIoT user behavior, 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, and 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 terrorists groups' attacks on critical infrastructure including through the use of communications technologies, the UN Security Council has stepped in and endorsed resolution 2341[8]. Under this resolution Member States are called to protect critical infrastructure from terrorist attacks including through cooperation domestically and across borders with governmental authorities, foreign partners, and private sector owners and operators to share knowledge and experience. Resolution 2341 calls on Member States to establish and strengthen public-private partnerships in order to protect, mitigate, investigate, respond to, and recover from damage from terrorist attacks on critical infrastructure facilities, including through joint training, and use or establishment of relevant communication or emergency warning networks. It also calls member states to identify and share good practices in the area of protection of critical infrastructure.

6. The Network should assist the insurance industry to develop the metrics and decision support material to help mitigate the IIoT risk and to help 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.

[6] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4076052/

[7] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4265800/

[8] https://www.un.org/sc/ctc/blog/document/s-res2341-2017-protection-against-critical-infrastructure/

Additionally, the few publicized instances of hacking or security breaches in the IIoT and the levels of vulnerability of IIoT as part of the broader digitally networked environment, is yet to be fully realised. There is a need to develop the sense of individual and collective responsibility towards the 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 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. 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 last 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 increase IIoT device and implementation security, and align user, manufacturer, and implementer behavior with the broader public interest goals of safety and security. The potential for harm is spread out over 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 those mechanisms that have historically been instituted to manage widely distributed risk. The goal is to use insurance programs, standards, and governance structures to create incentives—and realign demand/supply side economics—for best IIoT security design, implementation, and maintenance practices. The incentives are intended to ensure the availability of secure IIoT services using active hardening processes that can be validated using proven penetration, configuration, and compliance techniques.

Insurance is an important market-based incentive mechanism, especially for fostering security-enhancing behavior. Lower insurance premiums have prompted millions of business and consumers to install security and fire systems, and good driver reward programs create tangible economic incentives to engage in safer and more careful behavior. 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 have been met, but also to differentiate between the strength and reliability of the implementation to inform the underwriting decision process.

There are four distinct communities that are the target audience for this Protocol: 1) the financial sector, including the insurance industry community; 2) entities deploying IIoT systems in production; 3) manufacturing and production end users of IIoT devices and services; and 4) national governments and international governance bodies focused on protection of critical infrastructure.

For the insurance industry, the Protocol supports the development of more specified expectations on the criteria used in the issuance of insurance coverage. It allows for the advancement of the actuarial considerations applied to the area of safety and cybersecurity that is still mired in uncertainty in the prediction of harm and liability. For entities deploying IIoT systems, this document provides guidance on how to go about securing their IIoT services according to increasingly accepted industry-wide standards. It provides IIoT system deployers the necessary incentives to undertake changes through self-regulation in their operations and governance towards a preventative view of cybersecurity rather than waiting for government regulation to define the terms and obligations. For the manufacturing and production end users, this Protocol contributes to the creation and maintenance of a more safe and secure ecosystem for IoT devices and services that can be relied upon for uses throughout the production process. The improvement of safety and cybersecurity practices in IIoT system deployments will serve as a benchmark of expectations for other deployments of IoT across the supply chain, and may have influence on cybersecurity in consumer devices and smart cities. For governments, 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.

In considering the approaches taken towards insurance, there is opportunity to enhance the preventative measures surrounding IIoT through: 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 DIGITAL PROTOCOL

I. Requirements for Insurability of IIoT Services

An entity that designs, develops, implements, deploys, maintains, monitors, services, or controls IIoT systems should be insurable only if that entity integrates cybersecurity and resilience against attack into its operations, processes, and work product. IIoT security must 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 must 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 focuses sets forth baseline requirements for insurability in three areas: (1) Line of Business IIoT Device Safeguards, (2) Internal Governance and Risk Management, and (3) Record Keeping and Data Management.

A. Line of Business IIoT Device Safeguards

An entity deploying IIoT systems must demonstrate that the following safeguards implemented for the IIoT devices or systems it designs, builds, installs, maintains, monitors, interacts with, or controls. The adoption and implementation of appropriate, existing, and recognized IIoT security standards is critical to the insurability of an IIoT system deployer.

1. **Risk Assessment Models**. Entities deploying 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.

2. **Hardware Integrity**. Due to changes in hardware components and configuration, hardware integrity must be assured throughout the endpoint lifecycle to deter uncontrolled changes to the hardware components. A potential vulnerability of the hardware is the usurpation of some part of the hardware resources. The endpoint must be able to protect itself against unauthorized access and the monopolizing of key resources such as memory, processing cycles and privileged processing modes.

3. **Encryption**. Entities deploying IIoT systems must ensure devices and associated applications support current generally accepted security and cryptography protocols and best practices. All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards.

4. **Patches and Updating**. Entities deploying IIoT systems must have a mechanism for automated safe and secure methods to provide properly authenticated software and/or firmware updates, patches, and revisions. Such updates must either be signed and/or otherwise verified as coming from a trusted source.

5. **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.

6. **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 modeling, 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.

7. **Service Trusted Computing Base**. Entities providing IIoT services must implement a Service Trusted Computing Base by standardizing the computing platform and defining the set of applications, libraries and configuration files that will run on the computing platform. Generate an application image and create a process for cryptographically signing the application image and for verification after signing.

8. **Organizational Root of Trust**. Entities deploying IIoT systems must implement a cryptographic based system to ensure that each computing platform in the IIoT service is authenticated when communicating with other computing platforms. Generate a root secret and/or certificate and ensure that it is stored securely and protected throughout its lifecycle.

9. **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. Developers should consider “bug bounty” programs, and crowdsourcing methods to help identify vulnerabilities that companies’ own internal security teams may not catch or identify.

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, or controls. The World Economic Forum’s *Advancing Cyber Resilience: Principles and Tools for Boards* 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 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).

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;

Security touches every element of an IIoT device and system lifecycle, and consequently IIoT safeguards require cross-functional, cross-departmental, and cross-company collaboration to achieve. The following are considered important insurance considerations for the design, manufacturing, service, distribution, integration, and other uses of IIoT, creating a Responsibility Assignment Matrix 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 plans

6. Secure data transport and storage assessment and gap remediation plans

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 plans.

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 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.

II. Operation of Protocol

Assessment mechanisms

For the operation of this Protocol as a safety incentivizing mechanism, an IIoT insurer may decline to provide insurance to an IIoT Firm unless the requirements for IIoT insurability in Section I are met. IIoT Insurers are likely to expect the following indicators of insurability:

1. Appropriate internal security safeguards to ensure that an IIoT Firm complies with Section 1 and regards security as a vital component of its overall business strategy.

2. Certification or assurance that the IIoT Firm has adopted the requirements of Section 1 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 in order 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 Section 1 to ensure security in the face of evolving IIoT security threats throughout the life cycle of the IIoT devices and systems.

Insurability requirements

The requirements set out in Section I, above, are incorporated into assessments of an IIoT Firm’s insurability and the good-faith application of the terms by an IIoT Insurer will bear on reinsurance assessments. IIoT Insurers will set out the specific insurability requirements based on an assessment of the overall risk of an IIoT Firm, device, and/or implementation.

III. Implementation of Protocol

Safeguards Assurance

Implementation of the Protocol will occur at or before the determination of insurability. Legacy IIoT devices or systems will not be grandfathered in: implementation of the Protocol must occur prior to issuing new insurance or renewing existing insurance. IIoT Insurers will assess IIoT Firms by using Section 1b and other requirements herein to determine insurability and provide guidance relating to this review. In order to provide vital incentives for IIoT security, IIoT Insurers will not provide insurance or other risk mitigation services to IIoT Firms unless and until they conform to the requirements of Section I.

Indicators & Data Clearinghouse

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

IIoT Firms and Insurers and interested third parties (security providers, consultants, and regulatory bodies) will provide relevant data and indicators (or results of analysis or proprietary data) to the indicators and data consortium described in Section Ic. This consortium is a vital source of the information necessary to assess insurability of the IIoT ecosystem. The insurance of IIoT Firms that violate or fall out of compliance with the Protocol will be suspended pending remediation of non-compliance.

IV. Verification of Protocol

Verification mechanisms for this Protocol relate to IIoT Firms and Insurers. IIoT Firms and Insurers will verify the operation of this framework in incentivizing security through insurability as well as the efficacy of the Protocol components. Verification procedures are to be determined by the IIoT community and regularly exercised and reviewed.

V. Maintenance of Protocol

In order 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 be incorporated into the Protocol. IIoT Insurers will regularly survey and monitor the IIoT security standards ecosystem to ensure that applicable standards listed in Section I 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 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 this Network Members to ensure the Protocol remains effective and up to date. This is essential when considering the role of Insurance brokerage later in this document, and the approach that is taken to the multitude of IIoT systems and products and cyber infrastructure.

Conflicts relating to this Protocol will 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

Indicative Chart of IIoT Resources:

Organization	Publication	Abstract	Focus Areas	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		11/15/16	Manufacturer & 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		09/19/16	Technological Perspective	Industrial IIoT
DHS (Department of Homeland Security)	Strategic Principles For Securing The Internet of Things (IIoT)	a) Highlights approaches and suggested practices to fortify the security of the IIoT 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:		11/16/16	Manufacturer & Consumer Perspective	Generic

		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 IIoT ecosystem 6. connecting carefully and deliberately				
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. https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/			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 they have taken to protect their products, services and components from cybersecurity risks. https://www.gsma.com/iot/iot-security-assessment/			Technological Perspective	Generic
IoTAA (IIoT Alliance Australia)	Internet of Things Security Guideline	a) Promotes a ‘security by design’ approach to the IIoT b) Assisting businesses, carriers and digital service providers (who use IIoT systems or devices) in various industries to better understand the practical application of security and privacy for IIoT device use c) Promoting awareness of the relevant legislative framework d) Assists industry to understand some of the relevant legislation around privacy and security		02/23/17	Technological Perspective	Generic

OWASP (Open Web Application Security Project)	IIoT Security Guidance	a) Manufacturer IIoT Security Guidance b) Developer IIoT Security Guidance c) Consumer IIoT Security Guidance		02/14/17	Technological Perspective	Generic
OTA (Online Trust Alliance)	IIoT Trust Framework	a) Includes a set strategic principles to help secure IIoT devices b) Key principles have been identified for different areas c) Outlines mandatory requirements including comprehensive and security patching post warrant		01/05/17	Technological Perspective	Generic
IoTSF (IIoT Security Foundation)	IIoT 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		12/06/16	Technological Perspective	Generic

Recommendations and Next Steps

[text to be completed]

Conclusion

[text to be completed]