IPC-1792

Standard for the Management and Mitigation of Cybersecurity Incidents in the Manufacturing Industry Supply Chain

Developed by the Cybersecurity Protection Standard Task Group (2-12c) of the Electronic Product Data Description Committee (2-10) of IPC

Users of this publication are encouraged to participate in the development of future revisions.

Contact:

IPC

Tel 847 615.7100
Fax 847 615.7105

Table of Contents

Figures

Tables

Standard for the Management and Mitigation of Cybersecurity Incidents in the Manufacturing Industry Supply Chain

1 SCOPE

This standard establishes requirements for companies to provide assurance that their products have been manufactured in cybersecure environments, ensuring that there has been no risk of impact to the product due to any cybersecurity incident. Requirements are specified covering actions that need to be taken in the event that a cybersecurity incident is detected, identifying all possibly affected products.

The target audiences for this standard are companies within the electronics manufacturing industry, cybersecurity supply chain managers and related organizations. This standard applies to the manufacture of final products as well as all component materials, paths and storage areas. External logistics processes are also covered via their responsibility to their customer.

This standard also defines levels of cybersecurity management that provide a choice when adopting this standard to meet the appropriate need. Pathways exist to enable progression from a basic level of cybersecurity maturity to higher levels. Appropriate levels for companies to adopt may be determined based on IPC Product Classification as well as risk analysis across all possible use cases of products.

This standard also includes mechanisms for third-party assessment to the cybersecurity levels defined in this standard.

1.1 Purpose As technologies related to Smart Cities and Internet of Things (IoT) advance, there is an increased risk that cybersecurity incidents will have serious impacts on society. Many cyberattacks are enabled through unauthorized manipulation of smart devices during manufacture, which creates opportunities for third parties to exploit vulnerabilities. The intent of this standard is to eliminate the opportunity for the manipulation of software and hardware throughout the end-to-end manufacturing process, ensuring that products are built as intended by the original designer. Application of this standard provides continued assurance against evolving cybersecurity threats in end-products as technology advances.

The use of this standard helps companies identify those products that may have been affected as a result of a cybersecurity incident during manufacture, ensuring all products released into the market are free from any risk of tampering related to hardware and software content.

This standard represents guidance to the various entities in the electronics manufacturing supply chain to provide a continuous cybersecurity focus, building on existing and evolving information technology (IT). Procedures and requirements provide manufacturing companies the ability to manage the effects of cybersecurity incidents, should they occur within their organization or upstream in the supply chain, with propagation of information in a timely manner, downstream in the supply chain.

Adoption of this standard enables companies to ensure appropriate practices and procedures related to required data management are established that identify the impact of Cybersecurity Incidents, involving, for example, preventing the leakage or alteration of critical information, to secure the product owner's supply chain. In the event of any cybersecurity incident, methodologies described in this standard identify the specific potential effect to the supply chain and how to minimize effects.

1.1.1 Industry Background The electronics manufacturing supply chain is multitiered, with multiple companies supplying individual products that ultimately create the final end-product for the customer. This distributed supply chain presents numerous opportunities where information related to and used by manufacturing operations can be intercepted and used for unauthorized or unlawful purposes, potentially significantly compromising the safety of the end-product. It is vital that each entity in the supply chain is able to provide assurance that such information has not been tampered with, intercepted or stolen, via interoperable exchange of information without compromise of privacy with other members of the supply chain as required. Should any cyberattack events be discovered, whether from outside of the secure environment or from within, it is essential to have documentation that proves how such attacks and any potential consequences have been addressed, as this allows the product owner to determine who is responsible for effects of the incident and which corrective actions have taken place.

The manufacturing supply chain is increasingly being targeted by individuals and entities seeking to obtain product-related information, with the intention of disrupting manufacturing operations, creating cloned or counterfeit products or to introduce Trojan horses that undermine the security in end-products. Supply chain risk is a key contributor to overall security risk with, for example, procurement of hardware or software that has been compromised, either by the creation of counterfeits or by being illegally obtained, or where the source has been subject to industrial espionage.

Product owners should expect their products to be manufactured in a secure supply chain and that the capability exists to detect and take appropriate action should a cybersecurity incident occur. To meet this expectation, the whole supply chain needs to be secured, as it is only as strong as its weakest participant. Failure to do so has been documented in numerous cases of cybersecurity breaches that have had serious consequences.

This standard describes a mechanism for assurance that products have been manufactured in an environment where no adverse effects of any cybersecurity incidents have occurred, ensuring the quality and reliability of products.

1.1.2 Key Elements of This Standard

The key elements within this standard include:

- Requirements related to the early determination of the potential impact of a cybersecurity incident
- Requirements related to the identification and relationship of certified materials and certified products throughout the supply chain, such that the extent of the effect of any incident can be easily and readily communicated in a timely manner
- Requirements for third-party validation for a company adopting this standard
- Requirements for the creation and receipt of a Digital Diploma at the time of certification
- Description of how to generate a Digital Certificate for each production unit as it is shipped
- Requirements relating to how Digital Certificates are stored and used to identify the extent of the potential effect of a cybersecurity incident

To facilitate the adoption of this standard, the ability to correctly associate specific instances of material consumption with the specific product being assembled is needed (see 3.1 and 4.1.3). IPC-1782 provides guidance about what is required for material traceability during assembly, with different levels of precision associated with the IPC product classification.

1.2 IPC Product Classification IPC standards recognize that electrical and electronic assemblies are subject to classifications, determined by intended end-use. Three general end-product classes have been established to reflect differences in manufacturability, complexity, functional performance requirements, and verification (inspection/test) frequency. It should be recognized that there may be overlaps of equipment between classes.

CLASS 1 General Electronic Products: Includes products suitable for applications where the major requirement is function of the completed assembly.

CLASS 2 Dedicated Service Electronic Products: Includes products where continued performance and extended life is required, and for which uninterrupted service is desired but not critical. Typically, the end-use environment would not cause failures.

CLASS 3 High Performance/Harsh Environment Electronic Products: Includes products where continued high performance or performance-on-demand is critical, equipment downtime cannot be tolerated, end-use environment may be uncommonly harsh, and the equipment must function when required, such as life support or other critical systems.

1.2.1 Relation Between IPC Classification and Urgency of Cyber Incident Impact Detection Response times related to activities required in this standard are defined according to whether there is specific urgency, or whether the normal rapid response will suffice.

IPC Product Classifications assist in the determination of how urgent the reporting of a cybersecurity incident may be, though there is not a direct relationship between them. In practice, the urgency of reporting depends on how large an impact may occur as a result of the attack on a product based on the most significant use cases. Consideration should be made that there can be many uses of products, including simple ones (e.g., removeable storage drives), where the impact can be extremely varied depending on how and where the device is used, as well as the context of the data stored. This can lead the customer to request a response level that may not be consistent with the IPC Product Classification.

Table 1-1 provides a guide as to how to respond to customer request, including consideration of IPC Product Classification.

Table 1-1 Guide for Response Levels Based on IPC Classification

Customer Preference	IPC Class 1	IPC Class 2	IPC Class 3+
Not specified	Rapid	Rapid	Urgent
Rapid reporting	Rapid	Rapid	Urgent
Urgent reporting	Urgent	Urgent	Urgent

1.2.2 Risk Assessment and the Urgency of Cyber Incident Impact Detection To complement guidance from the customer request and IPC Product Classification, a business risk assessment can also help determine the level of requirements for an urgent level of response to cybersecurity incidents. The required level can then be based on the degree of risk that customers and suppliers will accept for the potential use of materials and final products. Approaches to risk assessment may vary by industry and region. Risk assessment of an industry, product or key material can be an essential tool, using a typical risk assessment matrix as shown in Table 1-2.