Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements (JC-STAR) STAR-1 Application Supplementary Guidance

March 2025

Information-technology Promotion Agency, Japan (IPA)

Table of Contents

Introduction

This Supplementary Guidance is intended to provide additional information and answers to the questions received regarding STAR-1 applications. Refer to this guidance when you apply.

Revision History

Revision date	**Contents**
March 24, 2025	First edition published (Question 1-1 to 1-7, Question 2-1)

1. [STAR-1 Application Target Concept]

[Question 1-1]

What is the difference between an “applicant company,” “application agent,” “manufacturer,” “distributor,” “actual manufacturing vendor,” “OEM/ODM manufacturing,” and “parts/ components manufacturer?”

[Guidance]

A **manufacturer** is the company that owns the “product logo,” “brand logo,” or “company name logo” attached on IoT products. It is the company that has the ultimate manufacturing responsibility for those products.

An **applicant company** is a **manufacturer** of IoT products that applies for acquisition of a conformance label.

An **application agent** is a company that is delegated by an **applicant company** to perform the procedures for acquiring a conformance label on its behalf.

A **distributor** is a company that sells IoT products at wholesale from a **manufacturer**. It includes a retailer, sales agent, import agent, etc. It cannot act as an **applicant company** in the JC-STAR application process, but it can act as an **application agent**.

An **actual manufacturing vendor** is the company that actually manufactures IoT products in its own factory. If products are manufactured in the manufacturer's factory, the **actual manufacturing vendor** and the **manufacturer** are the same, but if not, the **actual manufacturing vendor** does not necessarily correspond to the **manufacturer**.

The **OEM/ODM manufacturing** is the outsourcing of all or part of the manufacturing process of the applicable IoT products to another company for manufacturing. This **includes cases where the manufacturing is outsourced to a fab factory**; if the OEM/ODM manufacturing is outsourced or the manufacturing is outsourced to a fab factory, the OEM/ODM manufacturing company or the fab factory company will become the **actual manufacturing vendor**.

A **parts/components manufacturer** is a production company that actually manufactures the parts/components to be embedded to the applicable IoT products. For example, if communication device modules are provided by another company for use as communication functions in IoT products and are embedded to the products as they are, the company that manufactures the modules is considered a **parts/components manufacturer**. For JC-STAR applications, the scope of **parts/components manufacturers** is defined as companies that manufacture parts/components which provide functions related to the security functions in the checklist. Even if a company receives a supply of base parts/components from another company, it is excluded from the scope if the company modifies any part of the parts/components before embedding them to its products.

[Question 1-2]

How should I use “in-house factory manufacturing,” “OEM/ODM manufacturing,” and “combination of in-house factory manufacturing and OEM/ODM manufacturing” in the manufacturing method category of the applied product?
In addition, for fabless manufacturing, should I select “in-house factory manufacturing”?

[Guidance]

“**In-house factory manufacturing**” shall be selected only if the manufacturing of the IoT products is completed in the company's own factory.

“**OEM/ODM manufacturing**” shall be selected if the entire manufacturing process is outsourced to another company. Even in the case of **fabless manufacturing,** “OEM/ODM manufacturing” shall be selected.

“**Combination of in-house factory manufacturing and OEM/ODM manufacturing**” shall be selected if a company outsources a part of the manufacturing process to another company, or if a company manufactures products both at its own factory and at a contractor’s factory.

Note that there is a possibility that the product may be outsourced to more than one manufacturer, in which case, make sure to describe the “largest manufacturing outsourcing company” as the “OEM/ODM manufacturer.”

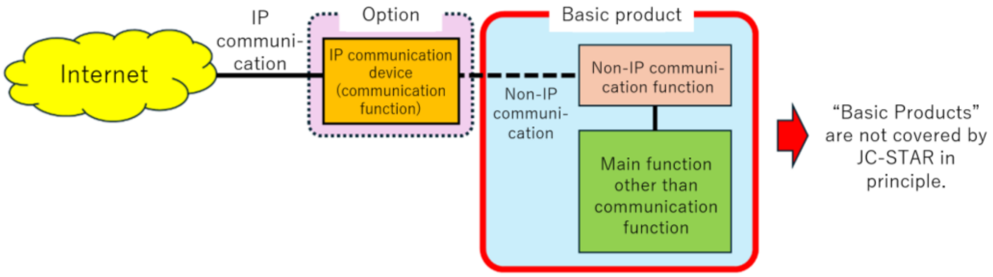
[Question 1-3]

- Please explain how to handle cases where product model numbers are divided by whether the product has a communication function with the Internet (IP communication device) or not.
- What is the handling of IoT products that do not have direct communication function with the Internet (IP communication device) in their base part, but can add direct communication function with the Internet (IP communication device) as an option?
- Please explain how to handle the case of IoT products that do not have communication function with the Internet (IP communication device) as a basic function of the product, but the installation operator enables communication with the Internet by installing an optional communication device (IP communication device) at the same time.
- For IoT products that have an optional communication function with the Internet (IP communication device), if we acquire a conformance label for IoT products with a communication function, can we also attach a conformance label to products without a communication function?

[Guidance]

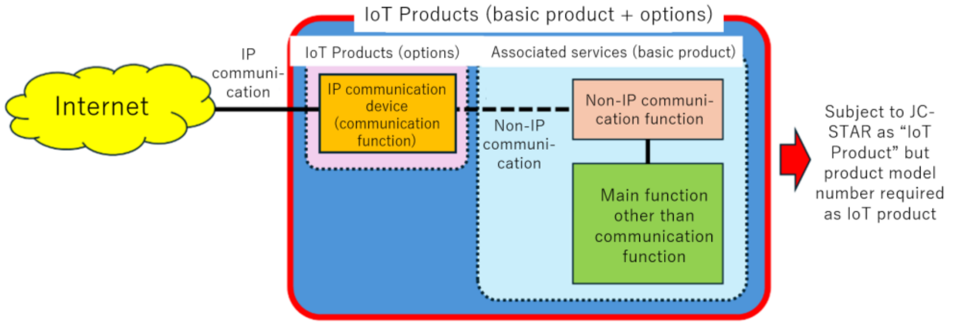
Products that do not perform communication with the Internet (IP communication) as a basic function of the product, but the communication function part with the Internet (IP communication device) is optional, are handled as follows:

1) Products that do not include a “communication function part (IP communication device)” are, in principle, not covered by JC-STAR. Attaching a conformance label is not acceptable.

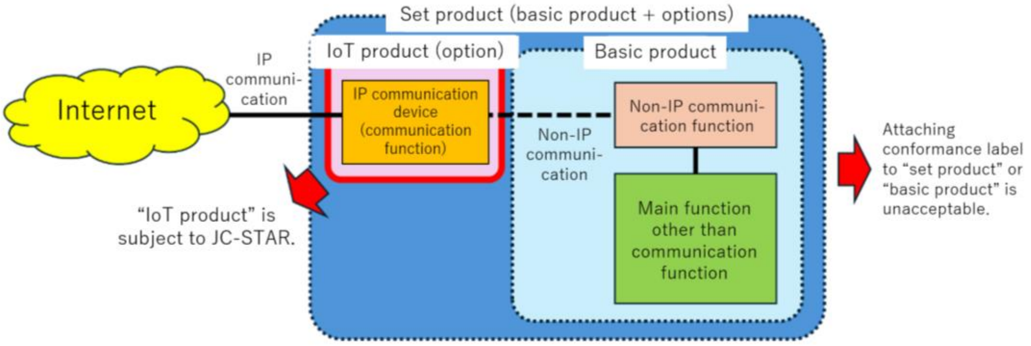

Internet
IP communi-cation
Option
IP communication device (communication function)
Basic product
Non-IP communi-cation
Non-IP communi-cation function
Main function other than communication function
“Basic Products” are not covered by JC-STAR in principle.

2) In the case of products that include a “communication function part (IP communication device)” (including simultaneous installation by the installation operator), the optional “communication function part (IP communication device)” is considered an “IoT device” in the JC-STAR Scheme. Even if the basic function part excluding the communication function part is the main function of the product, it will be positioned as “associated services.” In this case, the conformance label can be attached in a manner that includes the “communication function part (IP communication device).”

3) If the product model number does not include the “communication function part (IP communication device),” a new product model number (identification model number for JC-STAR) shall be set to identify the conformance label (the identification model number for JC-STAR may be different from the existing product model number. In such a case, make sure that the corresponding relationship is clear. (It is not necessary to use the identification model number for JC-STAR for other than JC-STAR). The identification model number for JC-STAR shall be described as the product model number on the conformance label application form.


IoT Products (basic product + options)
Internet
IP communi-cation
IoT Products (options)
Associated services (basic product)
IP communication device (communication function)
Non-IP communi-cation
Non-IP communi-cation function
Main function other than communication function
Subject to JC-STAR as “IoT Product” but product model number required as IoT product

4) The “communication function part (IP communication device)” alone may be subject to a conformance label. However, the conformance label can only be attached to the “communication function part (IP communication device),” not to the chassis that contains the device.


Set product (basic product + options)
IoT product (option)
Basic product
Internet
IP communi-cation
IP communication device (communication function)
Non-IP communi-cation
Non-IP communi-cation function
Main function other than communication function
"IoT product" is subject to JC-STAR.
Attaching conformance label to "set product" or "basic product" is unacceptable.

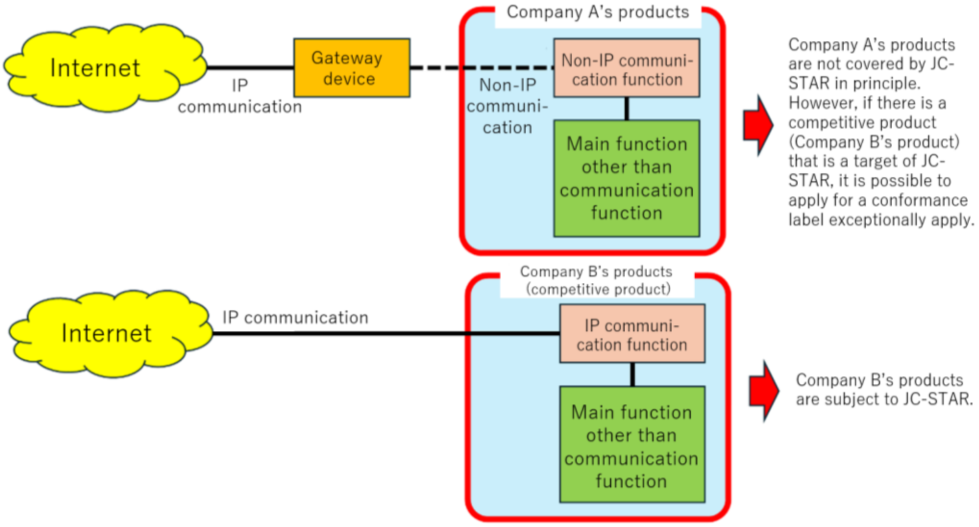
[Question 1-4]

If the product does not have a direct communication function with the Internet (IP communication function), but communicates with the Internet by converting the protocol using a separate gateway, is that possible to acquire a conformance label for the product? Note that some similar IoT products from other companies have a direct communication function with the Internet (IP communication function).

[Guidance]

In principle, products that do not have direct communication function with the Internet (IP communication function) are not eligible for JC-STAR. However, if there is a competing product that has a direct communication function with the Internet (IP communication function) and is subject to JC-STAR, the product may exceptionally apply for a conformance label.

This is because it is expected that it will not be easy to distinguish between cases where products that are and are not subject to JC-STAR are mixed together, and cases where "acquisition of a conformance label is not possible regardless of whether or not the conformance requirements are met" because the product is not subject to JC-STAR, and cases where "acquisition of a conformance label is not possible because the product is subject to JC-STAR but does not meet the conformance requirements." Therefore, in order to avoid misunderstandings, the JC-STAR is positioned as an exceptional measure to prevent business disadvantages caused by the former case, and in principle, even if a product is not subject to JC-STAR, it is possible to apply for a conformance label at the business discretion.


Internet
IP communication
Gateway device
Company A's products
Non-IP communication
Non-IP communication function
Main function other than communication function
Company A's products are not covered by JC-STAR in principle. However, if there is a competitive product (Company B's product) that is a target of JC-STAR, it is possible to apply for a conformance label exceptionally apply.
Internet
IP communication
Company B's products (competitive product)
IP communication function
Main function other than communication function
Company B's products are subject to JC-STAR.

[Question 1-5]

- If a product that has already been shipped can be made to conform to STAR-1 by updating the firmware, is it sufficient to apply for a conformance label with the firmware version that conforms to STAR-1? In this case, what points should I be careful of?

- If the same product (firmware version prior to acquisition) has already been shipped as the product for which the conformance was acquired, would it be considered STAR-1 certified even if the product is not labeled if the firmware is upgraded to the firmware that was applied for when the conformance was acquired?

[Guidance]

Make sure to apply with a conforming firmware version. If you have already shipped products that will not be conforming unless the firmware is updated, a note shall be added in the “Firmware Name/Version” field of the application form, stating that “Update is required for the products (by YYYY/MM, in version xxx) already shipped.”

Products using firmware versions prior to STAR-1 acquisition will be considered STAR-1 conformance on the condition that the firmware is updated. When displaying the conformance label for those products, include a note stating that “Firmware update is required.” The conformance label must be displayed in such a way that it cannot be misunderstood that the product is STAR-1 conformance without a firmware update.

IPA will also include a statement in the security information on the product information page.

[Question 1-6]

The group of applications, which are pre-installed in the OS used or installed freely by the user, have a mechanism that allows software updates outside the control of the IoT manufacturing vendor, and it is difficult to ascertain whether they have so-called “information assets to be protected," whether they are protected by appropriate technology, and whether they are properly updated. How would a product that can embed such group of applications be handled?

[Guidance]

The basic idea behind JC-STAR is to cover cases where the IoT manufacturing vendor controls the applications that can be installed. This is based on the condition that “security measures cannot be added later by means other than updates,” which is the concept of products covered by this Scheme. Therefore, products for which the IoT products manufacturing vendor does not control the applications that can be installed are, in principle, not eligible for JC-STAR.

As with Question 4, depending on whether or not IoT manufacturing vendors control the applications that can be installed, there are cases where products that appear to be the same may be mixed with products that are “eligible but do not acquire a conformance label” and products that are “not eligible and cannot acquire a conformance label.” In such cases where the two are indistinguishable, the IoT manufacturing vendor may exceptionally decide that “although it is not originally eligible, it is acceptable to acquire a conformance label as an eligible product.”

However, the difference from Question 4 is that in this case, it is necessary to clearly inform users that the IoT manufacturing vendor does not control whether necessary measures are taken for the group of applications to be installed. Therefore, it is necessary to clearly indicate the point of demarcation of responsibility, such as how far the IoT manufacturing vendor will check and manage, and from where the responsibility of the user will lie, as well as the actions that the user should take (e.g. “This conformance label does not cover the confirmation of whether the application to be installed has information assets to be protected, or the management of whether the necessary measures have been taken, and the user him/herself needs to check the security of the application.”) in a place that the user can easily check.

[Question 1-7]

1) If a user updates (activates) software that already has security functions installed in the IoT products, does this mean that the user can add security functions?

2) Should the addition of new security functions through software or firmware updates be considered a later addition of security functions?

[Guidance]

As is common to both, neither software/firmware provided under the administration of the IoT manufacturing vendor is considered the “addition of security functions by the user,” but rather “security functions that are provided (or will be provided).”

Regarding 1), if it is a case where third-party software is installed in IoT products as a trial product with which the IoT manufacturing vendor is not directly involved, then in a strict sense, it means the "addition of security functions by the user." In that sense, IoT products with such software are "not covered by JC-STAR."

However, products that are not equipped with third-party software, or products that are not available with software other than those which are installed under the control of the IoT manufacturing vendor as a trial product, are "subject to JC-STAR," so it may be possible to exceptionally apply for a conformance label even if they are not subject to JC-STAR by definition.

2. [Others]

[Question 2-1]

Is it necessary to apply for updates when firmware or product applications of IoT products are upgraded? In addition, is it also necessary to apply for updates when changes occur in parts other than firmware and product applications (OS security patches and component version upgrades)?

[Guidance]

If the judgment results of the items in the checklist used in the STAR-1 application are not affected, the conformance label will remain valid even if the version is upgraded. No renewal or reapplication is required.

Note that if the results of the checklist have an impact on the judgment results, the surveillance phase will begin. If the surveillance results are acceptable, the conformance label will be continued, but if they are not acceptable, the conformance label will be withdrawn (treated as a voluntary withdrawal). If it is withdrawn, the subsequent handling will be conducted at the discretion of the IoT device vendor.