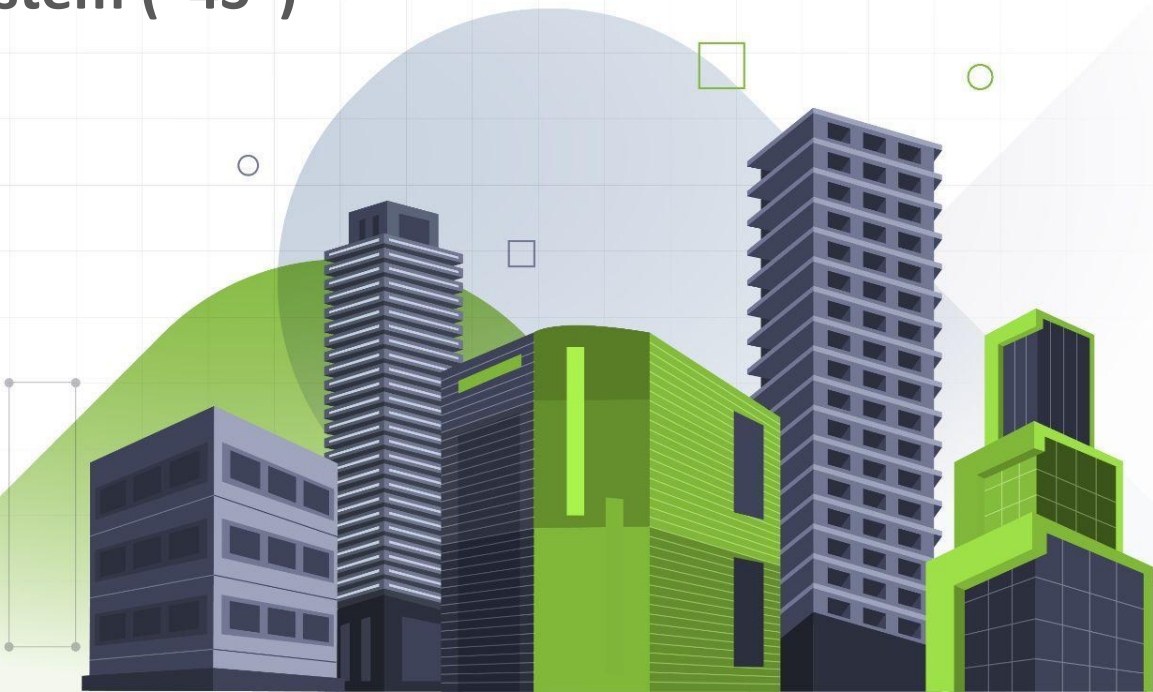


# Application Programming Interface (“API”) Standardisation for Smart Site Safety System (“4S”)

Safety Week

24 Aug 2026



# What is API (Application Programming Interface)?

## ➤ Definition

An API is a set of rules and protocols that allows different software applications to communicate with each other.

## ➤ Functionality

APIs enable developers to use functionalities of other services or applications without needing to understand their internal workings.

## ➤ Types

**Web APIs:** Facilitate communication over the internet, often using HTTP.

**Library APIs:** Provide specific functions within software libraries.

**Operating System APIs:** Allow applications to interact with the operating system.

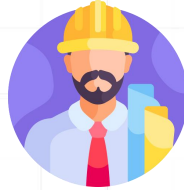
## ➤ Benefit

APIs enhance efficiency by allowing developers to build on existing services, promote innovation, and enable easier system integration.

# Overview of the API standard initiative

## ➤ Challenge

There are multiple CMP providers and numerous IoT companies, each with its own unique API standards, which require a lot of customizations to integrate with each other



Contractor



Purchased 4S devices & CMP

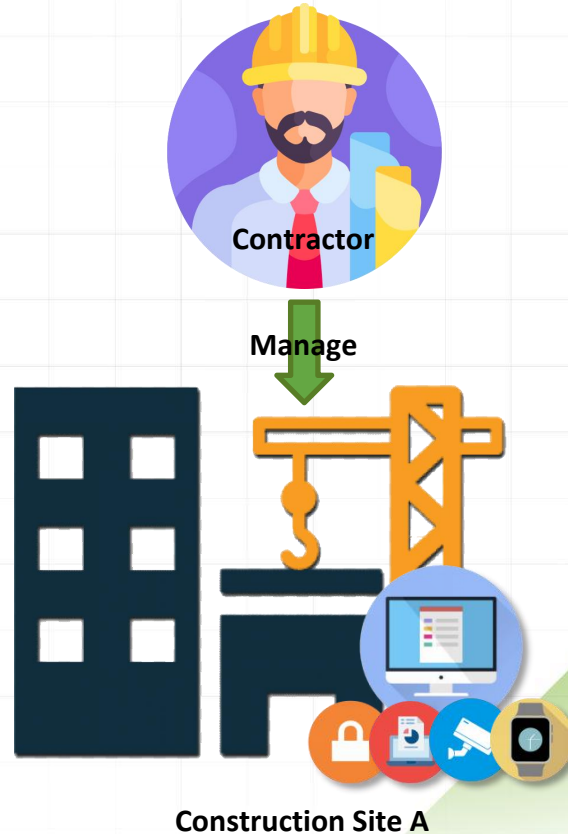


Construction Site A

# Overview of the API standard initiative

## ➤ Challenge

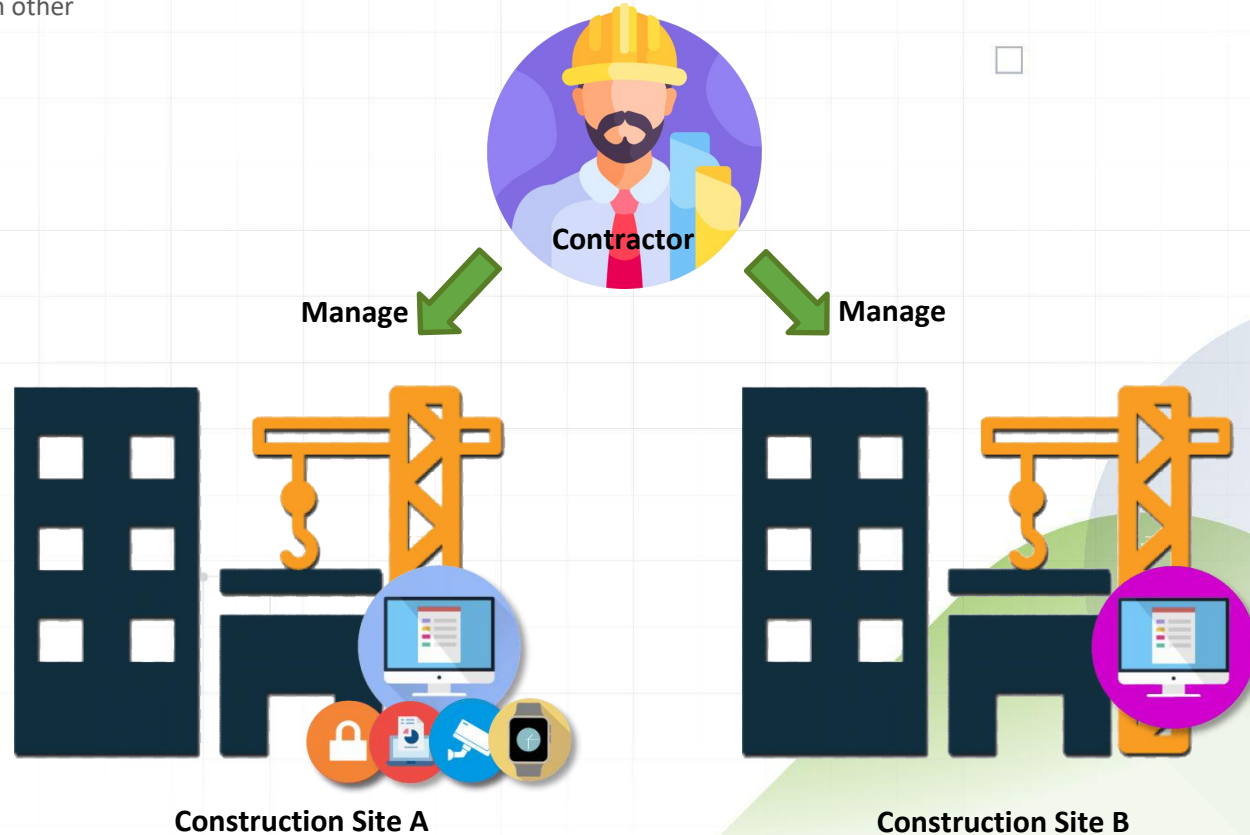
There are multiple CMP providers and numerous IoT companies, each with its own unique API standards, which require a lot of customizations to integrate with each other



# Overview of the API standard initiative

## ➤ Challenge

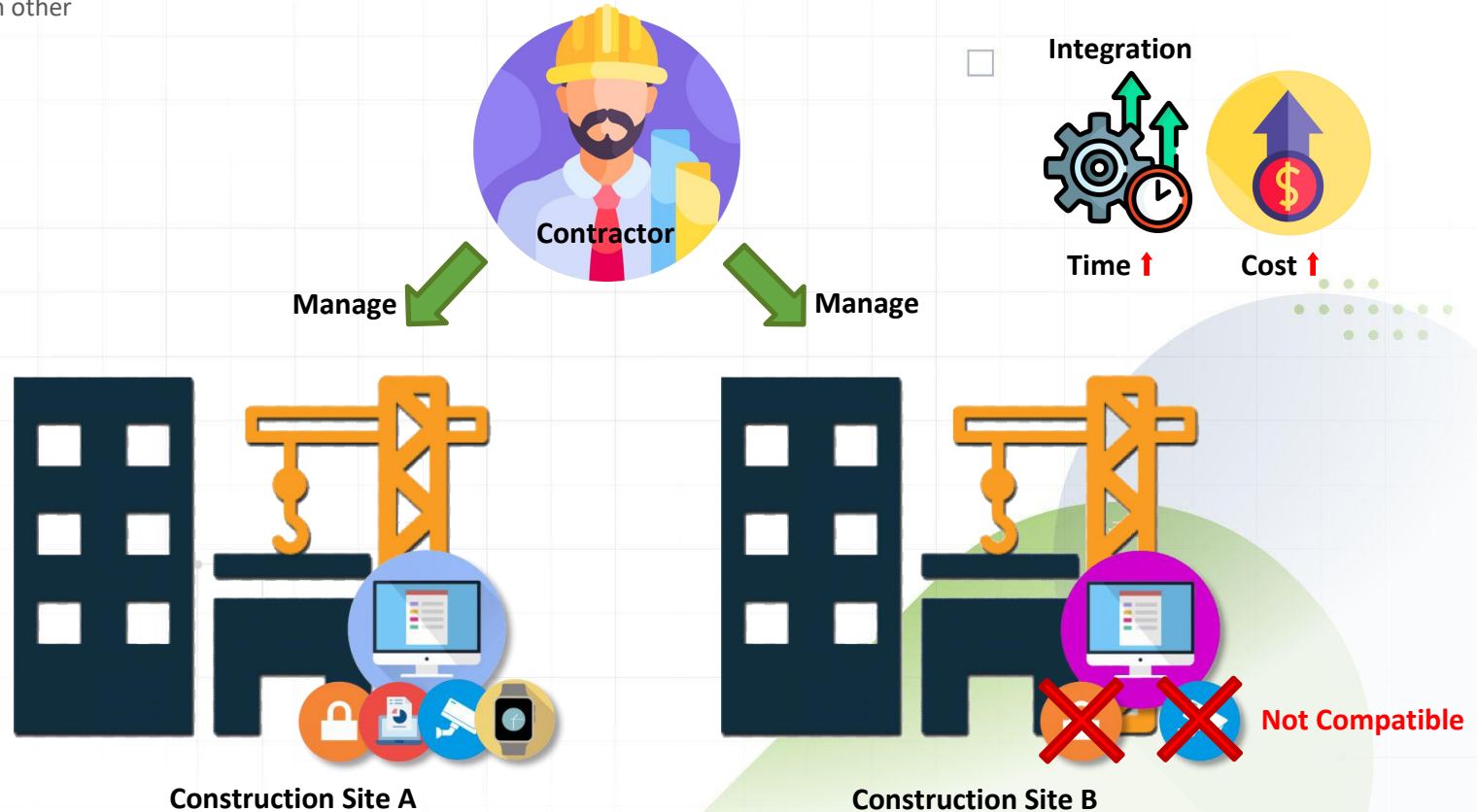
There are multiple CMP providers and numerous IoT companies, each with its own unique API standards, which require a lot of customizations to integrate with each other



# Overview of the API standard initiative

## ➤ Challenge

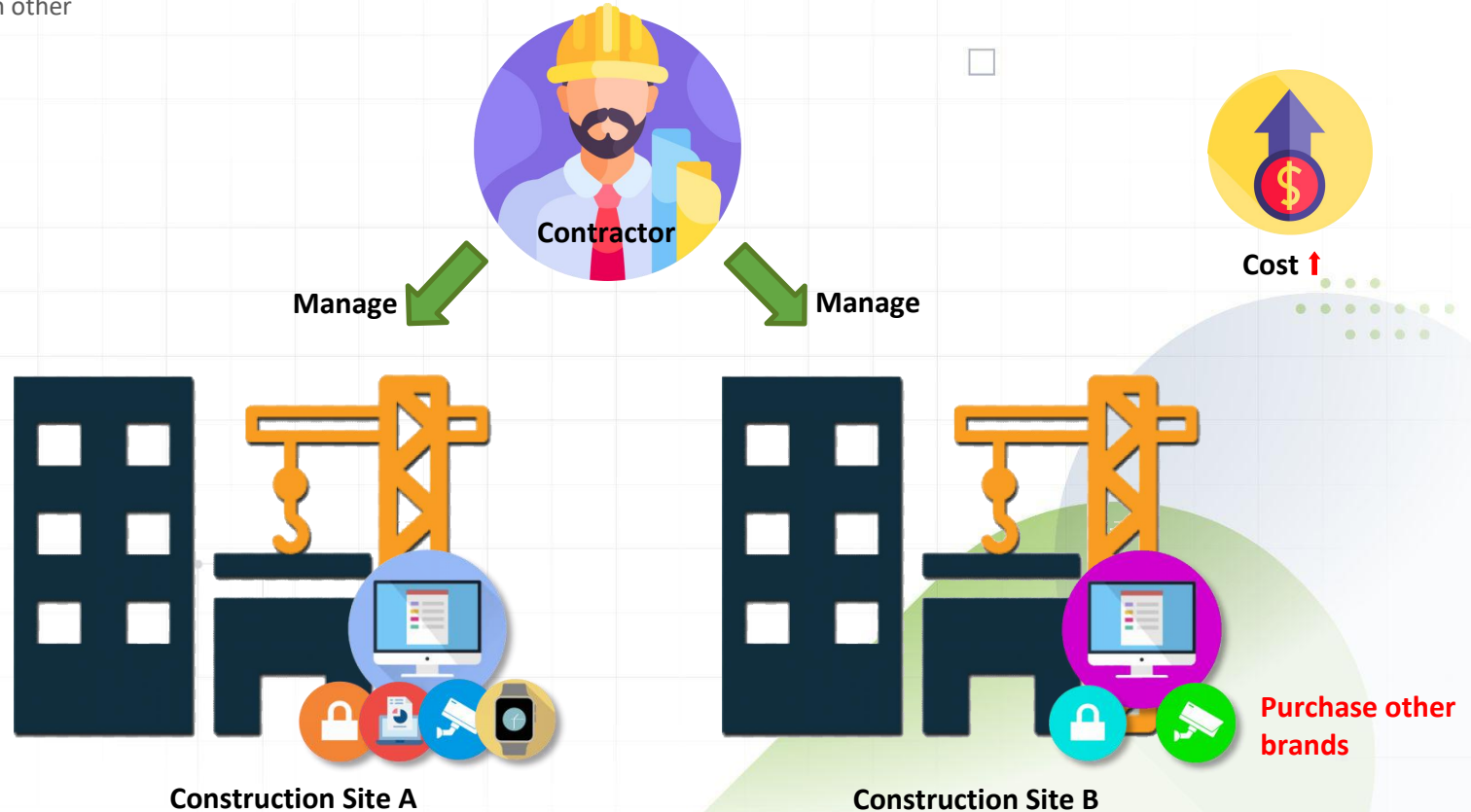
There are multiple CMP providers and numerous IoT companies, each with its own unique API standards, which require a lot of customizations to integrate with each other



# Overview of the API standard initiative

## ➤ Challenge

There are multiple CMP providers and numerous IoT companies, each with its own unique API standards, which require a lot of customizations to integrate with each other



# Overview of the API standard initiative

## ➤ Challenge

There are multiple CMP providers and numerous IoT companies, each with its own unique API standards, which require a lot of customizations to integrate with each other

**E.g.** In one case, a client had a large number of CCTV cameras already installed, but they were from a brand outside our existing solutions. Integrating this system would require substantial time and resources for customization.

## ➤ Objective

**To establish a unified framework** that enables efficient communication between CMPs and diverse IoT devices from various brands. ultimately achieving low costs for integration in the future. When all devices follow the same API specification, integration shifts from “developing separately for each vendor” to “**developing once for broad use**”.

## ➤ Solution

Develop a standardized API framework that allows resources and protocols to interoperate among different manufacturers through the API.

# Benefits



## Reduce Time and Cost

Minimise the time and costs associated with integrating 4S devices into existing Centralised Management Platforms (CMPs).



## Interoperability

Enhance Flexibility and freedom of choice and adoption between safety devices and Central Management Platforms(CMPs).



## Reduce Vendor Lock-in

**Provide** construction companies with more options by reducing dependence on proprietary integrations.



## Simplified Integration

Minimise the need for customisation when supporting devices for common safety monitoring scenarios.



## Necessity of Collaboration

Manufacturers are encouraged to widely adopt the API standards to maximise efficiency and ensure the reliable transmission of critical data.



## Flexibility

Standardised APIs make it easier to adapt to different environments and new technologies, allowing quick changes based on specific site needs and easy integration of new devices.



## Knowledge Sharing

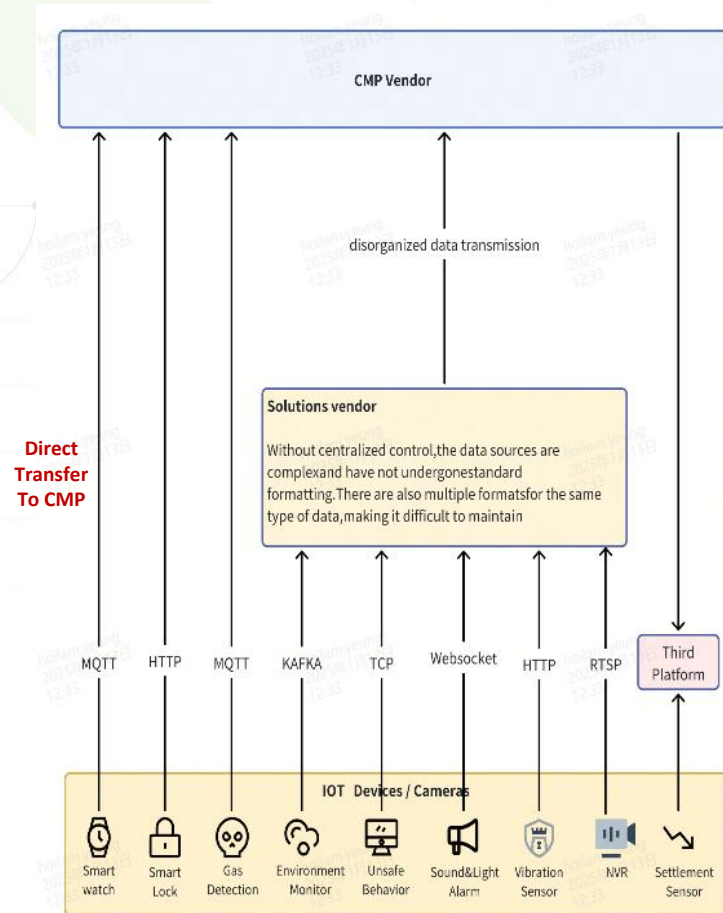
Standardised APIs help create a team environment where manufacturers, developers, and users can share useful tips and experiences with the industry and their team based on a set of unified API standards, leading to continuous improvement.



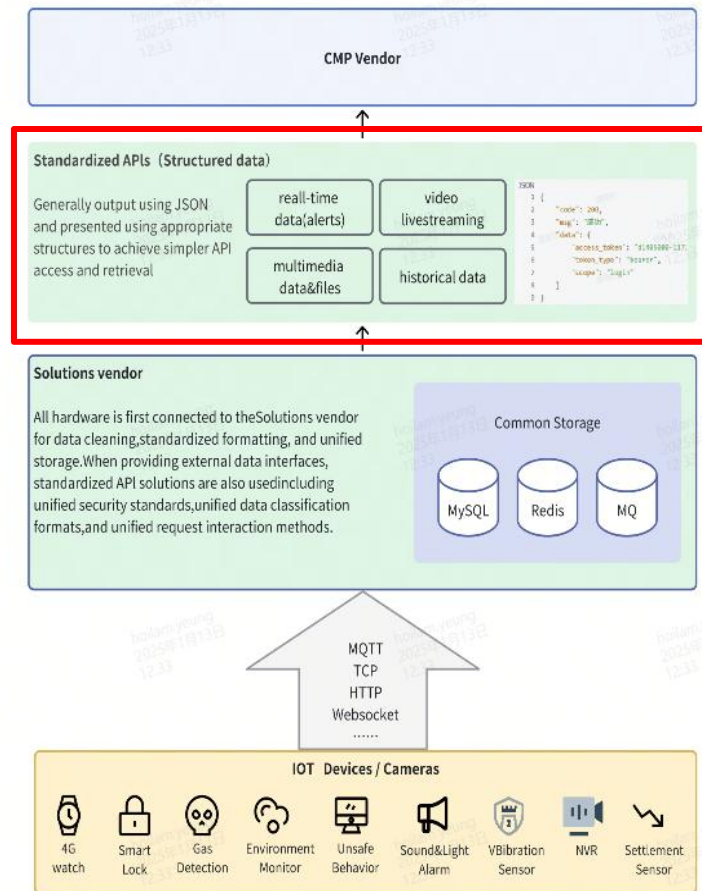
## Encourage Innovation

A solid API framework enables manufacturers to continue innovating while ensuring their products work well together, thereby promoting advancements in safety technology.

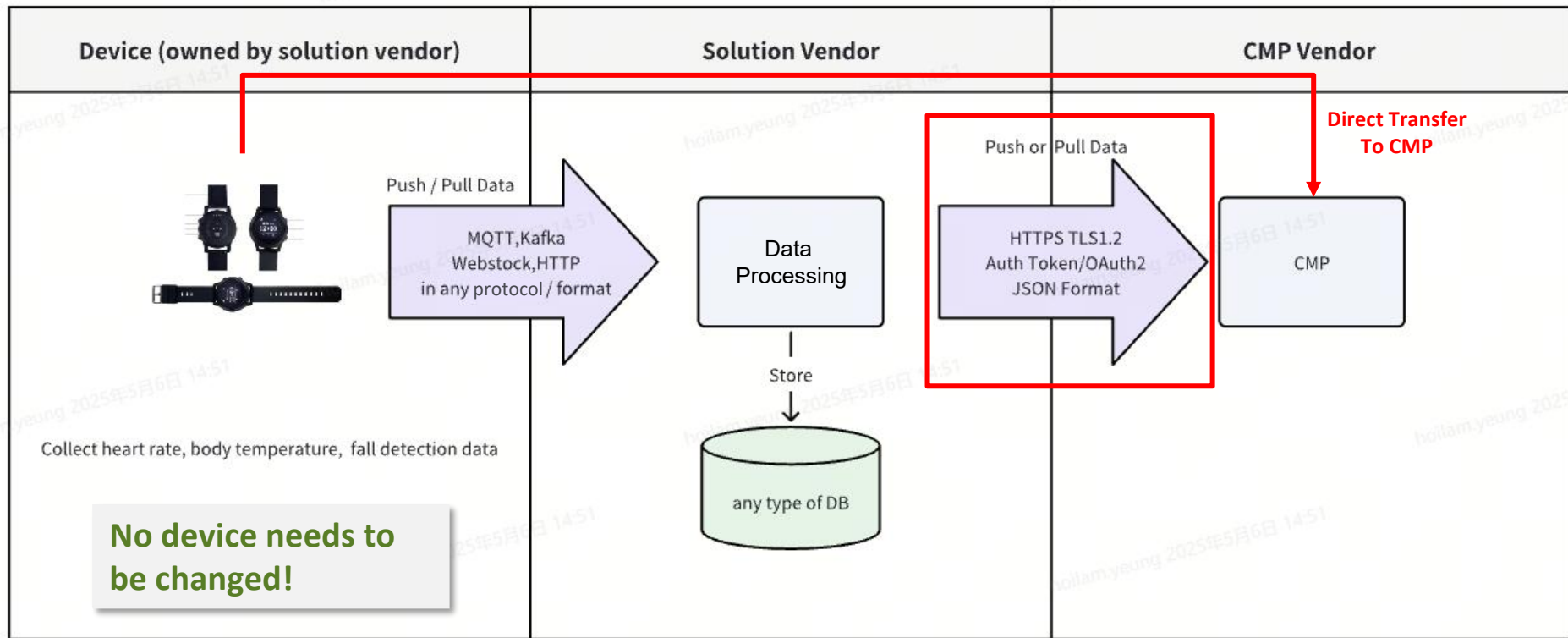
# API Standardization Overview



After  
API standardization



# API Standardization data flow



# Major Principles of API Standardization

1. **Outcome-Oriented Design:** The framework starts with desired outcomes and works backward to define the required telemetry, devices, platforms, and processes. It focuses on achieving results rather than prescribing internal workflows, enabling collaboration through resource definitions and standardised APIs. Implementation details are left to stakeholders. APIs will also support telemetry.
2. **Flexible and Modular Ecosystem:** Devices, platforms, and CMPs (Centralised Management Platforms) can operate independently, overlap, or coexist. Tasks such as telemetry processing, feedback routing, and false alarm suppression are dynamically assigned to suit deployment needs, ensuring adaptability across various configurations.
3. **Feedback Loop:** The framework ensures a complete round trip in scenario workflows. Devices send telemetry to CMPs, which process the data and generate feedback (e.g., reset alarms). This feedback flows back to devices, completing the loop and confirming actions.
4. **Interoperability:** Standardised APIs enable seamless communication across systems and vendors. The framework guarantees compatibility while giving implementers the freedom to decide how systems are integrated and deployed.
5. **Package-Based Certification:** Centered on certifying functional packages rather than entire deployments. Packages group capabilities such as telemetry types, scenario outcomes, and feedback mechanisms. This modular approach simplifies compliance, supports incremental certification, and allows stakeholders to focus on specific functions. It's a flexible and scalable model, and there is no need to rush to conclusions on the certification process/standard as the idea evolves.

# Basic Principles of API Standardization

## 1. Consistency:

*Follow consistent design style, naming conventions and data formats.*

## 2. Discoverability:

*Easily discoverable and understandable, includes clear documentation, well-defined interfaces, and metadata that describes the API's functionality*

## 3. Reusability:

*Design to be reusable across different applications*

## 4. Security:

*Includes authentication, authorization, and protection against common security vulnerabilities*

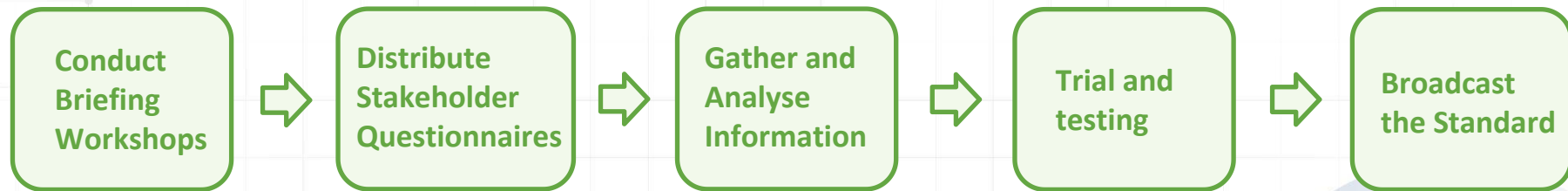
## 5. Performance:

*Design for optimal performance*

## 6. Extensibility:

*Design to be extensible, allow to add new functionality without breaking existing applications*

# Roadmap



Hold workshops with stakeholders to introduce the 15 standard safety scenarios and understand how different devices and CMP providers handle these situations.

Based on insights from the workshop, create questionnaires for stakeholders to be distributed before or during webinars, inviting contractors, solution providers, and other industry participants

Collect responses from the questionnaires, analyse the data, and summarise it into an API standard that appeals to the majority of the industry

Implement trials of the standard across various scenarios, fine-tuning it based on feedback and results, with contributions from all providers.

Promote the finalized API standard widely throughout the industry to encourage adoption

# Sandbox

Sandbox Environment. You can find the introduction to the sandbox environment, as well as the account application method and the sandbox login link.

The screenshot shows the '4S Open Platform' website. The header includes the Construction Industry Council logo, the text '4S Open Platform', and navigation links: 'About', 'Understanding 4S API Standardization', 'Reference Materials and User Guidelines' (highlighted), 'Latest Update', 'FAQ', and 'En'. A left sidebar lists 'Sandbox Environment' and 'Introduction' (highlighted), followed by 'Safety Scenarios' with four categories: '06: Unsafe acts / dangerous situation alert for tower crane lifting zone', '02: Digitalised Tracking System for Site Plants, Powered Tools, and Ladders', '03: Digitalised Permit-to-Work System for High-Risk Activities', and '04: Hazardous areas access control by electronic lock and key system'. The main content area is titled 'Sandbox Environment' and contains the following text:

**The sandbox environment is designed to support developers in testing and validating the 4S API Standard.**

Sandbox scenarios are first organised by 4S categories, along with an additional "Miscellaneous" category. Within each category, a set of commonly encountered safety scenario is provided. Developers should select a scenario that closely matches their product, or one with similar characteristics, as a starting point. If no suitable scenario is found, the "Miscellaneous" category offers flexibility for custom testing.

Once a scenario is selected, the central section allows developers to input code to simulate device registration, generate measurement data, and test conditions that trigger alerts. On the right-hand side, a conformity checklist is provided to verify whether each step complies with the CIC API Standard format. When all items are successfully checked, the result indicates conformity with the CIC API Standard.

**To access the sandbox environment, user authentication is required.**

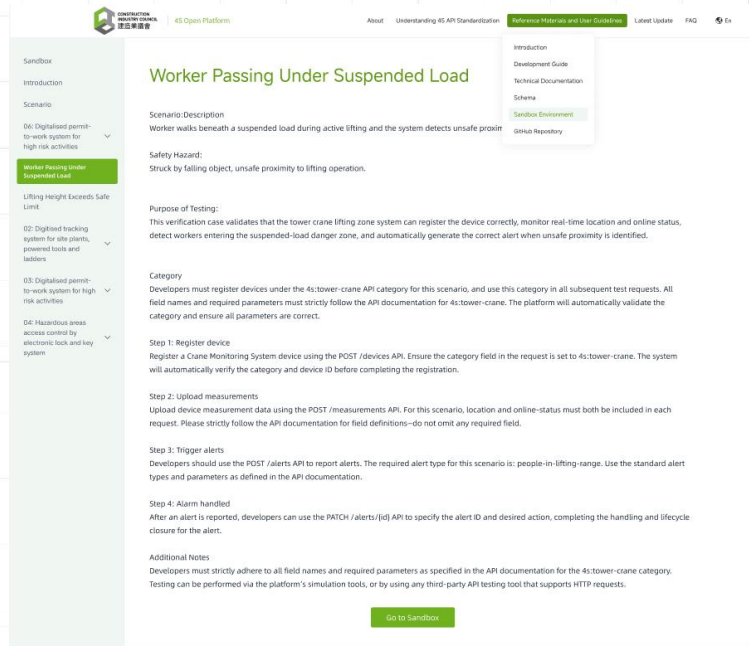
To begin, register an account by sending a request to the designated email address and specifying "CIC API Standardisation account". Email: [4S@cic.hk](mailto:4S@cic.hk)

Once your account has been created, you may login to the sandbox through the provided access link with your credentials. Sandbox login: [Link](#)

A right sidebar menu is visible, listing: 'Introduction', 'Development Guide', 'Technical Documentation', 'Schema', 'Sandbox Environment' (highlighted), and 'GitHub Repository'.

# Sandbox

Sandbox Environment, users can find different safety scenarios for each 4S category. Each scenario includes a description, safety hazards, testing objectives, and test steps, helping users understand what can be tested in each case.



The screenshot displays the '4S Open Platform' website. The top navigation bar includes links for 'About', 'Understanding 4S API Standardization', 'Reference Materials and User Guidance', 'Latest Update', 'FAQ', and 'En'. A sidebar on the left lists various scenarios under the 'Sandbox' section, with 'Worker Passing Under Suspended Load' highlighted. The main content area is titled 'Worker Passing Under Suspended Load' and contains the following information:

- Scenario-Description:** Worker walks beneath a suspended load during active lifting and the system detects unsafe proximity.
- Safety Hazard:** Struck by falling object, unsafe proximity to lifting operation.
- Purpose of Testing:** This verification case validates that the tower crane lifting zone system can register the device correctly, monitor real-time location and online status, detect workers entering the suspended-load danger zone, and automatically generate the correct alert when unsafe proximity is identified.
- Category:** Developers must register devices under the 4s:tower-crane API category for this scenario, and use this category in all subsequent test requests. All field names and required parameters must strictly follow the API documentation for 4s:tower-crane. The platform will automatically validate the category and ensure all parameters are correct.
- Step 1: Register device**  
Register a Crane Monitoring System device using the POST /devices API. Ensure the category field in the request is set to 4s:tower-crane. The system will automatically verify the category and device ID before completing the registration.
- Step 2: Upload measurements**  
Upload device measurement data using the POST /measurements API. For this scenario, location and online-status must both be included in each request. Please strictly follow the API documentation for field definitions—do not omit any required field.
- Step 3: Trigger alerts**  
Developers should use the POST /alerts API to report alerts. The required alert type for this scenario is: people-in-lifting-range. Use the standard alert types and parameters as defined in the API documentation.
- Step 4: Alarm handled**  
After an alert is reported, developers can use the PATCH /alerts/{id} API to specify the alert ID and desired action, completing the handling and lifecycle closure for the alert.
- Additional Notes**  
Developers must strictly adhere to all field names and required parameters as specified in the API documentation for the 4s:tower-crane category. Testing can be performed via the platform's simulation tools, or by using any third-party API testing tool that supports HTTP requests.

A 'Go to Sandbox' button is located at the bottom of the page.

# Sandbox

## Scenarios by 4S Categories



CONSTRUCTION  
INDUSTRY COUNCIL  
建造業議會

4S Open Platform | Sandbox

Digitalised permit-to-work system for high risk activities

Worker Passing Under Suspended Load

Lifting Height Exceeds Safe Limit

Digitised tracking system for site plants, powered tools and ladders

Digitalised permit-to-work system for high risk activities

Hazardous areas access control by electronic lock and key system

## Test Scenario Steps

### Worker Passing Under Suspended Load

Worker walks beneath a suspended load during active lifting and the system detects unsafe proximity.

SAFETY HAZARD

Struck by falling object unsafe proximity to lifting operation

DEVICE/SOFTWARE

Crane monitoring system

CATEGORY

4s:tower-crane

API 參考

Reset

API Interactions in this scenario must use the 4s:tower-crane category and strictly follow its standard parameter definitions.

1 post /devices This API is used to register devices and systems that require site safety monitoring.

| Parameter | Required | Example        | Description                                                                        |
|-----------|----------|----------------|------------------------------------------------------------------------------------|
| category  | Yes      | 4s:tower-crane | Must be set to 4s:tower-crane for this scenario. Any other value will be rejected. |

Request

Response

## Request input box

HTTP Request

```
{ "deviceName": "tower-crane 001",  
  {  
    {  
      "category": "4s:tower-crane",  
      "siteId": "1693279120646",  
      "cicSiteId": "250300001",  
      "solutionVendorId": "S-438",  
      "url": "https://api.4s.gov.hk/v1/devices/register"    }  
  }  
}
```

## OAS Spec document

Download OAS Spec

Download OAS Spec

Download the OpenAPI (OAS) specification for this scenario. Import directly into Swagger, Postman, or automation tools.

Other Ways to Call API

API Integration Guide

See how to call these APIs with Postman, curl, or other tools.

Checklist

0/4

Step1--Device registered

Verified

Step2--Monitoring reported

Not Verified

Step3--Alarm triggered

Not Verified

Step4--Alarm handled

Not Verified

## Report

# Sandbox

The API integration guide provides step-by-step instructions for using your sandbox credentials to connect to the server and test with tools such as Postman or your actual product.

 CONSTRUCTION INDUSTRY COUNCIL 建造業議會

45 Open Platform Sandbox

9 帮助

sandbox > API Integration Guide

### 45 开放平台 API 鉴权指南

所有业务 API 都需要使用 OAuth2 Bearer Token 访问。在编写代码或使用 Postman 等工具调用业务接口之前，请先按本指南完成鉴权，获取访问令牌（Access Token）。

1 获取凭证

2 换取 Token

3 使用 Token 访问

向平台注册申请 `client_id` 与 `client_secret` → 使用 POST `/oauth2/token` 获取访问令牌 → 请求头部 Authorization: Bearer `token`

#### 一、准备工作

##### 1.1 申请接入凭证

联系平台的运营开通接入账号，你将获得一组 `client_id` 与 `client_secret`。每组凭证绑定一个租户（企业账号），你只能访问该租户下的数据。

##### 1.2 地址约定

| 用途     | 地址                                             | 说明                                                                                       |
|--------|------------------------------------------------|------------------------------------------------------------------------------------------|
| 鉴权端点   | <code>https://choobv/oauth2/token</code>       | 端点请、不要 <code>/45/api/</code> 前缀                                                          |
| 业务 API | <code>https://choobv/45/api/current/...</code> | <code>current</code> 始终指向当前版本（当前为 20260724）；也可指向旧版本微服务 <code>/45/api/20260724/...</code> |

##### 1.3 占位符说明

本文字串中出现的 `<choobv>`、`<你的client_id>`、`<你的client_secret>`、`<access_token>` 等黄色高亮内容，请替换为你的实际值。

##### 1.4 选择授权模式

| 模式                                    | 适用场景                       | 凭证                                     |
|---------------------------------------|----------------------------|----------------------------------------|
| <code>client_credentials</code> 客户端模式 | 厂商系统服务间对接（定时任务、后台服务）、无用户参与 | <code>client_id + client_secret</code> |

平台面向开发者的系统对接统一使用 **客户端模式（第二节）**。

#### 二、客户端模式（client\_credentials）

厂商系统对接指南

使用你的 `client_id` / `client_secret` 直接调用鉴权接口，一步到位。

##### 2.1 请求说明

| 项目       | 值                                             |
|----------|-----------------------------------------------|
| 方法 / URL | POST <code>https://choobv/oauth2/token</code> |

**Thank you!**

