

ICS 35.100.01

CCS L 79



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 44121-2024

**Intelligent manufacturing - Requirements of identification and
resolution system**

智能制造 标识解析系统要求

Issued on: May 28, 2024

Implemented on: September 1, 2024

**Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC**

Table of Contents

1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	1
5 Overview	1
5.1 Functions and reference architecture of the identification and resolution system for intelligent manufacturing	1
5.2 Identifier types in intelligent manufacturing	2
6 Elements of the identification and resolution system for intelligent manufacturing	2
7 Requirements for identifiers in intelligent manufacturing	3
7.1 Functional requirements	3
7.2 Security requirements	3
7.3 Management and control requirements	3
8 Requirements for registration management in intelligent manufacturing	3
8.1 Functional requirements	3
8.2 Security requirements	3
8.3 Management and control requirements	4
9 Requirements for the resolution and query service in intelligent manufacturing	4
9.1 Functional requirements	4
9.2 Performance requirements	4
9.3 Security requirements	4
9.4 Management and control requirements	4
10 Requirements for the data management service in intelligent manufacturing	5
10.1 Functional requirements	5
10.2 Performance requirements	5
10.3 Security requirements	5

1 Scope

The document puts forward the functions and reference architecture, the identifier types and the element composition of the identification and resolution system for intelligent manufacturing, and it fixes the requirements for the identifiers, for registration management, for the resolution and query service and for the data management service.

It applies to the planning, design and application of identification and resolution systems inside an enterprise, and to the planning, design and application of public basic identifiers and industry-common identifiers deployed jointly across the identification and resolution systems of different enterprises. The document has no normative references.

3 Terms, definitions and abbreviated terms

Two terms are defined. An identification and resolution system is a system used to resolve and manage the information of the object being identified. A national-level node of identification and resolution is a public node that provides top level identifier resolution service to a country or a region together with management services such as identifier filing and identifier authentication.

Nine abbreviations are listed with their expansions: DDoS, distributed denial of service; ERP, enterprise resource planning; HTTPS, hyper text transfer protocol over secure socket layer; MES, manufacturing execution system; MQTT, message queuing telemetry transport; PLC, programmable logic controller; PLM, product lifecycle management; RFID, radio frequency identification; SCADA, supervisory control and data acquisition.

Note on the printed text: the expansion of MQTT is printed in the document as message queuing telemetry transport. The word is a misprint for message and is given above in its correct form; no other expansion has been altered.

5 Overview

The identification and resolution system for intelligent manufacturing has two functions: to register a unique identifier for objects such as products, parts and machines so that the objects can be told apart and managed, and to query, from that identifier, the network location of the target object or information related to it. The reference architecture of the system is given in Figure 1.

Three identifier types are recognised: public basic identifiers, used in the open domain; industry-common identifiers, used within one particular industry; and enterprise-internal identifiers, used inside an enterprise.

6 Elements of the identification and resolution system

The system is built from four elements: identifier rules, registration management rules, identifier resolution and query, and identifier data management. For each of them the document lists a content that is not exhaustive.

Identifier rules cover the identifier granularity, that is the number of objects an identifier stands for, divided into individual and collective; the identifier scope over which uniqueness is kept, divided into local and global; the identifier length, that is the size of the naming

space, divided into fixed length and variable length; the identifier structure, that is the field structure, which is structured; the identifier representation, that is the symbolic form, divided into numeric and alphabetic; and the identifier medium, the physical entity that stores the identifier, such as a two-dimensional code or an RFID electronic tag.

Registration management rules cover identifier application, the act by which a user applies to the identifier management body for ownership of an identifier; identifier allocation, the act by which the management body allocates that ownership; and identifier filing, by which the management body collects the user application information needed as a basis for later auditing.

Identifier resolution and query covers four capabilities: for a physical object resource that can itself communicate over the network, querying the network location of the target object and querying information related to it directly; and for a physical or virtual object that cannot itself communicate over the network, querying the network location of the physical entity resource associated with the target object and querying information related to the target object directly.

Identifier data management covers data maintenance, that is creation, modification and deletion of data in the resolution system and synchronisation of data between resolution systems; data association, which processes identifier data according to the relations between identifiers, for example the relation between the identifier of a container or outer packing case and the identifiers of the products inside it; data search, which finds the information corresponding to several associated identifiers from one identifier or finds the corresponding identifier backwards from non-identifier attribute data; and data application, which supports applications such as intelligent production, product traceability, supply chain management and life cycle management.

7 Requirements for identifiers

The functional requirements are uniqueness and extensibility. Uniqueness means that the identifier keeps its uniqueness within a certain range according to the particular scenario. Extensibility means that enough code positions are reserved in the identifier and that receiving positions are provided.

The security requirements are privacy and self-certification. Where an identifier scheme shows management information such as country and region, management body or resource classification explicitly, that information is made anonymous by means such as secondary mapping. Self-certification means that the identifier can identify the object identity uniquely and that the binding between the identifier, the real identity and the proof of authenticity is verified by means such as signatures and digests.

The management and control requirements are manageability and autonomous control. The naming space of the identifier is to be manageable: where management information

such as country and region, management body or resource classification is distinguished, that information can be used for statistical analysis and traffic control. The technical scheme of the identifier is to be under autonomous control.

8 Requirements for registration management

The functional requirements are openness and flexibility: several open forms of application for identifier registration are offered, and the prefix registration and allocation mechanism is kept simple while the suffix allocation method is kept flexible.

The security requirement is that registration data keep their privacy and that personal privacy be protected. An access control policy provides service to legitimate users and restricts access by illegitimate ones, the authenticity of users is assured, and access by users to network resources is logged lawfully so that it can be audited and traced afterwards.

The management and control requirements are autonomous control and auditability. Registration and allocation information of identifiers is kept locally. For auditability, the registration information of identifier application and allocation is stored and managed as needed and a sound filing and query mechanism is designed. Audit records cannot be deleted, modified or overwritten and a user cannot interrupt the audit process alone; the content of an audit record covers at least the event date, the time, the information about the initiator, the type, the description and the result, together with the operating state of the registration system, its traffic and user behaviour.

9 Requirements for the resolution and query service

The functional requirements are that resolution and query handle several identifier resolution schemes and extend effectively as intelligent manufacturing applications demand. Compatibility applies to all three levels: the resolution client, the enterprise node and the national-level node are each able to resolve several identifier schemes. The query terminal at the client recognises several identifiers; the enterprise node handles the various private identifiers within the enterprise and converts them outward into a specified public identifier; the national-level node handles the various public identifiers that conform to the relevant standards. Effective extension means that the network topology and the performance of the system can be extended.

The performance requirements are that the resolution offered by the service have low latency, that identifier data be collected by means such as RFID and that resolution performance be raised by means such as active caching, and that, while latency is kept, a suitable communication protocol such as HTTPS or MQTT be chosen according to the needs of the business scenario.

The security requirements are privacy protection, authorisation and authentication, and