Operations and Management Working Group
Internet-Draft
Intended status: Informational
Expires: 4 September 2025

A. An, Ed.
Korea Electronics Technology Institute
J. Jeong, Ed.
Sungkyunkwan University
S. Jang
Korea Electronics Technology Institute

3 March 2025

Interface to In-Network Computing Functions for Cooperative Intelligent Transportation Systems

draft-ahn-opsawg-i2icf-cits-00

Abstract

This document specifies a structured framework for orchestrating, managing, and monitoring In-Network Computing Functions (ICFs) in Cooperative Intelligent Transportation Systems (C-ITS). For example, in the context of Vehicle-to-Everything (V2X) communications, efficient management of Vehicle-to-Vehicle (V2V) communications and their integration with C-ITS can greatly benefit from in-network computing. By leveraging ICFs, it becomes possible to optimize real-time communication, streamline traffic management, and enhance data processing and security services at the network edge.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 4 September 2025.

Table of Contents

1. Introduction

In-network computing has recently gained significant attention and has been extensively explored as a promising research area. This growing interest stems from the increasing accessibility of data plane programmability, which has opened new opportunities for both application developers and network operators to optimize network operations and application performance. Over the years, rigorous research and numerous trials have validated the effectiveness of certain in-network computing capabilities, collectively referred to as In-Network Computing Functions (ICFs). These functions have proven to be highly beneficial in various domains, such as machine learning, real-time data processing, and large-scale distributed systems. For instance, in-network aggregation techniques have been shown to accelerate collective communication operations like Allreduce and Broadcast, which are critical in training machine learning models. These advancements have led to the gradual commercialization of many in-network computing capabilities. Several other works, such as [I-D.jeong-opsawg-i2icf-problem-statement][I-D.y

ao-tsvwg-cco-problem-statement-and-usecases][I-D.irtf-coinrg-use-case s]also provide additional use cases and scenarios for in-network computing applications.

Despite these promising developments, a critical challenge remains: the absence of a unified framework and standardized interfaces to effectively register, configure, manage, and monitor ICFs. The framework for Interface to Network Security Functions (I2NSF) defined in [RFC8329] provides a solid foundation for managing and orchestrating Network Security Functions (NSFs). However, these frameworks fall short when it comes to supporting the unique requirements of ICFs. Unlike NSFs, ICFs often require seamless coordination between endpoint computing capabilities and in-network nodes, such as Programmable Network Devices (PNDs), to accelerate application performance collaboratively. This highlights the need for a new framework that can integrate endpoint and in-network functionalities while leveraging and adapting existing frameworks, such as I2NSF, to define interfaces for ICFs effectively.

This document rigorously examines the applicability of ICFs within constrained environments, particularly in data center networks, and introduces a structured framework for their registration, configuration, management, and monitoring. Additionally, it evaluates extended use cases, including Vehicle-to-Everything (V2X) communication, wherein ICFs facilitate the efficient orchestration of vehicle-to-vehicle (V2V) networks, seamless integration with Cooperative Intelligent Transport Systems (C-ITS), and interoperability with Mobile Network Operators (MNOs). By leveraging ICFs, these architectures can achieve enhanced communication efficiency, improved traffic control, and secure data exchange. Furthermore, this document underscores the pivotal role of ICFs in strengthening cybersecurity measures for both private and public data within such interconnected ecosystems, addressing the increasing demand for resilient security mechanisms in contemporary networked infrastructures.

2. Framework and Interfaces

This section presents the detailed design of I2ICF framework and interfaces for C-ITS and MNO Networking.

2.1. I2ICF Framework for C-ITS and MNO Networking

Figure 1 shows the I2ICF framework of C-ITS and MNO networking. In this framework, there are several major components and relative interfaces.

* Central Cloud: A system that comprehensively controls the entire C-ITS (Cooperative Intelligent Transport Systems) environment. It manages information from various C-ITS centers, including regional centers and highway centers, and facilitates and oversees the connection between C-ITS data from the Government Public Center and end users. Additionally, it provides security functions through an integrated cybersecurity system.

* C-ITS Center: The C-ITS Center is a comprehensive term that encompasses both the Region Center and the Highway Center. It serves as the central hub for managing and coordinating intelligent transportation systems across various environments, including urban regions and highways. By integrating data from Region Centers and Highway Centers, the C-ITS Center ensures efficient traffic management, real-time data processing, and seamless communication between infrastructure and connected or autonomous vehicles.

* Region Center: The Region Center refers to local centers established at key locations. These regional centers are connected to Road-Side Units (RSU) and function as one of the C-ITS Centers. Each regional C-ITS center collaborates with the Government Public Center to share collected data, ensuring seamless integration and data exchange between local infrastructure and centralized management systems.

* Highway Center: The Highway Center operates similarly to the Region Center but is managed separately due to the unique characteristics of highways, which span multiple regions rather than being confined to a single city. Given the higher traffic volume on highways compared to regular roads, there is a significant increase in data generation, necessitating dedicated network management for highway environments. Highways are equipped with a greater number of RSUs than general roads, enabling the delivery of critical information to autonomous vehicles. As a result, the Highway Center focuses on managing areas that require more real-time processing to support safe and efficient autonomous driving.

* Government Public Center: The Government Public Center is a C-ITS information provision system managed by the government. Due to the nature of road traffic infrastructure, it is challenging for private companies to manage this data effectively, and concerns over reliability make it difficult for users to utilize privately managed data. The Government Public Center ensures the delivery of highly reliable, government-provided data to users, enabling them to effectively utilize infrastructure-based information. It oversees the provision and management of trustworthy data essential for safe and efficient transportation systems.

* C-ITS Data Linkage System: The C-ITS Data Linkage System is a platform designed to provide C-ITS data to external users. By offering data through methods such as Open APIs, this system connects C-ITS infrastructure information with users, enabling seamless access to real-time traffic and transportation data. It facilitates the integration of C-ITS data into various applications and services, supporting the development of innovative mobility solutions and enhancing the overall efficiency and safety of transportation systems.

* Cyber Security System: The Cyber Security System is responsible for managing the security of communications between Software-Defined Vehicles (SDV), Vulnerable Road Users (VRU), RSU, Mobile Network Operators (MNO), and C-ITS infrastructure. Security technologies are fundamentally integrated into all communications to ensure encrypted data transmission. Outgoing data is encrypted using a public key, while receiving devices decrypt the data using a private key to securely access the information. The Cyber Security System oversees the protection of both private and public keys across all modules, ensuring robust security against potential exposure and safeguarding the integrity and confidentiality of transmitted data.

* C-ITS Infra: The C-ITS Infrastructure is a system designed to collect and provide various types of information, including traffic signal data, roadside environment information, VRU data, and RSU data. The specific C-ITS information available may vary depending on the devices and equipments installed on the road. This infrastructure enables real-time data exchange between the transportation system and connected or autonomous vehicles, supporting safer and more efficient traffic management.

* RSU: The RSU is a device that connects the C-ITS Infrastructure with SDVs. Through the RSU, SDVs can transmit and receive data between vehicles via V2V and between vehicles and infrastructure via V2I. RSUs play a critical role in enabling real-time communication, providing essential information such as traffic signals, road conditions, and safety alerts, thereby enhancing the safety and efficiency of autonomous and connected vehicle operations.

* SDV1 and SDV2: SDV1 and SDV2 are examples depicted in the diagram, but in real-world scenarios, there can be an arbitrary number of vehicles. An SDV (Software-Defined Vehicle) consists of two main communication interfaces (External Communication Interface : Enables communication with external systems such as RSUs (Roadside Units), other vehicles (V2V), and infrastructure (V2I/V2N), supporting seamless interaction within the C-ITS ecosystem. Internal Vehicle Network (IVN) Interface : Manages internal communication within the vehicle, connecting various onboard systems and components to ensure

smooth operation and integration of vehicle functionalities) This dual-interface structure allows SDVs to efficiently exchange data both externally with the C-ITS infrastructure and internally for optimized vehicle control.

* IVN-Network1 and IVN-Network2: IVN-Network1 and IVN-Network2 are examples, but in practice, the internal communication system of a vehicle can consist of N different networks. These networks are part of the In-Vehicle Network (IVN), which facilitates communication within the vehicle. In an SDV (Software-Defined Vehicles), the IVN is designed based on a Zonal Architecture, where communication interfaces connect various devices and components within specific zones of the vehicle. This architecture improves data transmission efficiency, reduces wiring complexity, and enhances the integration of advanced systems for autonomous driving and vehicle control. Through this zonal design, SDVs can effectively manage high-speed data exchange between sensors, controllers, and actuators, supporting real-time processing and safer driving operations.

* VRU: A VRU refers to users who can communicate either with an MNO or directly with SDVs. VRUs typically include pedestrians, cyclists, and motorcyclists who are more susceptible to traffic accidents due to their limited protection. By connecting with MNO networks, VRUs can receive real-time safety alerts and traffic information. Additionally, direct communication with SDVs enables VRUs to exchange critical safety data, such as location and movement intentions, which helps autonomous and connected vehicles detect and respond to nearby vulnerable users, ultimately enhancing road safety.

* MNO: An MNO is a service provider that owns and manages wireless communication infrastructure, including network towers, core networks, and data centers. In the context of C-ITS, MNOs play a critical role in enabling real-time communication between vehicles, infrastructure, and VRUs by providing seamless connectivity through cellular networks (e.g., LTE, and 5G). MNOs facilitate the transmission of safety messages, traffic updates, and vehicle data, ensuring low-latency, high-reliability communication essential for autonomous driving and connected vehicle ecosystems. Additionally, MNOs collaborate with C-ITS infrastructure to enhance data security and manage network resources for efficient traffic management and mobility services.

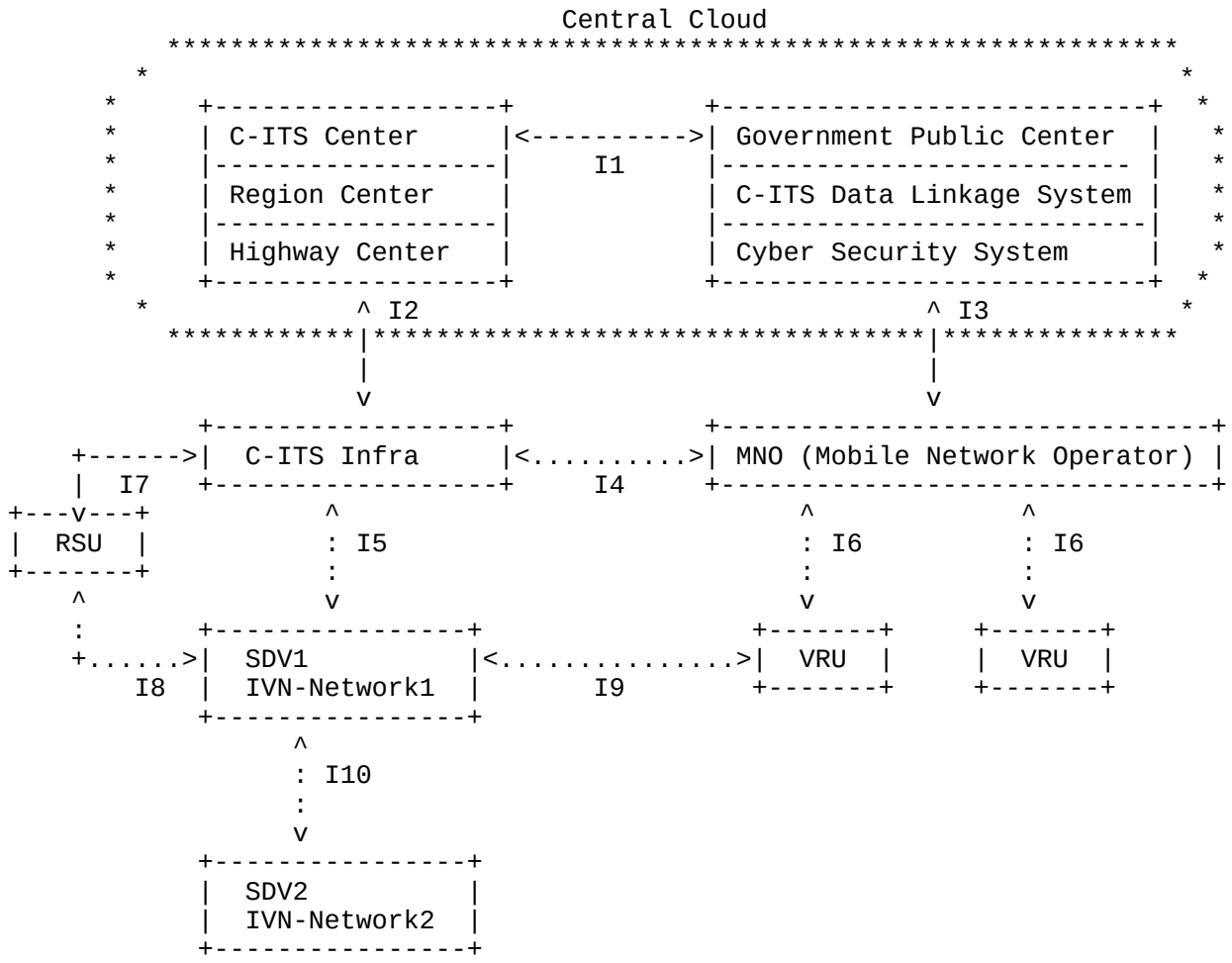

Figure 1: I2ICF Framework and Interfaces

2.2. I2ICF Interfaces

According to the framework described in the previous section, there are major interfaces that I2ICF of C-ITS and MNO networking should define.

Interface 1 (I1): This is the registration interface between the C-ITS Center and the Government Public Center. It facilitates the exchange of C-ITS infrastructure data, such as traffic information and real-time road conditions, ensuring the Government Public Center

can provide accurate and trustworthy data to external users. This interface also supports secure data sharing through standardized protocols and encryption.

Interface 2 (I2): This interface connects the C-ITS Center with the C-ITS Infra. It is responsible for distributing infrastructure data, such as traffic signal information, road environment data, and RSU status, from the C-ITS Center to the C-ITS Infra for real-time processing and delivery to connected vehicles. It ensures continuous data flow for effective traffic and infrastructure management.

Interface 3 (I3): This is the data exchange interface between the Government Public Center and the MNO (Mobile Network Operator). It enables the secure transmission of C-ITS data to MNOs, allowing mobile networks to deliver critical traffic and safety information to VRUs and vehicles. This interface must ensure data integrity and security during transmission.

Interface 4 (I4): This interface connects the C-ITS Infra with the MNO. It supports the sharing of network resources and real-time communication between infrastructure components and mobile networks. This connection allows for efficient distribution of data, such as traffic alerts and safety notifications, to mobile users and vehicles.

Interface 5 (I5): This is the communication interface between the C-ITS Infra and SDVs. It enables bidirectional data exchange, allowing SDVs to receive real-time infrastructure information (e.g., traffic signals, road hazards) and transmit vehicle status data back to the infrastructure. This interface is critical for supporting V2I communications.

Interface 6 (I6): This interface connects the MNO with both VRUs and SDVs. It is used to deliver real-time safety messages, navigation updates, and other critical data. It also allows VRUs and SDVs to send status or emergency signals back to the network. This interface must ensure low-latency and secure data transmission to prevent accidents and improve traffic efficiency

Interface 7 (I7): This is the management interface between the RSU and the C-ITS Infra. It facilitates the configuration, monitoring, and management of RSUs to ensure stable communication between roadside infrastructure and vehicles. It also handles firmware updates and diagnostics for RSUs.

Interface 8 (I8): This interface supports V2I communication between SDVs through the RSU. It allows SDVs to exchange critical information such as speed, direction, and emergency signals, enabling

collision avoidance and cooperative driving. This interface must provide real-time and reliable data exchange in dynamic traffic environments.

Interface 9 (I9): This is the communication interface between SDVs and VRUs. It ensures that vulnerable road users receive immediate safety notifications from nearby vehicles and infrastructure. For example, SDVs can warn pedestrians of approaching vehicles or detect VRU movements in blind spots, enhancing road safety.

Interface 10 (I10): This is the external and internal communication interface between multiple SDVs It enables secure and efficient communication within the vehicle’s zonal architecture, facilitating seamless data exchange between various internal systems (e.g., sensors, controllers) and supporting autonomous driving functions.

3. Use Cases

This section introduces practical use cases of the I2ICF framework within the context of C-ITS and MNO networking. These use cases focus on emerging technologies such as SDVs, End-to-End (E2E) communication, and Cybersecurity, highlighting how the I2ICF framework can improve network efficiency, safety, and security in intelligent transportation environments.

* Real-Time Data Processing for SDV: The I2ICF framework enables seamless communication between SDVs and C-ITS infrastructure through interfaces such as I5 (C-ITS Infra <-> SDV) and I8 (V2V Communication via RSU). Real-time data such as traffic signals, road conditions, and obstacle detection are transmitted to SDVs for immediate processing. By offloading certain data processing tasks to network devices (e.g., RSUs), SDVs can reduce internal computational load, allowing faster decision-making for functions like emergency braking or lane changes. This distributed data processing model improves the overall safety and efficiency of autonomous driving.

* E2E Communication for Cooperative Driving: The integration of MNO networks with C-ITS through interfaces like I4 (C-ITS Infra <-> MNO) and I6 (MNO <-> VRU/SDV) allows for reliable and low-latency E2E communication. This connectivity is essential for cooperative driving scenarios, where multiple SDVs coordinate lane changes, merging, or platooning in real time. The I2ICF framework ensures that the network can dynamically manage traffic loads and prioritize safety-critical data transmission, enabling vehicles to share and act on real-time information seamlessly.

* Enhanced Cybersecurity for C-ITS and MNO Integration: Given the extensive data exchange between vehicles, infrastructure, and network operators, cybersecurity is a critical component. The Cyber Security System within the I2ICF framework, managed through interfaces like I3 (Government Public Center <-> MNO) and I10 (Internal SDV Communication), provides E2E encryption and secure key management. Private keys are stored securely in the cloud and can be updated via Over-The-Air (OTA) mechanisms if compromised. If a critical security breach occurs, the system can initiate a global reset to reissue encryption keys, ensuring system-wide security integrity. This proactive approach minimizes the risk of cyberattacks on connected vehicles and infrastructure.

* Dynamic Resource Allocation for High-Density Traffic Environments: In high-traffic conditions such as highways or urban intersections, efficient data management is crucial. The I2ICF framework, through I7 (RSU <-> C-ITS Infra) and I9 (SDV <-> VRU), enables dynamic resource allocation. For example, RSUs can prioritize data transmission for emergency vehicles or redirect network resources to manage traffic congestion. This adaptive data flow management reduces latency and prevents network bottlenecks, ensuring that all vehicles and infrastructure components receive critical information in real time.

* Edge Computing for Latency-Sensitive Applications: Edge computing capabilities are integrated into the I2ICF framework using RSUs and Programmable Network Devices (PNDs) to handle latency-sensitive tasks. Interfaces like I1 (C-ITS Center <-> Government Public Center) and I8 (SDV <-> SDV via RSU) allow certain computational tasks such as object detection or predictive path planning to be processed at the network edge rather than relying on centralized cloud servers. This significantly reduces response time for autonomous driving actions and enhances road safety by enabling faster vehicle reactions.

* These use cases demonstrate how the I2ICF framework can enhance the performance, security, and reliability of intelligent transportation systems by integrating C-ITS infrastructure with MNO networks. By supporting real-time data processing, secure communication, and dynamic resource management, the framework addresses the complex demands of modern SDVs and connected mobility solutions.

4. Security Considerations

The I2ICF framework for C-ITS and MNO Networking offers numerous advantages for various applications. However, due to the framework's extensive connectivity between diverse vehicles, devices, centers, clouds, and VRUs, a vast amount of information and functionalities are exposed during network configuration, leading to potential security risks. To ensure the overall security of the entire system, the following measures are recommended: First, the application development system should be controlled by the same service providers (e.g., cloud service providers or network operators) that own the network and computing infrastructure. Second, devices within the cloud center should be pre-configured with security zones to isolate traffic, preventing it from affecting other network traffic. Third, encryption keys for each device should be centrally managed by the cloud center. In the event of key exposure, the system should support Over-The-Air (OTA) updates to promptly replace compromised keys. Fourth, if a security breach occurs within the centralized management system, exposing encryption keys, the entire system should undergo a reset to perform a security initialization. This process will generate and distribute new encryption keys to ensure the continued protection of sensitive data.

5. IANA Considerations

TBD.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8329] Lopez, D., Lopez, E., Dunbar, L., Strassner, J., and R. Kumar, "Framework for Interface to Network Security Functions", RFC 8329, DOI 10.17487/RFC8329, February 2018, <https://www.rfc-editor.org/info/rfc8329>.

[RFC8799] Carpenter, B. and B. Liu, "Limited Domains and Internet Protocols", RFC 8799, DOI 10.17487/RFC8799, July 2020, <https://www.rfc-editor.org/info/rfc8799>.

6.2. Informative References

[I-D.irtf-coinrg-use-cases]
Kunze, I., Wehrle, K., Trossen, D., Montpetit, M., de Foy, X., Griffin, D., and M. Rio, "Use Cases for In-Network Computing", Work in Progress, Internet-Draft, draft-irtf-coinrg-use-cases-07, 4 December 2024, <https://datatracker.ietf.org/doc/html/draft-irtf-coinrg-use-cases-07>.

[I-D.jeong-opsawg-i2icf-problem-statement]
Jeong, J. P., Shen, Y., Ahn, Y., Kim, Y., Jr., E. P. D., and K. Yao, "Interface to In-Network Computing Functions (I2ICF): Problem Statement", Work in Progress, Internet-Draft, draft-jeong-opsawg-i2icf-problem-statement-00, 3 March 2025, <https://datatracker.ietf.org/api/v1/doc/document/draft-jeong-opsawg-i2icf-problem-statement/>.

[I-D.yao-tsvwg-cco-problem-statement-and-usecases]
Yao, K., Shiping, X., Li, Y., Huang, H., and D. KUTSCHER, "Collective Communication Optimization: Problem Statement and Use cases", Work in Progress, Internet-Draft, draft-yao-tsvwg-cco-problem-statement-and-usecases-00, 23 October 2023, <https://datatracker.ietf.org/doc/html/draft-yao-tsvwg-cco-problem-statement-and-usecases-00>.

Acknowledgments

This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea Ministry of Science and ICT (MSIT) (No. 2022-0-00199, 5G-NR-V2X performance verification for connected Autonomous Driving).

This work was in part supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea Ministry of Science and ICT (MSIT) (No. RS-2024-00398199 and RS-2022-II221015).

Authors' Addresses

Byoungman Robert An (editor)
Intelligent Information R and D Division Mobility Platform Research Center
Global R and D Center 6th floor
#22, Daewangpangyo-ro 712beon-gil
Seongnam
Gyeonggi-Do
13488
Republic of Korea
Phone: +82 31 739 7463

Email: bman@keti.re.kr
URI: https://www.keti.re.kr/eng/main/main.php

Jaehoon Paul Jeong (editor)
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4957
Email: pauljeong@skku.edu
URI: http://iotlab.skku.edu/people-jaehoon-jeong.php

Seonghyun Alex Jang
Intelligent Information R and D Division Mobility Platform Research Center
Global R and D Center 6th floor
#22, Daewangpangyo-ro 712beon-gil
Seongnam
Gyeonggi-Do
13488
Republic of Korea
Phone: +82 31 739 7465
Email: jang.sh@keti.re.kr
URI: https://www.keti.re.kr/eng/main/main.php