WORLD SUMMIT ON
THE INFORMATION SOCIETY

WSIS FORUM 2021

Starting from January
Final Week 17-21 May 2021

Coordinated by

ITU

Organized by

UNESCO
United Nations
Educational, Scientific and
Cultural Organization

UNITED NATIONS
UNCTAD

UNDP

ITU

www.wsis.org/forum

WSIS FORUM 2021

Session 265
Cybersecurity track: Automotive Cybersecurity

13:00 ~ 14:00(UTC+2) Friday 16 April 2021

WSIS FORUM 2021

Overview of standardization of cybersecurity in ITS (intelligent transport system) environment in ITU-T SG17

Sang-Woo Lee

Rapporteur, ITU-T Q13 in SG 17

Information Security Research Deparment,
ETRI(Electronics and Telecommunications Research Institute)

Contents

- Introduction of Q13 in SG17
- Current status of work items related to ITS security
- Future plan

ITU-T SG17 Q13

- SG17
  - SG 17 in ITU Telecommunication Standardization Sector (ITU-T) has been working on security aspects including generic security architecture, mechanisms and management guidelines for heterogeneous networks/systems/services, cloud computing, smart grid, intelligent transportation systems (ITS) including V2X communication, the 5G cellular network, software-defined networks, Big Data analytics, Internet-of-Things, protection of the personally identifiable information (PII) as **the lead Study Group on Security in ITU-T.**

- Question 13 in SG 17
  - a lead Question for developing Recommendations regarding security aspect for ITS including road transport, railway, maritime and air transport as well.

WP1/17	**Security strategy and coordination**
Q1/17	Security standardization strategy and coordination
Q15/17	Security for/by emerging technologies including quantum-based security
WP2/17	**5G, IoT and ITS security**
Q2/17	Security architecture and network security
Q6/17	Security for telecommunication services and Internet of Things
Q13/17	Intelligent transport system security
WP3/17	**Cybersecurity and management**
Q3/17	Telecommunication information security management and security services
Q4/17	Cybersecurity and countering spam
Q5/17	(DELETED IN JANUARY 2021, MERGED INTO Q4/17) Countering spam by technical means
WP4/17	**Service and application security**
Q7/17	Secure application services
Q8/17	Cloud computing and Big data infrastructure security
Q14/17	Distributed Ledger Technology (DLT) security
WP5/17	**Fundamental security technologies**
Q9/17	(DELETED IN JANUARY 2021, MERGED INTO Q10/17) Telebiometrics
Q10/17	Identity management and telebiometrics architecture and mechanisms
Q11/17	Generic technologies (such as Directory, PKI, Formal languages, Object Identifiers) to support secure applications
Q12/17	(DELETED IN JANUARY 2021, MERGED INTO Q11/17) Formal languages for telecommunication software and testing

ITS security

Work Items in Q13(1)

Number	Acronym	Title	Plan
1	**X.1371 (Published)**	Security threats in connected vehicles	**2020.05 (Approved)**
2	**X.1372 (Published)**	Security guidelines for Vehicle-to-Everything(V2X) communication	**2020.03 (Approved)**
3	**X.1374 (Published)**	Security requirements for external interfaces and devices with vehicle access capability	**2020.10 (Approved)**
4	**X.1375 (Published)**	Methodologies for intrusion detection system on in- vehicle networks	**2020.10 (Approved)**
5	**X.1376 (Published)**	Security-related misbehavior detection mechanism for connected vehicles	**2021.01 (Approved)**
6	X.1373Rev	Software update capability for ITS communications devices	2022.4Q
7	X.itssec-5	Security guidelines for vehicular edge computing	2021.4Q
8	X.srcd	Security requirements for categorized data in V2X communication	2021.4Q
9	X.eivnsec	Security guidelines for Ethernet-based In-Vehicle networks	2021.4Q
10	X.edrsec	Security guidelines for cloud-based data recorders in automotive environment	2021.4Q
11	X.fstiscv	Framework of security threat information sharing for connected vehicles	2022.4Q
12	X.ipscv	Methodologies for intrusion prevention system in connected vehicles	2022.4Q
13	X.rsu-sec	Security requirements for road-side units in intelligent transportation systems	2022.4Q
14	X.evtol-sec	Security guidelines for an electric vertical take-off and landing (eVTOL) vehicle in an urban air mobility environment	2024

Work Items in Q13(2)

ITS security threat

- **X.1371**

ITS application security

- **X.1373Rev:** Software update capability for ITS communications devices
- **X.edrsec**: Security guidelines for cloud-based data recorders in automotive environment

eVTOL security

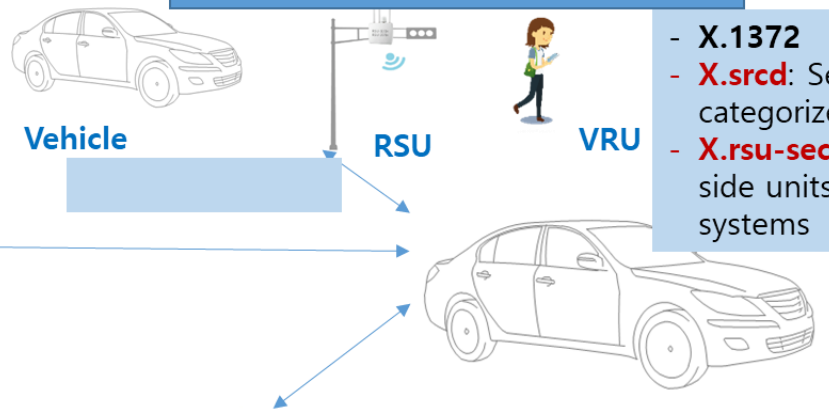
- **X.evtol-sec**: Security guidelines for an electric vertical take-off and landing (eVTOL) vehicle in an urban air mobility environment

Vehicular edge computing security

Cloud

- **X.itssec-5**: Security guidelines for vehicular edge computing

V2X security



- **X.1372**
- **X.srcd**: Security requirements for categorized data in V2X communication
- **X.rsu-sec**: Security requirements for road-side units in intelligent transportation systems

Traffic management center

Vehicular infrastructure security

- **X.1376**
- **X.fistiscv**: Framework of security threat information sharing for connected vehicles

External device security

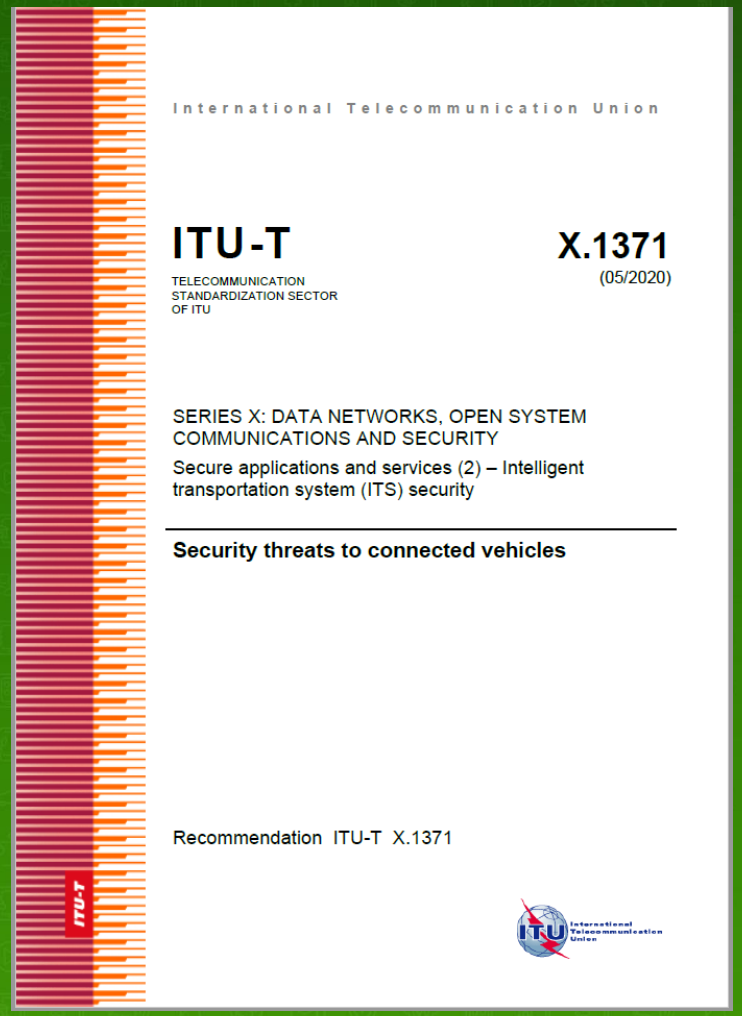
- **X.1374**

In-vehicle security

- **X.1375**
- **X.eivnsec**: Security guidelines for Ethernet-based In-Vehicle networks
- **X.ipscv**: Methodologies for intrusion prevention system in connected vehicles

X.1371(1)

- Title: Security threats in connected vehicles
- Status: Approved at May 2020
- Scope:
  - This Recommendation describes security threats to connected vehicles.
  - These threats can be referred to and utilized in other Recommendations developed by ITU-T to consistently develop Recommendations in the context of the security aspects of intelligent transport systems (ITSs).
- This Recommendation is closely related to recommendation on cybersecurity in UNECE WP29


International Telecommunication Union

ITU-T

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

X.1371

(05/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Intelligent transportation system (ITS) security

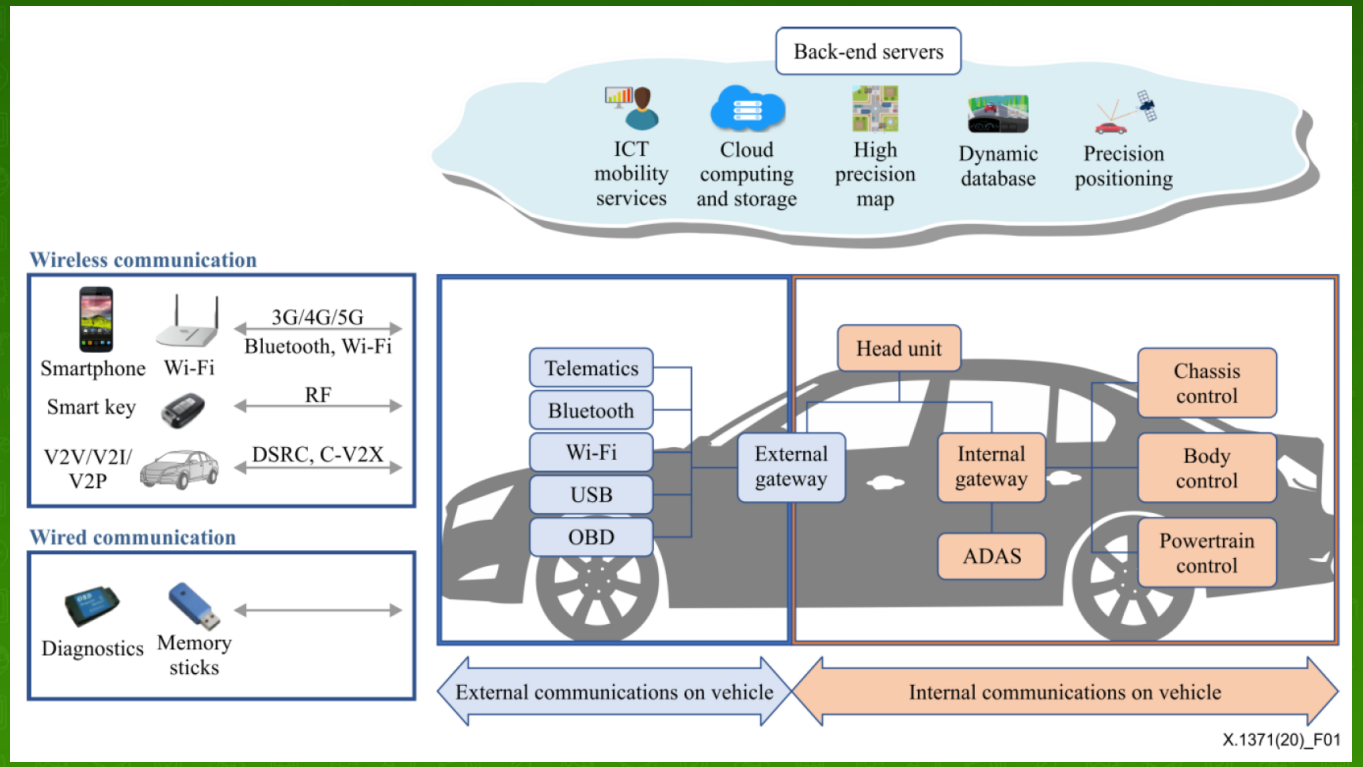
Security threats to connected vehicles

Recommendation ITU-T X.1371

Ref) https://www.itu.int/rec/T-REC-X.1371/en

X.1371(2)

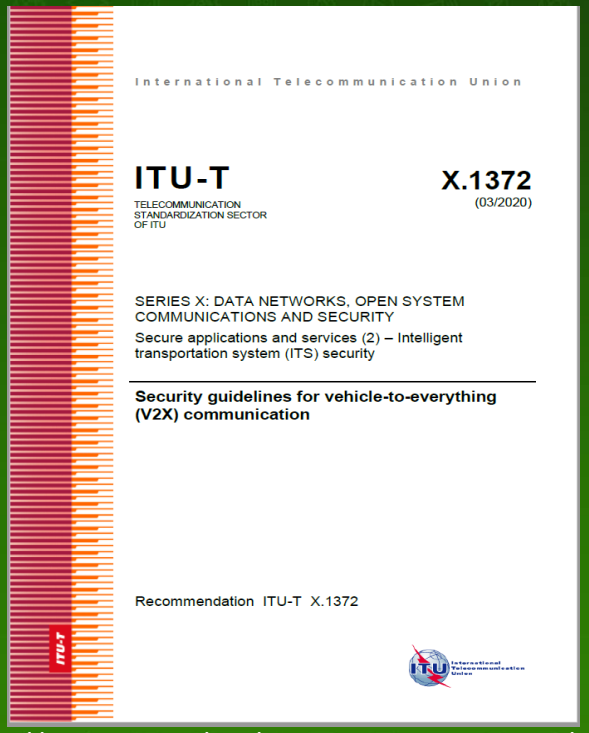
- Threat analysis in connected vehicles
  - Back-end servers
  - Communication channels
  - Software update procedures
  - Unintended human actions
  - External connectivity and connections
- Potential information related to threats
  - Potential targets
  - Potential vulnerabilities



<A concept of connected vehicle (vehicle ecosystem)> (source: X.1371)

X.1372

- Title: Security guidelines for Vehicle-to Everything(V2X) Communication
- Status: Approved at March 2020
- Scope:
  - This Recommendation provides security guidelines for vehicle-to-everything (V2X) communication.
  - V2X is a generic term comprising the communication modes termed as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-nomadic devices (V2D) and vehicle-to-pedestrian (V2P) when discussed in this Recommendation.
  - This Recommendation identifies threats in the V2X communication environment, specifies security requirements and provides description of possible implementation of V2X communication with security.


International Telecommunication Union

ITU-T
TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

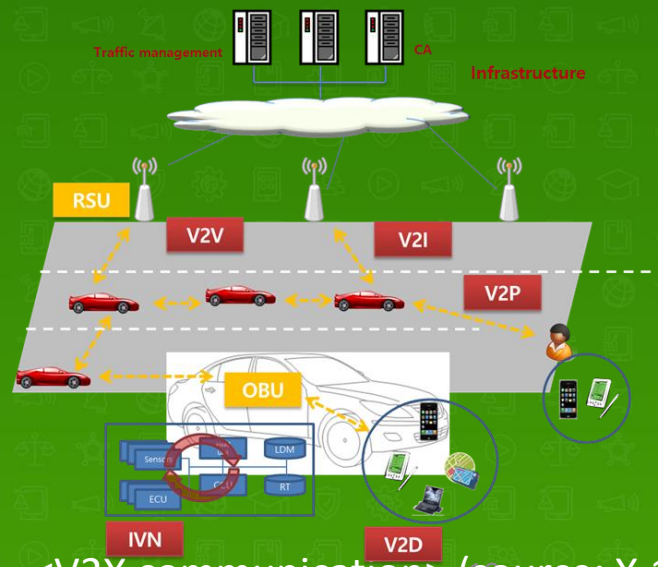
X.1372
(03/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY
Secure applications and services (2) – Intelligent transportation system (ITS) security

Security guidelines for vehicle-to-everything (V2X) communication

Recommendation ITU-T X.1372

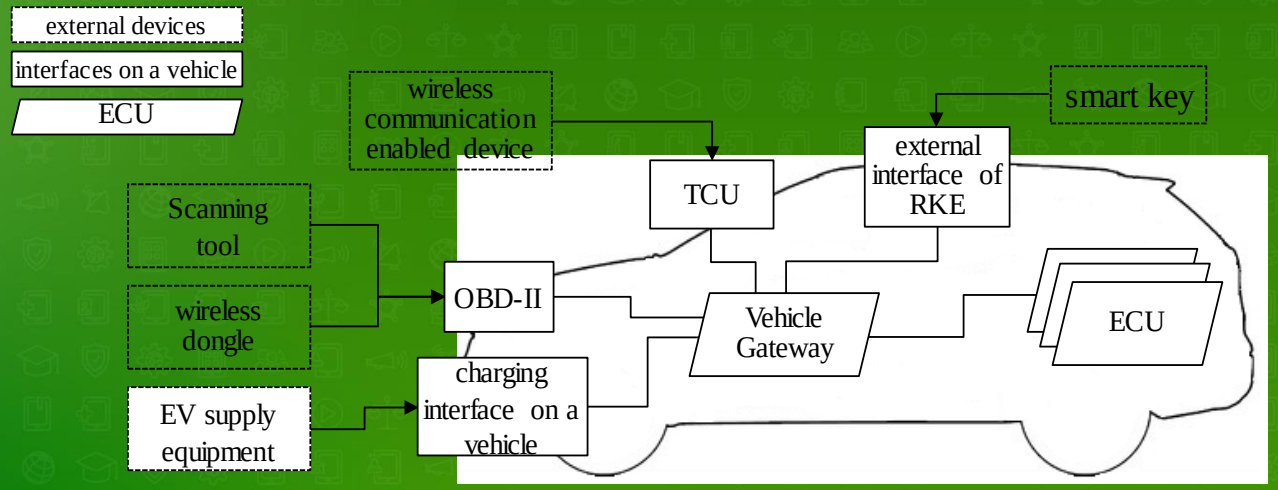
Ref)https://www.itu.int/rec/T-REC-X.1372-202003-I/en



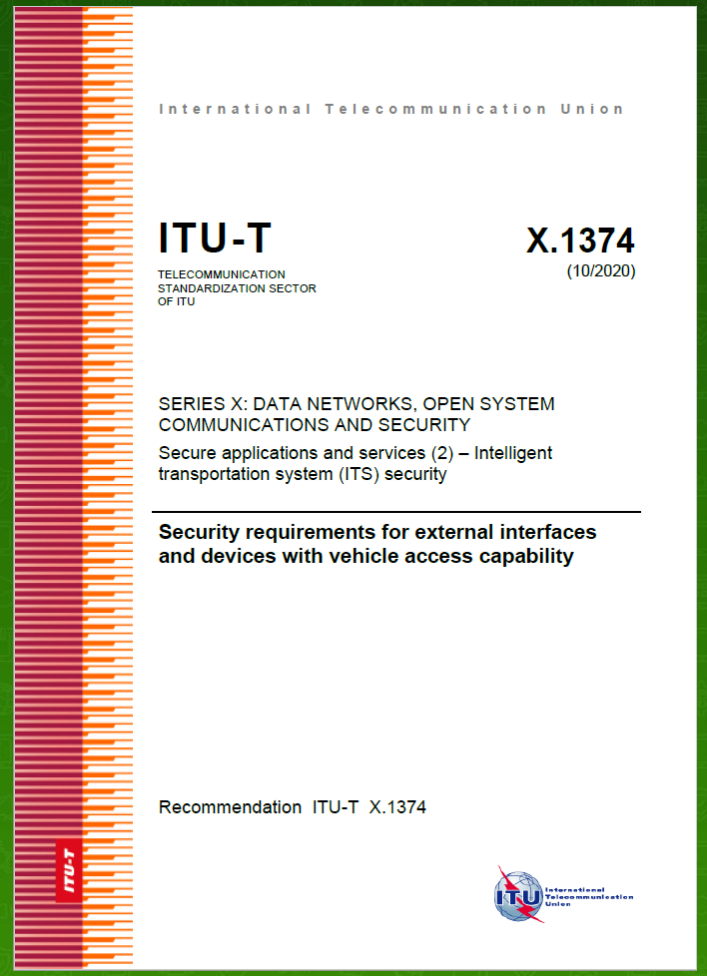
<V2X communication> (source: X.1372)

X.1374

- Title: Security requirements for external interfaces and devices with vehicle access capability
- Status: Consented at 03 Sep. 2020, Approved at 29 Oct. 2020
- Scope:
  - identifying security threats against vehicle external interfaces and external devices;
  - defining security requirements for the external interfaces and devices with vehicle access capability to address the identified threats depending on the types of access interfaces.



<Overview of vehicle external interfaces and external devices> (Source: X.1374)


International Telecommunication Union

ITU-T

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

X.1374
(10/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Intelligent transportation system (ITS) security

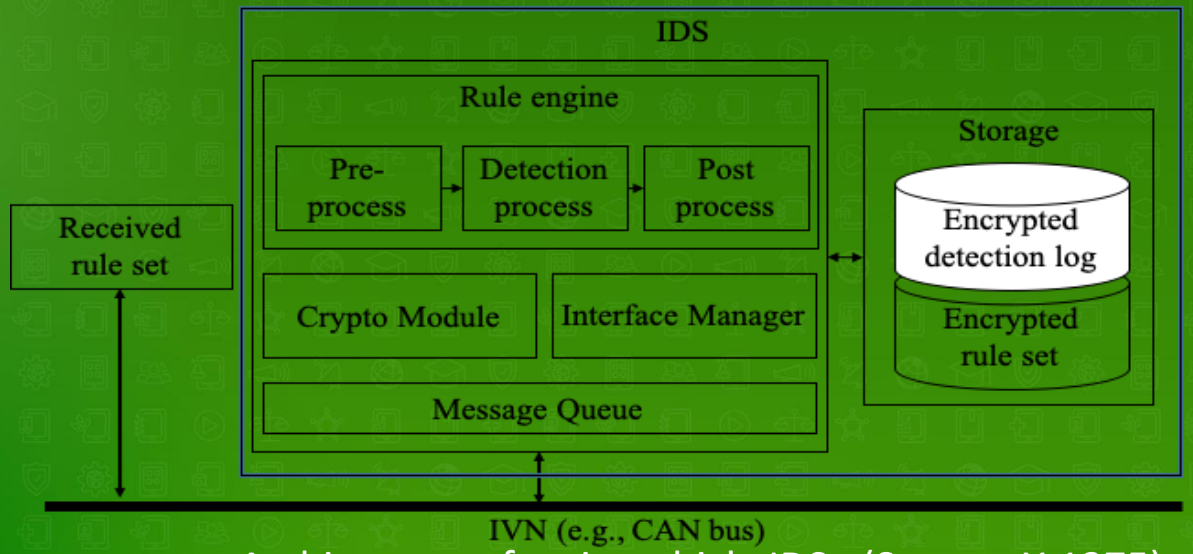
Security requirements for external interfaces and devices with vehicle access capability

Recommendation ITU-T X.1374

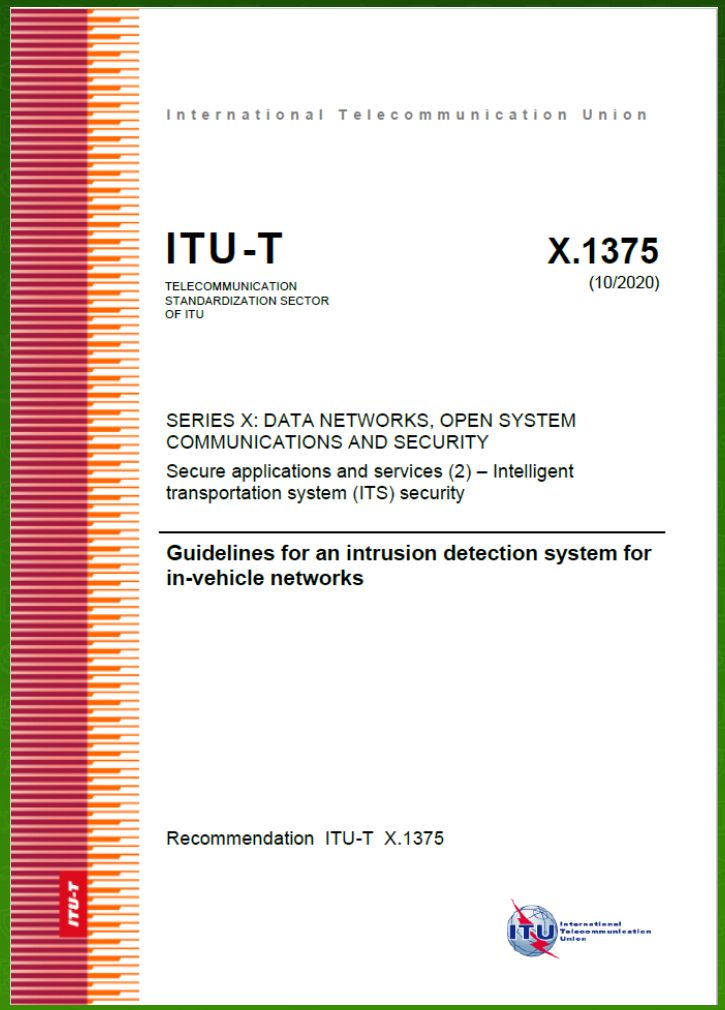
Ref)https://www.itu.int/rec/T-REC-X.1374/en

X.1375

- Title: Guidelines for an intrusion detection system for in-vehicle networks
- Status: Consented at 03 Sep. 2020, Approved at 29 Oct. 2020
- Scope:
  - This Recommendation aims to provide the methodologies for intrusion detection systems (IDSs) on in-vehicle networks (IVNs). This Recommendation identifies threats to in-vehicle networks such as controller area network (CAN), which is widely used in modern vehicles.
  - This Recommendation mainly focuses on aspects of detecting intrusion and malicious activities in in-vehicle networks such as CAN that cannot be supported by general IDSs currently used in Internet.



<Architecture of an in-vehicle IDS> (Source: X.1375)


International Telecommunication Union

ITU-T
TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

X.1375
(10/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Intelligent transportation system (ITS) security

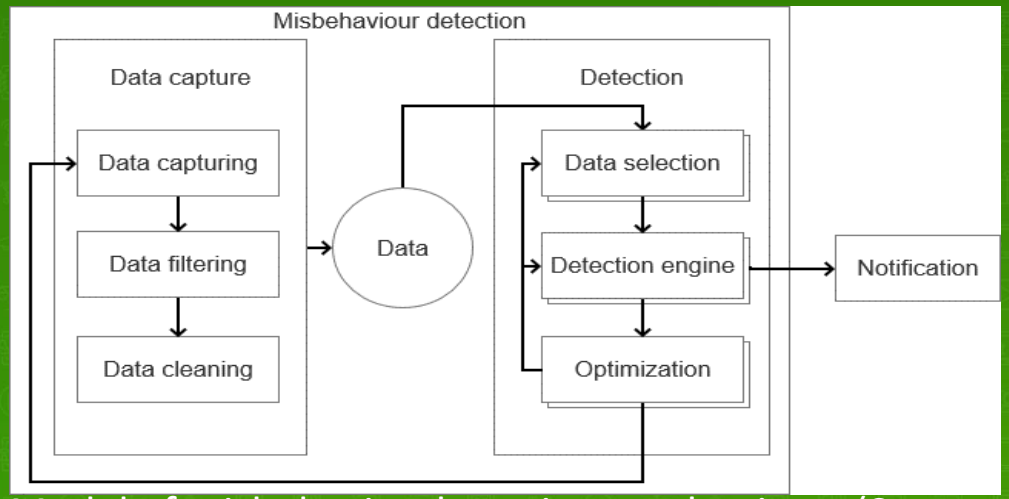
Guidelines for an intrusion detection system for in-vehicle networks

Recommendation ITU-T X.1375

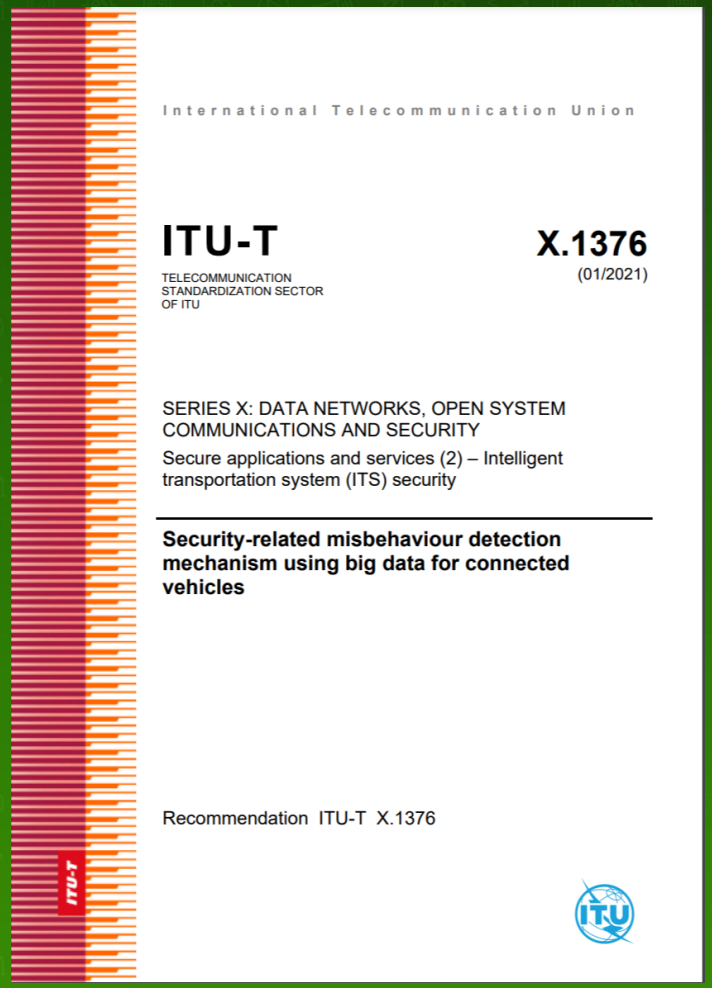
Ref)https://www.itu.int/rec/T-REC-X.1375/en

X.1376

- Title: Security-related misbehavior detection mechanism using big data for connected vehicles
- Status: Approved at 07 Jan. 2021
- Scope: This Recommendation describes a security-related misbehavior detection mechanism for connected vehicles. The mechanism includes the following steps.
  - a) Data capture. Definition of the types of data and information that can be captured from different sources, including automotive, infrastructure, original equipment manufacturers (OEMs) and suppliers, for misbehavior detection..
  - b) Detection. Analysis of the data captured to detect misbehavior.



<Model of misbehavior detection mechanism> (Source: X.1376)


International Telecommunication Union

ITU-T

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

X.1376 (01/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Intelligent transportation system (ITS) security

Security-related misbehaviour detection mechanism using big data for connected vehicles

Recommendation ITU-T X.1376

Ref)https://www.itu.int/rec/T-REC-X.1376/en

Future plan

- Next study period of SG17
  - SG17 will start next study period, 2021 ~ 2024.
    (WTSA 20 was postponed to 2021.)
  - SG17 proposed 15 Questions for next study period.
  - Q13 will continue to develop recommendations of security aspects of ITS
    - Proposed Question title: Intelligent transport system security
    - 9 on-going work items including X.1373 revision work
    - Scope of Q13/17 should be expanded to cover broader ITS security

- Next meeting
  - Next SG17 meeting
    - Q13/17 meetings are planned to hold in the next SG17 meeting in April 2020.

- Liaison Collaborations
  - SG16 and FG-VM – VMS security
  - CITS
  - UNECE – Event Data Recoding
  - Hoping to collaborate with TC22 and TC204