ISO 23255 Development

# Task 180703Z01

Develop a draft table of the various flow/link types

*Consider at minimum the following characteristics: latency, cardinality, directionality (bi vs. uni), confidentiality, integrity, pseudonymity, unlinkability, non-repudiation, throughput, Quality of Service*

*Provide examples*

## Approach

The basis for the analysis will be the HARTS reference. HARTS includes 1445 flow triples inclusive of FRAME and CVRIA. HARTS also includes an analysis of flow characteristics that can provide the basis for grouping. The database will be used to determine rough groupings, and as much consolidation of characteristics will be done as possible (where two are seemingly linked; i.e. not independent). Example flows, preferably non-obscure flows that will be meaningful to analysts, implementers and standards developers, will be called out.

## HARTS Characteristics

This analysis is focused on the HARTS information flow triple: source->information flow->destination. A flow triple represents the provision of information or data from a source ITS station (ITS-S) to a destination ITS-S. An information flow may include multiple dialogs, each of which may contain multiple messages. The directionality of an information flow describes the flow of information only; messages may transit in both directions to aid in the accomplishment of the information exchange.

The HARTS communications database includes the following characteristics that are set for each p-object flow triple.

|  |  |  |
| --- | --- | --- |
| Characteristic | Value Range | Definition |
| Availability | Low, Moderate, High | “Ensuring timely and reliable access to and use of information...” [FIPS 199; 44 U.S.C., Sec. 3542], Within HARTS, this attribute indicates the degree to which the information flow triple requires timely and reliable access to and use of information. Low, Moderate and High values represent the impact of failure to meet the availability requirement. |
| Cardinality | Unicast, Multicast, Broadcast | Source-to-destination flow architecture.   * Unicast: the source provides information for a single destination. * Multicast: the source provides information for a subset of potential receivers * Broadcast: the source provides information for all potential receivers   (a potential receiver is another ITS-S within range of the physical communications media being employed) |
| Confidentiality | Low, Moderate, High | The degree to which a subsystem needs to preserve “… authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...” [FIPS 199; 44 U.S.C., Sec. 3542]  Within HARTS, this attribute indicates the degree to which the information flow requires authorised restrictions on information access and disclosure. Low, Moderate and High values represent the impact of failure to meet the Confidentiality requirement. |
| Integrity | Low, Moderate, High | “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity...” [44 U.S.C., Sec. 3542]. Within HARTS, this attribute indicates the degree to which the information flow requires guarding against improper information modification or destruction. Low, Moderate and High values represent the impact of failure to meet the Integrity requirement. |
| Latency | Ultralow, Low, Medium, | A property that characterizes the time difference between the time at which the source ITS-S becomes aware of the data in an information triple and the time at which the destination ITS-S receives it. Within HARTS, latency includes the time that data may be stored within the source of the information triple as well as any network delays.   * Ultralow: < 100ms * Low < 2s * Medium < 10s * High: other |
| Non-repudiation | Yes, No | A property that none of the entities involved in a communication can deny in all or in part its participation in the communication. [ISO 24534-4] |
| Pseudonymity | Yes, Reversible, No | Ability of a user to use a resource or service without disclosing its user identity while still being accountable for that use. [ISO 24534-4] |
| Quality-of-service | High, Medium, Low | A property describing the “totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service.” From the HARTS perspective, this property is used to indicate the relative importance of satisfaction of the information flow. |
| Throughput | Low, Medium, High | A property that characterizes the relative amount of data exchanged through the information flow. This typically represents the worst-case, highest amount of information exchanged over a nominal period and is not intended to represent continuous transmission. |
| Unlinkability | Yes, No | The property that user’s transactions are not linked with other transactions of the same user. ISO/IEC 19286:2018] |

Confidence in the accuracy of these characteristic settings is moderate. Due to the scale and scope of the architecture, many of these assignments have not undergone review. Some validation exercises have been performed looking for questionable assignments, and some small numbers of potential errors have been found. These exercises suggest the error rate is <5%. Given the scope of the data distribution analysis, the projected error rate should not have a significant impact.

### Notes on Directionality and Flow Link

Most flows in HARTS are uni-directional information provision, but allow for bidirectionality for the purposes of flow control, authentication and non-repudiation. Flows with cardinality set to ‘broadcast’ are the exception to this rule; these flows are all one-way transmissions. As a result, directionality is not a readily available independent value, so cardinality will serve as a proxy to include notion of directionality.

Link is the term HARTS uses to describe the interconnect between class of ITS-S (Center, Vehicle, Personal or Field). Links include entries for Center-to-Center, Center-to-Field and Field-to-Field as distinct link types. For the purposes of the DDS analysis however, we are most concerned with whether or not the link must accommodate a mobile user or not; consequently, when differentiating between link types we only identify whether one (or both) parties in the information exchange require a wireless medium, and if so whether the exchange is expected to be short range, indefinite (wide area) or large area broadcast with mobile receiver.

Also, HARTS includes 172 triples that fall into one of the following categories that are out-of-scope for data distribution:

* Vehicle-on board: between a vehicle ITS-S and other on-board systems
* Human interface
* Network time protocol
* Contact or proximity (such as a traveler card)
* Data distribution system as source or destination, which if included would corrupt this analysis

## Analysis

Initial analysis using all of the fields noted above (Confidentiality, Integrity, Availability, Latency, Throughput, Cardinality, Psuedonymity, Unlinkability, non-repudiation, Quality of Service, Wireless need) lead to 220 flow groups of the remaining 1273 flow triples. However, many of these groups include a small number of triples. If the results are limited to those groups with at least 5 triples, the number of groups drops to 59, inclusive of 1008 triples. If the results are limited to those groups with at least 10 triples, the number of groups drops to 31, inclusive of 831 triples.

Further, since the flows identifed as both Broadcast and Short Range Wireless are typically well covered by existing standards development efforts, we might remove those triples from the analysis. Of the “ten triples or more (10plus)” subgroup, Broadcast/SRW triples make up four groups totalling 88 triples.

Lastly, it should be noted that when the Broadcast/SRW triples are removed from consideration, all triples in the 10plus group share three common characteristics: unicast cardinality, unlinkability is not required, and non-repudiation is required. Consequently the summary table below will not list these characteristics to save on space.

The following table provides example triples for each of the remaining 27 10plus triple groups. Abbreviations:

* C = Confidentiality; I= Integrity, A = Availability
  + L = Low, M= Moderate, H = High
* Lat = Latency
  + U = Ultralow, L = Low, M = Medium
* Thr = Throughput
  + L = Low,
  + M = Medium: large data sets sporadically updated such as road network conditions or large scale strategic data
  + H = High: typical of full-motion video
* Ps = Pseudonymity
  + N = Not required
  + R = Reversible psuedonymity required
* QoS = quality of service
  + L = Low, M = Medium, H = High
* Wireless = Wireless or Fixed point-to-point communications
  + Fixed = fixed end points (field to field, field to center, center to center)
  + WAW = wide area wireless required
  + SRW = short range (direct connect) wireless required
* C2C = Center-Center
* C2F, F2C = Center-to-Field, Field-to-Center
* C2V = Center-to-Vehicle
* C2P = Center-to-Personal
* C2X = Center-to-Any
* F2F = Field-to-Field
* EMCD = Emergency Management Center
* CVRSE = Connected Vehicle Roadside Equipment, including both the DSRC radio device and local processing capability
* ITSRE = ITS Roadway Equipment, such as traffic signal controller, detector or dynamic message sign controller
* MCMC = Maintenance and Construction Management Center
* PAC = Payment Administration Center
* TMC = Traffic Management Center

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | # | C | I | A | Lat | Thr | Ps | QoS | Wireless | Example Flows and/or Subcategories |
| 1 | 161 | M | M | M | L | L | N | M | Fixed | C2C, F2C flows containing some PII, often related to commercial vehicle applications  CVRSE->[application] status ->TMC that may contain or imply PII  ITSRE->[equipment/app] status ->TMC/MCMC that may contain or imply PII  F2F flows containing tracking data (e.g. vehicle entries and exits) |
| 2 | 80 | M | M | L | L | L | N | M | Fixed | C2C flows containing PII with low time priority, but some importance to eventual exchange (transaction reports, payment setup and reports, often involving PAC, CVAC)  CVRSE->[application] status ->TMC for apps with more field autonomy  TMC->[equipment/app] control ->ITSRE for low priority devices like detectors, ESS  F2F flows that may contain PII but are not time-critical |
| 3 | 66 | L | M | M | L | L | N | M | Fixed | C2C flows regarding service coordination between modes, traveler information  CVRSE->[application] status ->TMC without PII  ITSRE->[equipment/app] status ->TMC without PII  F2F flows without PII that provide time critical warning or coordination |
| 4 | 50 | M | M | M | L | L | N | M | WAW | Payment-related from PID  Transit (vehicle) operating data, transit passenger functions  Commercial vehicle declarations |
| 5 | 43 | H | H | M | L | L | N | M | Fixed | C2C commercial vehicle records, status and logs exchange  Security credentials distribution |
| 6 | 29 | L | M | L | L | L | N | M | Fixed | C2C modal and route restriction information sharing  C2F non-time critical data |
| 7 | 24 | M | H | M | L | L | N | M | Fixed | C2F device configuration and control |
| 8 | 22 | H | H | M | L | L | N | M | WAW | Commercial vehicle log data  Personal payment-related information  Security credentials for mobile users |
| 9 | 22 | M | M | M | L | L | N | H | Fixed | Multimodal safety data  Freight clearance, personal registration/DMV data |
| 10 | 21 | L | M | M | M | M | N | M | Fixed | C2C broad area traveler information such as road network conditions, incident data |
| 11 | 20 | H | H | M | L | L | N | H | Fixed | Security credentials enrollment for fixed point users  Commercial vehicle processing data |
| 12 | 20 | L | H | M | L | L | N | M | Fixed | C2F border, commercial vehicle, roadside device data/status |
| 13 | 19 | H | H | H | L | M | N | H | Fixed | EMC-related C2C coordination, routing and response |
| 14 | 17 | M | M | L | M | L | N | M | Fixed | C2F TMC ->[equipment/app] control -> CVRSE |
| 15 | 15 | M | M | M | L | M | N | M | Fixed | C2C freight data sharing, maintenance information sharing |
| 16 | 15 | M | M | M | L | L | N | M | SRW | Commercial vehicle parking and loading, maintenance vehicle local device control |
| 17 | 14 | H | M | L | L | L | N | M | Fixed | C2C License and violation information |
| 18 | 13 | M | M | L | L | L | N | M | WAW | C2P trip planning, C2V/P interactive traveler information |
| 19 | 13 | L | H | M | L | M | N | H | Fixed | C2C evacuation coordination, infrastructure restrictions |
| 20 | 13 | L | M | M | L | L | N | M | WAW | C2V intersection status, specialized vehicle information exchange |
| 21 | 12 | H | H | H | L | L | N | H | Fixed | C2C security credentials coordination, HAZMAT route details |
| 22 | 12 | M | M | L | L | L | N | L | Fixed | C2C emissions zone information |
| 23 | 11 | H | M | M | L | L | N | M | Fixed | C2C freight movement credentials and status, C2F transit stop request |
| 24 | 11 | L | H | M | U | L | N | H | Fixed | C2X object registration and discovery, F2F commercial vehicle check data |
| 25 | 10 | L | H | M | L | M | N | M | Fixed | C2C, C2F roadway and parking facility map exchanges |
| 26 | 10 | M | M | M | L | L | R | M | WAW | C2V traveler request/response, C2V/P privacy protection |

Clearly, there is no one group that we can point to and say what the requirements that should apply to a DDS solution. While some of the groups defined above may not be good candidates for a DDS solution (e.g., payment information that is typically transactional), clearly many of these exchanges are good candidates for publish-subscribe. We will need to be able to quantize DDS solutions according to their ability to meet various aspects of these characteristics. In order to do this, we likely need a little more insight into what some of these requirements take in order to be satisfied.

### Strawman Technical Requirements

For each characteristic, what is necessary on the part of the DDS to meet this requirement?

#### Confidentiality

Low – none

Moderate – encryption facilities meet the requirements of FIPS 140-2 level 3. For example, keys stored in a hardware security module, all crypto operations performed in the HSM. Requirements related to access control, auditing, configuration management, authentication, personal privacy, system and information integrity. May include the ability to maintain confidentiality to the application (i.e., DDS middleware cannot decode the information, only the subscribing application can)

High- as Moderate, and additionally intrusion detection and mitigation functions can inspect DDS messages.

#### Integrity

Moderate – integrity assurance facilities meet the requirements of FIPS 140-2 level 3. For example, keys stored in a hardware security module, all crypto operations performed in the HSM. Requirements related to access control, auditing, configuration management, authentication, personal privacy, system and information integrity. May require the ability for subscribing application to be able to verify message integrity and perform source authentication.

High- as Moderate, and additionally intrusion detection and mitigation functions can inspect DDS messages.

#### Availability

Low – none

Moderate – communications media increased robustness. Requirements related to access control, auditing, configuration management, authentication, personal privacy, system and information integrity.

High- as Moderate, and multiple communications mechanisms available.

#### Latency

Ultralow – DDS provides less than 100ms delay in between the production of data by the initiating application and reception by every consuming application

Low – DDS provides less than 2s delay in between the production of data by the initiating application and reception by every consuming application

Medium – DDS provides less than 10s delay in between the production of data by the initiating application and reception by every consuming application

#### Throughput

Low – DDS can sustain 10 kb/s satisfaction of aggregate data subscriptions from a typical ITS-SU source

Medium – DDS can sustain 500 kb/s satisfaction of aggregate data subscriptions from a typical ITS-SU source

High – DDS can sustain 10 Mb/s satisfaction of aggregate data subscriptions from a typical ITS-SU source

#### Pseudonymity

Yes/Rev: Does the DDS permit the usage of pseudonyms that are *not easily* associated with particular devices?

#### Quality of Service

Low – no requirements

Medium – does the DDS solution provide reasonable assurance that subscriptions up to its expected throughput will be satisfied?

High – does the DDS solution effectively guarantee that it will satisfy subscriptions up to its expected throughput will be satisfied?

## Summary

So what does this mean? There are a significant number of information exchanges with most combinations of flow characteristics. This suggests that first and foremost, *any data distribution technology should be flexible in its ability to satisfy these requirements.* There are a few individual requirements that, since they appear relatively infrequently, would not seem to be as critical:

* Ultralow latency
* Reversible pseudonymity

Secondly, any flow that is by nature a transactional data exchange is likely better suited to a client-server transaction-based information exchange rather than any sort of publish-subscribe. Most of those types of information flows are low bandwidth, tend toward higher confidentiality and integrity requirements. Removing those from the over list of information flows does not demonstrably change the analysis however. Any chosen DDS technology should be able to support all variations of the strawman technical requirements noted above.

In addition, we should ask a few other questions about the technology.

* How mature is it?
* On what platforms is it available?
* How many suppliers on each platform?
* Does it require a separate registration/discovery service for data and providers? If yes, how does the architecture of that service impact deployment? If yes, does the registration service allow subscription by meta-data including time start/stop, geographic location, type of source?
* Does it require any particular lower layer protocols?
* Does it support IP-multicast?
* Does it work with existing ITS security mechanisms, including requirements for crypto-operations to be performed in an HSM?
* Are there any independent performance-based analyses available that demonstrate the performance, scalability, installation and maintenance challenges related to using this technology?
* What impacts does this technology have on other services operating on the device on which it is installed?

This last question may be the most impactful. What kinds of impacts might there be? Technology updates, installation procedures, licensing requirements and resource consumption are all possible. Strongly related to the latter, we should note that there are two basic architectural mechanisms for publish-subscribe architectures, and these use resources in different ways:

1. Source-as-publisher: the source device is both data source and data publisher. This implies requirements on the device: it must manage subscriptions and it must provide the physical communications mechanism for satisfying subscriptions. This suggests a peer-to-peer relationship between all participants; however, since a subscriber may be a publisher, a client-server model may be constructed if data sources limit subscriptions.



1. Source-as-provider: the source device is data source only. This requires that another device serve as publisher, and that the source device have a physical communications mechanism that can reach the publisher.



It is likely that both of these models will be advantageous for different types of information flow triples. Ideally both approaches are viable and the decision on which approach to use will depend on the type of data provided and its intended use. While a given standard may support both peer-to-peer and client-server architectures as described under (1) above, it is likely that any compliant implementation of (1) is significantly more complex than an implementation of (2), suggesting that if nothing else, approach (2) suggests a smaller footprint on data sources.

Might we define criteria that help us determine this?

* Impact of the publication on resources can be considered constrained by the availability of bandwidth and other resources necessary to satisfy publication
* What are the characteristics of data that suggest it would be a better candidate for one approach versus the other?
* What are the anticipated characteristics of data usage that suggest