# Standardization of ITS protocol messages using ASN.1

Lan Lin, Hitachi Europe Ltd., Sophia Antipolis, France

Andras Kovacs, BroadBit, Komarno, Slovakia

Sebastian Müller, ETSI, Sophia Antipolis, France

# Abstract

ETSI TC ITS Working Group 1 -- Application Requirements and Services -- currently funds the development of Conformance Test Suites using TTCN-3 and ASN.1. Led by ETSI’s Centre for Testing and Interoperability (CTI), Special Task Forces (STFs) have already been initiated to implement and validate the test suites focusing on testing Co-operative Awareness Messages (CAM) [1] and Decentralized Environmental Notification Basic Service Message (DENM) [2] standards. In a side task one STF supported ETSI TC ITS to optimize the initial ASN.1 modules. In this paper we report our implementation approach and experiences made in the STFs on using ASN.1. Special attention has been given to reuse of knowledge and existing best practices.

# Introduction

As stated in [3] the production of large conformance test suites is a software development process. Different expertise is required such as definition of tests, knowledge of base specifications, knowledge of the System Under Test (SUT) specification) and techniques (testing methodology, test description languages, protocol design). Several guides for the various test activities have been published such as the ITS testing framework [4] or the handbook of validation methods [5]. These guides briefly cover the aspects of using ASN.1. This paper addresses ITS specification requirements, ASN.1 design decisions and the ASN.1 validation activities. Finally, a project review from the management viewpoint is given.

# ITS specification requirements

ETSI TC ITS develops and maintains freely available standards to support the development and implementation of ITS Service provision for transport networks, vehicles and transport users in order to achieve global interoperability between all ITS systems. The interoperability of products can only be guaranteed if the specified data formats and encodings are clear and unambiguous. As CAM/DENM protocols, which are application layer protocols in the OSI protocol stack model, run over-the-air, it is therefore important to constrain the CAM and DENM message size and its encoding in order to allow for an optimal usage of the bandwidth.

While network and transport layer protocols are generally encoded using tabular bit-wise descriptions, such an approach is not considered to be a good practice for application layer protocols. The main issues are the increasingly complex structure of application protocols (often involving a whole hierarchy of containers), the frequent presence of optional fields, and the requirement for extensibility and version management. The description and encoding/decoding of such application protocols through tabular bit-wise specifications would quickly become overly complicated and error-prone.

Therefore the best practise in application layer specification involves the use of XML or ASN.1 syntax. Opinions diverge on the preference of XML vs. ASN.1. XML is usually preferred by computer scientists - whose university curriculum covers this technology - pointing out that many computer languages have built-in capabilities for handling XML encoding. The inherently sparse XML encoding can be transparently compressed by complementing technologies, such as the EXI encoding specification. ASN.1 is usually preferred by telecom engineers - whose university curriculum covers this technology - pointing out that ASN.1 is best suited for handling complex protocols with many optional, conditional, and inter-dependent fields. However for many application protocols both are equally suitable. ASN.1 gains an advantage only for complex protocols; as the number of inter-dependencies and optional elements increases, the use of ASN.1 syntax becomes gradually more favourable.

# ASN.1 design decisions

In a first step ETSI TC ITS Working Group 1 defined some basic requirements for the design of the ASN.1 modules:

**Encoding/Decoding**

One of the top requirements was to have an optimized codec. Therefore the decision was taken to support only unaligned PER codec in order to get a bit-level optimization of the data transferred. See also the section on “ASN.1 Design Choice Evaluation”.

**Default values**

Similar to the point above it was decided to use default values where applicable.

**Versioning and extensibility**

While ITS systems are planned to provide an over-the-air application updating capability the simultaneous update of applications in each ITS station cannot be guaranteed or assumed. Since ITS applications are safety related, it is therefore required to ensure interoperability between differing application versions. Two different types of updates should be possible:

* Minor updates which extend the existing ASN.1 structure could occur in the short- to mid-term and should be backwards compatible.
* Major updates are significant changes to the ASN.1 structure which cannot be backwards compatible (e.g. similar to the change from IPv4 to IPv6).

The main focus was on how to handle minor updates, where two questions needed to be answered:

1. which data structures to make extensible to allow for a viable long term backwards compatibility and
2. which technique to choose in order to avoid custom programming of processing logic.

For DENM question a) was answered by introducing a data structure of containers whereby the last container is extensible and thus allowing extension of the data structure by adding a new container. For CAM more than only the last container was made extensible because it is thought that CAM will need to change more than DENM. For both, CAM and DENM, data elements which are application-related were made extensible as well (e.g., data elements describing a reference position do not need to be extensible as longitude can only span from -1800 to 1800).

In the case of question b) different alternative extension mechanisms exist, e.g., placeholder techniques where one empty SEQUENCE (and whose values are specified in the next release) is defined at the very end of the ASN.1 definitions, or where one empty SEQUENCE is defined inside a fixed-length-structure so that a decoder can skip the extensions. Another technique is to use the ‘…’ extensibility notation of ASN.1. Fields added by future versions are within extension brackets. An older version of the protocol knows how to skip extensions it does not recognize and a newer version knows how to handle the absence of an extension. The group decided to use the standard ASN.1 practice of extension markers as this is the only technique which avoids any custom programming. Since there is a 1 bit additional encoding length cost for each extensible structure, it has been decided not to use the ‘EXTENSIBILITY IMPLIED’ feature (which would make every structure extensible), but to check which containers could be potentially extended in future protocol versions and to make only those structures extensible.

**Optional data elements**

During validation of the test suite (see below) some companies requested the ASN.1 structure be optimized so as to allow for easier codec implementation by moving all optional data elements to the end of structures.

**Range restrictions**

For INTEGER type fields, which describe parameters such as the vehicle length or geographic position, it is necessary to define explicitly a minimum-maximum range. The reason is that PER encoding automatically calculates from such range restrictions the number of bits which are actually needed to represent each field. Also, we reserved the largest value of the range to indicate an unavailable/unknown value for that field; this is a more bandwidth-efficient way than reserving a separate flag (or optional bit) for each field in order to indicate an unavailable/unknown value.

**Named integer**

A further consideration for INTEGER type fields is that the received information is interoperable only when both sender and receiver agree on the meaning of the unit value for the corresponding INTEGER type. This is not as obvious as it sounds: for example, some length fields use a unit of 10 cm (e.g., for describing the length of the vehicle), while other length fields may use some different unit. In general the unit is individually selected for each field by considering its granularity requirement. In order to avoid unit misinterpretations we used a named integer notation describing the unit value for each INTEGER type. This way the implementer of the standard has the unit descriptions appearing explicitly in his source code, and thereby the chance of misinterpretations is mitigated.

**ASN.1 Design Choice Evaluation**

Protocol design decisions must be based on the analysis of the operating environment and use cases for the given application.

An important decision to make is the choice of ASN.1 encoding. Since ITS applications are transmitted over a wireless interface, the use of PER encoding, which is an efficient bit-oriented encoding type, is required. It has two variants: aligned and unaligned. Unaligned PER is more bandwidth-efficient, while aligned PER requires slightly more processing power. Recent ASN.1 tools provide very similar processing speeds for aligned/unaligned variants; still it has been of interest to quantify this speed, because the embedded hardware which will implement ITS protocols should also be optimized in terms of required processing power. Since the planned CAM/DENM applications are broadcast based, every generated message will be decoded by hundreds or even thousands of recipients. Therefore only the decoding speed is of interest in terms of quantifying the required processing power. The figure below shows the results of a performance test, where aligned/unaligned encoding of the same message type was compared in terms of required processing time for decoding and required bandwidth. This result indicates that switching from aligned to unaligned PER encoding saves 20% bandwidth, while requiring only 7% more decoding power. Therefore the use of unaligned PER encoding for ITS applications is justified. The figure below is taken from [6], where more detailed information on the ASN.1 Design Choice Evaluation is provided.



# Validation

**Implicit Validation**

The ETSI TC ITS test programme has produced conformance test specifications for the CAM and DENM standards and their ASN.1 definitions. The process of producing test specifications requires close inspection of the standards. This can result in a level of validation similar to that offered by a rigorous peer review. This is defined in [5] clause 6.3 as ‘implicit validation’.

Typical issues found in the ASN.1 modules during implicit validation were syntactical errors, and inconsistencies in the application of design rules. Also, duplication of data types or the definition of similar data types was detected, and through merging the overall structure these duplications could be optimized.

**Test Suite Validation**

A prototype test system (so called ITS Conformance Validation Framework) was designed and built. It allows execution of the test suites against real devices, and thus enables test suite validation (see [5] clause 6.2.3). The test suites were validated using two commercially available implementations. In addition, the prototype test system was provided to a broad range of companies and several R&D projects, such as DRIVE C2X, eCoMove, SCORE@F, Testfeld Telematik, thus further validating the prototype test system and allowing industry to assess the compliance of their implementations.

No issues were found in the ASN.1 modules. Some companies requested optimization of the ASN.1 structure so as to allow for easier codec implementation. Typical requests were to move OPTIONAL data elements to the end of a SEQUENCE, or to limit integers with reasonable range restrictions.

**Product-based Validation**

ETSI TC ITS and ERTICO co-organise Cooperative Mobility Services Plugtests™, at which prototype or production implementations of the CAM and DENM standards are interconnected and tested for interoperability. These events provide validation of both the base standards and the implementations of the standards (see [5] clause 6.2.4).

No issues were found in the ASN.1 modules. Rather, issues with the different ASN.1 tools were detected such as missing support for the ASN.1 extensions feature, support for extended integer ranges and decoder errors for charstrings in PER unaligned mode.

It was concluded that choosing a quality ASN.1 compiler is essential to achieve interoperability.

# Effort

The work was organized in a way whereby ETSI TC ITS provided in the form of a spreadsheet a high level description of the data elements. It contained information such as a short description of the purpose of the data elements, their values and possibly their types. As part of the consensus based decision making process, these spreadsheets went through a couple of iterative processes to allow discussion of the received feedback and to provide a stable version (during this process International Harmonization was achieved by involving SAE in the discussions). Based on these stable versions, the ASN.1 development started, and fed back recommendations to the group. Altogether this process was active for 1 year, with the result of a final spreadsheet and final ASN.1 modules ready for approval. In summary, the total effort to produce the ASN.1 modules was 20 person days (not taking into account the time spent in discussions and meetings with ETSI TC ITS).

# References

[1] ETSI EN 302 637-2: " Intelligent Transport Systems (ITS); CAM Basic Service".

[2] ETSI EN 302 637-3: " Intelligent Transport Systems (ITS); DEN Basic Service".

[3] M. Gläser, S. Müller, A. Rennoch, P. Schmitting: Standardized TTCN-3 specifications for SIP-ISUP/ISDN interworking testing. STTT, Springer, April 2008

[4] [ETSI EG 202 798](http://www.etsi.org/deliver/etsi_eg/202700_202799/202798/): "Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperability testing".

[5] [ETSI EG 201 015](http://www.etsi.org/deliver/etsi_eg/201000_201099/201015/): "Methods for Testing and Specification (MTS); Standards engineering process; A handbook of validation methods".

[6] ETSI STF 424: "ASN.1 Design Choice Evaluation report ASN.1 evaluation report".