ASN.1
and the Connected Vehicle

Alessandro Triglia
sandro@oss.com
OSS Nokalva, Inc.

2nd International Summit on the State of the Connected Vehicle
Troy, MI 2010-09-30

ASN.1

- ASN.1 = Abstract Syntax Notation One
- International standards
  - jointly published by ISO/IEC and ITU-T
- Originally developed in the 1980's...
  - ...but still alive and well, and still evolving
- Used in several industries
  - mainly, but not only, telecommunications

Uses of ASN.1

- Some traditional applications of ASN.1:
  - Signaling standards for the public telephone network (SS7)
  - Network management standards (SNMP, CMIP)
  - Directory standards (X.500 family, LDAP)
  - Public Key Infrastructure standards (X.509, etc.)
  - PBX control (CSTA)
  - IP-based Videoconferencing (H.323 family)
- Some more recent applications:
  - Aeronautical Telecommunication Network
  - Biometrics (BIP, CBEFF, ACBio)
  - Transportation (SAE J2735)
  - Cellular telephony (GSM, GPRS/EDGE, UMTS, LTE)

The SAE J2735 standard

- SAE J2735 – “Dedicated Short Range Communications (DSRC) Message Set Dictionary”
- 2nd Edition, November 2009
- Specifies a set of messages to be used with 5.9 GHz DSRC communications systems
- Uses ASN.1 to specify its messages and their data elements
- Example (Basic Safety Message):

```
BasicSafetyMessage ::= SEQUENCE {
   msgID              DSRCmsgID,
   blob1              BSMblob,
   safetyExt          VehicleSafetyExtensions OPTIONAL,
   status             VehicleStatus OPTIONAL,
   ...
}
```

ASN.1 standards

- Three sets of standards:
  - ASN.1 notation (X.680)
    - a formal language for the definition of messages
  - Encoding rules
    - BER – *Basic Encoding Rules* (X.690)
    - DER – *Distinguished Encoding Rules* (X.690)
    - PER – *Packed Encoding Rules* (X.691)
    - XER – *XML Encoding Rules* (X.693), *…*
  - Other ASN.1 standards
    - Mapping from XML Schema to ASN.1 (X.694)
    - Fast Infoset (X.891)
    - Fast Web Services (X.892)

ASN.1 modules and ASN.1 schemas

- ASN.1 modules are written in ASN.1 notation
  - Easy to recognize from the pervasive presence of the symbol `::=` (colon-colon-equals) and open and closed braces `{ }`
- Each ASN.1 module contains a set of definitions – mostly data type definitions
- An "ASN.1 schema" (or "ASN.1 specification") is a coherent set of ASN.1 modules
- Each user-defined data type within an ASN.1 module is built from other user-defined data types and/or built-in ASN.1 data types
- A message type is a user-defined data type
- ASN.1 modules are typically published as part of standards (such as SAE J2735)

Tool support

- ASN.1 Tools used in the VII Proof of Concept (2007)
  - http://www.oss.com/news/VII_poc_pr.pdf
- ASN.1 Tools used in the Connected Vehicle Proving Center (2008)
  - http://www.oss.com/news/CVPC%20OSS%20ASN1%20Tools%20Press%20Release.pdf
- ASN.1 encoder/decoders available on over 250 different platforms, most of which are embedded platforms

From "IntelliDrive^{SM} Principles" * Active safety applications

- "One goal is to enable *active safety applications*"
- "... active safety research and deployment..."
- "It will focus on *5.9GHz Dedicated Short Range Communications (DSRC)* to enable necessary communications characteristics, including low latency, fast connection speeds, security and privacy"
- "It includes both *vehicle-to-vehicle* and *vehicle-to-infrastructure* systems"

(*) http://www.intellidriveusa.org/documents/PrinciplesFlier.pdf

How it works

1. The sending application creates a message conforming to a certain message type within the ASN.1 schema
   - the message is represented in a data structure that is appropriate to the programming language in use (e.g., a Java class or a C struct)
2. The sending application encodes the message using the designated set of ASN.1 encoding rules
   - BER – DER – PER – XER *...*
3. The encoded message is transferred from the sending endpoint to the receiving endpoint
4. The receiving application decodes the encoded message using the designated set of ASN.1 encoding rules
   - the message is now represented in a data structure appropriate to the programming language in use
5. The receiving application processes the message

Thank you!

Alessandro Triglia
sandro@oss.com
OSS Nokalva, Inc.

SAE/CVTA
Connected Vehicle Summit
Troy, MI 2010-09-30