IEC 62351-7 IS
Status Report

Gian Luigi Pugni
IEC TC57/WG15

Madrid 28 April 2015

IEC 62351

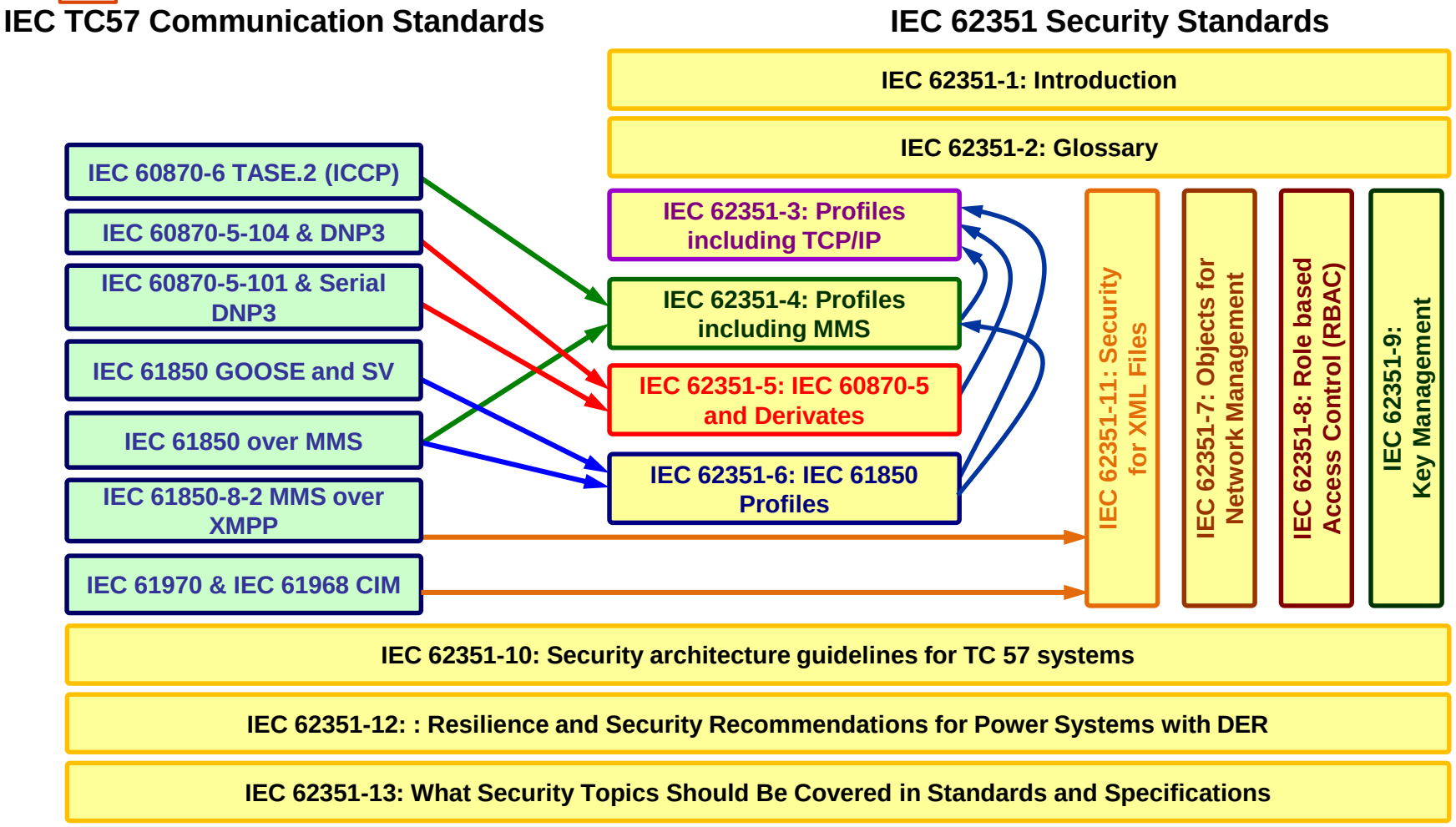
POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE

DATA AND COMMUNICATIONS SECURITY

Mission and Scope of IEC TC57/WG15 on Cybersecurity

- **Undertake the development of standards for security of the communication protocols defined by the IEC TC 57**
  - **Specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series.**
  - **Review and advise on cyber security of TC57 standards**
- **Undertake the development of standards and/or technical reports on end-to-end security issues.**

Mission and Scope of IEC TC57/WG15 on Cybersecurity



“Part 7: Network and System Management (NSM) data object models”

IEC 62351-7
NSM and Security

The **Network and System Management is handled by WG15** because the **availability of systems and data** is one of the most delicate aspect for **resiliency of critical infrastructure**.

Basically we need to:

- try to **avoid attacks** or at **least delay** them long enough to **decide what action to take.**
- **Detect attempts to attack** in order to **activate the security measures** in advance because in the case of a fully deployed attack you'll have less success chance in countering that.
- **Rate the importance of attacks**, to determine the nature and severity of the attack potential effective damage.
- **Communication and notification**, in order to make the systems and network managers to **be aware of the attack in a timely manner**.

IEC 62351-7
Edition 2 - Concepts

The goal is to define **Network and System Management (NSM) data object models that are specific to power system operations**. These NSM data objects will be used to monitor the health of networks and systems, to detect possible security intrusions, and to manage the performance and reliability of the information infrastructure.

These "data object" shall be "Abstract" because it must be possible to transport them with different monitoring protocols.

A first **translation of the Abstract Object into** a real monitoring protocol is provided with IEC 62351-7 edition2. This protocol is **SNMP (Simple Network Management Protocol)** and the Abstract object are translated into **MIB (Management Information Base) objects**.

IEC 62351-7
Why SNMP?

SNMP is a widely used IT standard monitoring protocol.

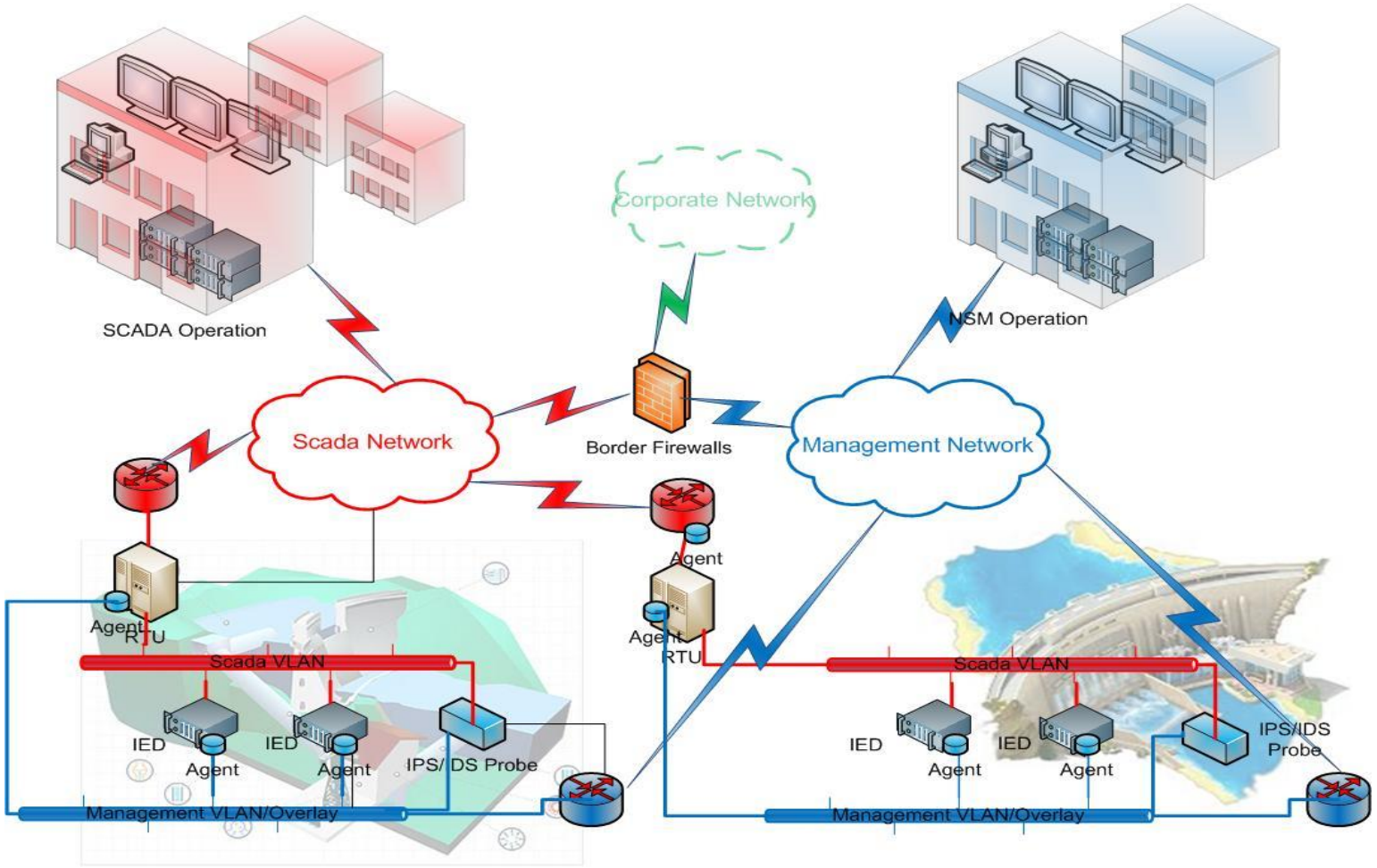
Simpler correlation of information Objects and Alert is possible with other monitoring information (e.g. from **routers, switches, IDS/IPS, Firewalls**).

IEDs Management can become part of General System and Network Management

Monitoring of IEDs and RTU can be designed as **independent** form the usual SCADA operation allowing the **adoption of a parallel and independent monitoring infrastructure** (possibly integrated with the one already in use for Network and Security devices monitoring)

SNMP MIBs are already available to cover Network and Transport layer monitoring of IEDs, we do not need to reinvent the wheel.

IEC 62351-7
NSM overall view



IEC 62351-7
Current edition constrains and improvements

TC57/WG15 during meeting in Vittorio Veneto on May 2013, decided to review IEC 62351-7, in order to apply this standard to a more real environment

The goal was defined as follows:

- Collect **additional use cases** related to NSM
- Define a mandatory and **standard Abstract Object set starting from Use Cases results**
- **Map toward SNMP MIBs** the set of Abstract Objects

The **SNMP MIBs mapping allow a seamless integration** of the management of grid systems inside the Enterprise NSM environment, allowing a real world Proof of Concept and deployment of IEC 62351-7.

On december 2013 EPRI published the technical report 3002000373 “Network System Management: End-System-Related International Electrotechnical Commission (IEC) 62351-7 Object Definitions.” with many suggestions for the improvement of part 7.

Revision Request document circulated at the **end of 2013**, comments received at the beginning of 2014.

At the beginning of 2014 the activity of the task for new edition of IEC 62351-7 has been formally started.

62351-7 UML model adoption

Brief history

Around April 2014 WG15 -7 task decided the adoption of **UML model to address the description of IEC 62351-7 Abstract Objects.**

A first Enterprise Architect **UML Model of 62351-7 Abstract Object was drafted**, also according to some EPRI report suggestion. Actually UML allow a very flexible expression form for the part 7 objects.

This approach (and EA tool) has been already adopted for the production of some IEC TC57 standards. **Starting from the UML Model the standard document could be in fact produced using an automated way.** JCleanCim tool is already available to simplify this task.

Agent/Subagent Mapping will also become almost natural using UML modeling

The advantages of using UML and a modeling tool are significant, even if we discovered the the road to a manageable UML model was not so direct. The model allow a flexible update of the Abstract Objects and a coherent alignment of the standard as well. Basically what **we developed was a methodology for Abstract Objects definition and maintenance**.

The idea was to **automatically map UML model toward SNMP MIBs** while producing the self generated part of the document. This task required the development of a **semantic translation process and a tool that could automate this task.**

IEC 62351-7
From UML model to Standard and MIB

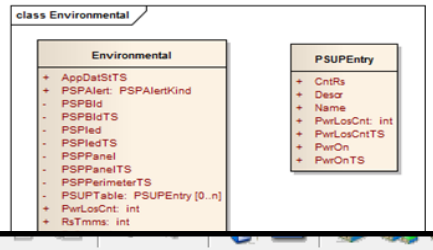
IEC 62351-7 IS

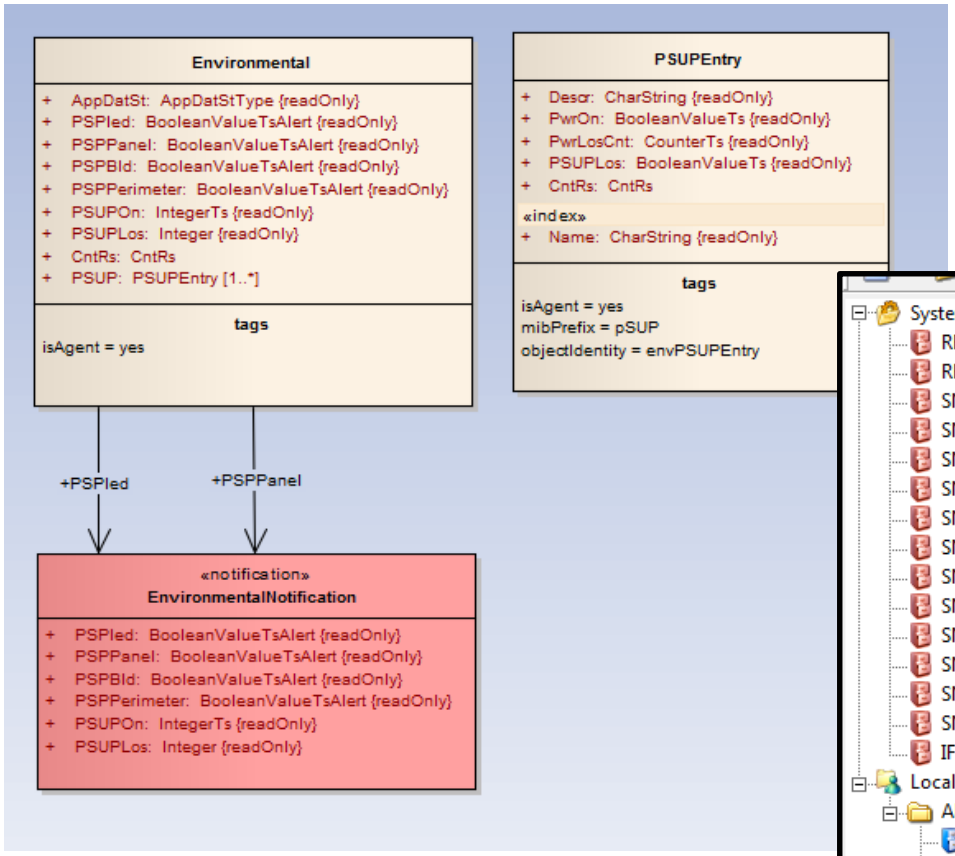
6 Abstract Objects

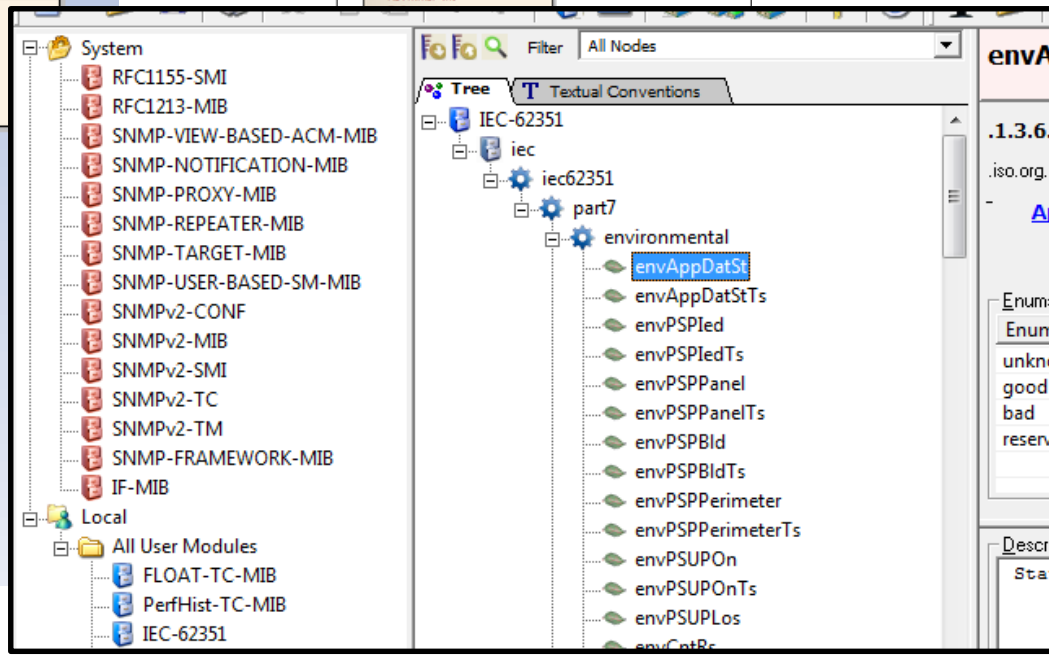
6.1 Package Environmental

6.1.1 General

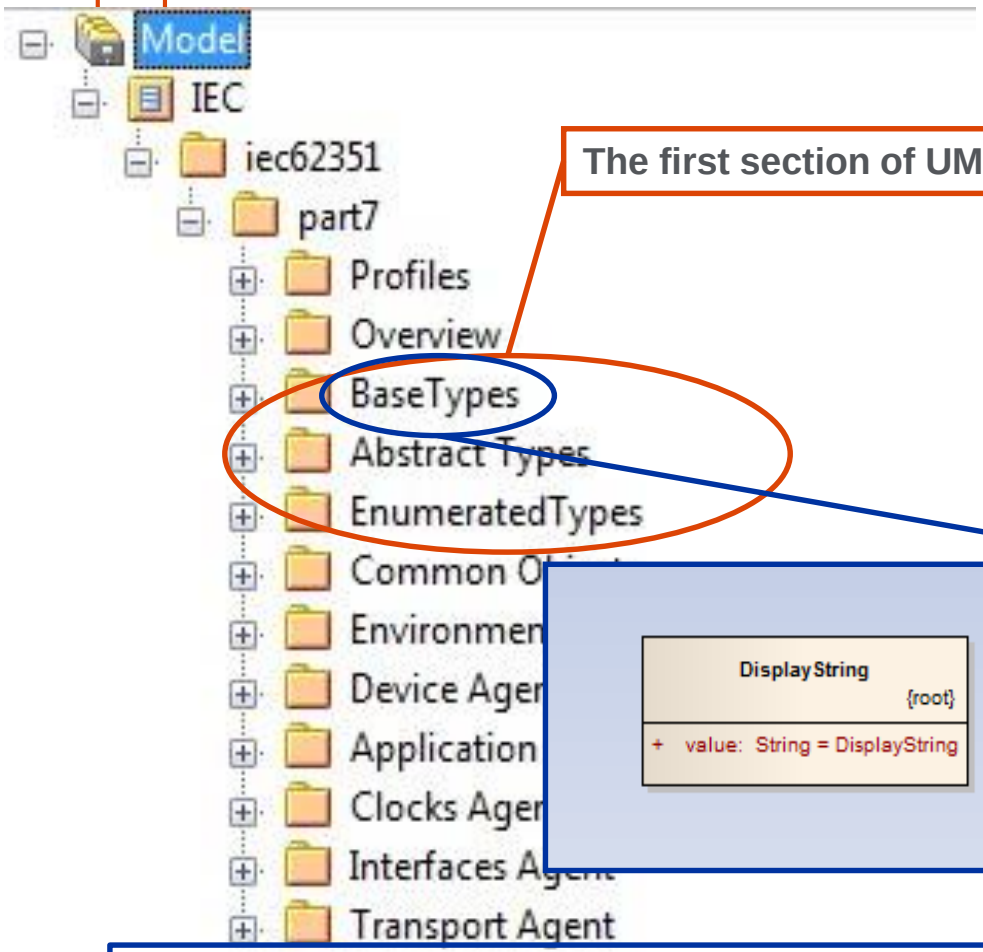
Figura 1 shows class diagram Environmental.



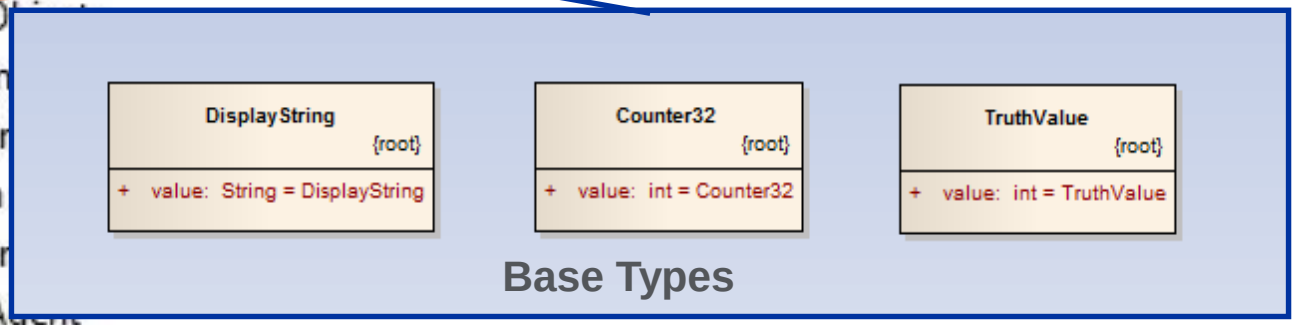




IEC 62351-7 UML model
Overall structure

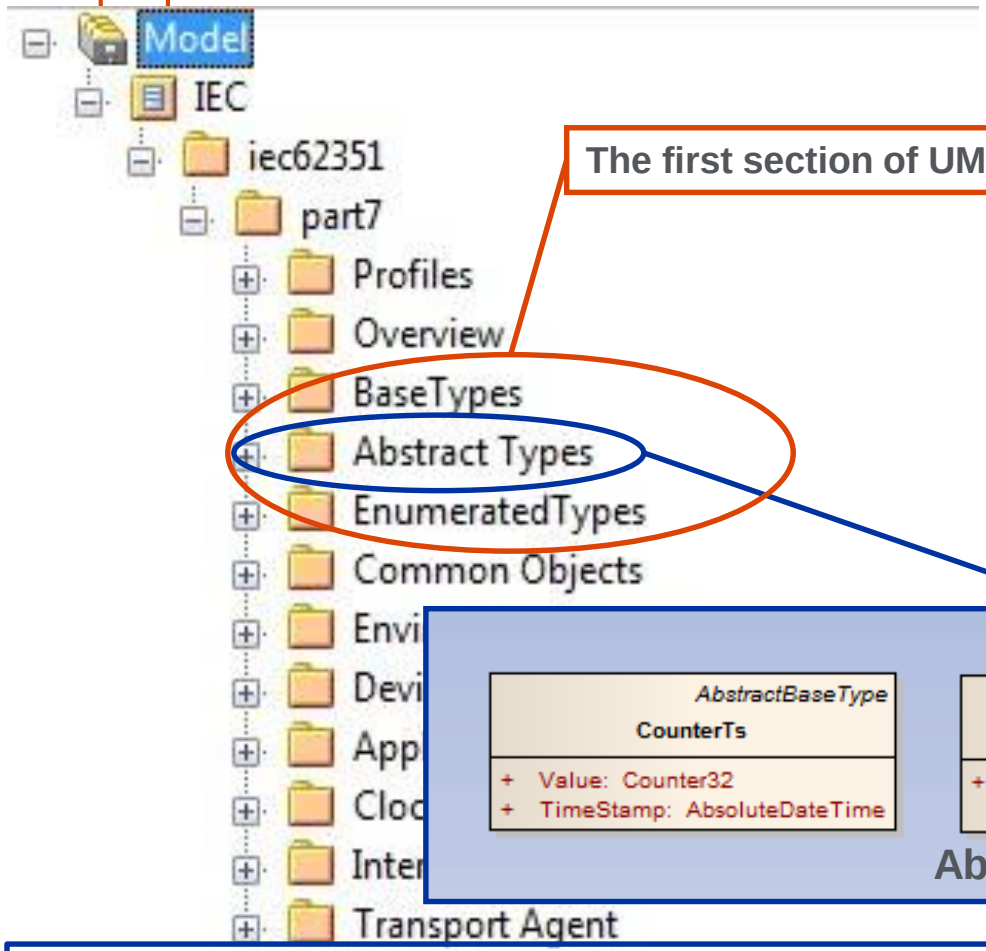


The first section of UML model is responsible of Type declaration

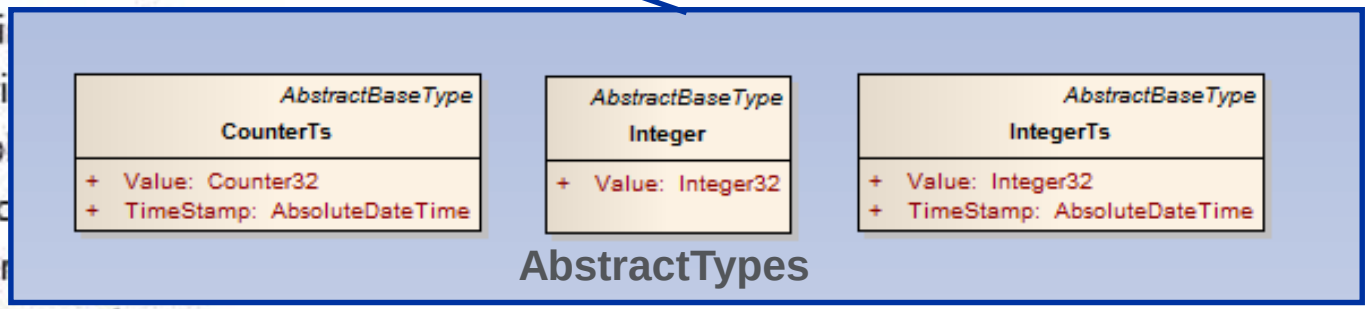


This object type description is the "low level bridge" towards SNMP and other "real" NSM protocols

IEC 62351-7 UML model
Overall structure

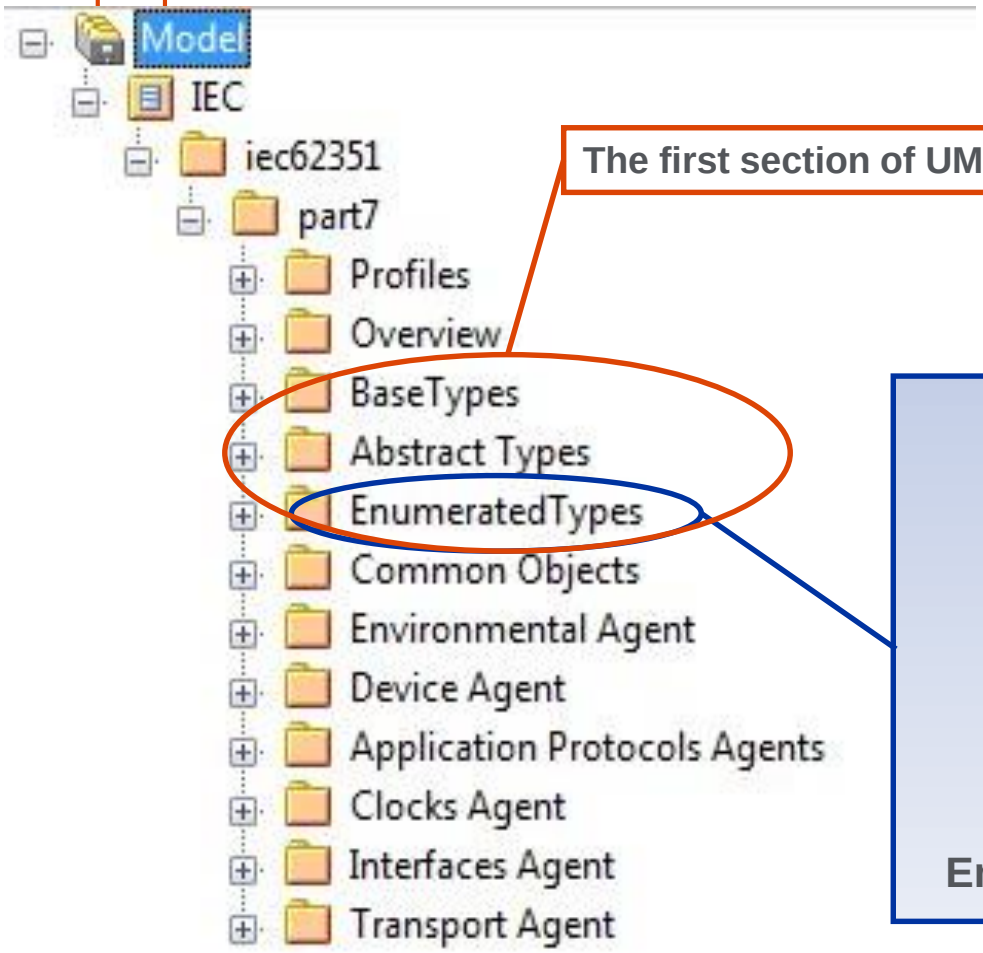


The first section of UML model is responsible of Type declaration

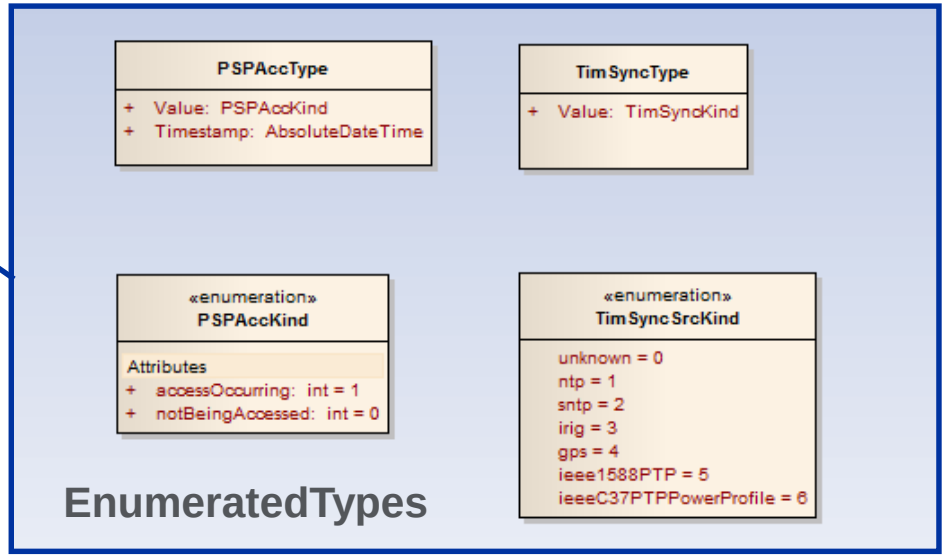


The goal is to keep the UML model as much as possible indipendent from SNMP, that is the first protocol mapping

IEC 62351-7 UML model
Overall structure

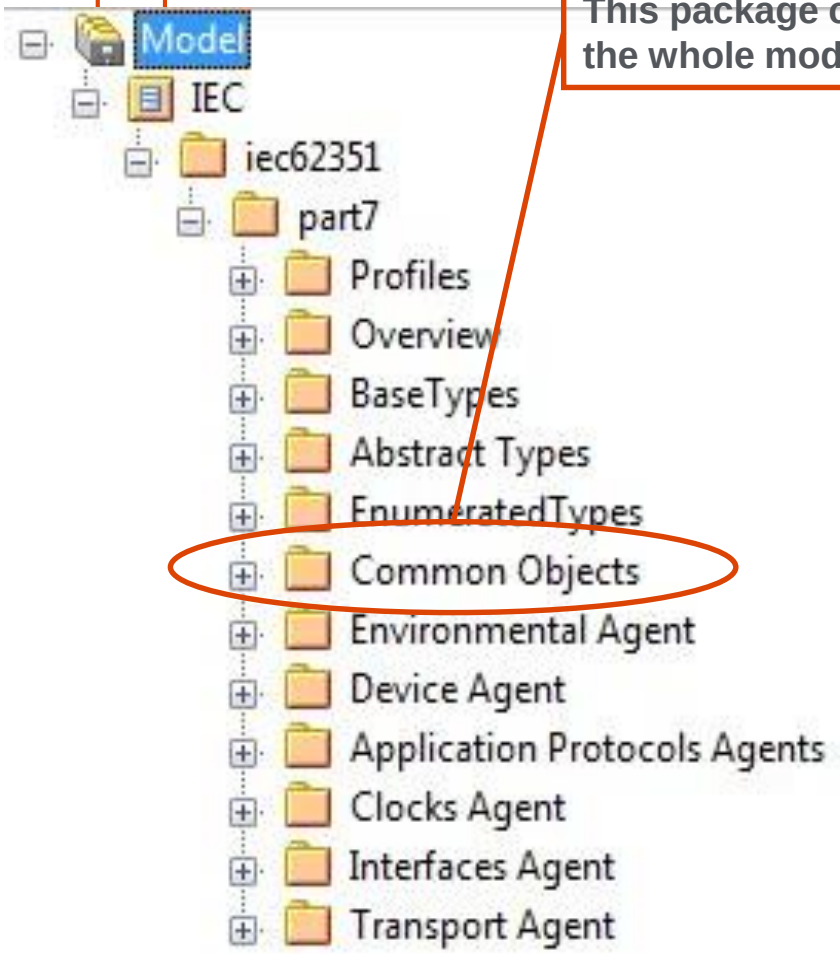


The first section of UML model is responsible of Type declaration

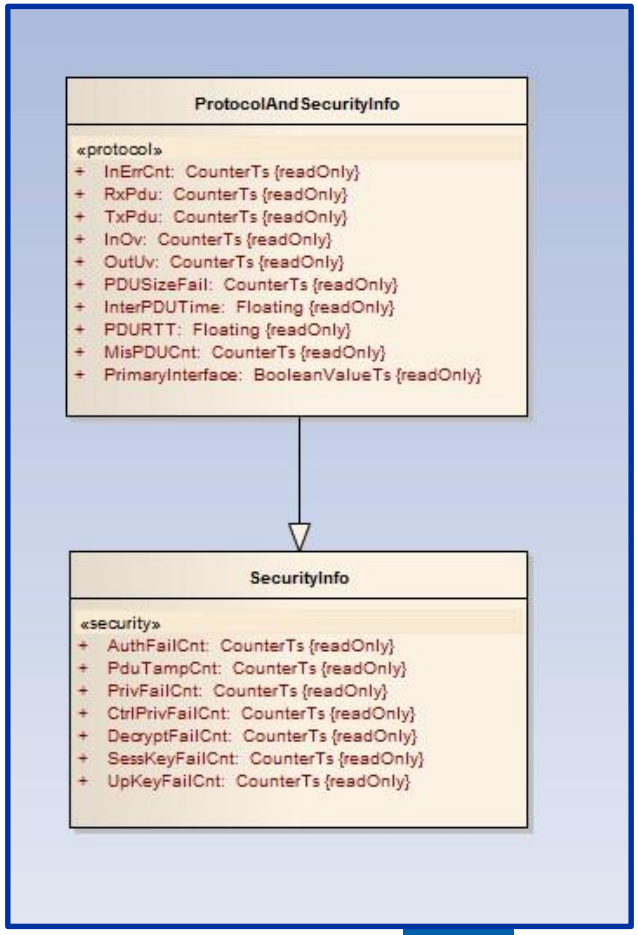


IEC 62351-7 UML model

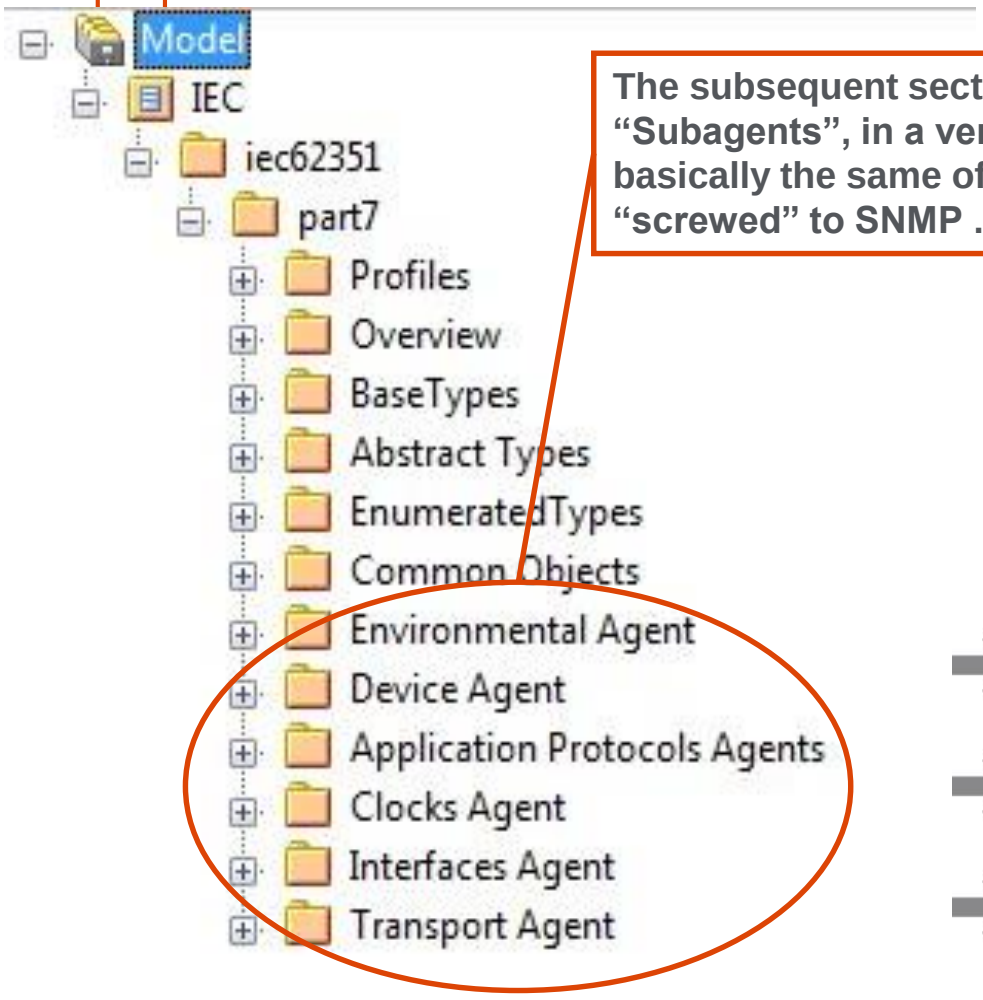
Overall structure



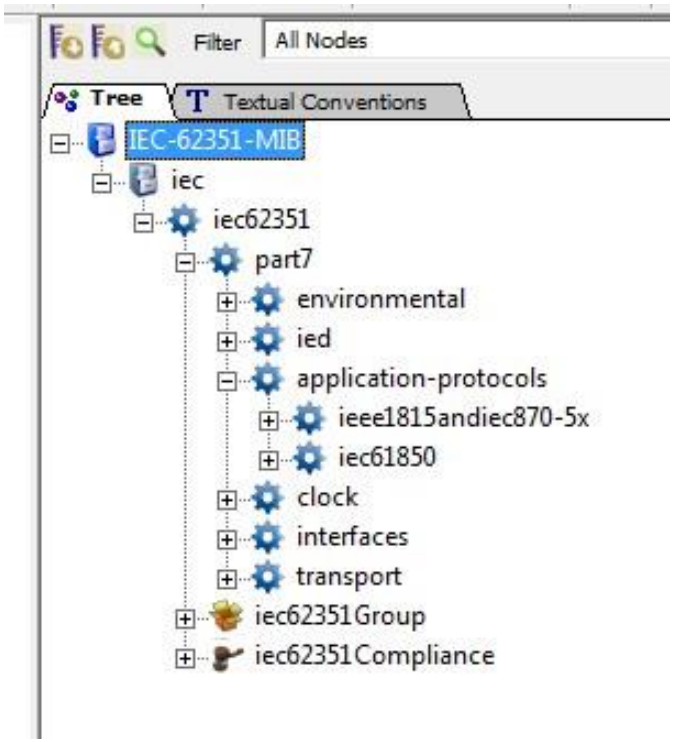
This package contains the common set of object, reused within the whole model



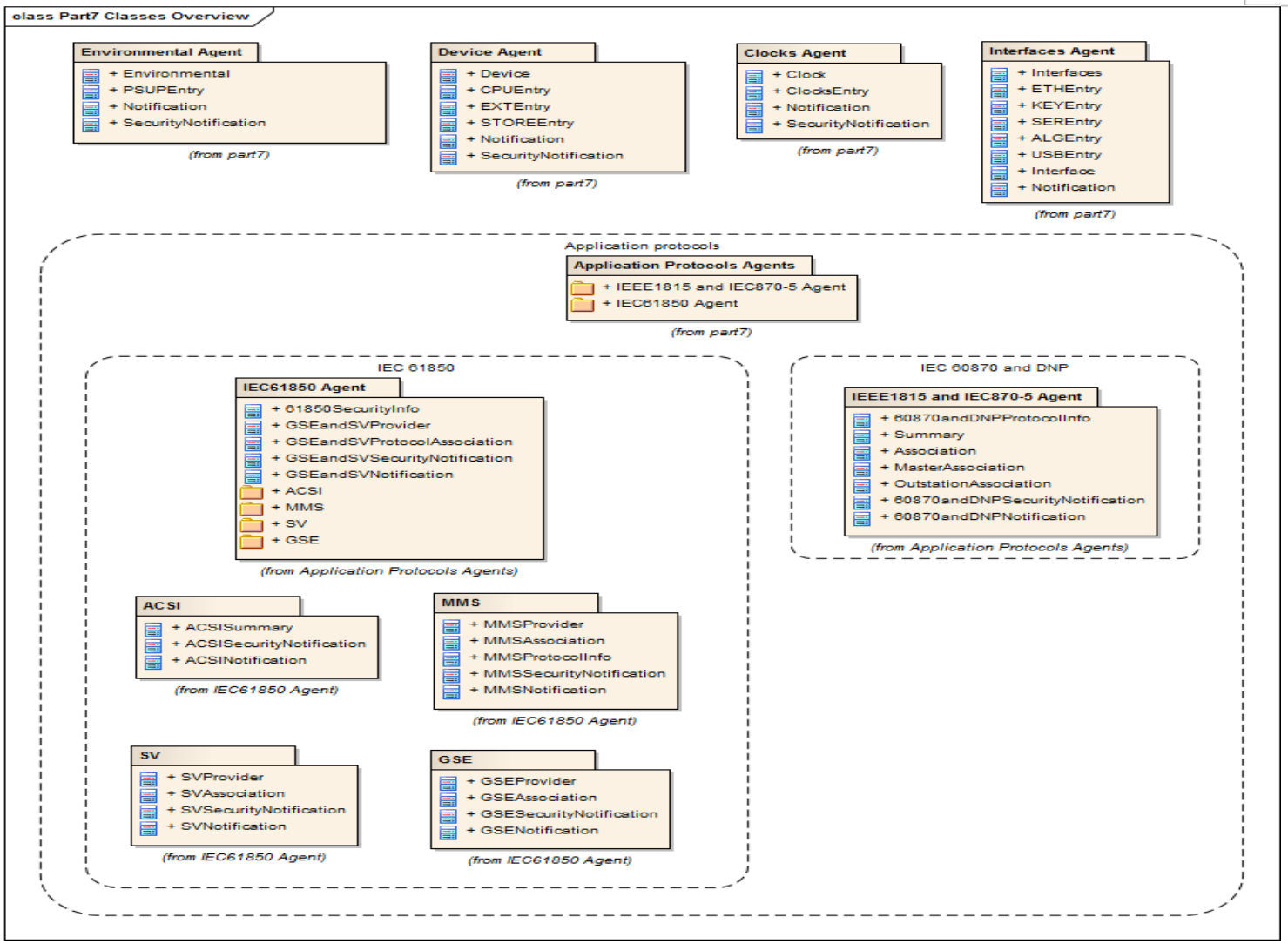
IEC 62351-7 UML model
Overall structure



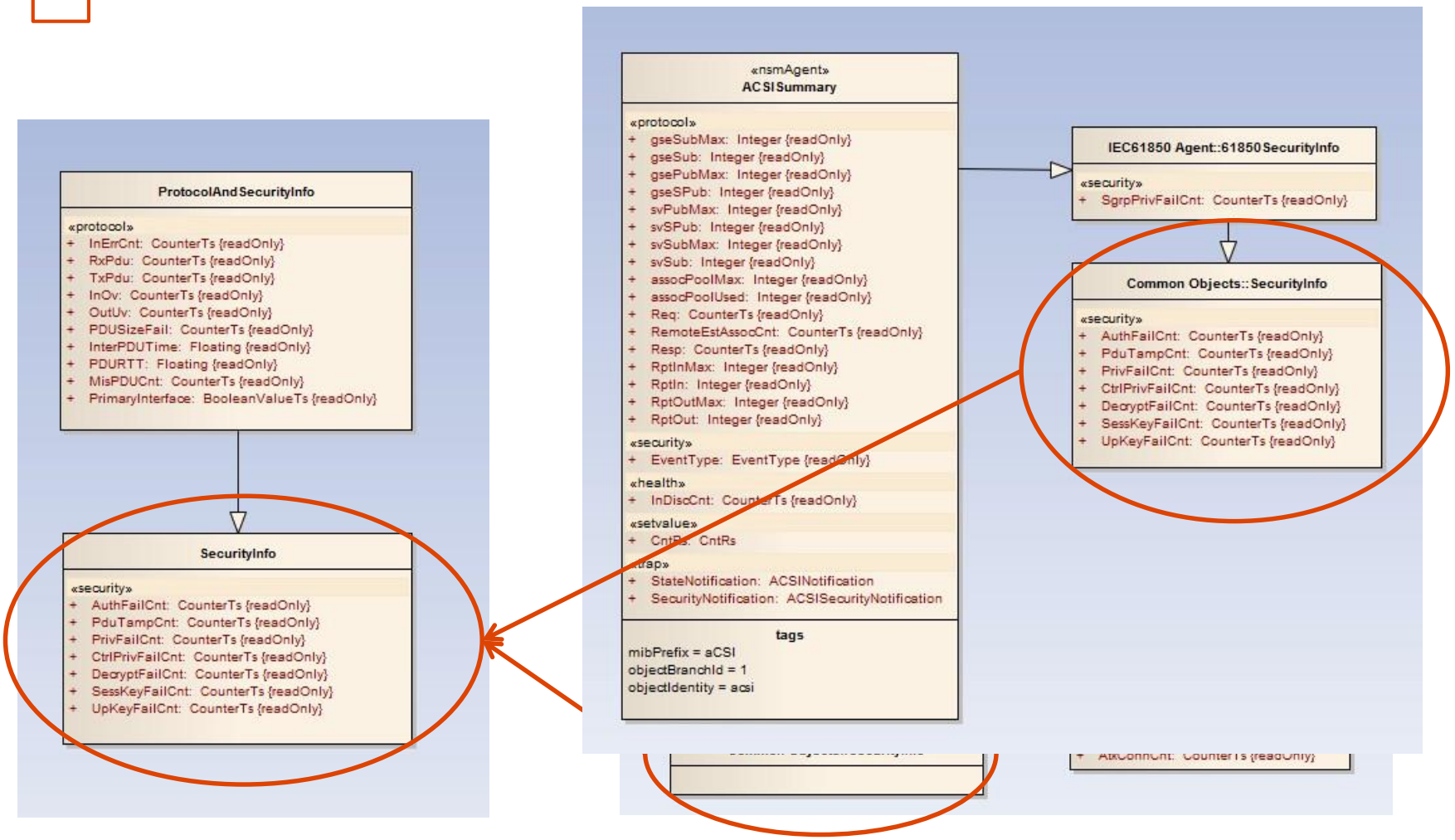
The subsequent sections of UML model correspond to the "Subagents", in a very abstract way … even is the concept is basically the same of SNMP subagents, but again we are not "screwed" to SNMP …



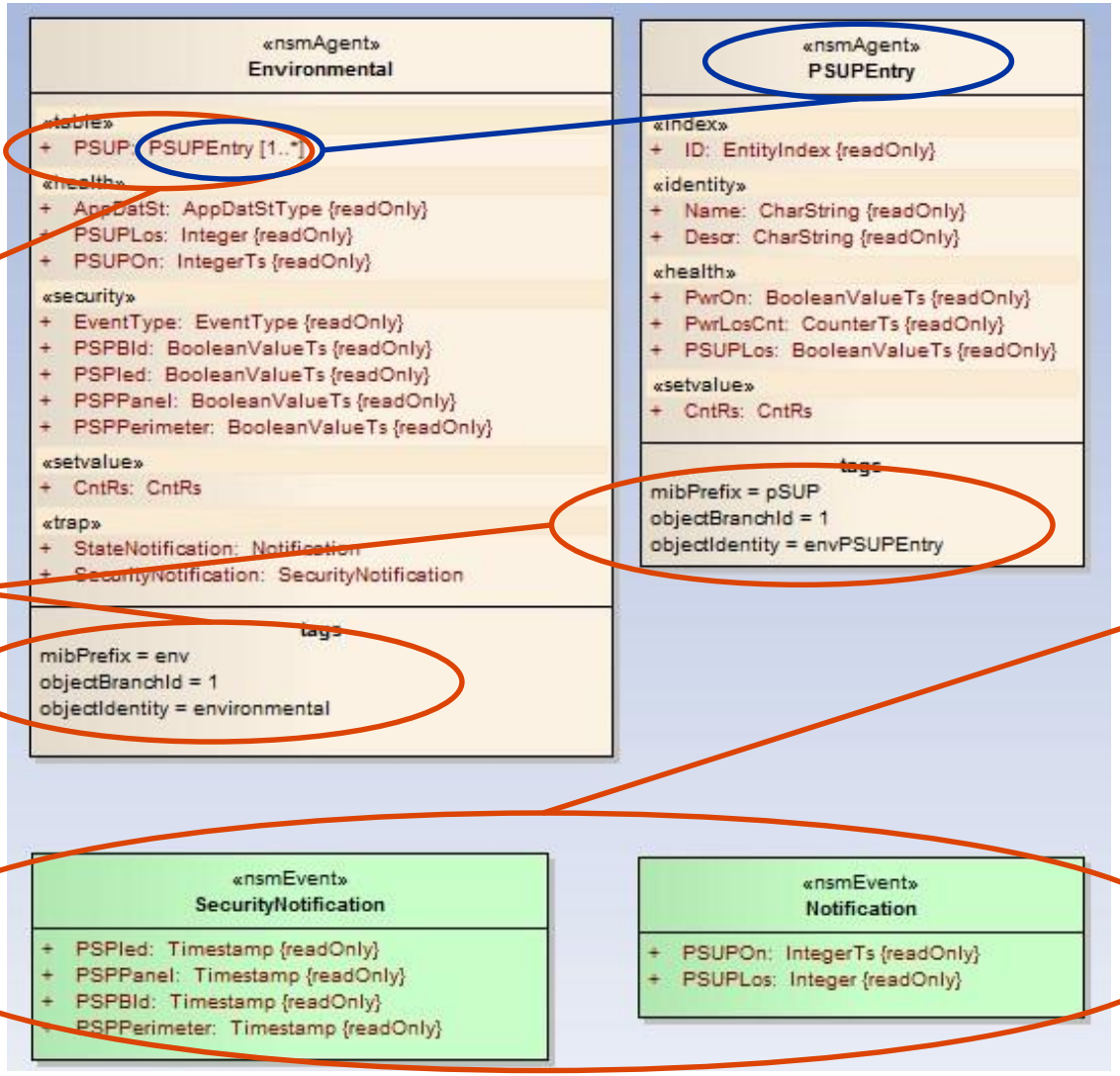
The Subagents overview



UML Class reuse and inheritance



Some UML to SNMP translation hints



Multiplicity instead of tables

SNMP MIB tags

Event Handling

Abstract Objects translation into NSM objects

SNMP MIBs and future

IEC 62351-7 IS already include the SNMP MIBs mapping. Beside this objective we had anyway the goal to **keep the Abstract Objects modeling indipendent from SNMP MIBs** specific syntax and logic:

- **Instead of SNMP table concept the UML Model adopt the concept of multiplicity** (… that translates into tables for SNMP)
- **UML Model Abstract Object are expressed as attributes of classes**. This concept is not easy to be directly translated into MIBs syntax because **MIB syntax do not allow the reuse of same object name even within different MIB branches**. For this reason we used stereotypes in order to define for **each subagent it's own "prefix"** for the each object within a subagent branch
- **Attribute versioning is provided** in order to keep track of model changes
- The Abstract nature of the UML model allow the translation toward different NSM protocols

Beside IEC 62351-7 we have now a methodology that allow the maintenance of the model and the flexible Standard document, MIBs update and extension toward other protocols.

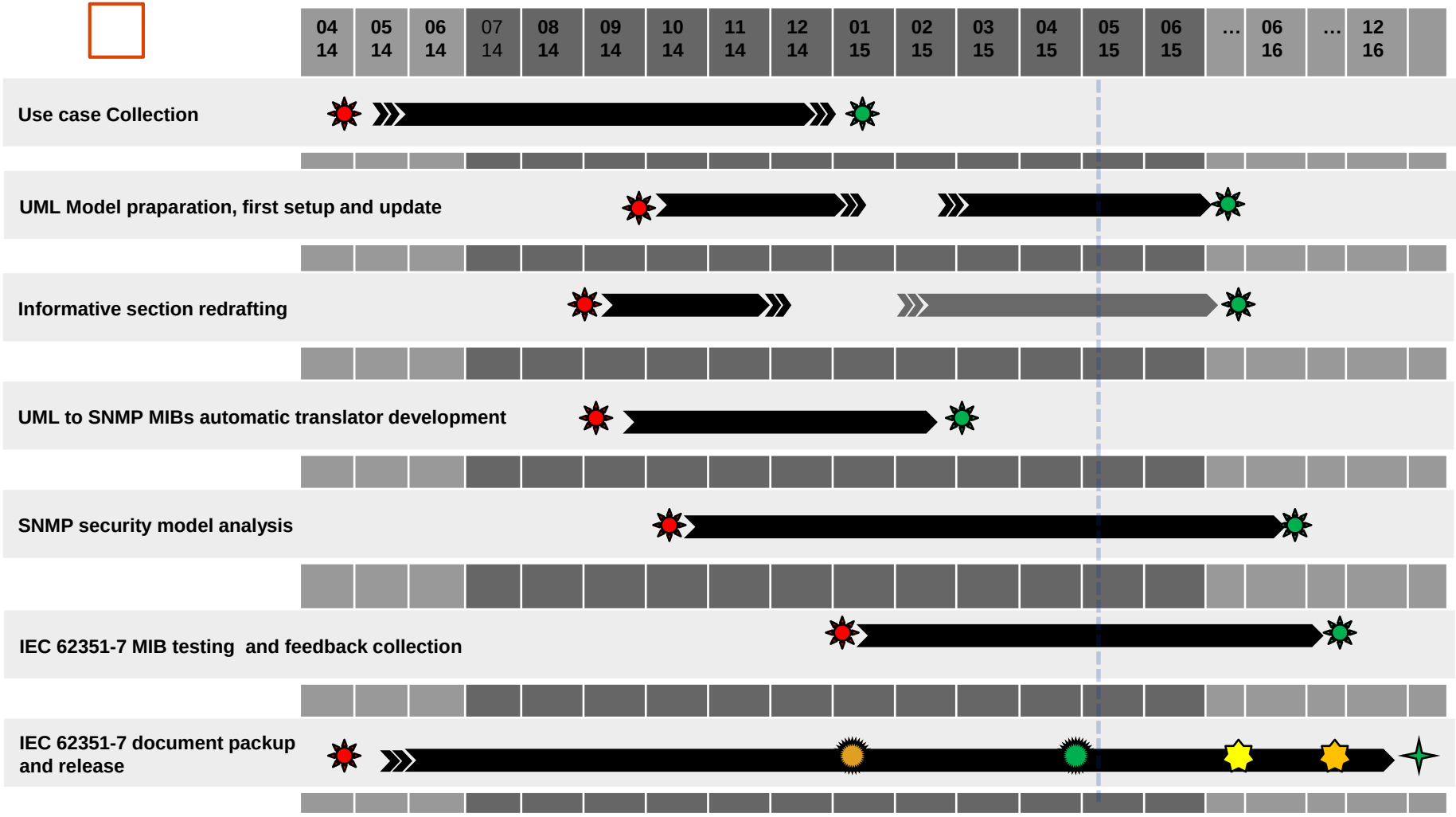
Main Milestones

- ✓ May 2013: (Vittorio Veneto WG15 meeting): decision about a PWI (Proposed Work Item) and NWIP (New Work Item Proposal) for Part 7 ed.2 task startup
- ✓ December 2013: EPRI Report with good set of suggestion for IEC 62351-7 ed.2
- ✓ April 2014: Formal RR submission and task startup
- ✓ December 2014: new EPRI report: Implementations and Applications of IEC 62351-7 standard
- ✓ January 2015: IEC 62351-7 CD release
- ✓ April 2015: Expected (received?) NC comments

Very Next Steps:

- ➢ May 2015: NC Comment review and discussion (Montreal meeting)
- ➢ New CD/CDV document issue

Planning



Relevant Topics

Model and Abstract Object refinement:

- IEC 62351-7 CD should be subject to a “real world” test, using the attached MIB this can allow a refinement both in object semantics and in the detection of missing/useless objects. The feedback about implementation effort on IEDs is very welcome.
- Currently all the objects (UML agent class Attributes) are selected as mandatory. We have the chance to define as optional some of this, if and when this will make sense.
- Whole subagents could be set as mandatory or optional in order to reduce the weight of the MIB and the processing effort (i.e. when the IED is not running 104 protocol stack it seems not to make sense having the 60870 subagent up)
- SNMP security section refinement: currently SNMP v3 is required but in order to have a good interoperability scenario it should be fine to make a choice among the different options of SNMPv3 (USM, TSM). This is related also with the central NSM tools support of those different options.

Thank You

Gian Luigi Pugni

Enel S.p.A.

Viale Italia, 26

20099 Sesto San Giovanni (MI)

mail: gianluigi.pugni@enel.com