Software Standards
State of the Art

Tony Coletta – Qual. I.T. Consulting
Head of Italian delegation to ISO/IEC JTC1 SC7
email: tony.coletta@virgilio.it

Automotive SPIN Italy – 2° workshop on Automotive Software
Milan (Italy) – 11 Oct. 2007
Agenda

- Overview of SC7 and its standards
- Brief history of ISO/IEC 15504 and Automotive SPICE
- Current developments in systems and software engineering standards
ISO/IEC JTC1 SC7 – System and Software Engineering (structure)
Overview of the SC 7 collection of standards

Foundation
- Vocabulary
  - 24765

Governance
- Quality System
  - 9001

Gov. Study Group
- 19759

Software Body of Knowledge (SWEBOK)
- 14759

Tools, Methods
- 5806 – 5807 – 6593
- 8631 – 8790 – 11411

SC7 Legacy Standards
- 3535
- 42010 TBD
- 6592
- 9294
- 15910
- 18019

Software Standards – State of the Art

MANAGING RISK

DVV

Product Characteristics
- Product packaging
  - 9127

Product Evaluation
- 25051

SC7 Legacy Standards
- 10746, 13235
- 14568, 19760
- 14750, 14752
- 14753, 14756
- 14758, 14769
- 14771, 18018
- 19500

Specifications
- CDIF
- 14568
- 15437
- 15474
- 19501

Modeling
- 8807

5806 – 5807 – 6593
8631 – 8790 – 11411

SC7 Legacy Standards
- 14102
- 14471
- 15940
- 18018

Tools and environment
- 14102
- 14471
- 15940
- 18018

10746, 13235
14750, 14752
14753, 14756
14771, 15414
15935, 19500

14143
19761
20926
20968
24570

Software Quality

SQuaRe Series

250xx

Risk & Integrity
- 90003

Life Cycle Management
- 12207
- 24783

Software Engineering
- 15271
- 90003

Documentation
- 15289

Process Implementation and Assessment
- 15288
- 19760
- 26702
- 24783

Life Cycle
- 15288

Systems Engineering
- 15288

Asset Management
- 19770

Project Management
- 16326

Measurement
- 15939

IT Service Management
- 20000

Software Functional size measurement
- 14143
- 19761
- 20926
- 20968
- 24570

Software Quality

SQuaRe Series

250xx

Software Maintenance
- 16085
- 15026

Software body of Knowledge (SWEBOK)
- 19759

Overview of the SC 7 collection of standards

TBD
Software Life Cycle Processes from ISO/IEC 12207

- **Acquisition**
- **Supply**
- **Development**
- **Operation**
- **Maintenance**
- **Problem Resolution**

**Supporting Processes**

- **Documentation**
- **Configuration Management**

- **Quality Assurance**
- **Verification**
- **Validation**
- **Joint Review**
- **Audit**

**Organisational Processes**

- **Management**
- **Infrastructure**
- **Improvement**
- **Training**

- **Conformity standard**
- **Specifies mandatory requirements to be met on order to declare conformity**
Example of 12207 conformity requirements

5.3.5 **Software architectural design.** For each software item (or software configuration item, if identified), this activity consists of the following tasks:

5.3.5.1 The developer shall transform the requirements for the software item into an architecture that describes its top-level structure and identifies the software components. It shall be ensured that all the requirements for the software item are allocated to its software components and further refined to facilitate detailed design. The architecture of the software item shall be documented.

5.3.5.2 The developer shall develop and document a top-level design for the interfaces external to the software item and between the software components of the software item.

5.3.5.3 The developer shall develop and document a top-level design for the database.

5.3.5.4 The developer should develop and document preliminary versions of user documentation.

5.3.5.5 The developer shall define and document preliminary test requirements and the schedule for Software Integration.

5.3.5.6 The developer shall evaluate the architecture of the software item and the interface and database designs considering the criteria listed below. The results of the evaluations shall be documented.
ISO/IEC TR 15504 – Process Assessment

- Focus on **process objectives** (what to achieve not how) and **process management** (measured as process capability)

- Capability Level 1 achievement means (somehow) achieving purpose and outcomes

- From level 2 to level 5 – increasing level of process management effectiveness

- Embedded process reference model (TR part 2) with definition of “Purpose” and “Outcomes”

- Strongly related to ISO/IEC 12007 processes but with some differences

- Recognition of management features common to all process (capability levels and attributes)

- ISO/IEC 12207 is a mixture of levels for the different processes

- Exemplar Process Assessment Model (TR part 5) provided **indicators** to determine level of capability during assessment
ISO/IEC TR 15504 Capability Levels for processes

Process Capability Levels

- Optimising
- Predictable
- Established
- Managed
- Performed
- Incomplete

Processes assessed

1998
Issues

- Standard users confused about different models for software lifecycle processes
- Lack of harmonization between 12207 and 15504
- After 3 year trial of 15504 TR → decision to revise and publish as IS
- Agreement between WG7 (12207) and WG 10 (15504) on harmonization approach:
  - Amendments (AMD1 and AMD2) to 12207 to include a Process Reference Model (PRM) with “purpose” and “outcomes” suitable for use with 15504
  - 15504-2 removes embedded PRM and defines requirements for “external” PRMs and PAMs
  - 15504-5 provides an exemplar Process Assessment Model (PAM) based on 12207 PRM (AMD1)
- Debate on who should define/approve PRMs/PAMs:
  - Only ISO/IEC (eg. 12207 AMD) vs open market approach (eg. Automotive SPICE)
  - OK for open market but need to demonstrate and document consensus by a user community
ISO/IEC 15504 International Standard

- **ISO/IEC 15504-2**
  - Requirements for PRM
  - Measurement Framework
  - Requirements for PAM

- **Process Assessment Model**
  - Linked to "15504-5 PAM"

- **Process Reference Model**
  - Linked to "12207 AMD1"

Linked PRM and PAM for Software Life Cycle Processes
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MAN.1 Organizational alignment</td>
<td>A ENG.1 Requirements elicitation</td>
<td>A SUP.1 Quality assurance</td>
</tr>
<tr>
<td>MAN.2 Organization management</td>
<td>A ENG.2 System requirements analysis</td>
<td>A SUP.2 Verification</td>
</tr>
<tr>
<td>A MAN.3 Project management</td>
<td>A ENG.3 System architectural design</td>
<td>A SUP.3 Validation</td>
</tr>
<tr>
<td>MAN.4 Quality management</td>
<td>A ENG.4 Software requirements analysis</td>
<td>A SUP.4 Joint review</td>
</tr>
<tr>
<td>A MAN.5 Risk management</td>
<td>A ENG.5 Software design</td>
<td>A SUP.5 Audit</td>
</tr>
<tr>
<td>A MAN.6 Measurement</td>
<td>A ENG.6 Software construction</td>
<td>A SUP.6 Product evaluation</td>
</tr>
<tr>
<td></td>
<td>A ENG.7 Software integration</td>
<td>A SUP.7 Documentation</td>
</tr>
<tr>
<td></td>
<td>A ENG.8 Software testing</td>
<td>A SUP.8 Configuration management</td>
</tr>
<tr>
<td></td>
<td>A ENG.9 System integration</td>
<td>A SUP.9 Problem resolution management</td>
</tr>
<tr>
<td></td>
<td>A ENG.10 System testing</td>
<td>A SUP.10 Change request management</td>
</tr>
<tr>
<td></td>
<td>ENG.11 Software installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ENG.12 Software and system maintenance</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ACQ.1 Acquisition preparation</td>
<td>RIN.1 Human resource management</td>
<td>OPE.1 Operational use</td>
</tr>
<tr>
<td>ACQ.2 Supplier selection</td>
<td>RIN.2 Training</td>
<td>OPE.2 Customer support</td>
</tr>
<tr>
<td>A ACQ.3 Contract agreement</td>
<td>RIN.3 Knowledge management</td>
<td></td>
</tr>
<tr>
<td>A ACQ.4 Supplier monitoring</td>
<td>RIN.4 Infrastructure</td>
<td></td>
</tr>
<tr>
<td>ACQ.5 Customer acceptance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A ACQ.11 Technical requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A ACQ.12 Legal and administrative requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A ACQ.13 Project requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A ACQ.14 Request for proposals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A ACQ.15 Supplier qualification</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A SPL.1 Supplier tendering</td>
<td>PIM.1 Process establishment</td>
<td>REU.1 Asset management</td>
</tr>
<tr>
<td>A SPL.2 Product release</td>
<td>PIM.2 Process assessment</td>
<td>A REU.2 Reuse program management</td>
</tr>
<tr>
<td>SPL.3 Product acceptance support</td>
<td>A PIM.3 Process improvement</td>
<td>REU.3 Domain engineering</td>
</tr>
</tbody>
</table>

- A Automotive-SPICE
- new HIS-Scope
- not included in ISO/IEC IS 15504-5
Automotive SPICE - Process Reference Model

**PRIMARY**

**Acquisition**
- Contract agreement
- Supplier monitoring
- Technical Requirements
- Legal and Administrative Req.s
- Project Requirements
- Request for proposals
- Supplier Qualification

**Supply**
- Supplier tendering
- Product release

**Engineering**
- Requirements elicitation
- System requirements analysis
- System architectural design
- Software requirements analysis
- Software design
- Software construction
- Software integration test
- Software testing
- System integration test
- System testing

**Support**
- Quality assurance
- Verification
- Joint review
- Documentation Management
- Configuration Management
- Problem Resolution management
- Change Request management

**Management**
- Project management
- Risk management
- Measurement

**Process Improvement**
- Process improvement

**Reuse**
- Reuse program management

**ORGANISATIONAL**

**2005**
## New HIS Automotive SPICE™ Scope:

### Engineering Process Group
- ENG.2  System requirements analysis
- ENG.3  System architectural design
- ENG.4  Software requirements analysis
- ENG.5  Software design
- ENG.6  Software construction
- ENG.7  Software integration
- ENG.8  Software testing
- ENG.9  System integration
- ENG.10 System testing

### Support Process Group
- SUP.1  Quality assurance
- SUP.8  Configuration Management
- SUP.9  Problem resolution management
- SUP.10 Change request management

### Management Process Group
- MAN.3  Project management

### Acquisition Process Group
- (optional)
- ACQ.4  Supplier Monitoring

**Note:** This scope defines the minimum of processes to be assessed by each member. Evaluation of ENG.2/3 and ENG.9/10 depends on the project/product. Further processes may be evaluated individually, if necessary. Based on Automotive SPICE™ 2005.
### System Life Cycle Processes

#### Agreement Processes
- Acquisition Process (Clause 6.1.1)
- Supply Process (Clause 6.1.2)

#### Project Processes
- Project Planning Process (Clause 6.3.1)
- Project Assessment and Control Process (Clause 6.3.2)
- Decision Management Process (Clause 6.3.3)
- Risk Management Process (Clause 6.3.4)
- Configuration Management Process (Clause 6.3.5)
- Information Management Process (Clause 6.3.6)
- Measurement Process (Clause 6.3.7)

#### Technical Processes
- Stakeholder Requirements Definition Process (Clause 6.4.1)
- Requirements Analysis Process (Clause 6.4.2)
- Architectural Design Process (Clause 6.4.3)
- Implementation Process (Clause 6.4.4)
- Integration Process (Clause 6.4.5)
- Verification Process (Clause 6.4.6)
- Transition Process (Clause 6.4.7)
- Validation Process (Clause 6.4.8)
- Operation Process (Clause 6.4.9)
- Maintenance Process (Clause 6.4.10)
- Disposal Process (Clause 6.4.11)

#### Project-Enabling Processes
- Life Cycle Model Management Process (Clause 6.2.1)
- Infrastructure Management Process (Clause 6.2.2)
- Project Portfolio Management Process (Clause 6.2.3)
- Human Resource Management Process (Clause 6.2.4)
- Quality Management Process (Clause 6.2.5)
Structure of ISO/IEC 15288

- Process
  - The purpose of the process is stated in a paragraph that describes at a high level the overall goal for performing the process

- Outcomes
  - An outcome is an observable result of the successful achievement of the purpose of the process.

- Activities
  - The Activities attribute is used to provide a structural decomposition of a process
Example process from ISO/IEC 15288

6.2.4 Human Resource Management Process

6.2.4.1 Purpose

The purpose of the Human Resource Management process is to ensure the organization is provided with necessary human resources and to maintain their competencies, consistent with business needs.

This process provides a supply of skilled and experienced personnel qualified to perform life cycle processes to achieve organization, project and customer objectives.

6.2.4.2 Outcomes

As a result of the successful implementation of the Human Resource Management Process:

a) Skills required by projects are identified.

b) Necessary human resources are provided to projects.

c) Skills of personnel are developed, maintained or enhanced.

d) Conflicts in multi-project resource demands are resolved.

e) Individual knowledge, information and skills are collected, shared, reused and improved throughout the organization.

6.2.4.3 Activities and Tasks

The organization shall implement the following activities and tasks in accordance with applicable organization policies and procedures with respect to the Human Resource Management Process:

a) **Identify Skills.** This activity consists of the following tasks:

   1) Identify skill needs based on current and expected projects.

   2) Identify and record skills of personnel.
ISO/IEC 15504 applied on 15288

Linked PRM and PAM for System Life Cycle Processes

ISO/IEC 15504-2
- Requirements for PRM
- Measurement Framework
- Requirements for PAM

Process Assessment Model
- e.g. 15504-6 PAM

Process Reference Model
- e.g. 15288 PRM
ISO/IEC 15288 – Relationship with ISO/IEC 12207

- Hardware Implementation
  - Software Implementation
    - Refer to ISO/IEC 12207
  - Human Task Implementation

- Enterprise Environment Management
- Investment Management
- System Life Cycle Processes Management
- Resource Management
- Quality Management
- Acquisition
- Supply

- Project Planning
- Decision Making
- Stakeholder Requirements Definition
- Requirements Analysis
- Architectural Design
- Implementation

- Project Assessment
- Risk Management
- Verification

- Project Control
- Configuration Management
- Integration
- Transition
- Validation

- Usability
- Information Management
- Operation
- Maintenance
- Disposal

- Stakeholder
- Requirements
- Definition

- Human Task
- Implementation

- System Life Cycle
- Processes Management

- Software Implementation

- Information Management
- Usability
The Agreement Processes form the relationship between acquirer and supplier organizations.

The Project-Enabling Processes form the relationship between the organization and its projects.

The Project Processes manage the project.

The Technical Processes deal with the system.

The Software Processes are used to implement a software element of the system.

- Software Implementation
- Software Support
- Software Reuse
Process Assessment Models in CMMI

**Staged Model**

- ML5
- ML4
- ML3
- ML2
- ML1

...for an established set of process areas across an organization

**Continuous Model**

- Process Area Capability
  - 0 1 2 3 4 5
  - PA PA PA

...for a single process or Process area
The CMMI Maturity Levels (staged)

1. Process unpredictable, poorly controlled and reactive
2. Process characterized for projects and is often reactive
3. Process characterized for the organization and is proactive
4. Process measured and controlled
5. Focus on process improvement

Optimizing
Quantitatively Managed
Defined
Managed
Performed
Source: SEI
New developments in ISO/IEC 15504

- ISO/IEC 15504-7 – Assessment of Organizational Maturity
  - Linked with process capability PRM/PAM – Organizational maturity derived from capability profiles
  - Same approach as Part 2 – no embedded OMM (Organizational Maturity Model) – requirements for external models

- ISO/IEC 15504-8 – An exemplar PAM for IT Service Management
  - Aligned with ISO/IEC 20000-1 (IT Service Management)
  - Process Reference model as part of the ISO/IEC 20000 series (part 4)
  - Same harmonization approach as 12207 and 15288
2004: National initiatives by FAKRA (G) and BNA (Fr)

ISO 26262 Plan:
- 2005-06: PWI (Preliminary Work Item – ISO TC22 SC3 WG16)
- 2005-11: Kick-off
- end 2007: CD (ISO TC22 Committee Draft) ???
- 2008: DIS (ISO Draft International Standard)

ISO TC22 SC3 WG16:
- Chairman: Christoph Jung - BMW
- Nations: Germany, United Kingdom, Austria, Japan, Sweden, Italy, USA, France
- Companies: BMW, DaimlerChrysler, Volkswagen, Contiteves, Bosch, Land Rover, MIRA, Magna Steyr, Nissan, Honda, JARI, Volvo, Fiat, TRW, (GM, Ford), Delphi, Renault, PSA, Valeo, Siemens VDO
2. Management of functional safety

2.4 Management during complete safety lifecycle
2.5 Safety management during development
2.6 Safety management activities after SOP

3. Concept phase

3.4 Item definition
3.5 Initiation of safety lifecycle (modification and derivates)
3.6 Hazard analysis and risk assessment
3.7 Functional safety concept

4. Product development system

4.4 Initiation of product development system
4.5 Specification of technical safety concept
4.6 System design

5. Product development H/w

5.4 HW requirements analysis
5.5 HW architecture design
5.6 Quantitative requirements for random HW failures
5.7 Measures for avoidance and control of systematic HW failures
5.8 Safety HW integration and verification
5.9 Qualification of parts and components
5.10 Overall requirements for HW-SW interface

6. Product development S/W

6.4 Initiating SW development
6.5 SW safety requirements specification
6.6 SW architecture and design
6.7 SW implementation
6.8 SW unit test
6.9 SW integration and test
6.10 SW safety acceptance test

7. Production and operation

7.4 Production
7.5 Operation, service and decommissioning

8. Supporting processes

8.4 Interfaces within distributed developments
8.5 Overall management of safety requirements
8.6 Configuration management
8.7 Change management
8.8 Safety analysis
8.9 Analysis of CCF, CMF, cascading failures
8.10 Verification activities
8.11 Documentation
8.12 Overall quality management
8.13 Qualification of software tools
8.14 Qualification of software libraries
8.15 Proven in use argumentation

9. Annexes
Once again !!!!!

- No harmonization ????
- Many overlap with SC7 standards… and not only
- Similar concepts to 12207 and 15288
  - Focus on safety but why not refer to SC7 for life cycle management processes ?
  - See similar experience in medical device industry (i.e 14971 risk management in software development)
  - ISO/IEC 16085 - SC7 risk management standard could it be useful ?
- It’s still a WD (Working Draft) – let’s do something before it’s too late
Thank you?

Questions?