Software Standards
State of the Art

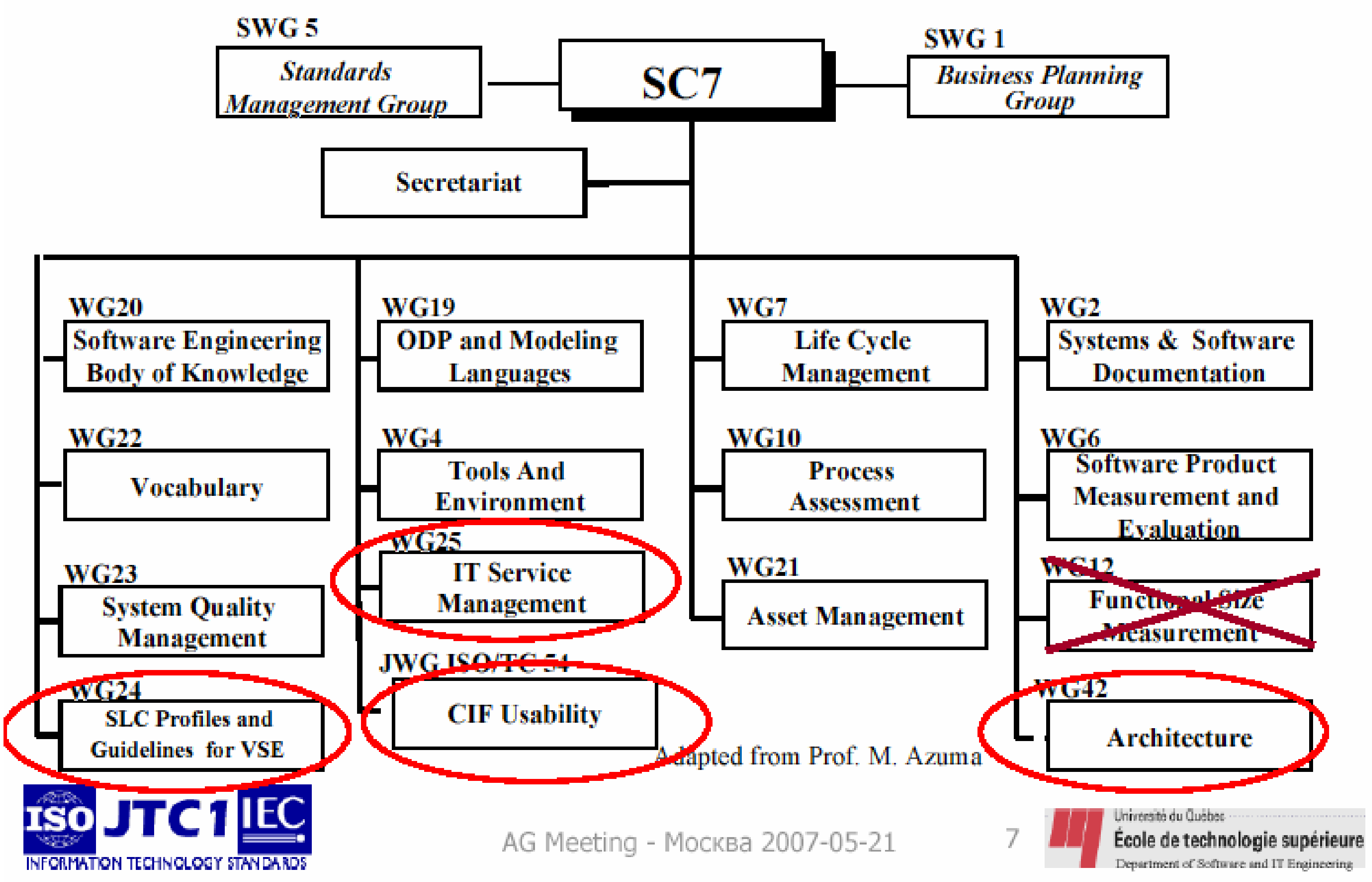
Tony Coletta – Qual. I.T. Consulting
Head of Italian delegation to ISO/IEC JTC1 SC7
email:tony.coletta@virgilio.it

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)



SC7

SWG 5 – *Standards Management Group*

SWG 1 – *Business Planning Group*

Secretariat

WG20 – Software Engineering Body of Knowledge

WG22 – Vocabulary

WG23 – System Quality Management

WG24 – SLC Profiles and Guidelines for VSE

WG19 – ODP and Modeling Languages

WG4 – Tools And Environment

WG25 – IT Service Management

JWG ISO/TC 54 – CIF Usability

WG7 – Life Cycle Management

WG10 – Process Assessment

WG21 – Asset Management

WG2 – Systems & Software Documentation

WG6 – Software Product Measurement and Evaluation

~~WG12 – Functional Size Measurement~~

WG42 – Architecture

Adapted from Prof. M. Azuma

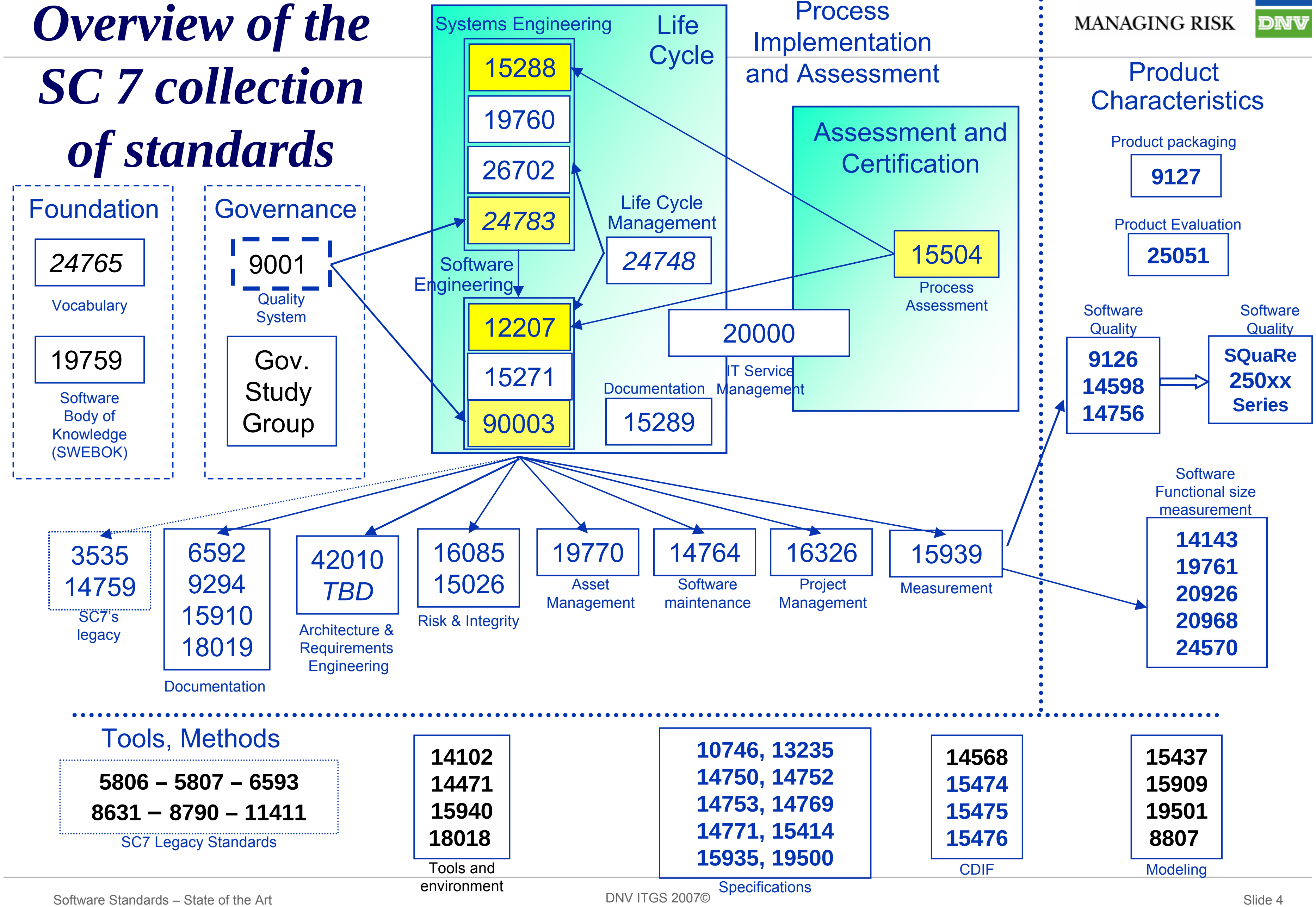
ISO JTC1 IEC INFORMATION TECHNOLOGY STANDARDS

AG Meeting - Москва 2007-05-21

7

Université du Québec École de technologie supérieure Department of Software and IT Engineering

Overview of the SC 7 collection of standards



Foundation

24765 Vocabulary

19759 Software Body of Knowledge (SWEBOK)

Governance

9001 Quality System

Gov. Study Group

Systems Engineering

Life Cycle

15288

19760

26702

24783

Software Engineering

12207

15271

90003

Life Cycle Management

24748

Documentation

15289

Process Implementation and Assessment

Assessment and Certification

15504 Process Assessment

20000 IT Service Management

Product Characteristics

Product packaging

9127

Product Evaluation

25051

Software Quality

9126 14598 14756

Software Quality

SQuaRe 250xx Series

Software Functional size measurement

14143 19761 20926 20968 24570

3535 14759 SC7's legacy

6592 9294 15910 18019 Documentation

42010 TBD Architecture & Requirements Engineering

16085 15026 Risk & Integrity

19770 Asset Management

14764 Software maintenance

16326 Project Management

15939 Measurement

Tools, Methods

5806 – 5807 – 6593

8631 – 8790 – 11411

SC7 Legacy Standards

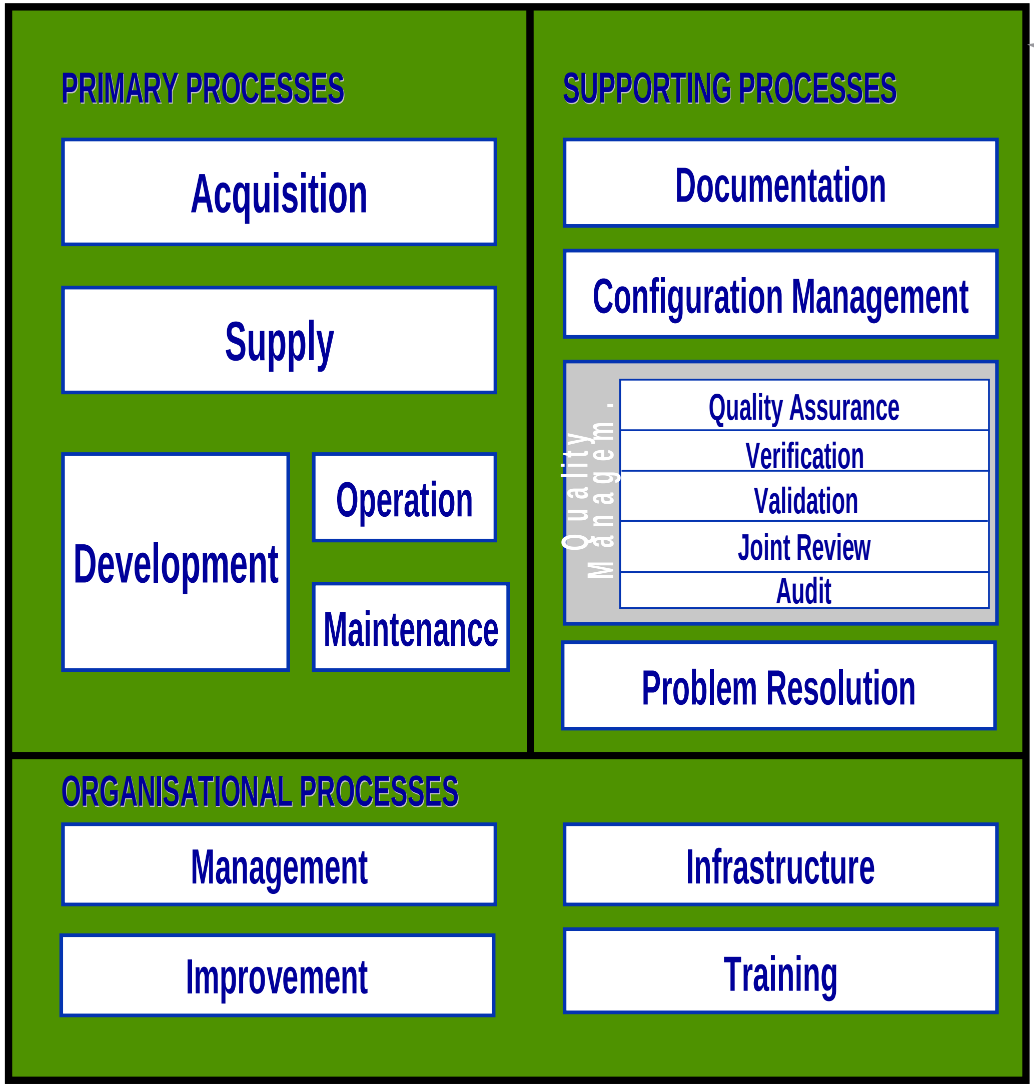
14102 14471 15940 18018 Tools and environment

10746, 13235 14750, 14752 14753, 14769 14771, 15414 15935, 19500 Specifications

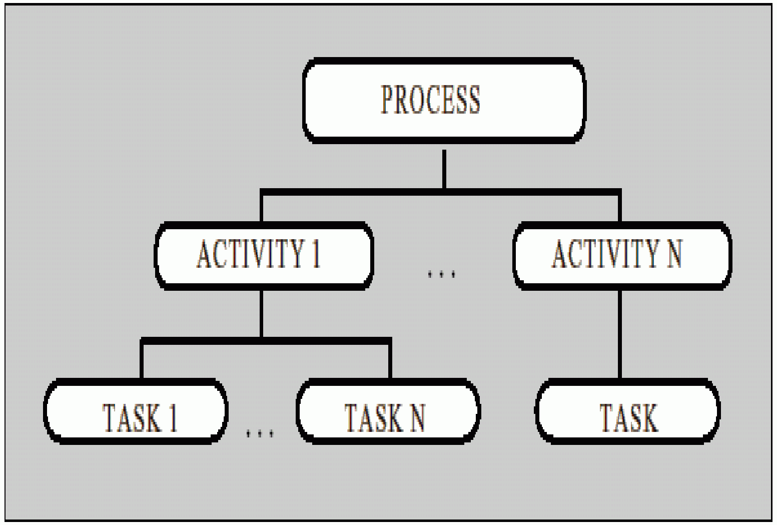
14568 15474 15475 15476 CDIF

15437 15909 19501 8807 Modeling

Software Life Cycle Processes from ISO/IEC 12207



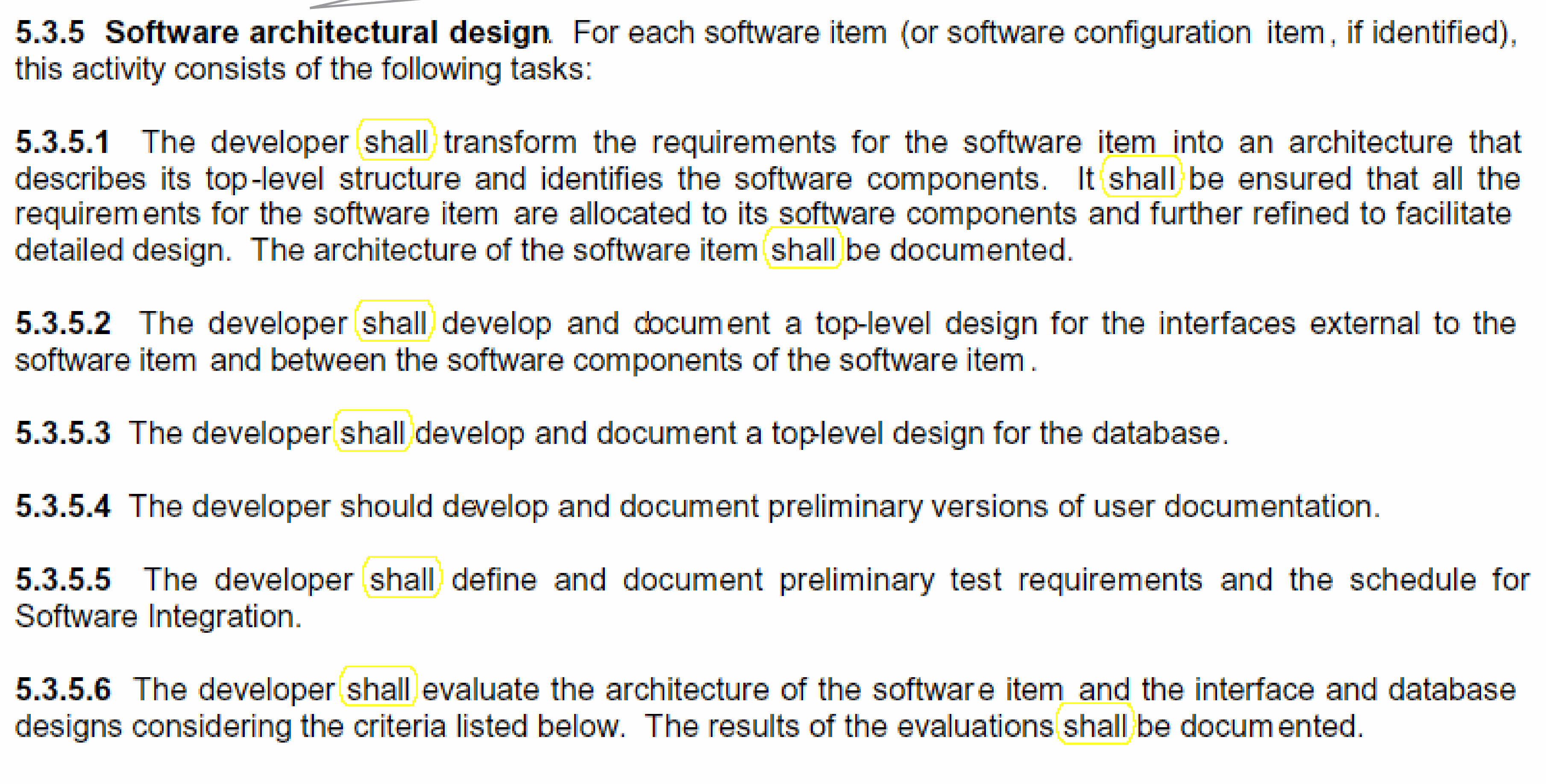
1995



- Conformity standard
- Specifies mandatory requirements to be met on order to declare conformity

Example of 12207 conformity requirements

Activity within
Development process



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

MANAGING RISK DNV

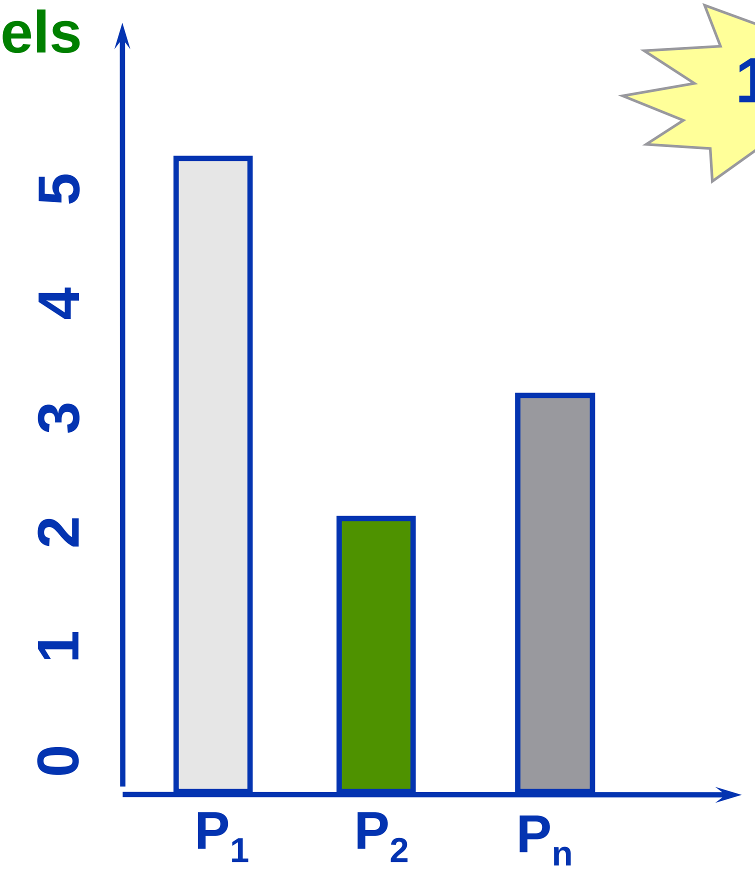
1998

- 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

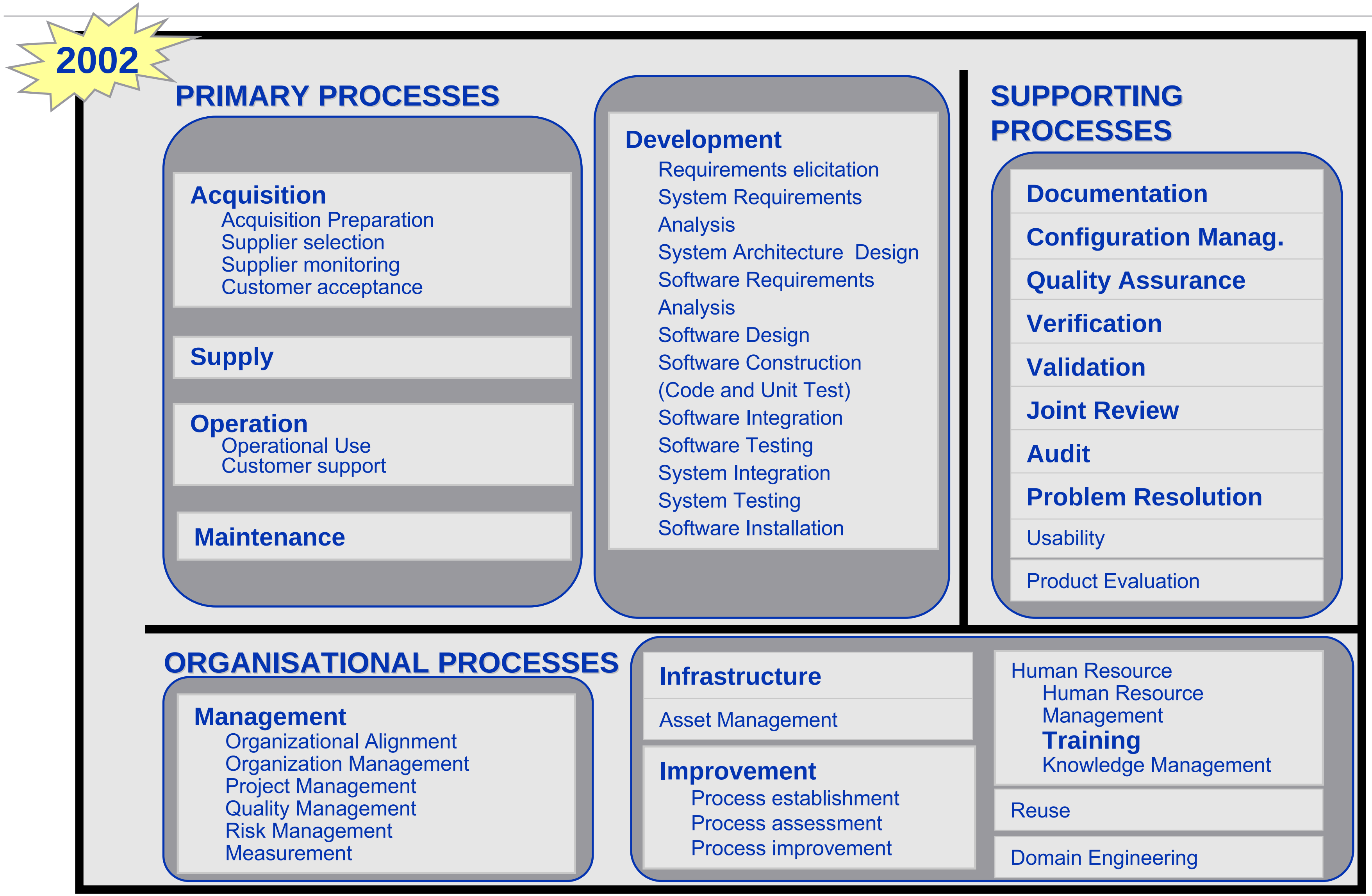
1998

Issues

2001

- 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

Process Reference Model – 12207 AMD1



2002

PRIMARY PROCESSES

Acquisition
- Acquisition Preparation
- Supplier selection
- Supplier monitoring
- Customer acceptance

Supply

Operation
- Operational Use
- Customer support

Maintenance

Development
- Requirements elicitation
- System Requirements Analysis
- System Architecture Design
- Software Requirements Analysis
- Software Design
- Software Construction (Code and Unit Test)
- Software Integration
- Software Testing
- System Integration
- System Testing
- Software Installation

SUPPORTING PROCESSES

Documentation

Configuration Manag.

Quality Assurance

Verification

Validation

Joint Review

Audit

Problem Resolution

Usability

Product Evaluation

ORGANISATIONAL PROCESSES

Management
- Organizational Alignment
- Organization Management
- Project Management
- Quality Management
- Risk Management
- Measurement

Infrastructure

Asset Management

Improvement
- Process establishment
- Process assessment
- Process improvement

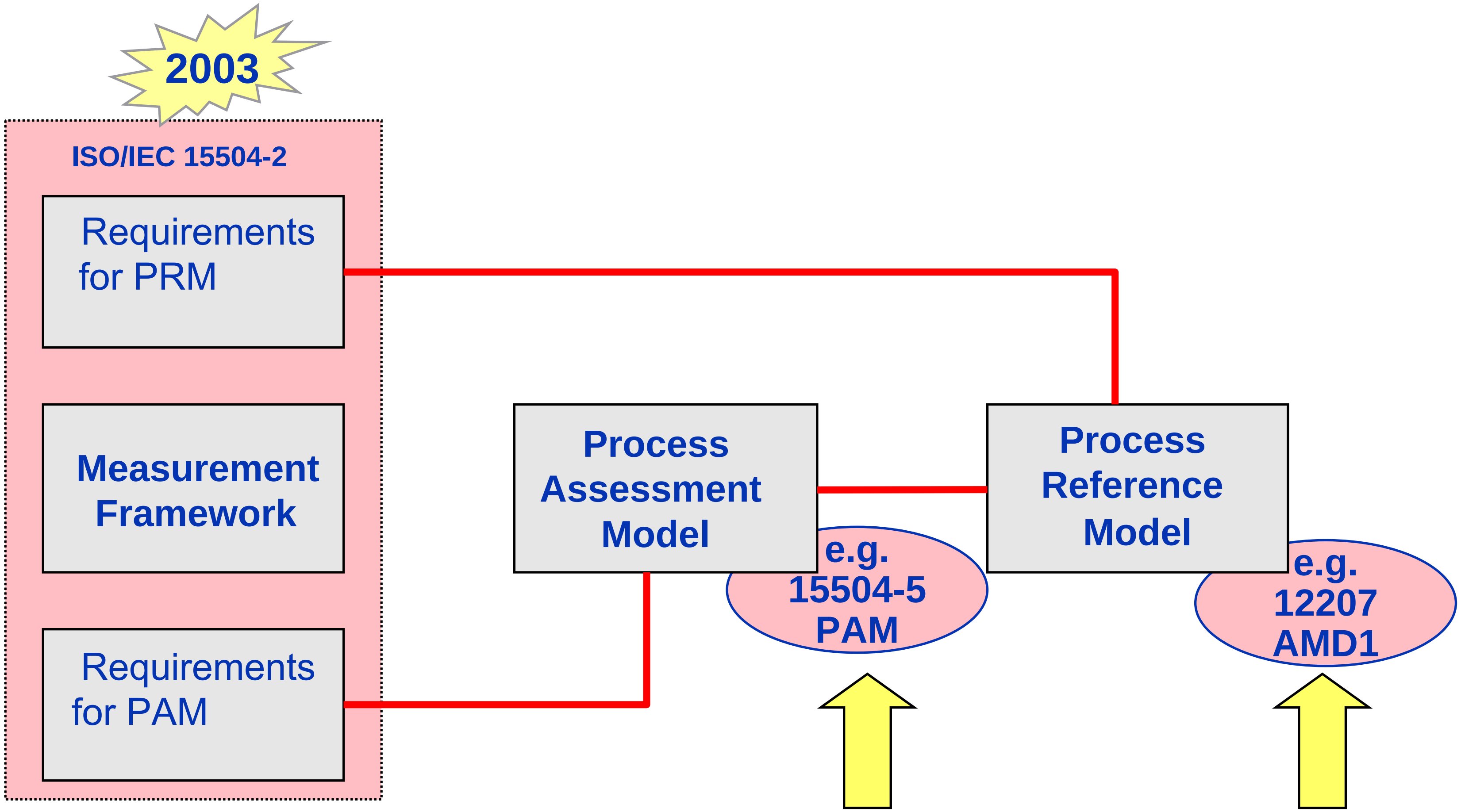
Human Resource
- Human Resource Management
- **Training**
- Knowledge Management

Reuse

Domain Engineering

ISO/IEC 15504 International Standard

MANAGING RISK



Linked PRM and PAM for Software Life Cycle Processes

Process Reference Model – 12207 AMD2

Acquisition

Acquisition preparation
Supplier selection
Contract agreement
Supplier monitoring
Product acceptance

Supply

Supplier tendering
Contract agreement
Product release
Product acceptance support

Engineering

Requirements elicitation
System requirements analysis
System architectural design
Software requirements analysis
Software design
Software construction
Software integration
Software testing
Software installation
System integration
System testing
System and software maintenance

2004

PRIMARY

Configuration Control

Documentation management
Configuration management
Problem resolution management
Change request management

Product Quality

Product evaluation

Quality Assurance

Quality assurance
Verification
Validation
Joint review
Audit

SUPPORTING

ORGANISATIONAL

Management

Organisational alignment
Organisational management
Project management
Quality management
Risk management
Measurement

Process Improvement

Process establishment
Process assessment
Process improvement

Resource and Infrastructure

Human resource management
Training
Knowledge management
Infrastructure

Reuse

Asset management
Reuse program management
Domain engineering

2005-2006

15504-5 (PAM)/Automotive SPICE/HIS scopes

MANAGING RISK

DNV

Management Process Group (MAN)

MAN.1 Organizational alignment
MAN.2 Organization management
A MAN.3 Project management
MAN.4 Quality management
A MAN.5 Risk management
A MAN.6 Measurement

Engineering Process Group (ENG)

A ENG.1 Requirements elicitation
A ENG.2 System requirements analysis
A ENG.3 System architectural design
A ENG.4 Software requirements analysis
A ENG.5 Software design
A ENG.6 Software construction
A ENG.7 Software integration
A ENG.8 Software testing
A ENG.9 System integration
A ENG.10 System testing
ENG.11 Software installation
ENG.12 Software and system maintenance

Supporting Process Group (SUP)

A SUP.1 Quality assurance
A SUP.2 Verification
SUP.3 Validation
A SUP.4 Joint review
SUP.5 Audit
SUP.6 Product evaluation
A SUP.7 Documentation
A SUP.8 Configuration management
A SUP.9 Problem resolution management
A SUP.10 Change request management

The Acquisition Process Group (ACQ)

ACQ.1 Acquisition preparation
ACQ.2 Supplier selection
A ACQ.3 Contract agreement
A ACQ.4 Supplier monitoring
ACQ.5 Customer acceptance
A ACQ.11 Technical requirements
A ACQ.12 Legal and administrative requirements
A ACQ.13 Project requirements
A ACQ.14 Request for proposals
A ACQ.15 Supplier qualification

Resource & Infrastructure Process Group (RIN)

RIN.1 Human resource management
RIN.2 Training
RIN.3 Knowledge management
RIN.4 Infrastructure

Operation Process Group (OPE)

OPE.1 Operational use
OPE.2 Customer support

Supply Process Group (SPL)

A SPL.1 Supplier tendering
A SPL.2 Product release
SPL.3 Product acceptance support

Process Improvement Process Group

PIM.1 Process establishment
PIM.2 Process assessment
A PIM.3 Process improvement

Reuse Process Group (REU)

REU.1 Asset management
A REU.2 Reuse program management
REU.3 Domain engineering

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

SUPPORTING

Support

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

2005

ORGANISATIONAL

Management

Project management
Risk management
Measurement

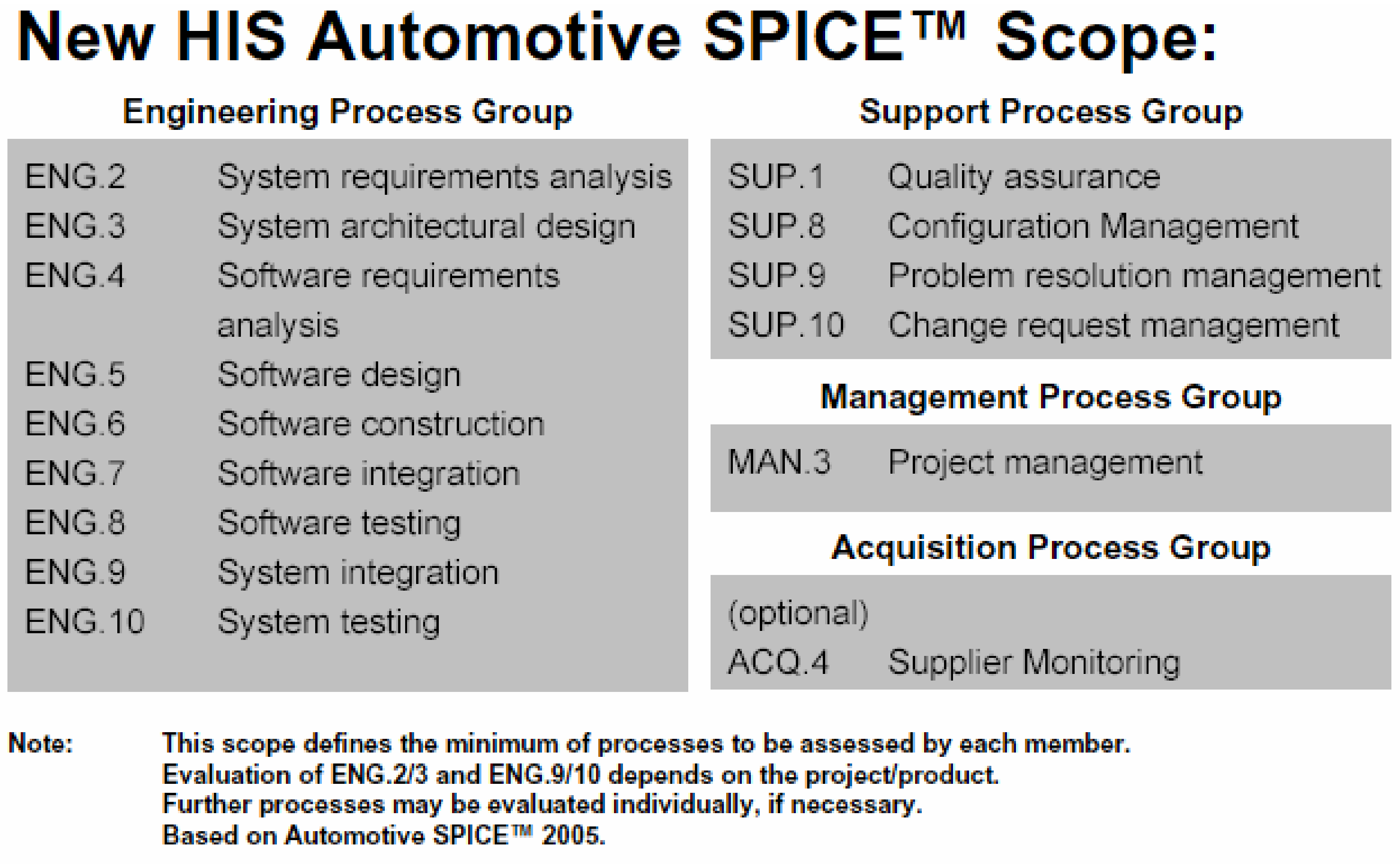
Process Improvement

Process improvement

Reuse

Reuse program management

2006



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

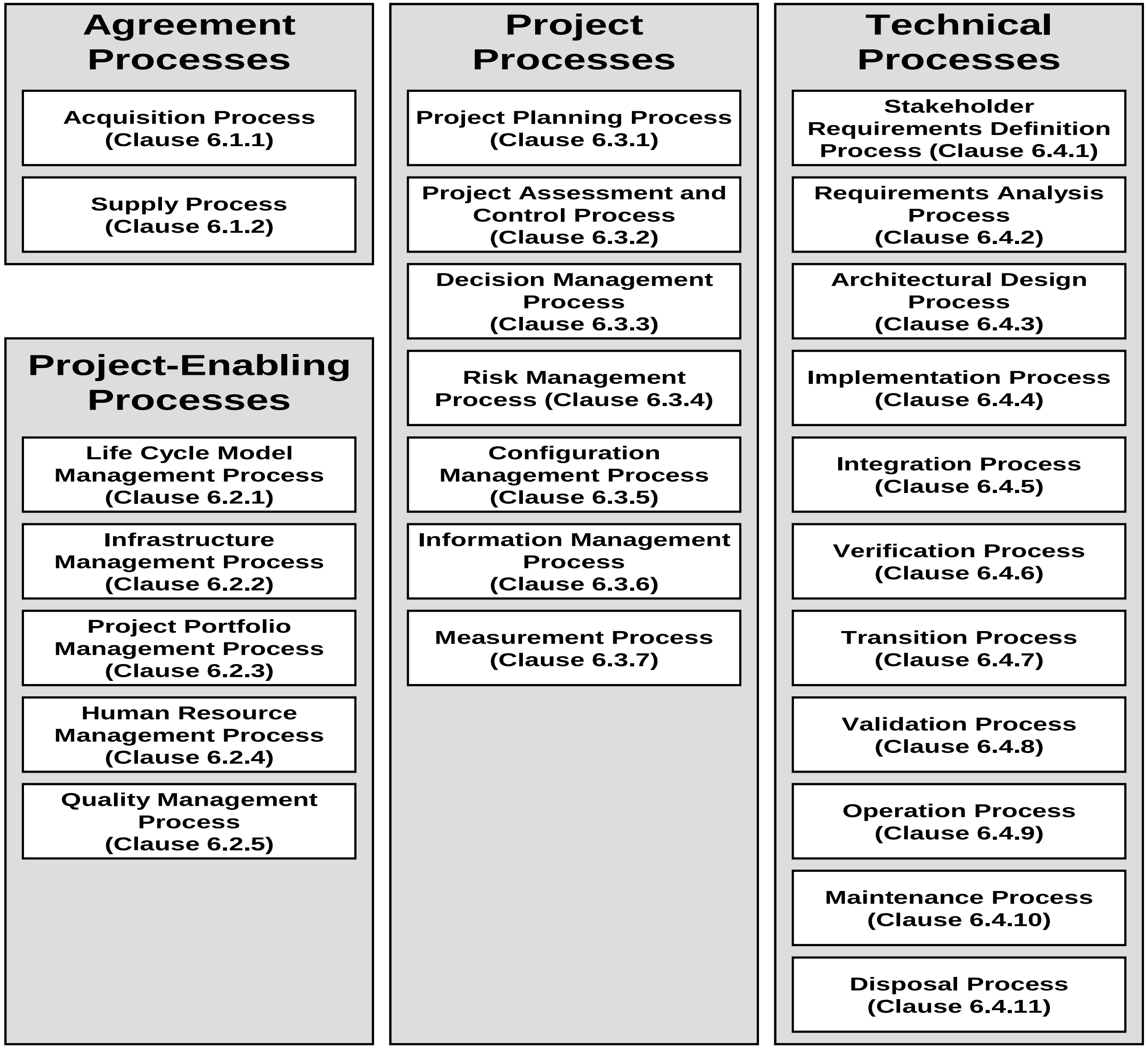
Note: **This scope defines the minimum of processes to be assessed by each member.**
Evaluation of ENG.2/3 and ENG.9/10 depends on the project/product.
Further processes may be evaluated individually, if necessary.
Based on Automotive SPICE™ 2005.

ISO/IEC 15288

MANAGING RISK

System Life Cycle Processes

2002



Agreement Processes

- Acquisition Process (Clause 6.1.1)
- Supply Process (Clause 6.1.2)

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)

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)

Structure of ISO/IEC 15288

2002

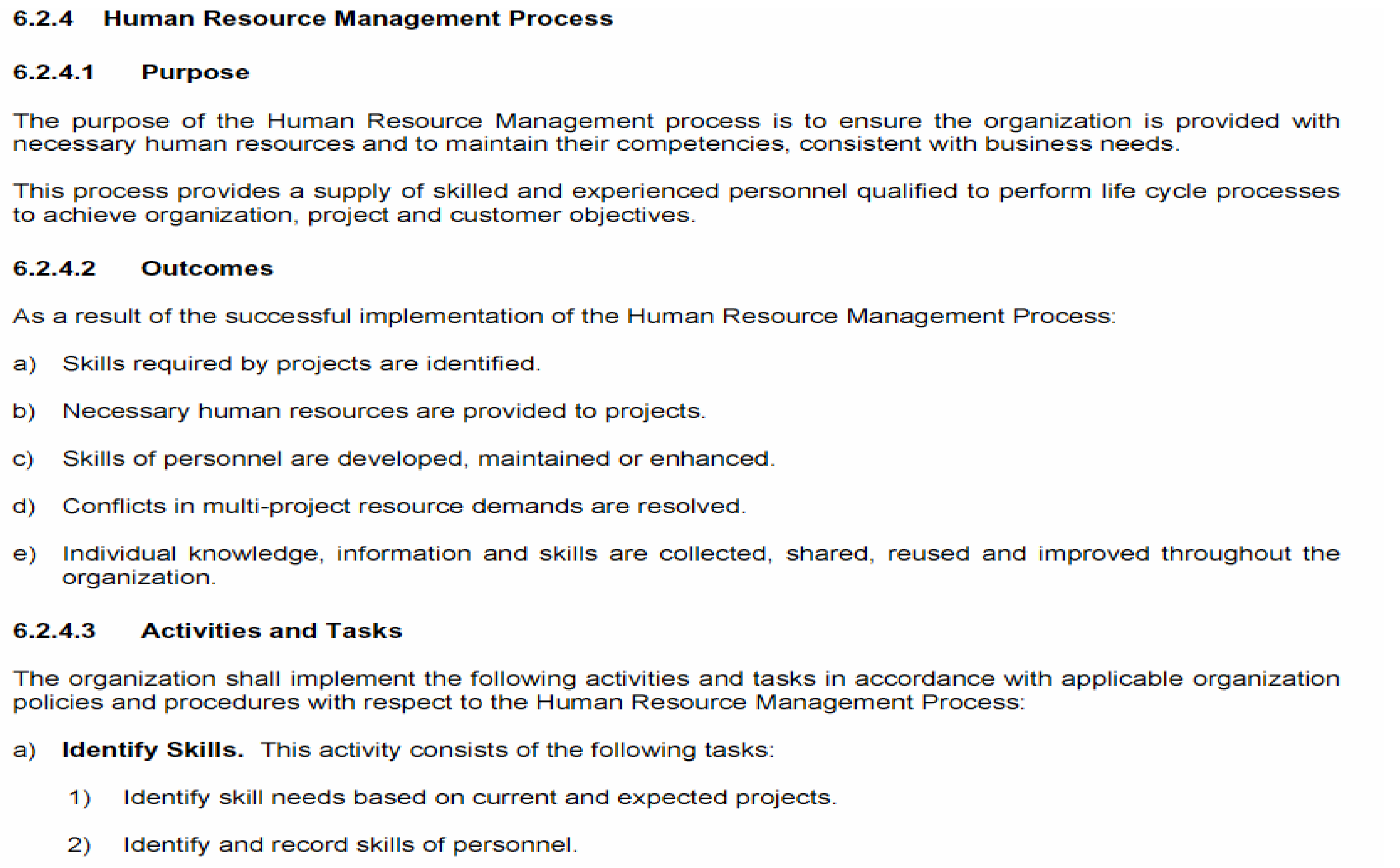
PRM
Process
Reference
Model

- 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.

Conformity Requirements

- 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:

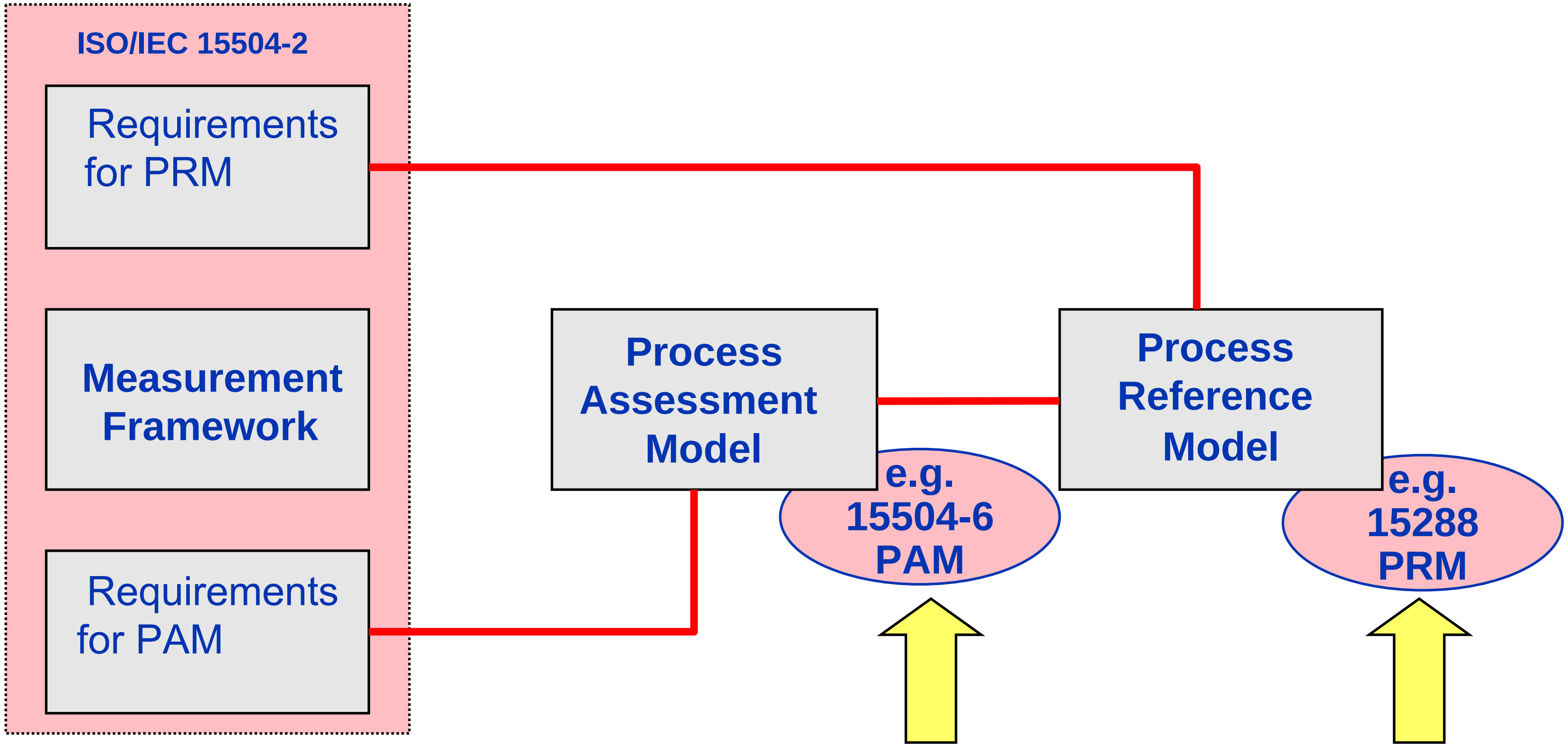
a) **Identify Skills.** This activity consists of the following tasks:

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

2) Identify and record skills of personnel.

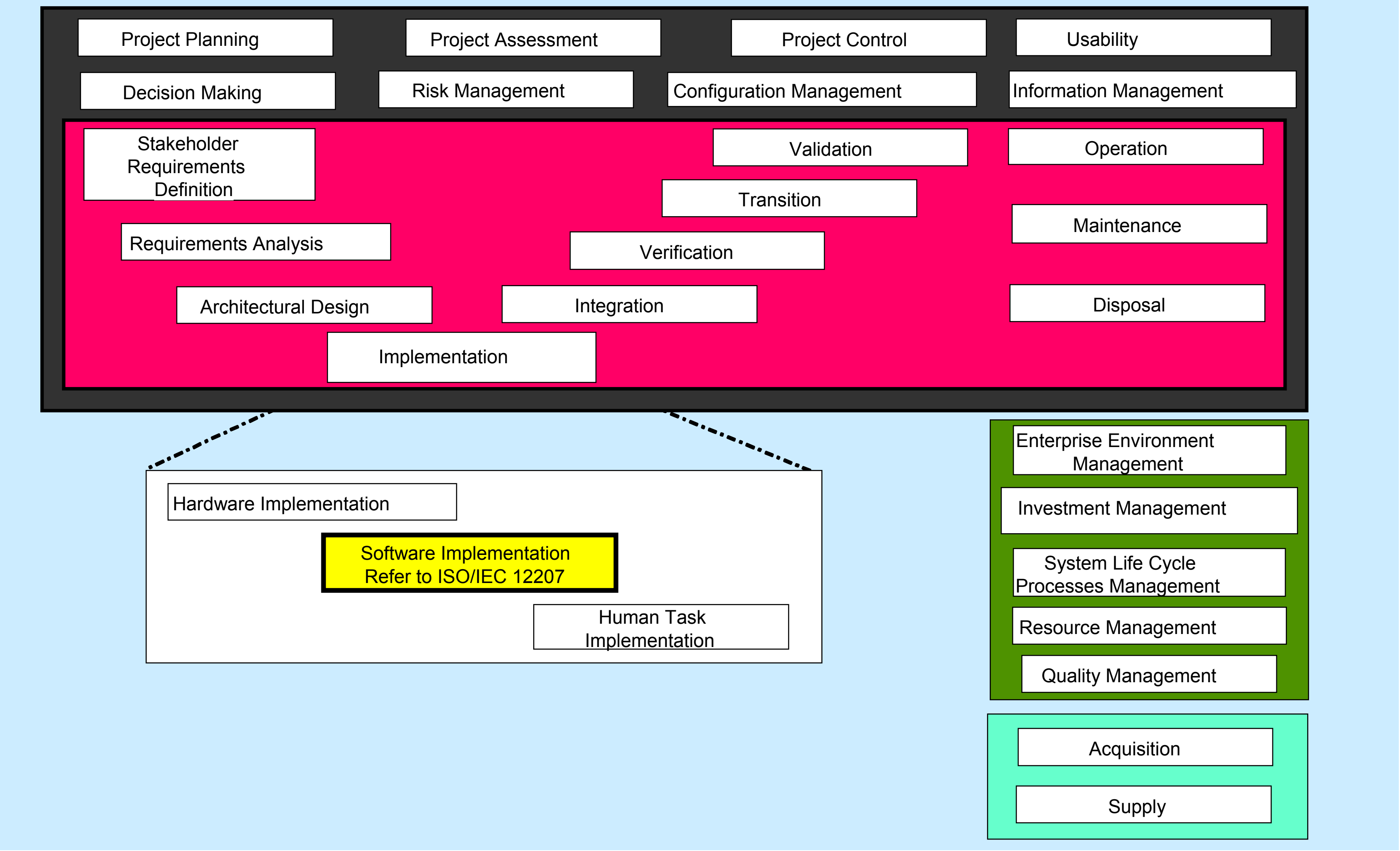
ISO/IEC 15504 applied on 15288

MANAGING RISK DNV



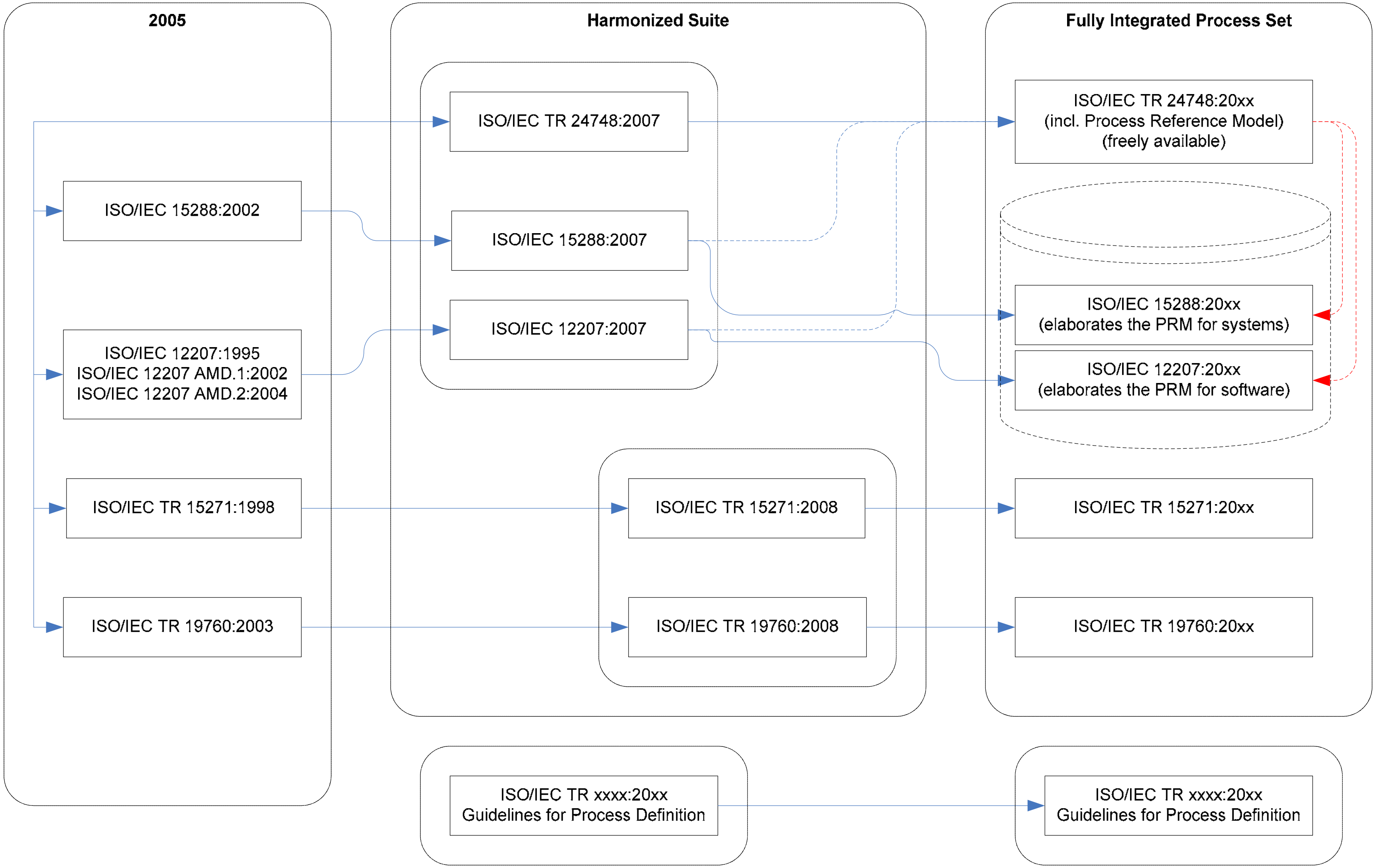
Linked PRM and PAM for **System** Life Cycle Processes

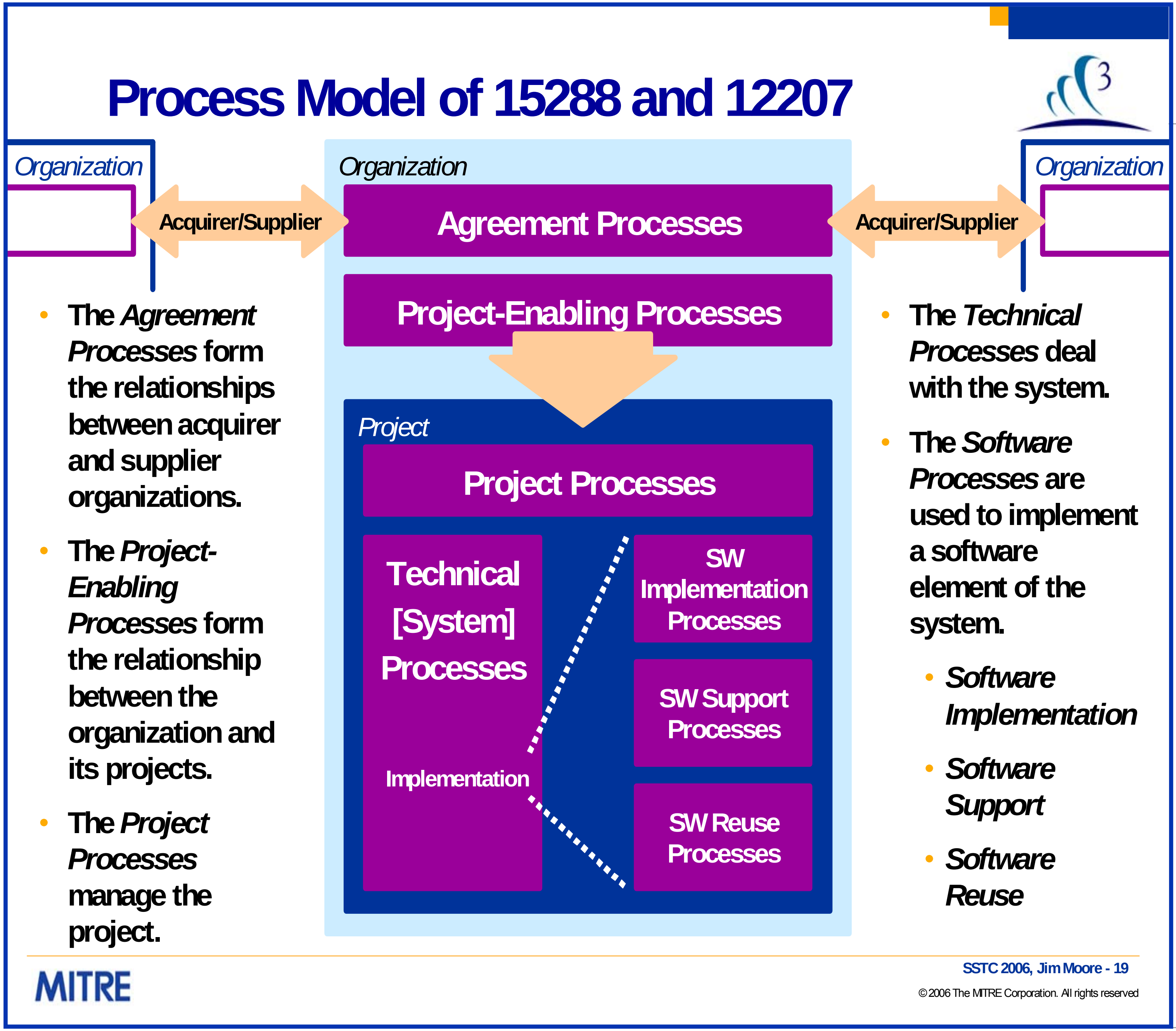
ISO/IEC 15288 – Relationship with ISO/IEC 12207



Harmonization 12207 - 15288

MANAGING RISK





Process Model of 15288 and 12207

- The *Agreement Processes* form the relationships between acquirer and supplier organizations.
- The *Project-Enabling Processes* form the relationship between the organization and its projects.
- The *Project Processes* manage the project.

Organization

Acquirer/Supplier

Organization

Agreement Processes

Project-Enabling Processes

Project

Project Processes

Technical [System] Processes

Implementation

SW Implementation Processes

SW Support Processes

SW Reuse Processes

Acquirer/Supplier

Organization

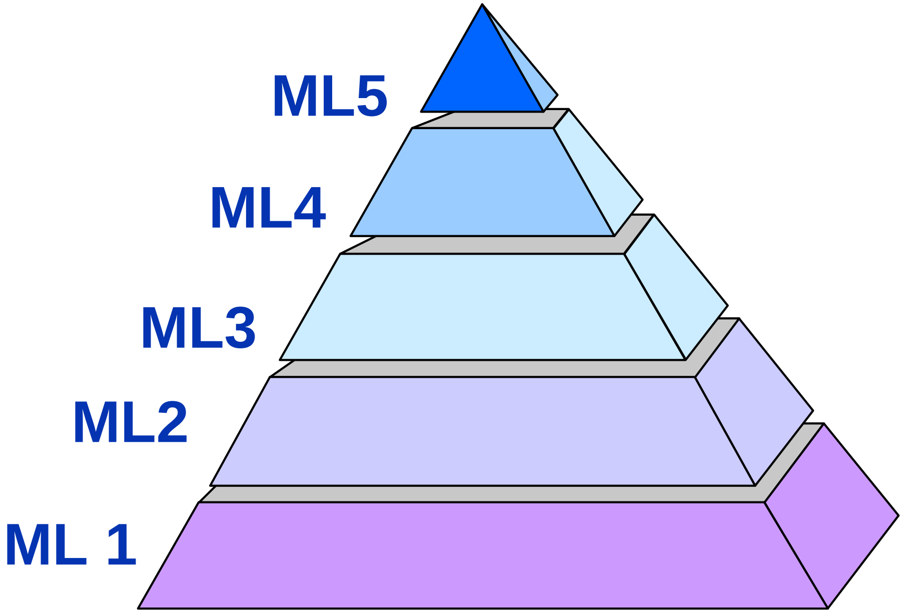
- The *Technical Processes* deal with the system.
- The *Software Processes* are used to implement a software element of the system.
  - *Software Implementation*
  - *Software Support*
  - *Software Reuse*

MITRE

SSTC 2006, Jim Moore - 19

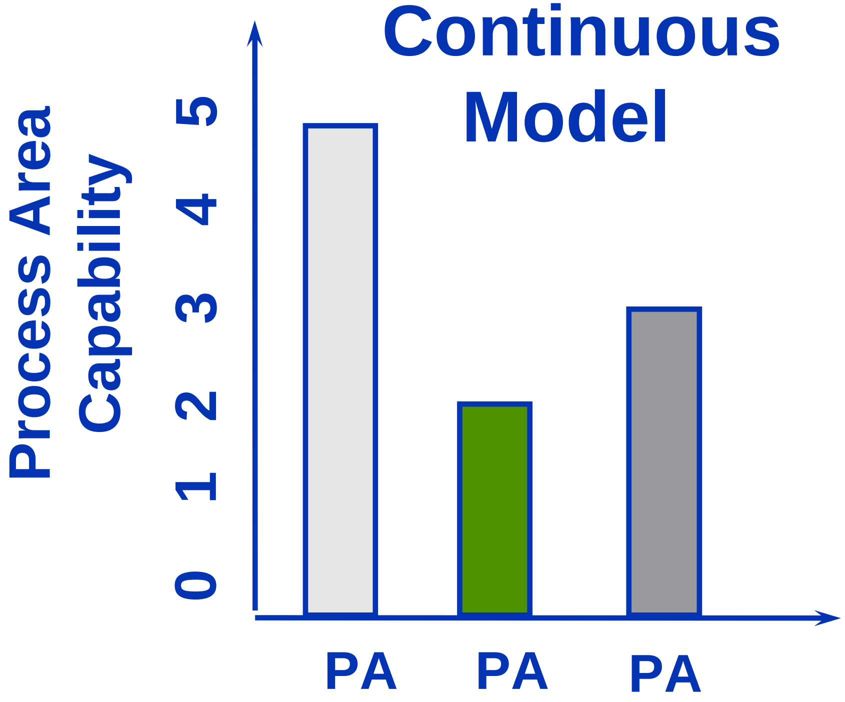
Process Assessment Models in CMMI

Staged Model



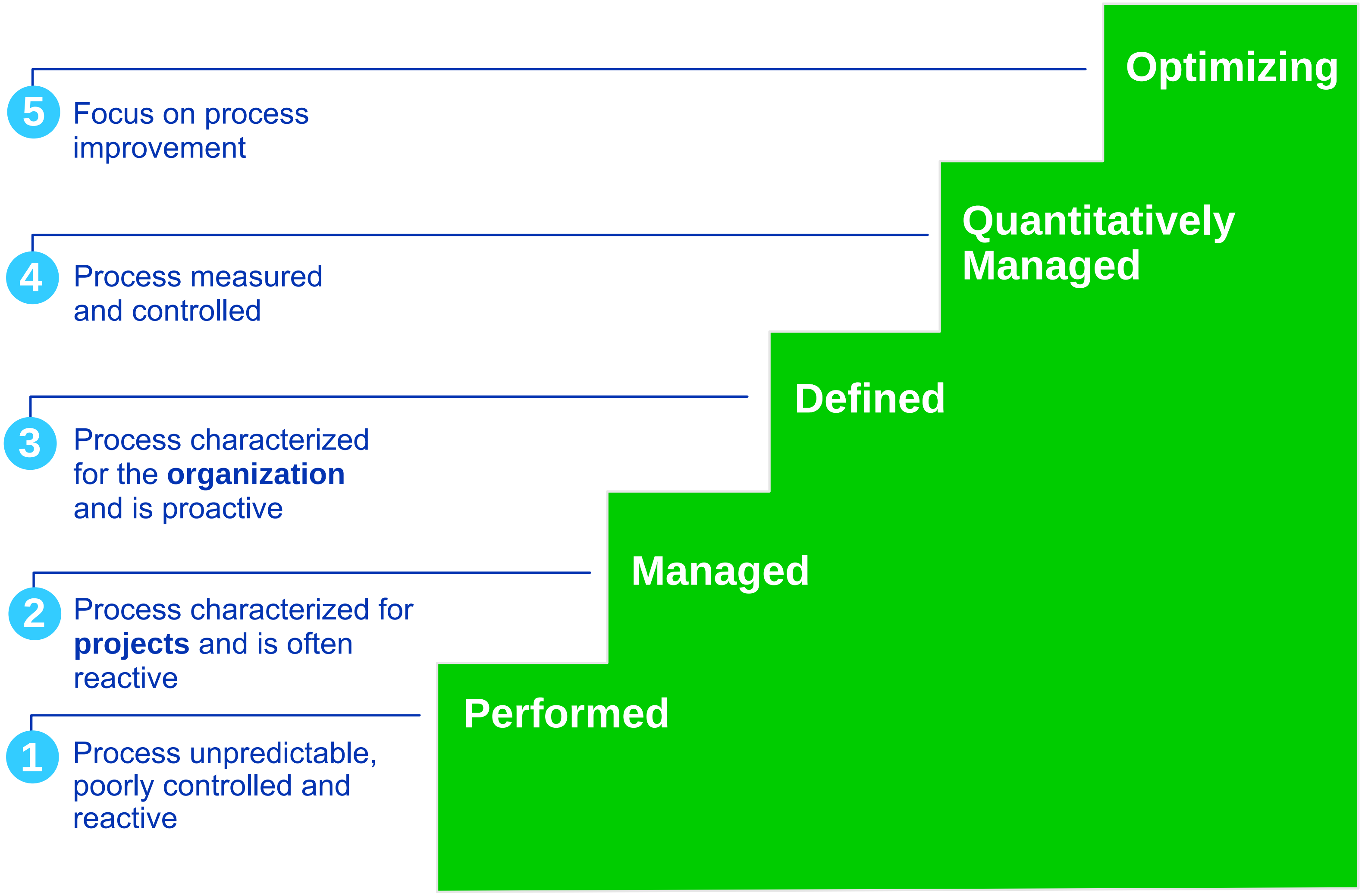
. . .for an established set of process areas across an organization

Continuous Model



. . .for a single process or Process area

The CMMI Maturity Levels (staged)



5 Focus on process improvement — **Optimizing**

4 Process measured and controlled — **Quantitatively Managed**

3 Process characterized for the **organization** and is proactive — **Defined**

2 Process characterized for **projects** and is often reactive — **Managed**

1 Process unpredictable, poorly controlled and reactive — **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

Functional Safety ISO 26262 Future Automotive Standard

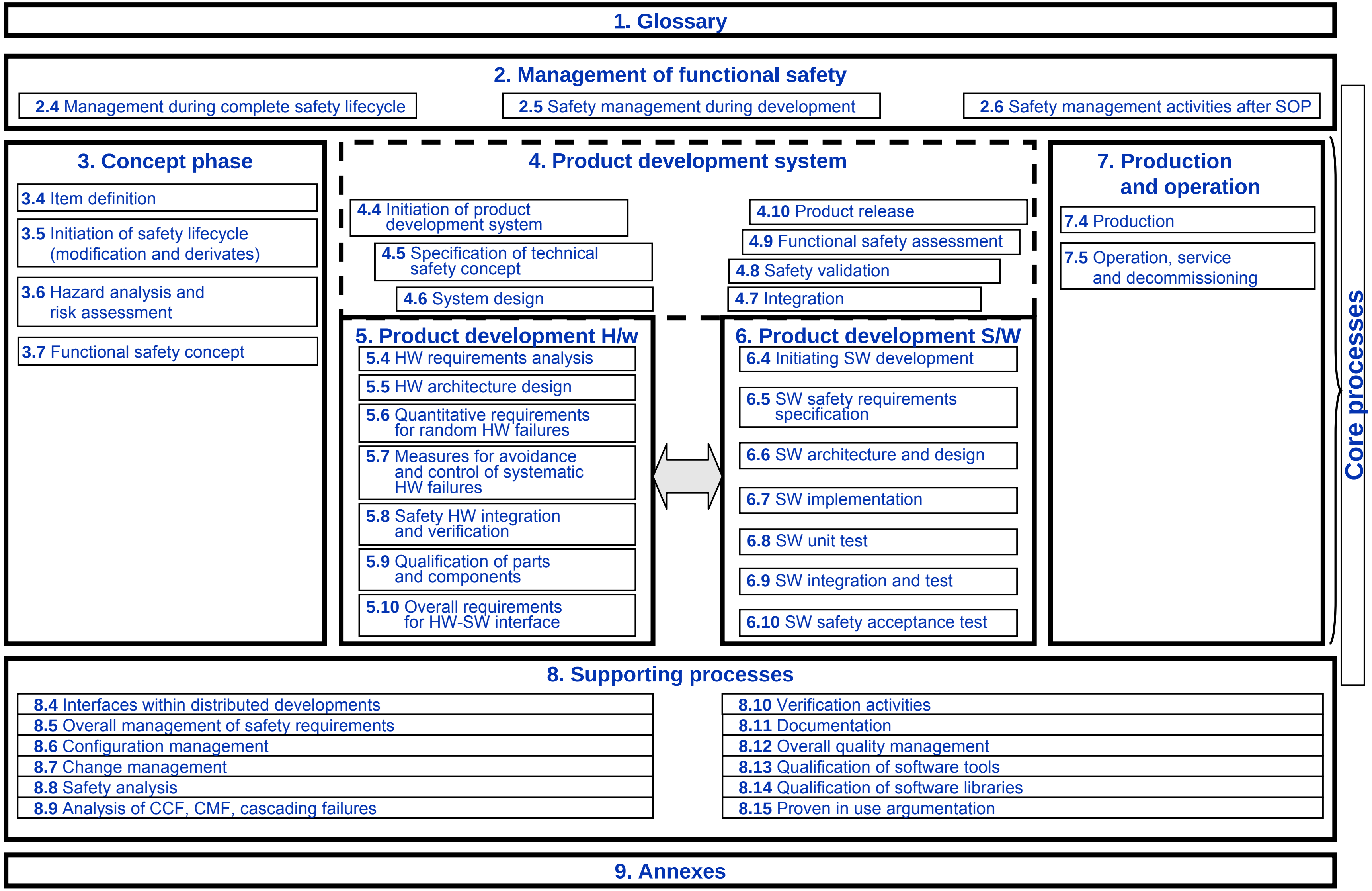
- 2004: National initiatives by FAKRA (G) and BNA (Fr)

- 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

Functional Safety ISO 26262 Future Automotive Standard

MANAGING RISK



1. Glossary

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
- **4.7** Integration
- **4.8** Safety validation
- **4.9** Functional safety assessment
- **4.10** Product release

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

Core processes

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

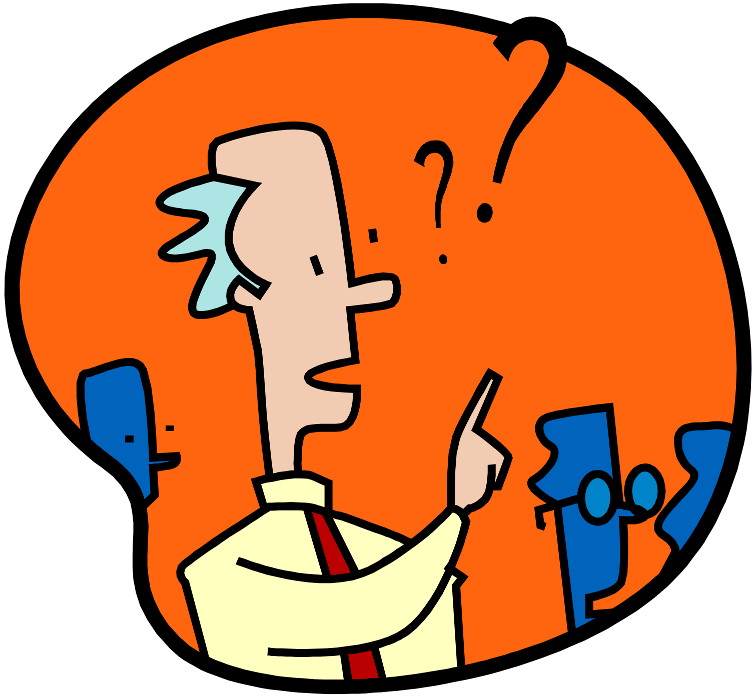
9. Annexes

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 ?

MANAGING RISK DNV



Questions ?