MANAGING RISK DNV

DNV IT Global Services

Enhancing Trust and Confidence in IT

Integrating the safety & security application area into a process assessment: first findings

Thierry Coq
Industry Department Manager, France
thierry.coq@dnv.com

Q-Labs *Echelon* Tireno CIBIT strengthening DNV

Integrating the safety & security application area (SSA) into a process assessment: first findings

MANAGING RISK DNV

- The automotive software market
- The Safety & Security Application Area
- Choices for Integration into the CMMI For Development, Version 1.2
- Impacts on Assessment Process Implementation in a first application to the Automotive Industry
- Open Issues
- Conclusion
- Bibliography

Integrating the SSA into a process assessment: The automotive software market

MANAGING RISK DNV

- Very high numbers, millions of vehicles produced per year,
- Embedded software of very high target reliability and/or high integrity
- High reuse from within vehicle models and series, many suppliers
- Limited development lead time (18 months ECU development time and decreasing)
- High versatility of requirements / specification freeze often late in the development : flexibility against market
- Increased complexity of software, added value in the software:
  - Mercedes: in 2000, described the software added value as up to 30% in vehicles in the coming years,
  - Mercer: «The cost for developing software is likely to raise from 4% of the total vehicle cost in 2002 up to 13% in 2010»
  - S. Stefans, IBM Corp: «Automakers are currently spending between 2 and 3 billion $ fixing software bugs»
  - Detroit News 18/05/2005: «32% warranty costs in U.S. are for software or related issues»

⇨ High concerns for the capability of processes for producing automotive software, including reliability and safety.

CMMI Process Areas by Category

MANAGING RISK DNV

Where is Safety?

Project Management	Project Planning (PP) Project Monitoring and Control (PMC) Supplier Agreement Management (SAM) Integrated Project Management (IPM) +IPPD Risk Management (RSKM) Quantitative Project Management (QPM)
Support	Configuration Management (CM) Process and Product Quality Assurance (PPQA) Measurement and Analysis (MA) Decision Analysis and Resolution (DAR) Causal Analysis and Resolution (CAR)
Engineering	Requirements Management (REQM) Requirements Development (RD) Technical Solution (TS) Product Integration (PI) Verification (VER) Validation (VAL)
Process Management	Organizational Process Focus (OPF) Organizational Process Definition (OPD) +IPPD Organizational Training (OT) Organizational Process Performance (OPP) Organizational Innovation and Deployment (OID)

Integrating the SSA into a process assessment: A Rationale For Adding a Safety Area

MANAGING RISK DNV

- CMMI is a generic set of process areas for assessment and improvement covering:
  - Standard process and project management processes
  - Generic Support processes,
  - Generic Engineering processes in a V-Lifecycle (from Requirements Development to Validation)
- However within this framework:
  - Specific safety or security practices are not addressed,
  - Safety within the model is treated as « for information only »
  - Guidance for applying the model in a Safety or Security context is judged not to be sufficient
  - Safety or Security regulations and standards are not taken into account

⇨ one or more additional areas are needed to address the safety issues, using the same goal and practice based strategy,

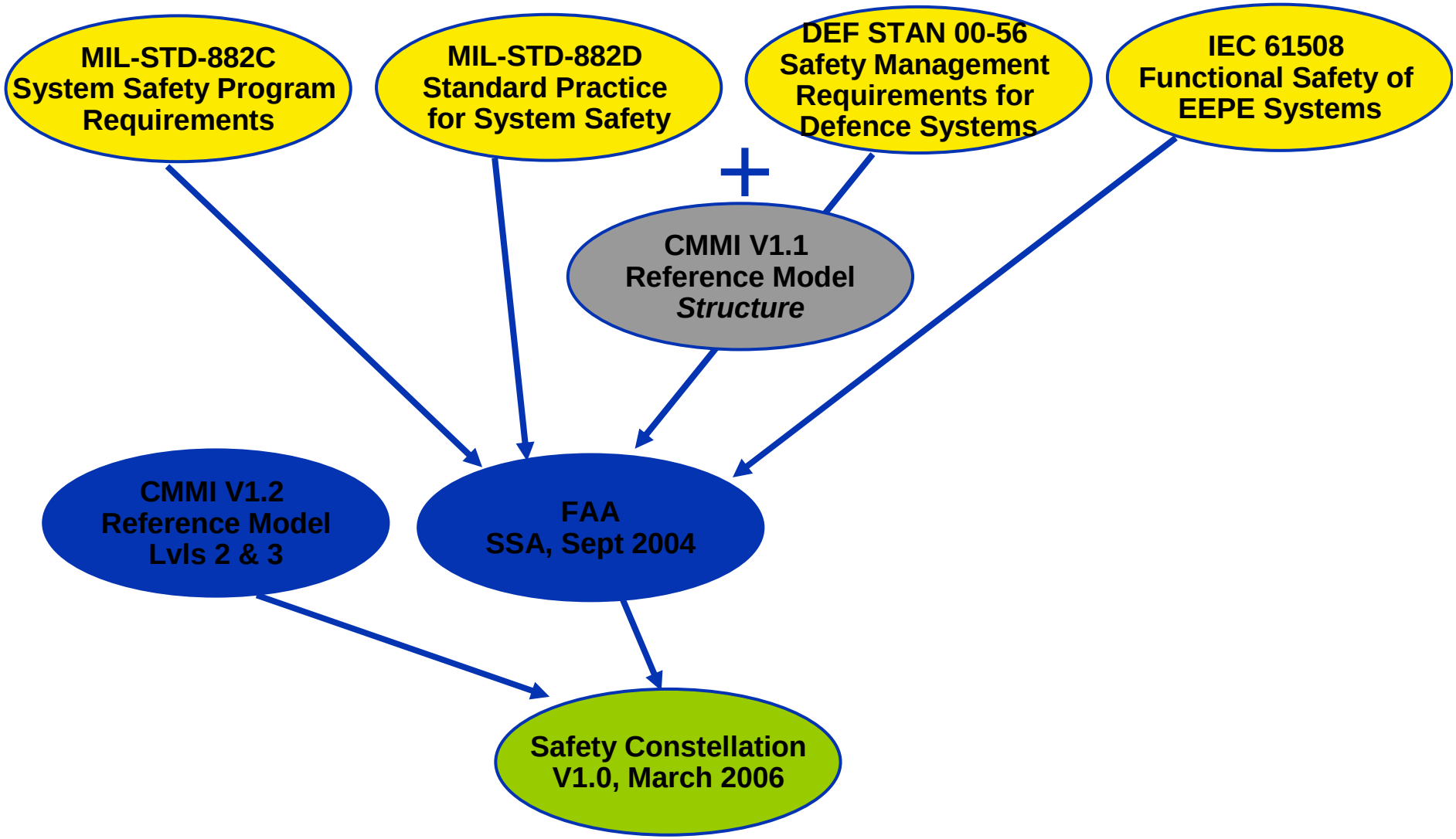
Integrating the SSA into a process assessment: A Rationale For Adding a Safety Area (2)

MANAGING RISK DNV

- SSA Main Objectives:
  - **Visible**: Safety and Security Concerns are first-class citizens
  - **Credible**: Created by a body of recognized expert organizations in the field of safety & security, FAA, MoD, DOD
  - **Compliant**: the SSA presents itself using goals, practices and disciplines
  - **Extends CMMI**: no changes are required to the CMMI model
  - **Assessable**: Safety and security practices are assessable, as other CMMI process areas.
  - **Improvable**: Safety and security practices are improvable, as other CMMI process areas.
  - **Long-lived**: Safety & security practices do not depend on a particular, prescription-based, standard or regulation

Integrating the SSA into a process assessment: Safety Constellation Genealogy

MANAGING RISK DNV



Integrating the SSA into a process assessment: The Safety Constellation: CMMI + SSA

MANAGING RISK DNV

- No changes to the CMMI Model
  - Compliant with the SEI model
- Safety and Security Application Area:
  - Little changes to harmonize the SSA practices and goals numbering to the CMMI model
  - Compliant with the original FAA model
- The Safety Constellation slightly reorganizes the Maturity Levels to take into account the Automotive concerns (it is a capability model):
  - VER (Verification) is moved from level 3 to level 2
    - In order to require verification practices from suppliers, and from vehicle manufacturers,
    - In order to provide a consistent set of process areas from the lifecycle point of view
  - A level 2+ is introduced:
    - Additional process areas at capability level 2: RD, TS, PI, VAL
    - SSA (Safety and Security Application Area) is introduced at CL2
    - Provides an intermediate maturity level easier to achieve
    - Provides an intermediate capability for suppliers and manufacturers
    - Provides a consistent baseline for supporting safety concerns
  - Other levels are identical
- This is NOT currently a SEI-approved Constellation.

Integrating the SSA into a process assessment: Safety & Security Application Area Purpose

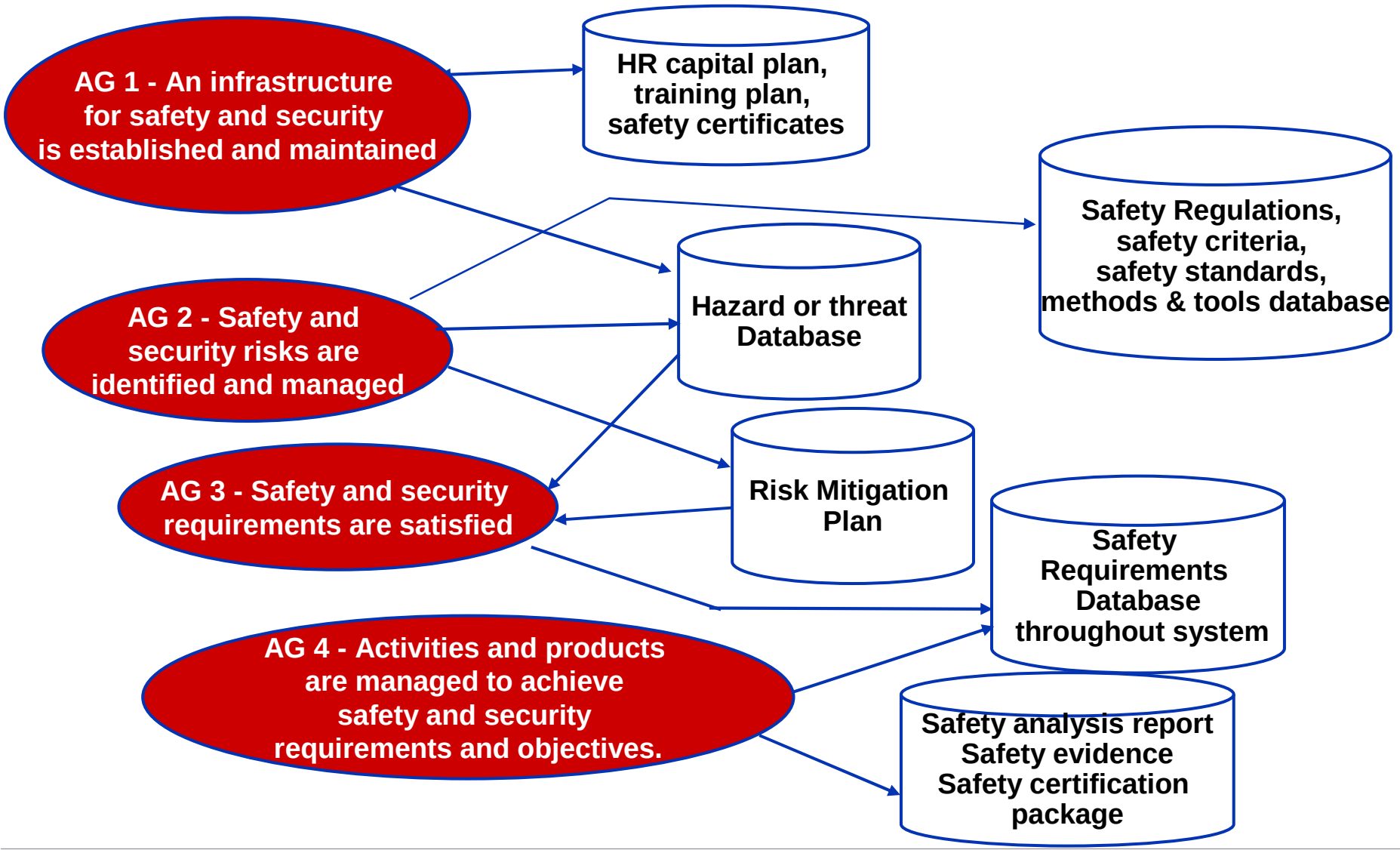
MANAGING RISK DNV

The purpose of the Safety and Security Application Area is:

- to establish and maintain a *safety* and *security capability*,
- define and manage *requirements* based on risks attributable to *threats*, *hazards* and *vulnerabilities*,
- and assure that products and services are *safe* and *secure* throughout their *life cycle*.

Integrating the SSA into a process assessment: SSA Goals and typical work products

MANAGING RISK DNV



Integrating the SSA into a process assessment: Application to the Automotive Industry

MANAGING RISK DNV

- The information provided here is of course limited to the assessment process for obvious reasons: no assessment results will be displayed

- Assessments have been conducted using the assessment process as described, in 2006, for Renault:
  - Scope: level 2 + Selected Process Areas at level 3 : RD, VER, VAL,
  - Includes Safety,
  - Non-official Assessments have been conducted within the vehicle vendor,
    - Scope: Electronic Equipment Acquisition, several projects
  - Non-official Assessments have been conducted within suppliers in the automotive industry
    - Scope: Electronic Equipment Development, several projects.

Integrating the SSA into a process assessment: Assessment Activities

MANAGING RISK DNV

Adaptations to the Assessment process and tools to integrate the SSA:

Phase 1: Preparing

- Decision
- Planning
- Training
- Team building
- Participants briefing
- Questionnaires
- Preliminary document review

Phase 2: Assessing

- Documents
- Opening session
- Interviews
- Demos
- Notes taking
- Consolidation
- Review with consensus
- Rating
- Risk Analysis

Phase 3: Reporting

- Results presentation
- Closing session
- Sponsor debriefing
- Archiving
- Destroy notes and confidential documents

Integrating the SSA into a process assessment: Application to the Automotive Industry (1)

MANAGING RISK DNV

- Assessment planning, training and team building:
  - Preparation duration:
    - 3 months to interview the sponsor(s), define the scope, build and train the team, prepare the process and the assessment materials, gather the documents
  - Training required:
    - 5 days for each assessor (3 days Safety Constellation, 2 days Assessment Process),
    - Including 2 hours for the SSA application area
  - Assessment Onsite duration:
    - Between 3 days and a week per site for several projects of one ECU Type
    - Including several interviews with safety-related questions
    - Interviews between ½ hour and 1 and ½ hours, depending on role and number of interviewees
    - a 1-hour final findings presentation
    - a 2-hour debriefing for the management (vehicle manufacturer, supplier)

Integrating the SSA into a process assessment: Application to the Automotive Industry (2)

MANAGING RISK DNV

- Team Structure has been adapted to take into account safety concerns
- A Team of 4 assessors has been assembled for the assessments. Up to 6 people may be required for a full Level 3 scope
- Assessment Leader: responsible for the assessment process and the consistency of assessment results
  - Experienced, 20 years of experience in software development,
  - Experienced in leading CMMI-based assessments,
  - From an independent trustworthy third-party organization;
- Assessment Team Members:
  - Experienced, 6 to 15 years of experience in software development,
  - Trained to the Safety Constellation, to the assessment process,
  - Included one or two members from the target organizations, vehicle vendor and supplier
  - At least one team member had experience in safety issues.

Integrating the SSA into a process assessment: Application to the Automotive Industry (3)

MANAGING RISK DNV

- Document Lists (for gathering purposes):
  - Included typical work products from the SSA, such as:
    - Safety plan, safety activity schedule, Safety requirements, Safety Risk List, Feared Events, Safety Arguments, Safety Test Plan, etc.
- Questionnaires and Interviews:
  - Included safety-related open questions for :
    - Programme and Project Software Managers, Quality Personnel, Safety Personnel, Testers, etc.
- Consolidation sheets and ratings:
  - Included the SSA practices and the SSA goals

Integrating the SSA into a process assessment: Application to the Automotive Industry (4)

MANAGING RISK DNV

- Scope has been defined based on business objectives, particularly risk mitigation
- Organizational scope: Software
  - One ECUs types (Electronic Control Units)
  - Several ECUs projects
  - Vehicle manufacturer and supplier: both
  - Several sites in Europe
- Process scope:
  - Standard Level 2 for standard embedded software with no particular integrity or reliability levels,
  - Level 2+ for high reliability or average integrity embedded software, within ECUs,
  - Level 3 for high-risk, high-reliability and high integrity embedded software.
- Interviews and Questionnaire:
  - Adapted for specific automotive context (regulations and laws, state of the art, acceptable safety levels, etc.)

Integrating the SSA into a process assessment: Application to the Automotive Industry

MANAGING RISK DNV

- Assessment results are built upon the assessment's team consensus
- Assessment results:
  - Strengths and opportunities to improve
    - per process area
    - Specifically for the Safety Practices,
    - Overall,
  - Goal and practice ratings,
  - Organizational Risks
  - Recommendations
- Reviewed with management and sponsor has improved buy-in.
  - Generally, the assessment are well perceived, are said to be performed in-depth,
  - Results are regarded as fair, a true picture of the strengths and opportunities to improve of the assessed organizations.

REQM	PP	PMC	SAM	MA	PPQA	CM	SSA
-	-	-	-	-	-	-	+
NI	NI	NI	NI	NI	NI	NI	LI
	NI	NI	NI	NI	NI	NI	LI
	NI					NI	LI
							LI
NI	NI	NI	NI	NI	NI	NI	LI
NI	NI	NI	NI	NI	NI	NI	LI

		Impact		
		High	Medium	Low
Probability	Highly	D, G	F,	I
	Average	H,J	C, E	B
	Little			A

Integrating the SSA into a process assessment: First Assessments Results

MANAGING RISK DNV

- The changes to CMMI and to the assessment or improvement processes are few and easily taken into account.
- This safety constellation has been used to effectively identify strengths and opportunities to improve in Safety processes in first pilot projects in the Automotive Industry. The absence of SSA would not have permitted to identify such items.
- A stringent assessment process such as SEI's SCAMPI is required to make the best use of the constellations' features.

Integrating the SSA into a process assessment: Open Issues

MANAGING RISK DNV

- There are no product requirements in the SSA, which makes it usable in any context, but needs to be completed by product requirements for the automotive context.
- The SSA is not a safety certificate of a given product or set of products
  - In the same manner as for CMMI which is used to assess process capability of organizations, not of individual projects.
- In some cases, the interpretation of SSA may require expert knowledge of the subject field. To be obtained before an assessment. For example:
  - AP 01.09: Determine Regulatory Requirements, Laws, and Standards:
    - Has the state of the art applicable been identified?
    - Have the laws applicable for a process leading to products that may be used in several countries been identified?
  - AP 01.13: Establish Independent Safety and Security Reporting
    - How independent is independent, in the context?
  - AP 01.10: Develop and Deploy Safe and Secure Products and Services
    - How acceptable is an acceptable safety level, in the context?

Conclusion

MANAGING RISK DNV

- The SSA meshes efficiently into the CMMI framework to create a composite constellation to assess both generic and safety-related processes.
- Assessing safety processes is NOT a safety certificate:
  - It is NOT compliance of full ISO/IEC 61508 or WD 26262 others,
  - It IS however an assessment of the process requirements of such standards .
- Next steps:
  - Integrating SSA in Official Scampi Assessments,
  - Integrating Joint Process/Product Safety Assessments.

Bibliography

- CMMI For Development, Version 1.2, 25/8/2006
- *Safety and Security Extensions For Integrated Capability Maturity Models* Linda Ibrahim et al, FAA, September 2004
- Experience with Extending CMMI for Safety-Related Applications http://www.itee.uq.edu.au/~defsafe/Publications/INCOSE2002.pdf
- +SAFE, V1.2 A Safety Extension to CMMI-DEV, V1.2, http://www.sei.cmu.edu/pub/documents/07.reports/07tn006.pdf, March 2007

Thank You

Questions?

thierry.coq@dnv.com