

Safety Management im ATM

22. STEV-Österreich Fachtagung
2007-05-11
Susanne Lanzerstorfer

APAC

Your Service Provider for Success

2007-05-11, Susanne Lanzerstorfer

APA-PHO-AP0AUP-1.0b-0_Safety_in_ATM

1

AGENDA

- Einführung
- Safety Management in ATM (Air Traffic Management)
- Software Safety
- Safety und ISO/IEC 61508 bzw. SPICE

APAC

Your Service Provider for Success

2007-05-11, Susanne Lanzerstorfer

APA-PHO-AP0AUP-1.0b-0_Safety_in_ATM

2

Einführung

- Schwerpunkte der Fa. APAC
 - Projekt Management
 - Safety Management
 - Qualitäts- und Konfigurationsmanagement
 - Single European Sky Implementierung
- Aktuelle Projekte (Beispiele)
 - ECRA
 - NAV Canada
 - Slovenia Control

APAC

Your Service Provider for Success

2007-05-11, Susanne Lanzerstorfer

APA-PHO-AP0AUP-1.0b-0_Safety_in_ATM

3

Safety Management im ATM

- Aufgaben der Flugsicherung (ATM)
- Aufgaben des Safety Managements im ATM Kontext
- Rahmenbedingungen
- Geltungsbereich des Safety Managements
 - Gesamter Lebenszyklus
 - „People, Procedure and Equipment“

APAC

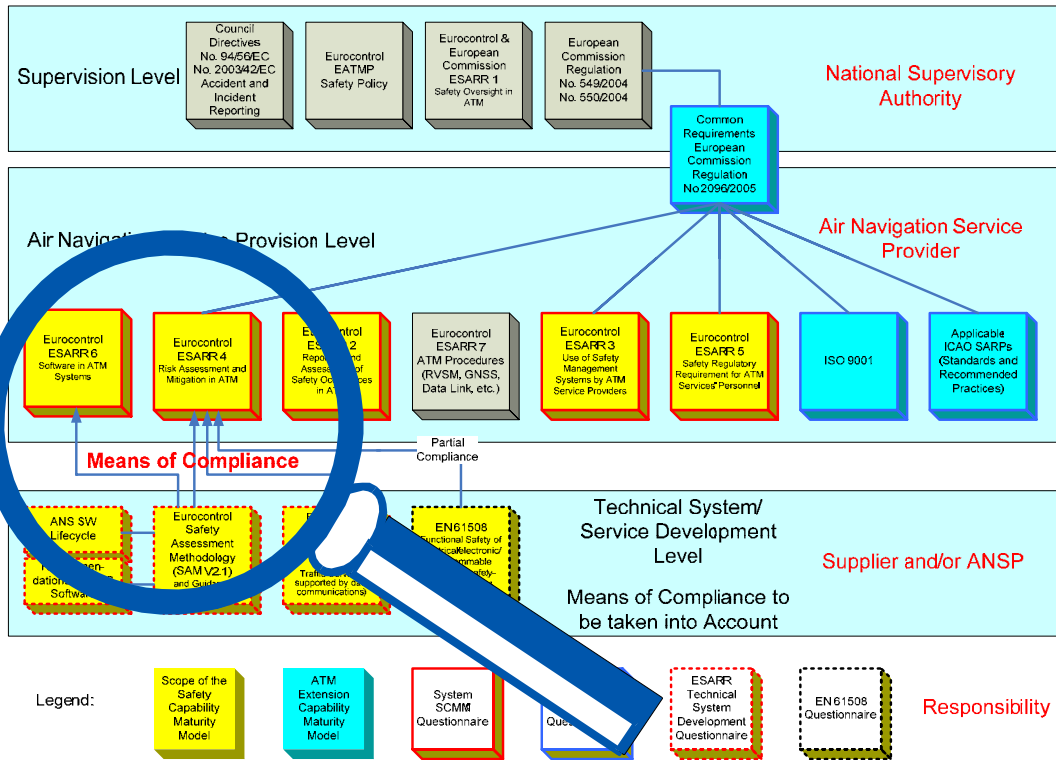
Your Service Provider for Success

2007-05-11, Susanne Lanzerstorfer

APA-PHO-AP0AUP-1.0b-0_Safety_in_ATM

4

Rahmenbedingungen



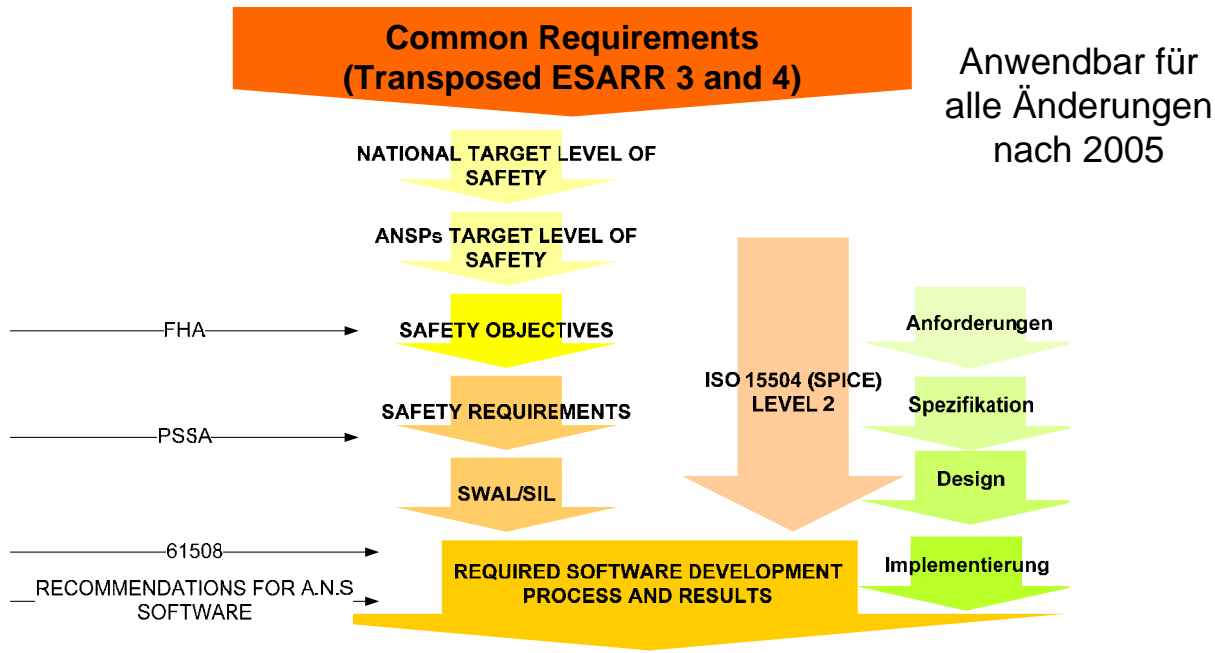
APAC Your Service Provider for Success

2007-05-11, Susanne Lanzerstorfer

APA-PHO-AP0AUP-1.0b-0_Safety_in_ATM

5

Safety Management Anforderungen



Minimum for ATM Systems: SWAL 4

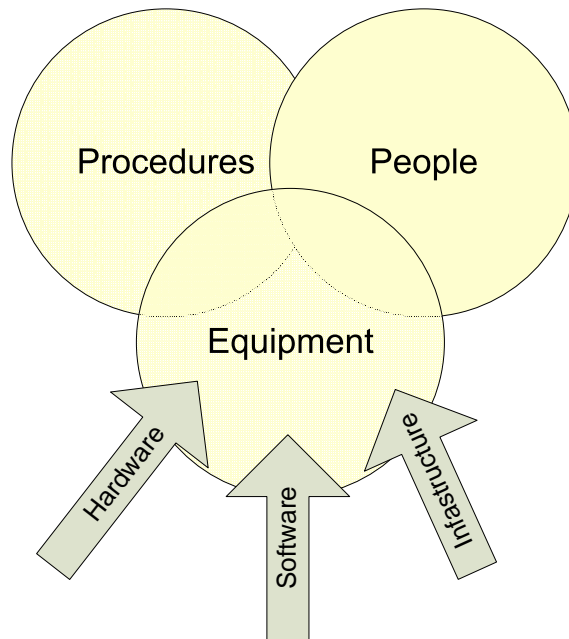
APAC Your Service Provider for Success

2007-05-11, Susanne Lanzerstorfer

APA-PHO-AP0AUP-1.0b-0_Safety_in_ATM

6

Safety Management Scope



APAC

Your Service Provider for Success

2007-05-11, Susanne Lanzerstorfer

APA-PHO-AP0AUP-1.0b-0_Safety_in_ATM

7

Software Safety

- SWAL (Software Assurance Level) wird im Rahmen des Risk Assessments festgelegt
 - Wahrscheinlichkeit, dass Hazard auftritt
 - Wahrscheinlichkeit, dass bei Auftreten des Hazards ein bestimmter Effect eintritt
- ATM spezifisches Guidance Material (Recommendations for A.N.S. Software) legt fest welche Maßnahmen bei welchem SWAL bei der Entwicklung (Life Cycle Prozesse) befolgt werden müssen
 - „Primary life cycle“ Prozesse
 - „Supporting life cycle“ Prozesse
 - „Organisational life cycle“ Prozesse

APAC

Your Service Provider for Success

2007-05-11, Susanne Lanzerstorfer

APA-PHO-AP0AUP-1.0b-0_Safety_in_ATM

8

Primary Life Cycle Prozesse

- Aquisitionsprozess
- Supplyprozess
- Entwicklungsprozess
- Betrieb
- Wartung

APAC

Your Service Provider for Success

2007-05-11, Susanne Lanzerstorfer

APA-PHO-AP0AUP-1.0b-0_Safety_in_ATM

9

Supporting Life Cycle Prozesse

- Dokumentationsprozess
- Konfigurations-Managementprozess
- Qualitätssicherungsprozess
- Verifikationsprozess
- Validierungsprozess
- Joint Review Prozess
- Auditprozess
- Problembehebungsprozess

APAC

Your Service Provider for Success

2007-05-11, Susanne Lanzerstorfer

APA-PHO-AP0AUP-1.0b-0_Safety_in_ATM

10

Organisational Life Cycle Prozesse

- Managementprozess
- Infrastrukturprozess
- Verbesserungsprozess
- Trainingsprozess

APAC

Your Service Provider for Success

2007-05-11, Susanne Lanzerstorfer

APA-PHO-AP0AUP-1.0b-0_Safety_in_ATM

11

Lieferanten Safety Maturity Model

- ATM spezifischer Standard (Recommendation for A.N.S. Software) verweist auf andere Standards für detailliertere Guidance
 - CMMI
 - EN 61508
 - ED12B bzw. ED109
- Kombination von ISO15504 (SPICE) mit EN 61508
 - Zur Umsetzung der allgemein formulierten Anforderungen in der Praxis
 - ISO15504 beinhaltet ein anerkanntes Referenzsystem zum Benchmarking inklusive Scoring

APAC

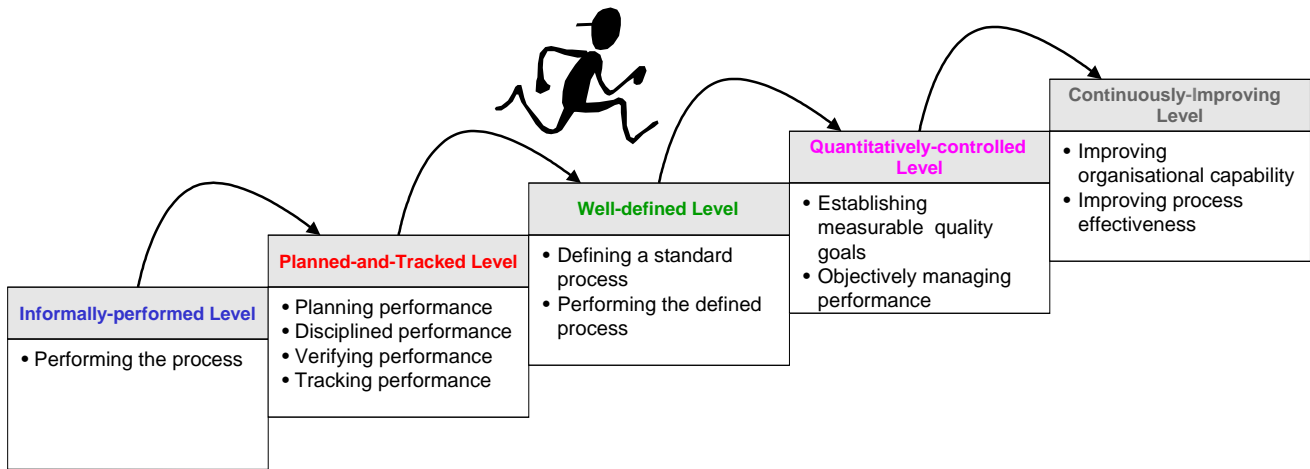
Your Service Provider for Success

2007-05-11, Susanne Lanzerstorfer

APA-PHO-AP0AUP-1.0b-0_Safety_in_ATM

12

Capability Level



APAC

Your Service Provider for Success

Architektur des Fragebogens

Process Categories	Level 1 (SPICE Processes and 61508 SIL2 methods)	Level 2	Level 3	Level 4	Level 5
Project process category	Plan project life cycle including safety life cycle	12 GENERIC PRACTICES	5 GENERIC PRACTICES	3 GENERIC PRACTICES	5 GENERIC PRACTICES
	Establish project plan including all safety tasks				
	Build project teams				
	Manage requirements				
	Manage quality				
	Manage resources and schedule				
	Manage subcontractors				
Engineering process category	⋮				
Support process category	⋮				
Organisation process category	⋮				

APAC

Your Service Provider for Success

Beispiel für Engineering Level 1 61508 und SPICE

Engineering Processes			
	QUESTION	REMARKS FOR SCORING SPICE	SIL 2 Methods&Techniques 61508
Level 1	1.1: Perform Processes		
2.1 Develop software requirements	Develop software requirements: Establish, analyse and refine the software requirements.	Determine software requirements; analyse software requirements; Determine operating environment impact; evaluate requirements with customer; update requirements for next iteration	R: Computer-aided specification tools; Tools without preference for one particular design method; R: Describe some critical parts with semi-formal methods e.g.: Logic-Function Block Diagrams, Sequence Diagrams Dataflow Diagrams, Finite State Machine/State Transition Diagrams, Time Petri Nets, Decision Truth Table R: Formal Methods including for example, CCS (Calculus of Communicating Systems), CSP (Communicating Sequential Processing), HOL, LOTOS, OBJ, temporal logic VDM

APAC

Your Service Provider for Success

2007-05-11, Susanne Lanzerstorfer

APA-PHO-AP0AUP-1.0b-0_Safety_in_ATM

15

Beispiel Entwicklungsprozess RECOMMENDATIONS FOR A.N.S SOFTWARE

4.3.4	SW requirements analysis	<p>ANS SW Lifecycle Part 1 Chapter 2 §3.4</p> <p>The developer should establish and document software requirements, using software requirements rules.</p> <p>The Software Requirements should, as a minimum:</p> <ul style="list-style-type: none"> • specify the functional behaviour of the ATM software, capacity, accuracy, timing performances, software resource usage on the target hardware, robustness to abnormal operating conditions, overload tolerance; • be complete and correct; • comply with the System Requirements. <p>Algorithms should be specified.</p>
-------	--------------------------	--

APAC

Your Service Provider for Success

2007-05-11, Susanne Lanzerstorfer

APA-PHO-AP0AUP-1.0b-0_Safety_in_ATM

16

Beispiel Engineering Level 2

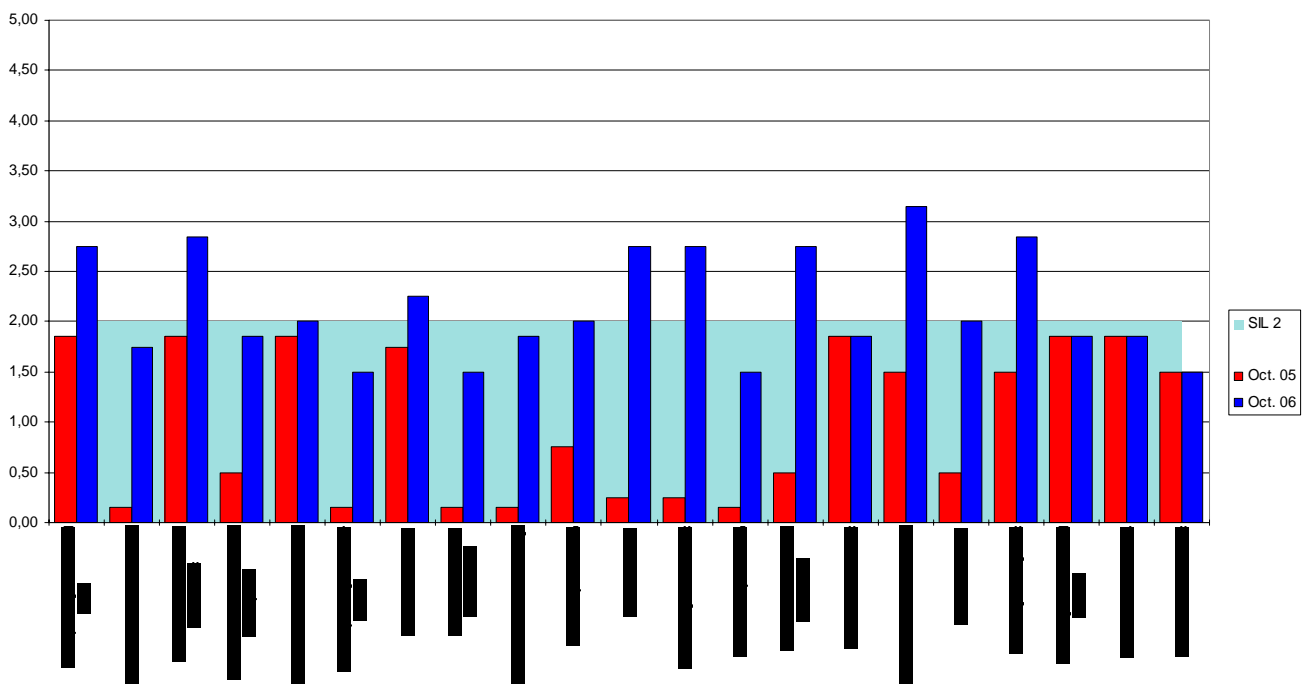
2.1: Planning Performance			
2.10	Allocate resources	Allocate adequate resources (including people) for performing the process category "engineering".	Evidence of resource allocation exists; records/plan indicate resources are allocated to perform job tasks
2.11	Assign responsibilities	Assign responsibilities for developing the work products and/or providing the services of the process category "engineering".	Assigned responsibilities are recorded; representative understands the process and tasks he is responsible for
2.12	Document the process	Document the approach to performing the process category "engineering" in standards and/or procedures.	Tasks to be performed; inputs and outputs; entry/exit criteria; control points; internal and external interfaces; process measurements
2.13	Provide tools	Provide appropriate tools to support performance of the process category "engineering".	Adequate training in the operation of the tool; documentation and/or instructions are available for the tool; support for the tool is available
2.14	Ensure training	Ensure that the individuals performing the process category "engineering" are appropriately trained in how to perform the processes.	Training is available for tools; training curriculum covers all tasks; resources are allocated for training
2.15	Plan the process	Plan the performance of the process category "engineering".	WBS; project standards; special needs; reuse strategy; resource estimation; risks; schedule

APAC

Your Service Provider for Success

Beispielergebnis

Assessments Result Example, October 2005 and October 2006



APAC

Your Service Provider for Success

