Software Classification Methodology and Standardisation

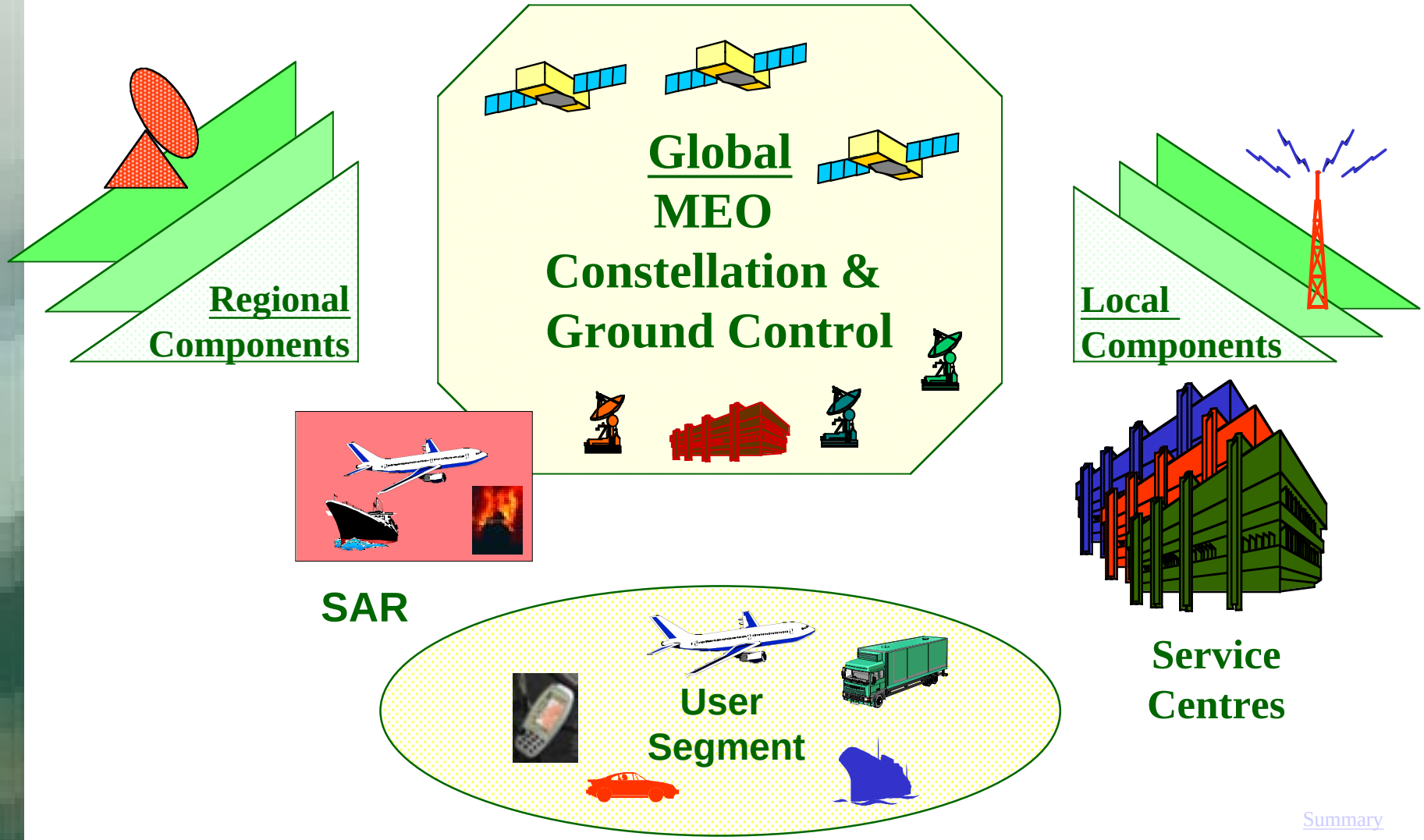
07 March 2003

esa

Table of Contents

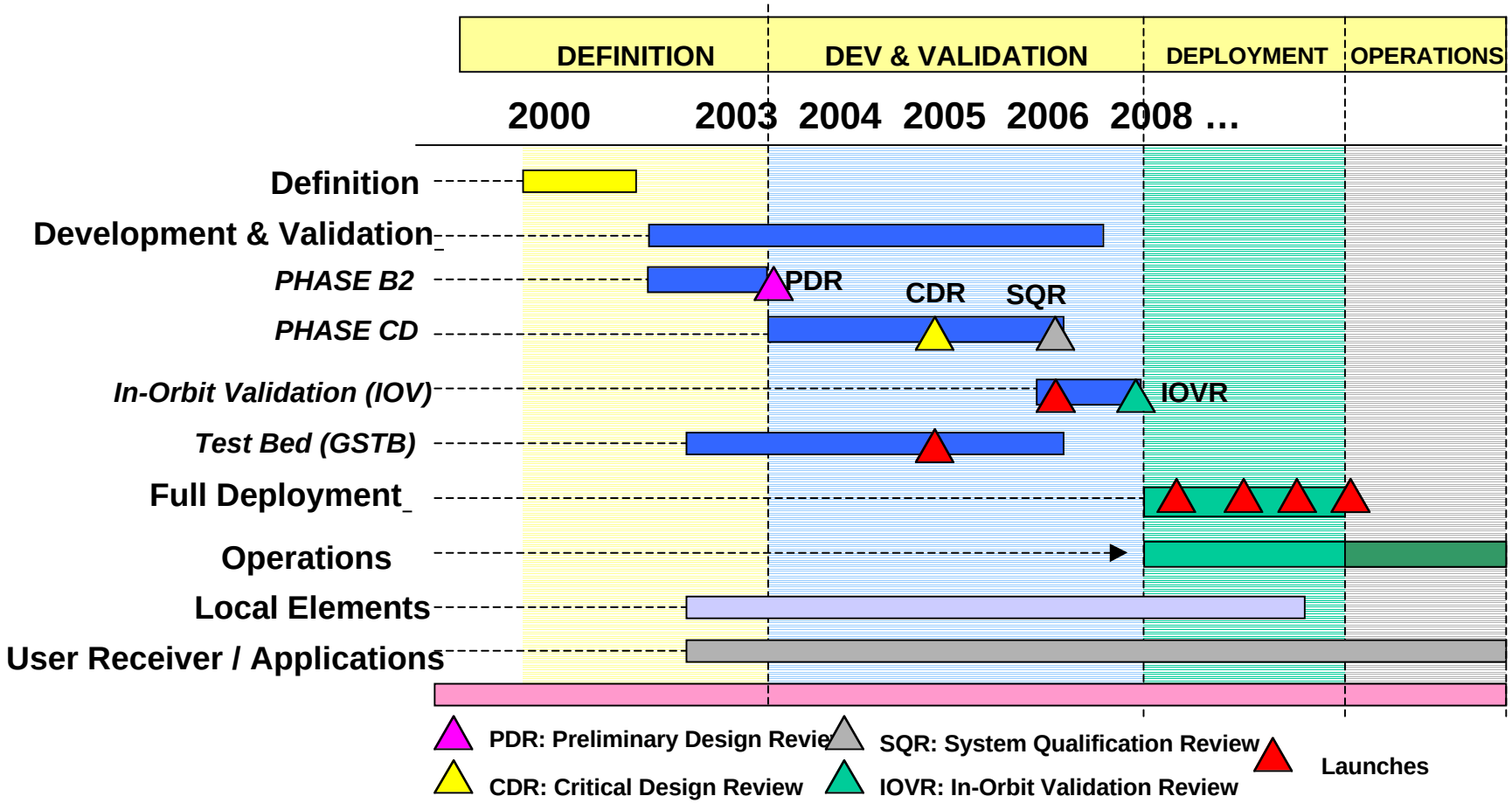
Summary

GALILEO System Overview



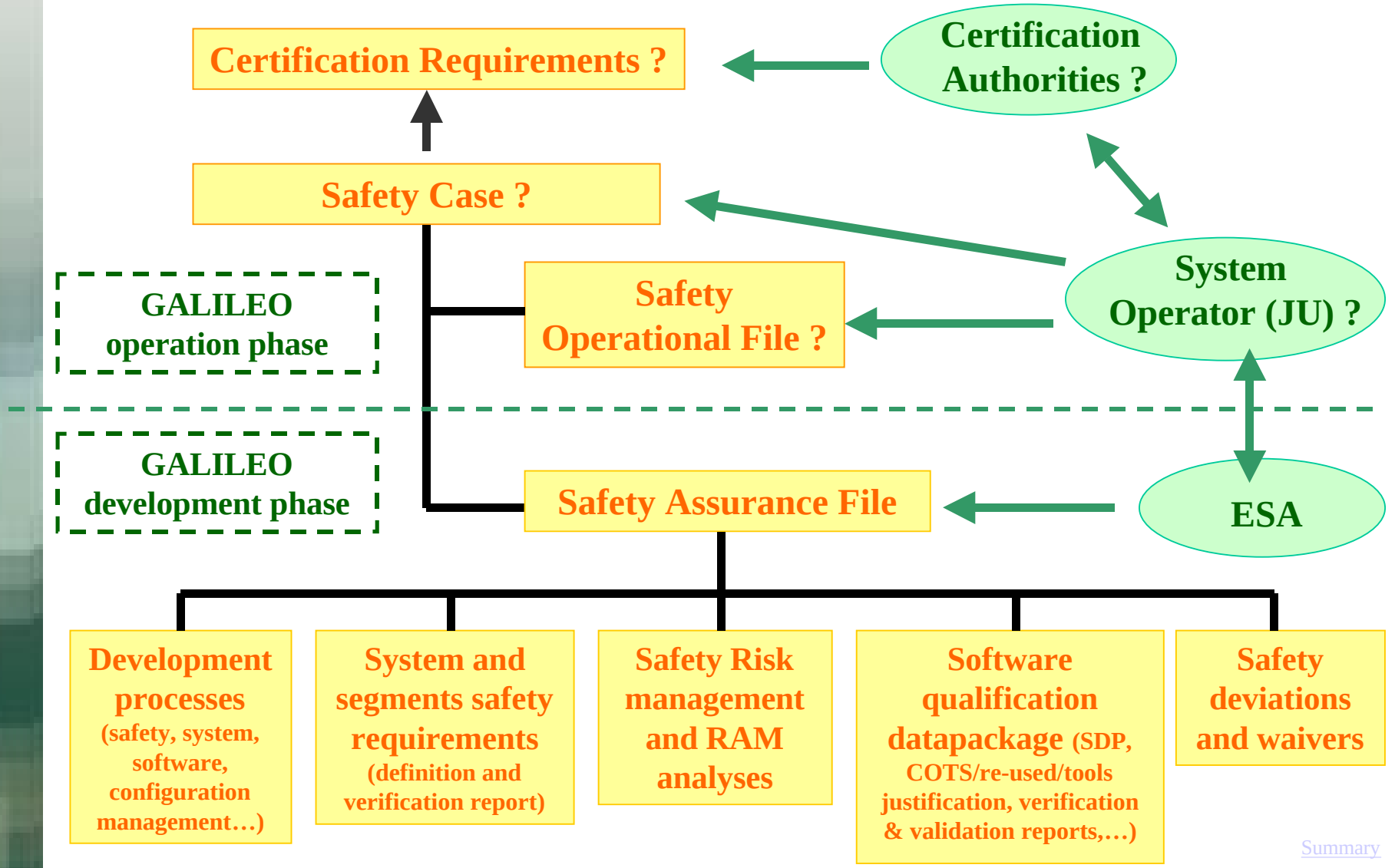
Summary

Master Schedule



Summary

GALILEO Safety Case Approach (TBC)



Summary

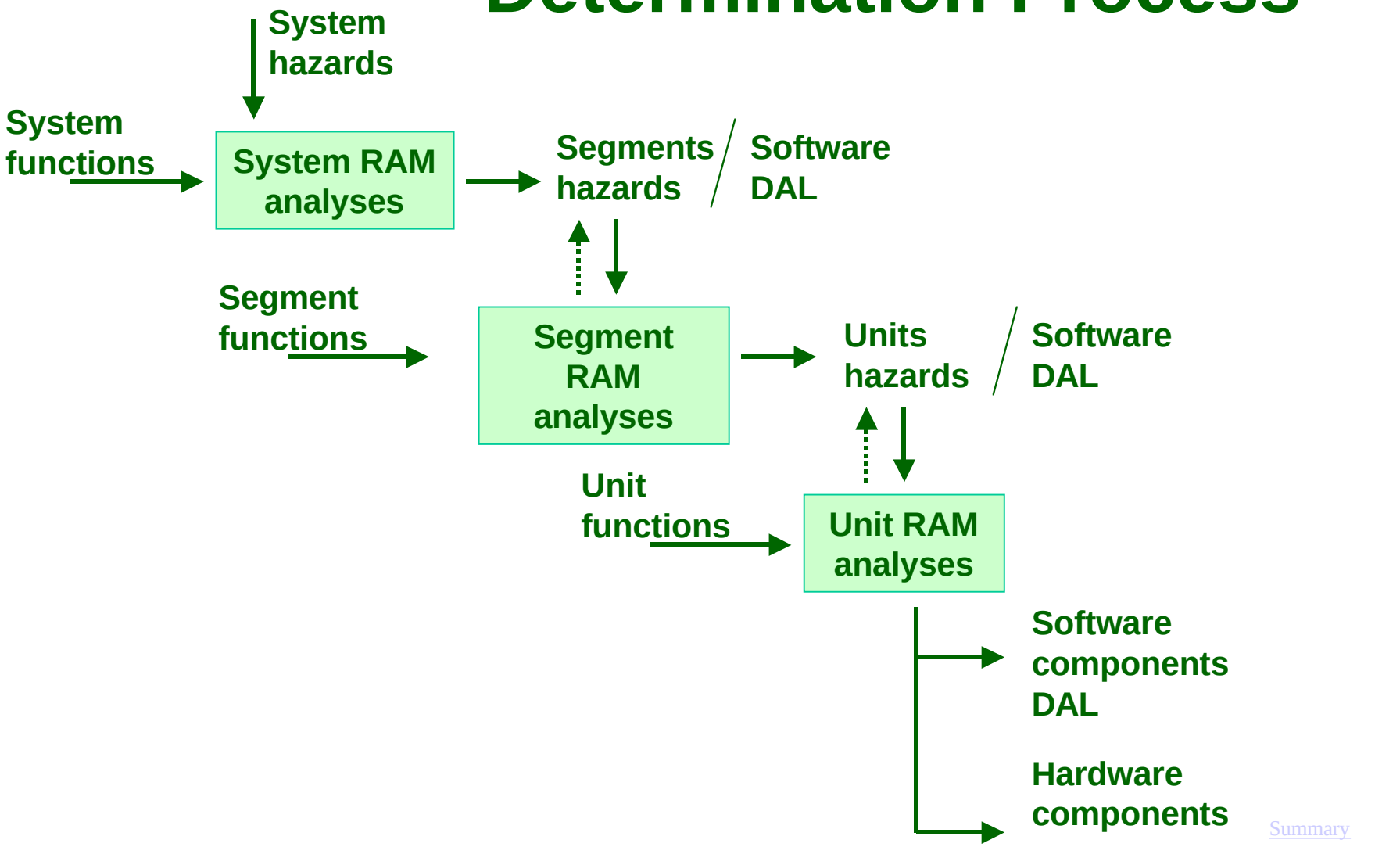
System Safety Hazards Definition and Related Software Classification

System safety hazards			Software DAL
Severity	**Direct "classical"**	**Indirect "navigation-related"**	
Catastrophic	• Loss of life, life threatening or permanently disabling injury or occupational illness • Loss of launch site facilities • Long-term detrimental environmental effects	None	A
Critical	• Temporarily disabling but not life threatening injury or temporarily occupational illness • Short-term environmental detrimental environmental effects • Loss or damage to public or private property	• The position error exceeds the specified Alert Limit and the user is not informed within the Time to Alert (Hazardous Misleading information / Integrity event)	B
Major	• Temporarily loss of satellite or ground facility not leading to catastrophic or critical event	• Loss of continuity • Loss of Search and Rescue Service	C
Minor	None	• Degradation of mission performances not leading to catastrophic / critical / major consequences (loss of availability)	D
Negligible	• All others	None	E

DAL = Development Assurance Level

Summary

System Hazards and Software DAL Determination Process



Summary

Software Standards : Objectives

- To define a “How” project standard in response to the “what” from ESA ECSS standards (E40B and Q80B)
- To have Software engineering and product assurance commonality (many European companies involved)
- To tailor ESA ECSS standards to Galileo software DAL (DO178B/IEC61508 and other standards used within relevant industry sectors - i.e. aviation, maritime, rail, road – are not applicable)
- To plan future software qualification means for Galileo certification purpose (currently no certification authority and no European certification requirements)

Summary

Software Standards : Content

- Software life-cycles vs. software types (I.e: algorithms, database, MMI, tool…)
- Software engineering methods (specification, design, coding, tests)
- Software documentation templates
- Software configuration management
- Software safety analyses
- Software re-used and COTS procedures
- Audits procedures
- Quality model and metrication
- Traceability Matrix to ESA ECSS E40B/Q80B
- Software DAL Applicability matrix

Summary

Conclusion

- No certification authorities and requirements established yet
- Safety case is the responsibility of the system operator only
- The current Safety Case approach will have to be validated with certification authorities
- Safety Assurance File is applicable to space, ground and user segments
- Diversity of industries involved in Galileo needs to define a common Galileo software standard
- Galileo Software standard is written so as to cover the DO178B objectives
- Complex software is covered by Galileo SW standard (I.e. algorithms, COTS, re-used software…)

Summary