WE
CAN DO
SO MUCH
TOGETHER

TECNALIA
Inspiring
Business

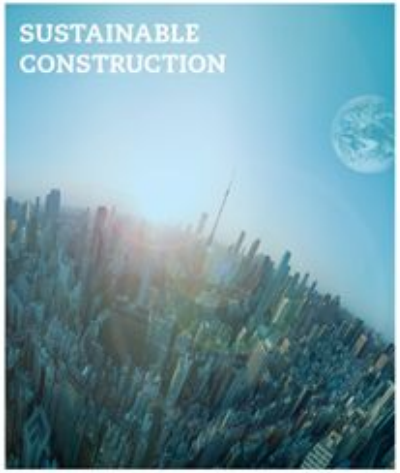
Variabilidad en torno al cumplimiento de normativas y estándares (safety, seguridad, privacidad)

tecnalia Inspiring Business

Jabier Martínez 27/10/2020

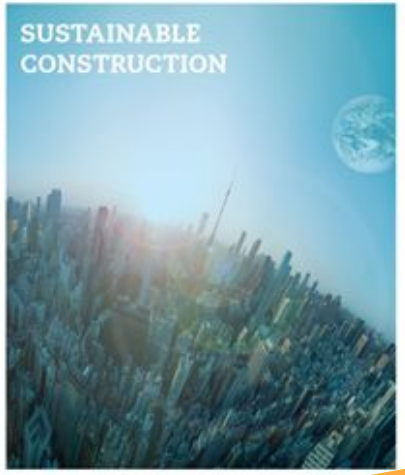
Divisiones

+ EMERGING BUSINESSES



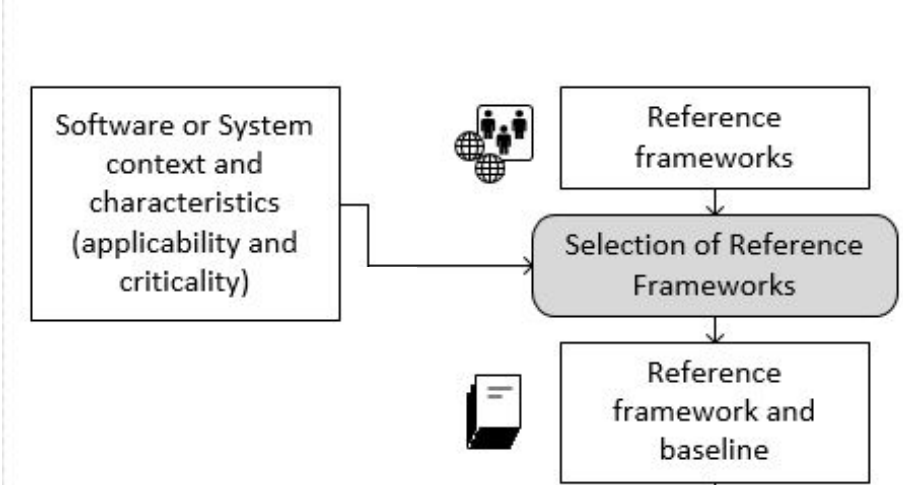
tecnalia Inspiring Business

Divisiones

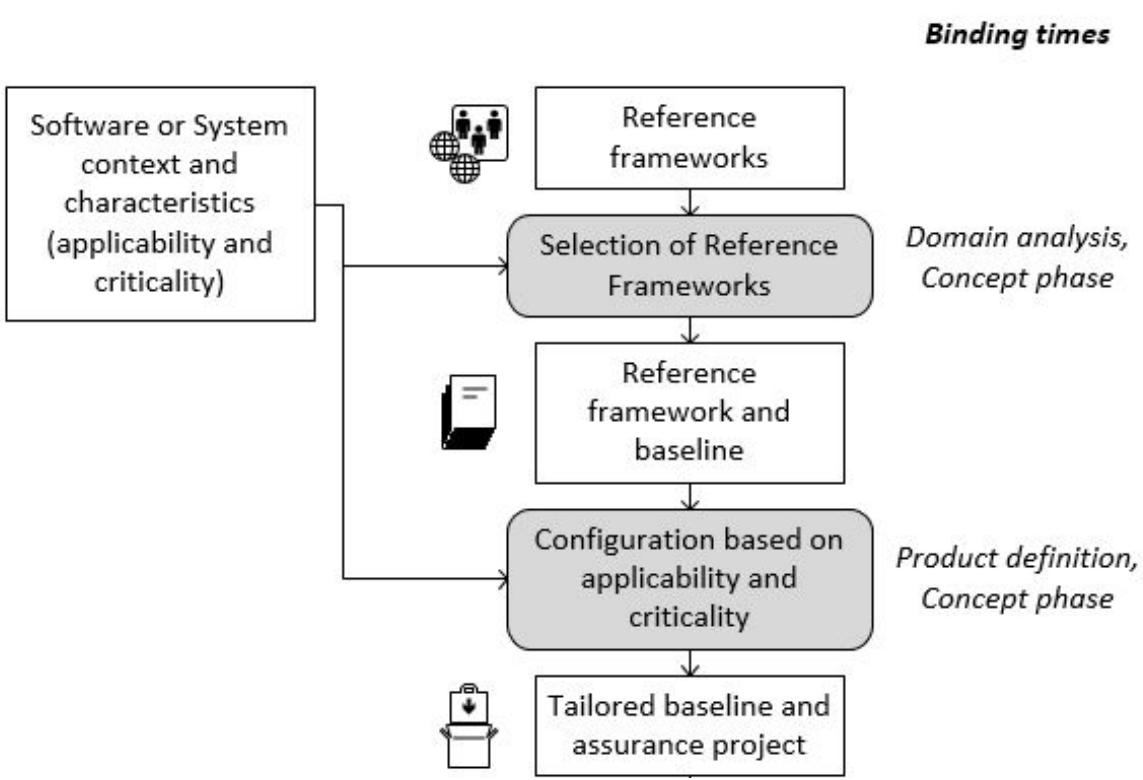


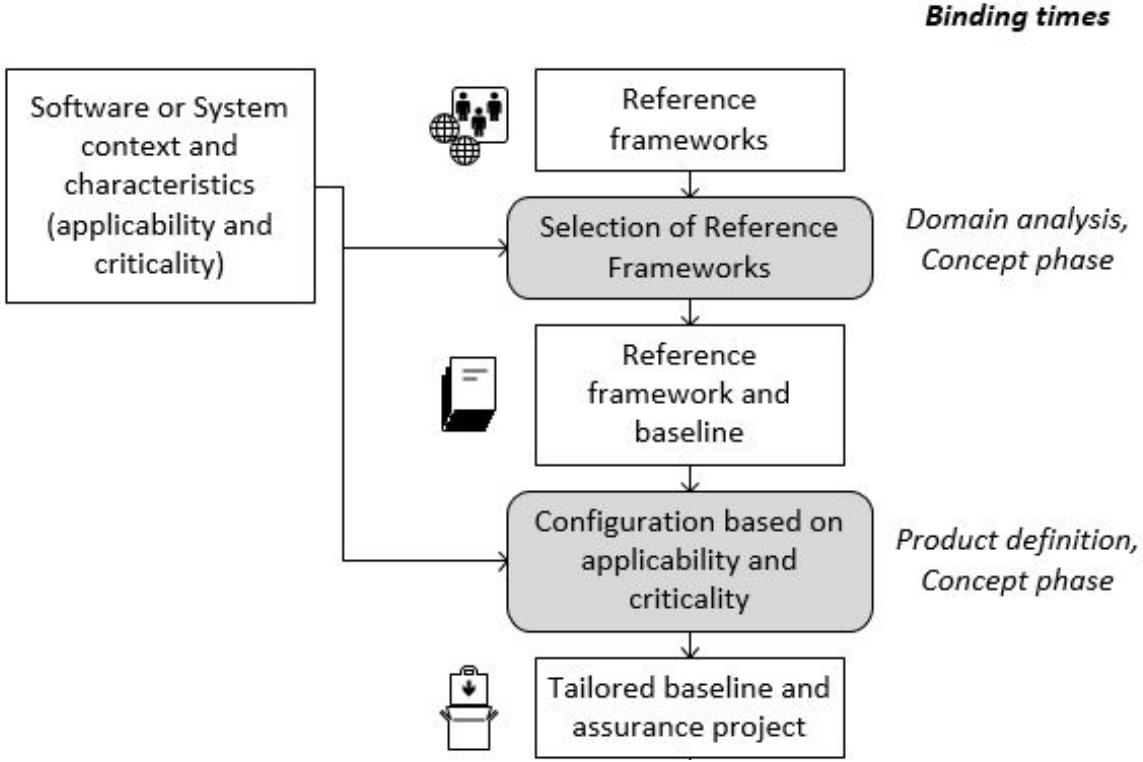
+ EMERGING BUSINESSES

grupo SLI (Software and Systems Lifecyle Innovation)

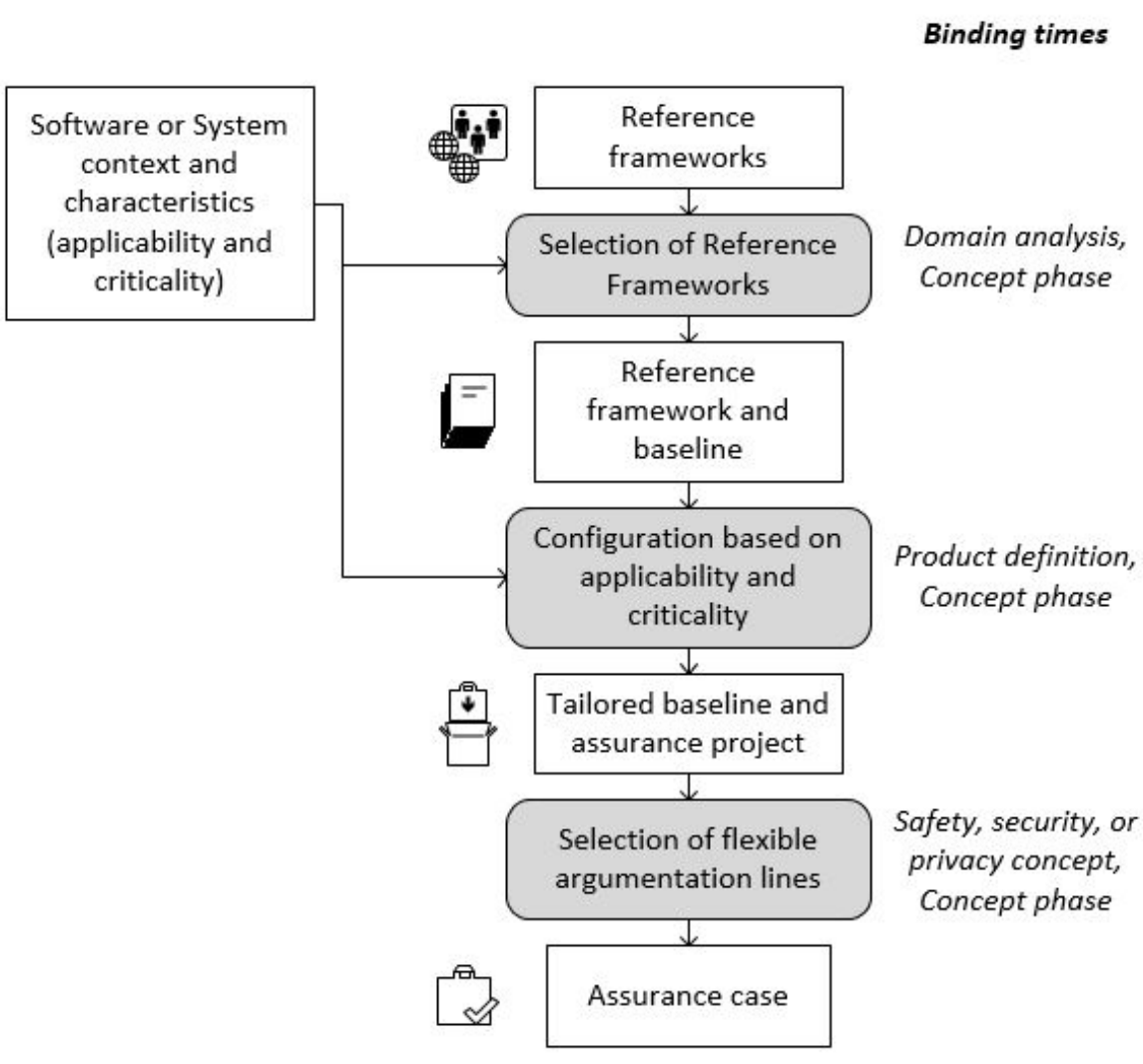


Standards, regulaciones, industrial guidelines


Binding times
Software or System context and characteristics (applicability and criticality)
Reference frameworks
Selection of Reference Frameworks
Domain analysis, Concept phase
Reference framework and baseline
Configuration based on applicability and criticality
Product definition, Concept phase
Tailored baseline and assurance project



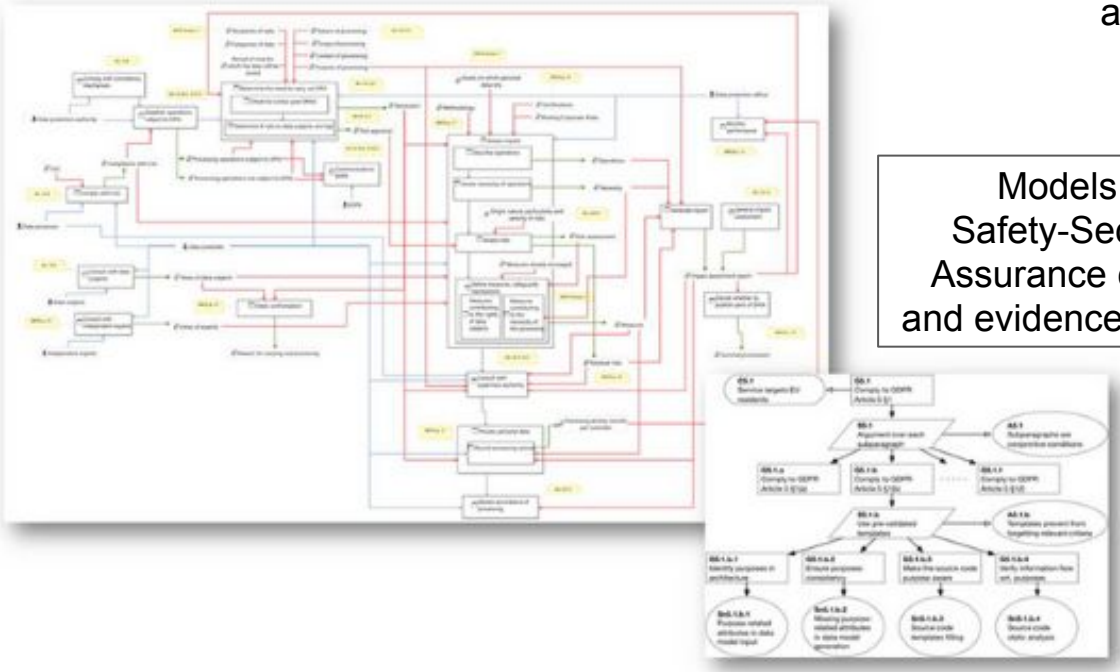
Concept	Standard DO-178C	EN 50128	IEC 61508	ISO 26262
Ref. criticality level Ref. applicability level	Software level A–E Objective satisfaction should be shown as Satisfied or Satisfied with independence, or is at applicant's discretion	SIL 0–4 Mandatory, highly recommended, recommended, not recommended, no recommendation for or against	SIL 1–4 Recommended, highly recommended, not recommended, no recommendation for or against	ASIL A–D Recommended, highly recommended, or no recommendation for or against


Binding times
Software or System context and characteristics (applicability and criticality)
Reference frameworks
Selection of Reference Frameworks
Domain analysis, Concept phase
Reference framework and baseline
Configuration based on applicability and criticality
Product definition, Concept phase
Tailored baseline and assurance project
Selection of flexible argumentation lines
Safety, security, or privacy concept, Concept phase
Assurance case

https://www.eclipse.org/opencert/

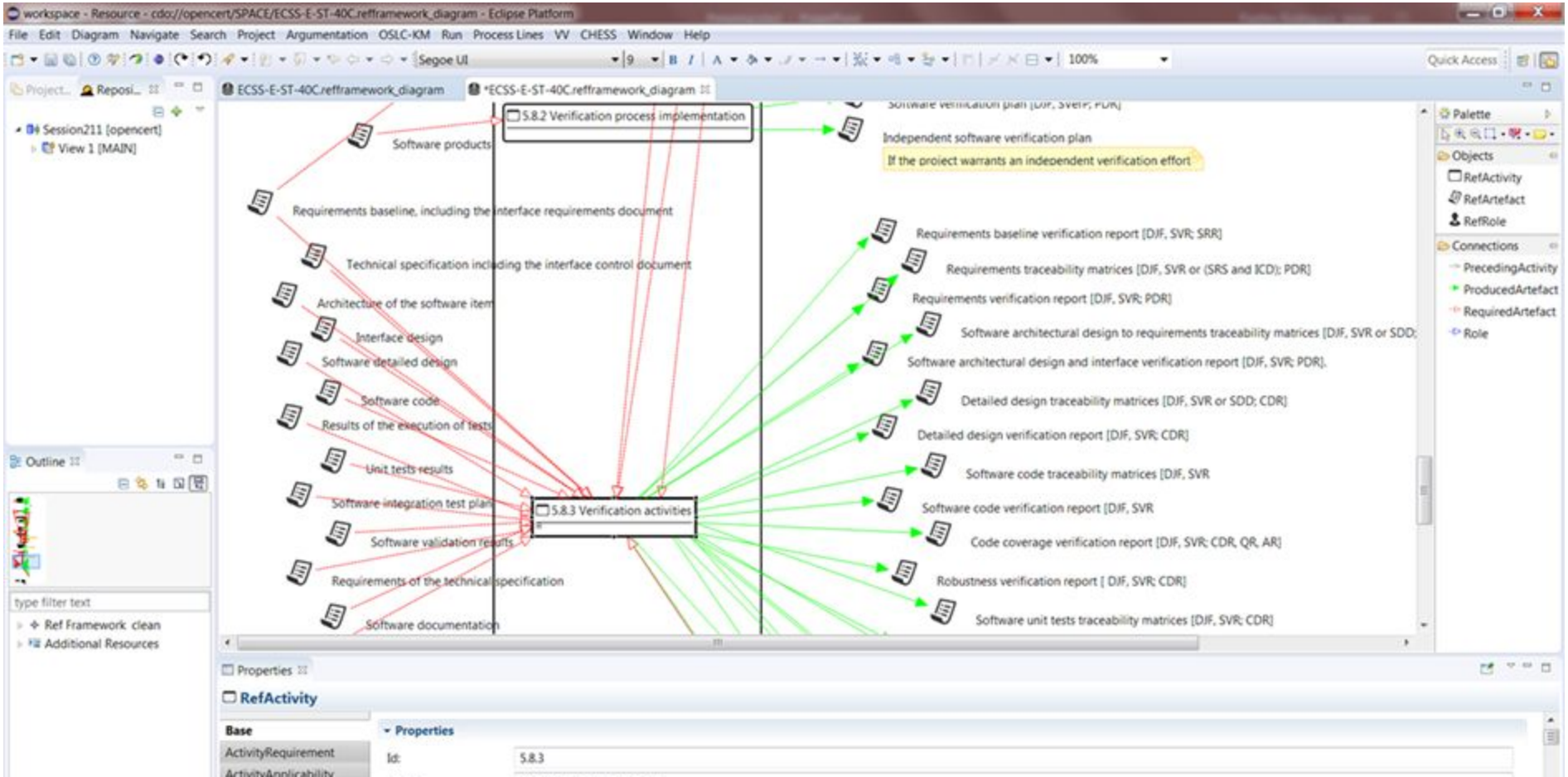
Models of standards, regulations, reference frameworks

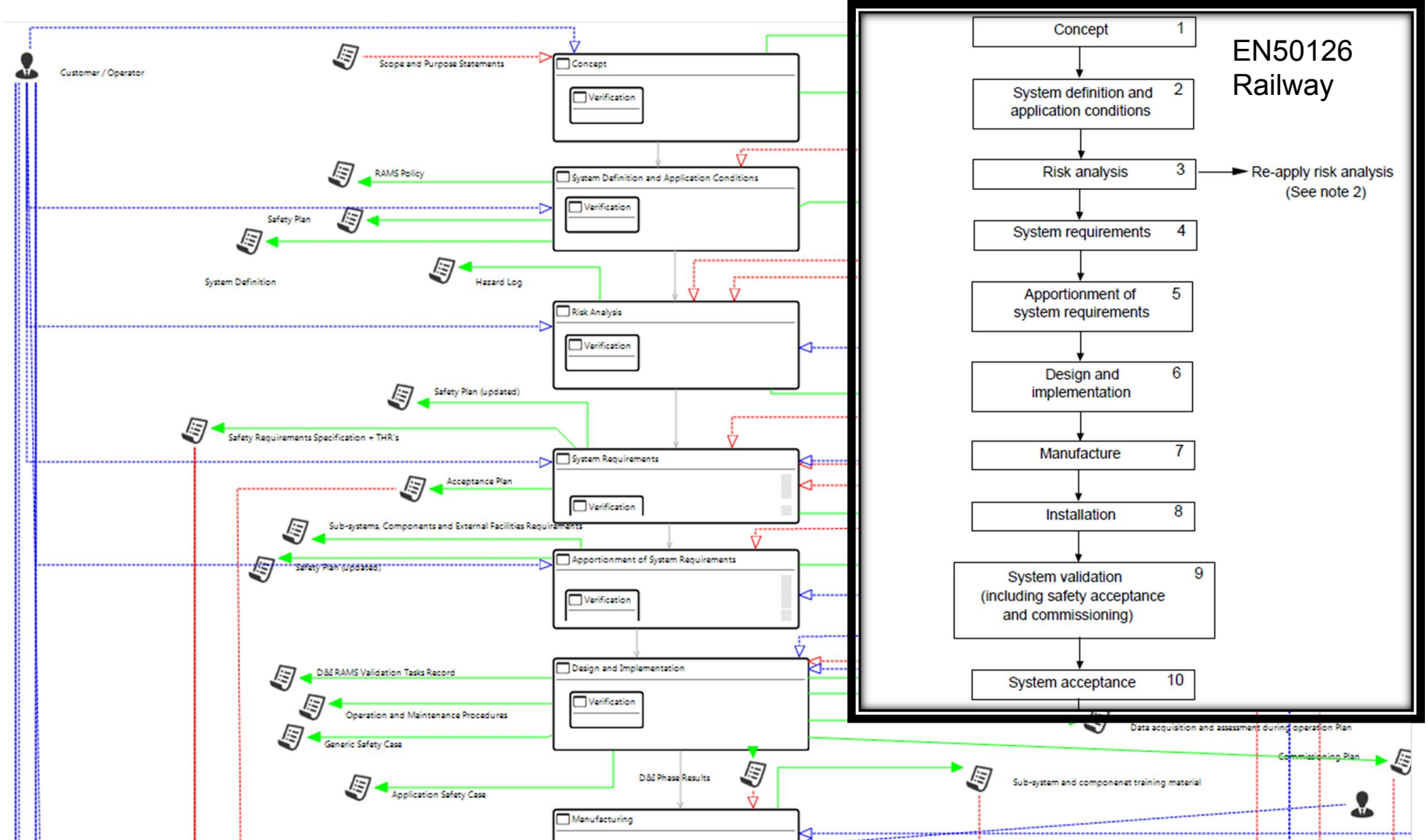
- Enforced processes and/or requirements
- Safety objectives, arguments, and evidences

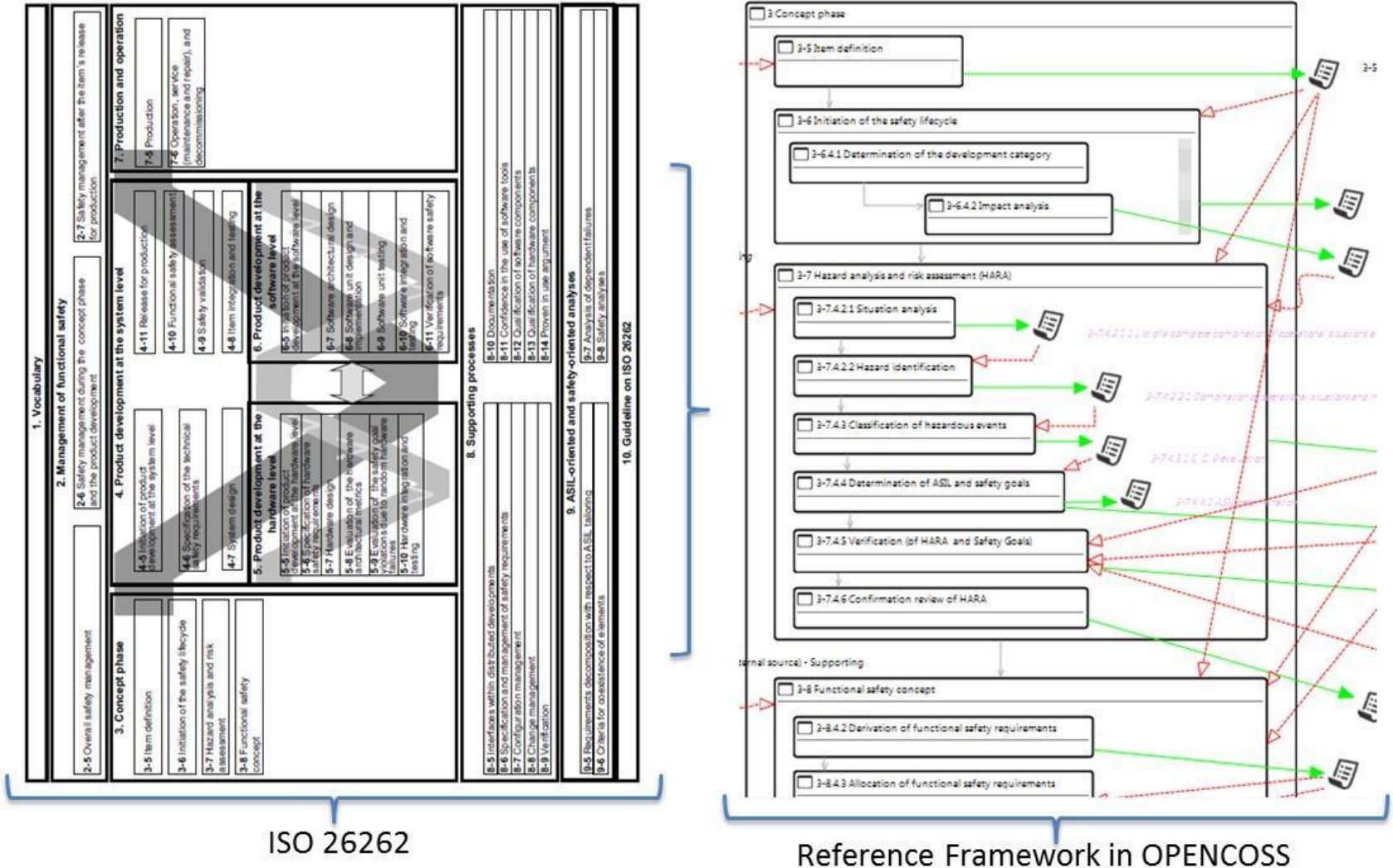


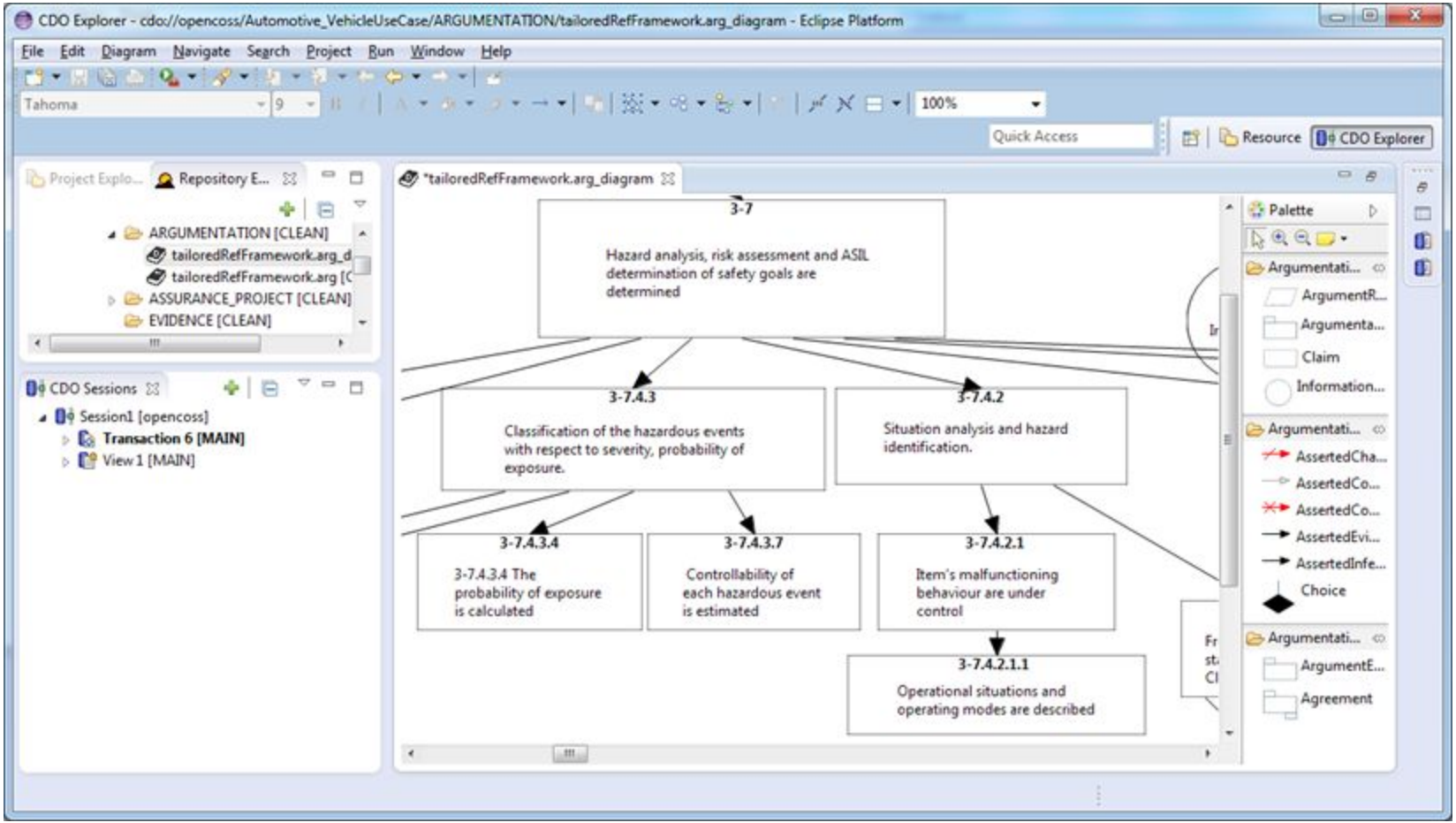
Models of Safety-Security Assurance cases, and evidence models

ECSS-E-ST-40C Space Engineering




Customer / Operator
Scope and Purpose Statements
Concept
Verification
RAMS Policy
System Definition and Application Conditions
Verification
Safety Plan
System Definition
Hazard Log
Risk Analysis
Verification
Safety Plan (updated)
Safety Requirements Specification + THR's
System Requirements
Verification
Acceptance Plan
Sub-systems, Components and External Facilities Requirements
Safety Plan (updated)
Apportionment of System Requirements
Verification
D&I RAMS Validation Tasks Record
Operation and Maintenance Procedures
Generic Safety Case
Design and Implementation
Verification
D&I Phase Results
Application Safety Case
Manufacturing
Concept 1
System definition and application conditions 2
Risk analysis 3
Re-apply risk analysis (See note 2)
System requirements 4
Apportionment of system requirements 5
Design and implementation 6
Manufacture 7
Installation 8
System validation (including safety acceptance and commissioning) 9
System acceptance 10
EN50126 Railway
Data acquisition and assessment during operation Plan
Commissioning Plan
Sub-system and componenet training material


1. Vocabulary
2. Management of functional safety
2-5 Overall safety management
2-6 Safety management during the concept phase and the product development
2-7 Safety management after the item's release for production
3. Concept phase
3-5 Item definition
3-6 Initiation of the safety lifecycle
3-7 Hazard analysis and risk assessment
3-8 Functional safety concept
4. Product development at the system level
4-5 Initiation of product development at the system level
4-6 Specification of the technical safety requirements
4-7 System design
4-8 Item integration and testing
4-9 Safety validation
4-10 Functional safety assessment
4-11 Release for production
5. Product development at the hardware level
5-5 Initiation of product development at the hardware level
5-6 Specification of hardware safety requirements
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
5-9 Evaluation of the safety goal violations due to random hardware failures
5-10 Hardware integration and testing
6. Product development at the software level
6-5 Initiation of product development at the software level
6-6 Specification of software safety requirements
6-7 Software architectural design
6-8 Software unit design and implementation
6-9 Software unit testing
6-10 Software integration and testing
6-11 Verification of software safety requirements
7. Production and operation
7-5 Production
7-6 Operation, service (maintenance and repair), and decommissioning
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and management of safety requirements
8-7 Configuration management
8-8 Change management
8-9 Verification
8-10 Documentation
8-11 Confidence in the use of software tools
8-12 Qualification of software components
8-13 Qualification of hardware components
8-14 Proven in use argument
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses
10. Guideline on ISO 26262
ISO 26262
3 Concept phase
3-5 Item definition
3-6 Initiation of the safety lifecycle
3-6.4.1 Determination of the development category
3-6.4.2 Impact analysis
3-7 Hazard analysis and risk assessment (HARA)
3-7.4.2.1 Situation analysis
3-7.4.2.2 Hazard identification
3-7.4.3 Classification of hazardous events
3-7.4.4 Determination of ASIL and safety goals
3-7.4.5 Verification (of HARA and Safety Goals)
3-7.4.6 Confirmation review of HARA
3-8 Functional safety concept
3-8.4.2 Derivation of functional safety requirements
3-8.4.3 Allocation of functional safety requirements
Reference Framework in OPENCOSS


CDO Explorer - cdo://opencoss/Automotive_VehicleUseCase/ARGUMENTATION/tailoredRefFramework.arg_diagram - Eclipse Platform
File Edit Diagram Navigate Search Project Run Window Help
Tahoma
9
100%
Quick Access
Resource
CDO Explorer
Project Explo...
Repository E...
ARGUMENTATION [CLEAN]
tailoredRefFramework.arg_d
tailoredRefFramework.arg [C
ASSURANCE_PROJECT [CLEAN]
EVIDENCE [CLEAN]
CDO Sessions
Session1 [opencoss]
Transaction 6 [MAIN]
View 1 [MAIN]
*tailoredRefFramework.arg_diagram
3-7
Hazard analysis, risk assessment and ASIL determination of safety goals are determined
3-7.4.3
Classification of the hazardous events with respect to severity, probability of exposure.
3-7.4.2
Situation analysis and hazard identification.
3-7.4.3.4
3-7.4.3.4 The probability of exposure is calculated
3-7.4.3.7
Controllability of each hazardous event is estimated
3-7.4.2.1
Item's malfunctioning behaviour are under control
3-7.4.2.1.1
Operational situations and operating modes are described
Palette
Argumentati...
ArgumentR...
Argumenta...
Claim
Information...
Argumentati...
AssertedCha...
AssertedCo...
AssertedCo...
AssertedEvi...
AssertedInfe...
Choice
Argumentati...
ArgumentE...
Agreement

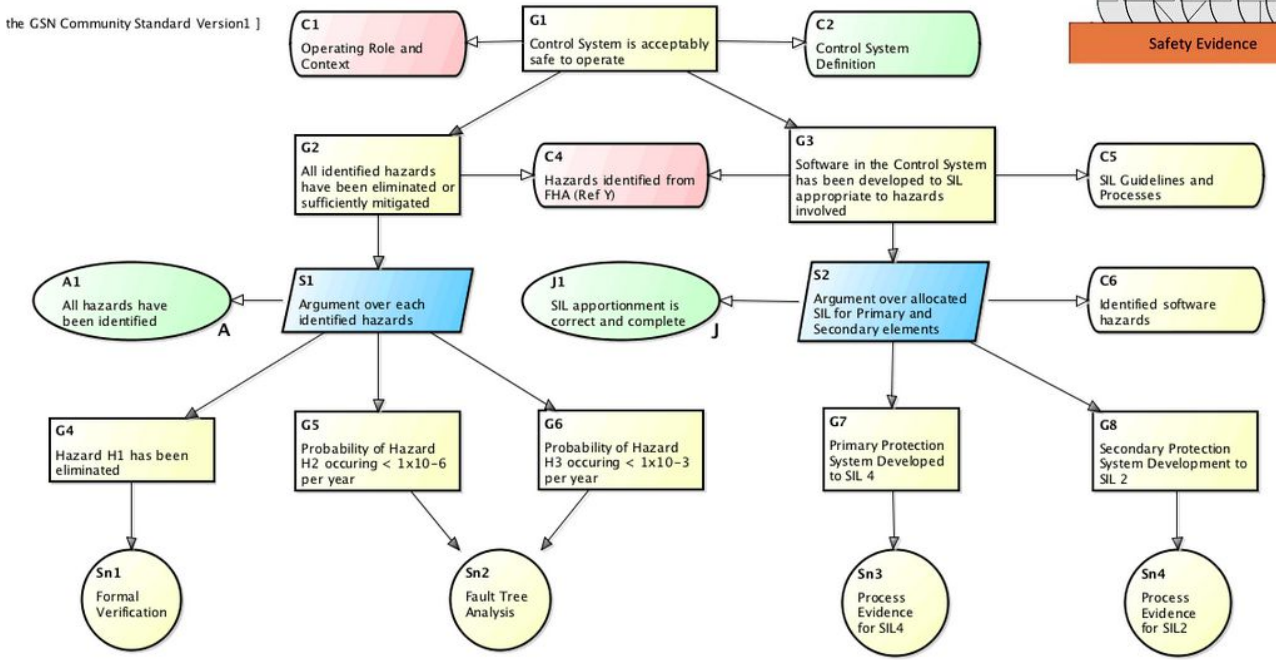
Assurance cases: Goal Structuring Notation

Table 4. Notation of elements in GSN.

Shape	Element
	Goal
	Strategy
	Solution
	Context
	Justification
	Assumption

Table 5. Notation of relations in GSN.

Line / arrow	Relation (origin and source)
	Supported by (from goal to goal / strategy / solution, or from strategy to goal)
	In context of (from goal / strategy to context / assumption / justification)



Assurance cases: Goal Structuring Notation

Built-in variability-related extensions to GSN

	A hollow ball indicates 'optional' (meaning zero or one).

A1.2.3 The extension to GSN shown in Figure 22 enables the representation of structural options using the notation. This figure introduces the GSN *option* symbol, which is rendered as a solid diamond. This symbol is defined for use over all existing GSN relation types. A GSN *option* can be used to denote possible alternatives in satisfying a relationship. It can represent 1-of-n and m-of-n selection, a textual annotation indicating the nature of the choice to be made. In Figure 22, one goal can be supported by any one of three possible sub-goals.

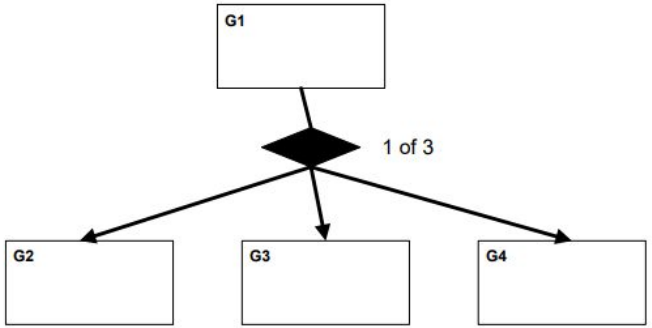
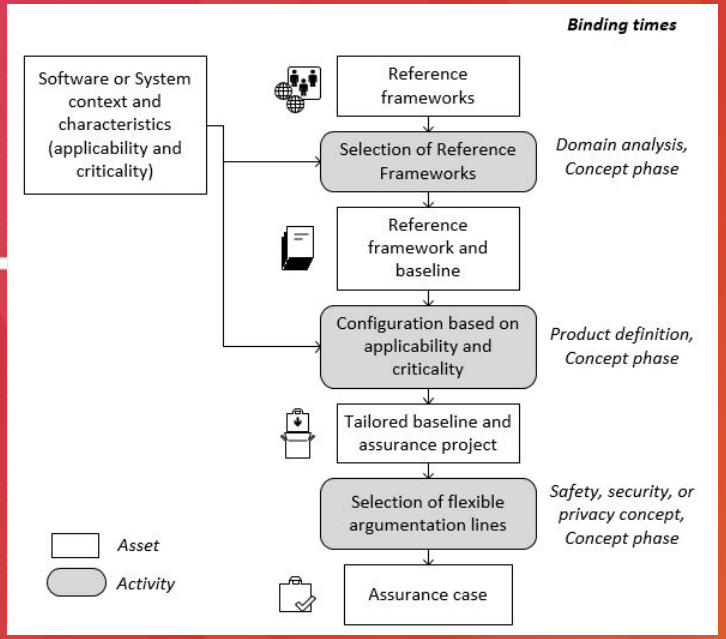


Figure 22: GSN Option Element

WE
CAN DO
SO MUCH
TOGETHER

TECNALIA
Inspiring
Business



Variabilidad en torno al cumplimiento de normativas y estándares (safety, seguridad, privacidad)

tecnalia Inspiring Business

Jabier Martínez 27/10/2020