Requirements-driven Verification Methodology for Standards Compliance

Serrie-justine Chapman (TVS)

in collaboration with
Test and Verification Solutions Ltd
Infineon Technologies UK
ARTEMIS CRYSTAL project

REQUIREMENTS ENGINEERING DEFINITIONS

Requirement:

(1) A condition or capability needed by a user to solve a problem or achieve an objective

(2) A condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification or other formally imposed documents

(3) A documented representation of a condition or capability as in (1) or (2)

[IEEE Std.610.12-1990]

Stakeholder*:

A stakeholder of a system is a person or an organization that has an (direct or indirect) influence on the requirements of the system

Requirements Engineering:

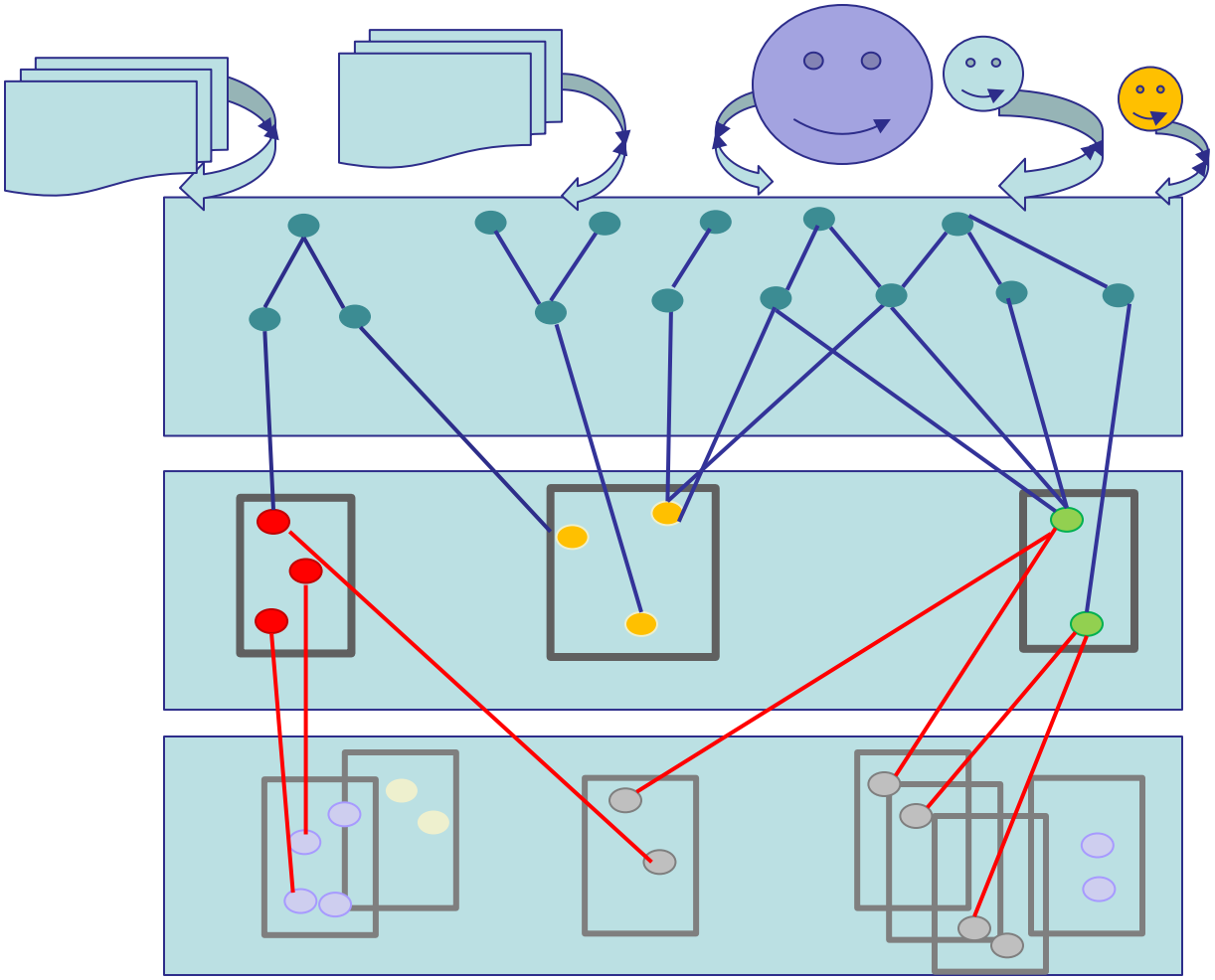
(1) Requirements engineering is a systematic and disciplined approach to the specification and management of requirements with the following goals:

(1.1) Knowing the relevant requirements, achieving a consensus among the Stakeholders about these requirements, documenting them according to given standards, and managing them systematically

(1.2) Understanding and documenting the stakeholders' desires and needs, then specifying and managing requirements to minimize the risk of delivering a system that does not meet the stakeholders' desires and needs

*** All Definitions taken from IREB**

REQUIREMENTS ENGINEERING

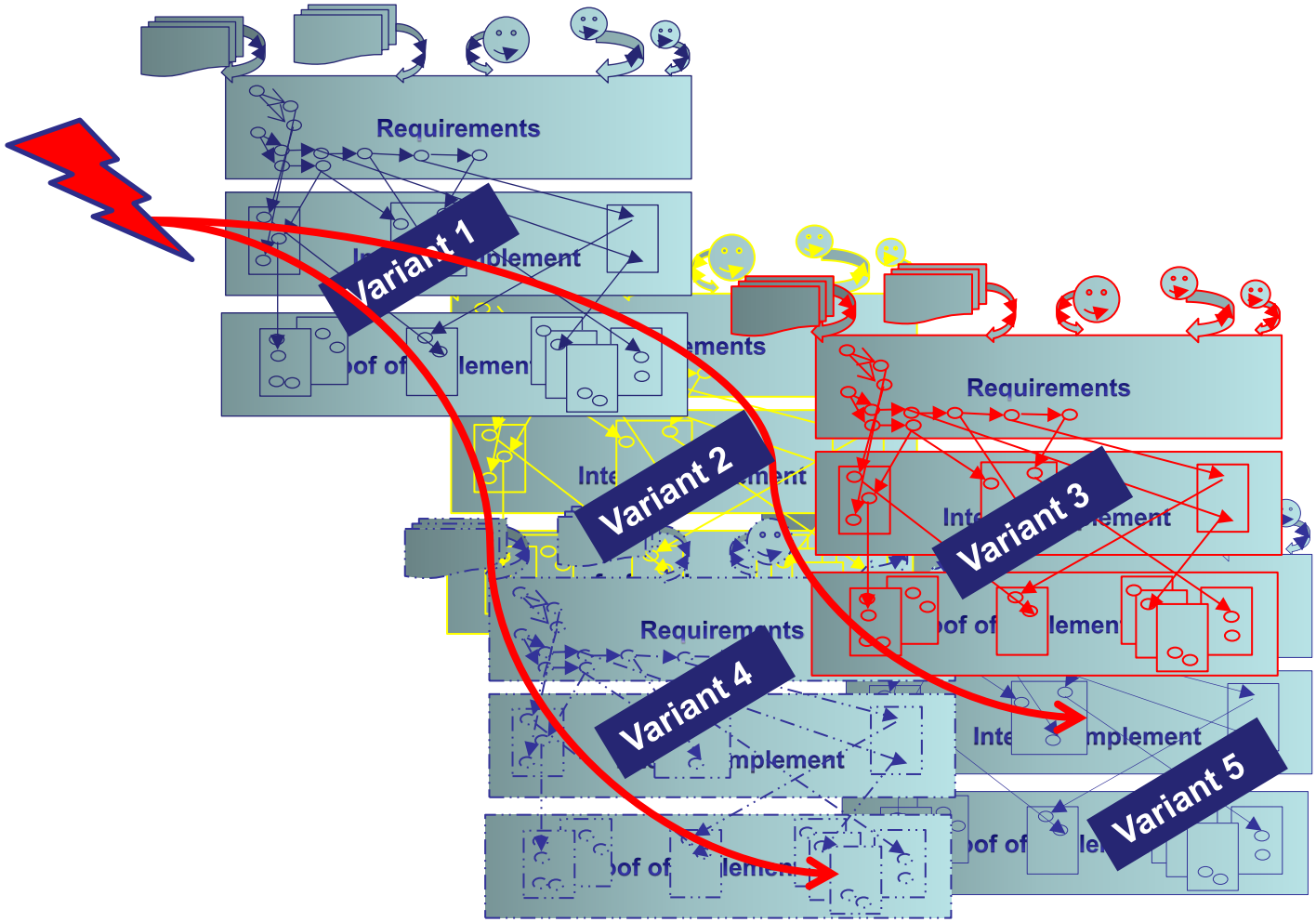


Requirements

Intent to Implement

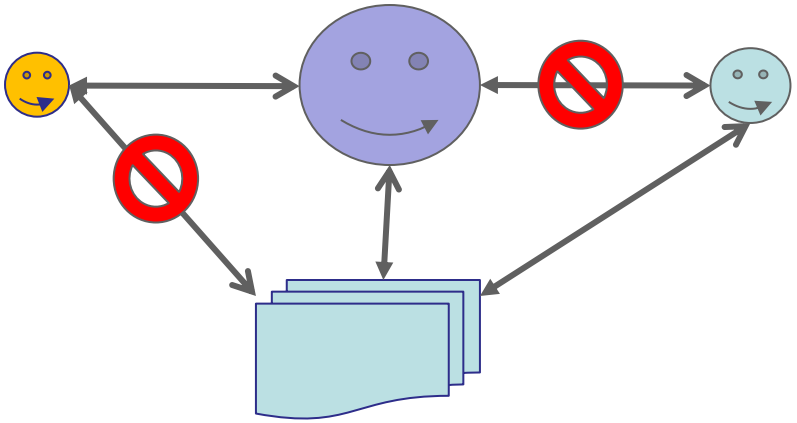
Proof of implementation

VARIANTS, REUSE & COMMUNICATION



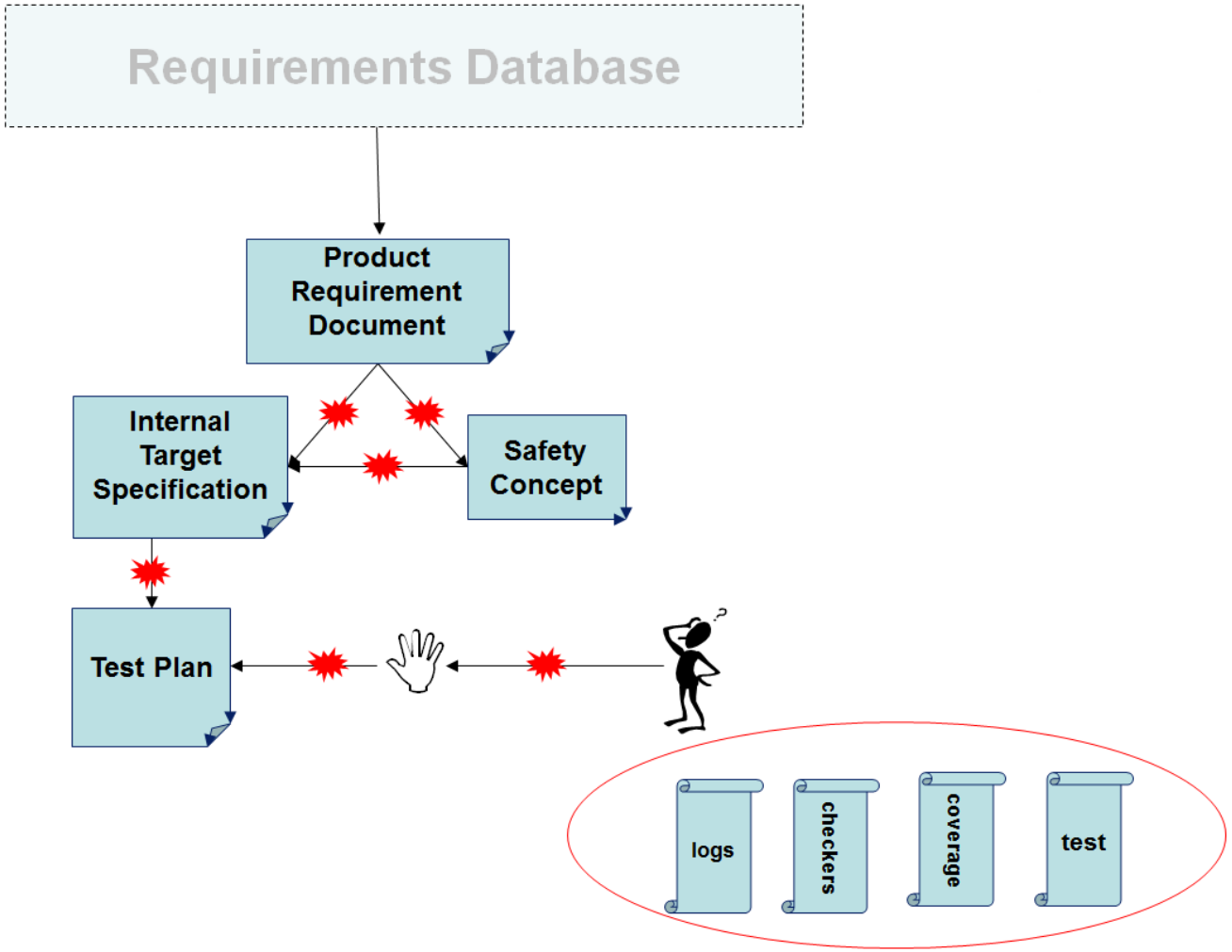
ISSUES

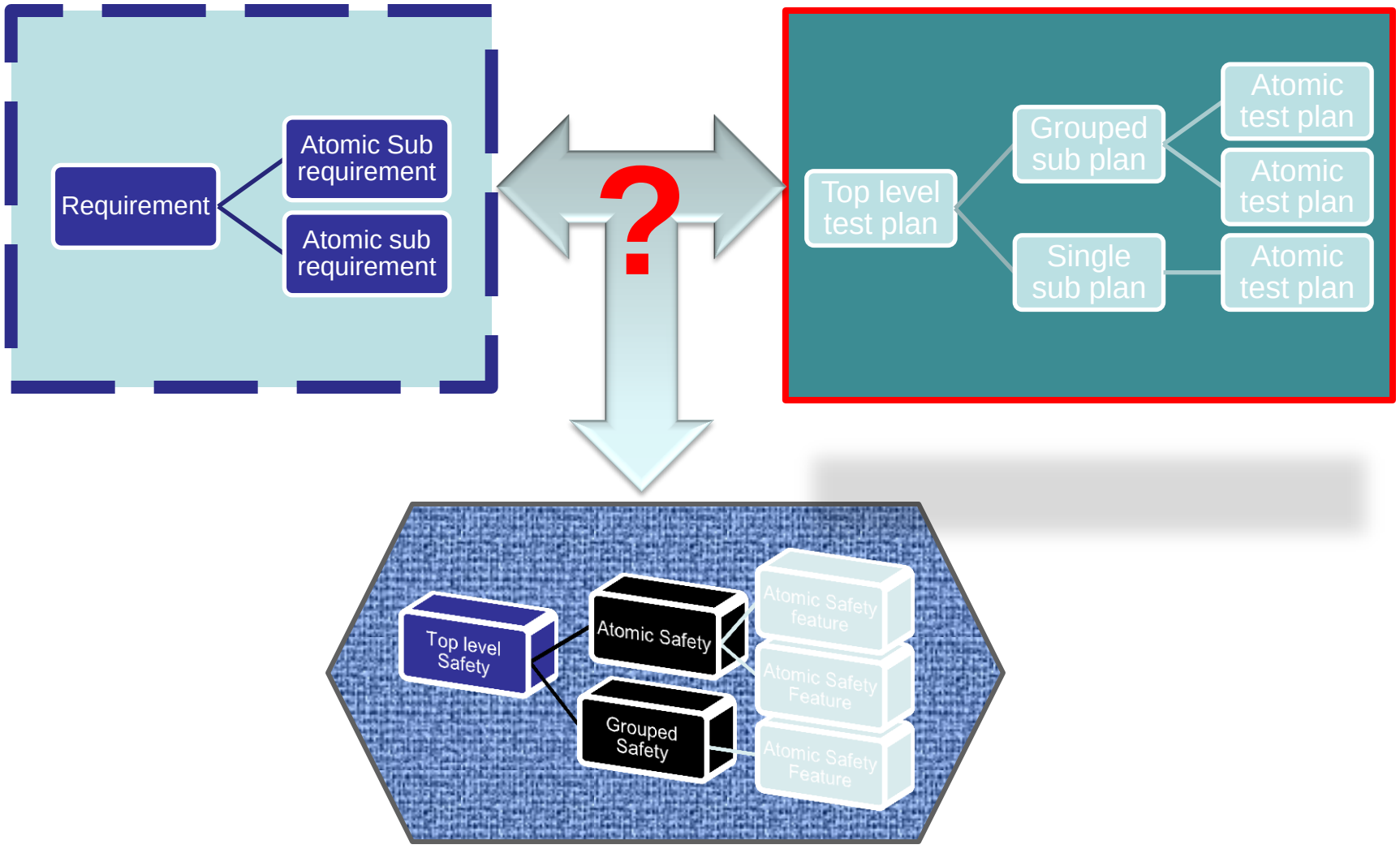
Conflicts



Comprehension

DATA INTEGRITY




Requirement
Atomic Sub requirement
Atomic sub requirement
?
Top level test plan
Grouped sub plan
Single sub plan
Atomic test plan
Atomic test plan
Atomic test plan
Top level Safety
Atomic Safety
Grouped Safety
Atomic Safety feature
Atomic Safety Feature
Atomic Safety Feature

AIMS


Tube map
tfl.gov.uk
0343 222 1234
tfl.gov.uk/emailupdates
@TfLTravelAlerts
MAYOR OF LONDON
TRANSPORT FOR LONDON
EVERY JOURNEY MATTERS

STANDARDS GUIDANCE

Elicitation

- Who
- How

Scope definition

- What are we building
- What are we interacting with
- What environment will we be in
- What dependencies and constraints do we face
- What influencers do we have
- What inputs and outputs (sources and sinks)

FUNCTIONAL HAZARD

Function

- What function ensures SH requirement is acheived

Functional Failures

- No Function
  - **HAZARD** : Doesn't do what its designed to
- Incorrect Function
  - **HAZARD** : Incorrectly does an incorrect function

Situational Analysis

- Usage situation - when is it likely to happen
- People at risk – who can be hurt by a failure

HAZARD LEVEL ANALYSIS

Lane Keeping assistant example

Identify hazards

Hazard	:	Doesn’t stay in lane
Situation	:	Unintended lane change
UID	:	123
Severity	:	S3
Rationale	:	Unintended change due to speed at which the system is active or required may be life threatening to multiple parties
Exposure	:	E4
Rationale	:	Possibility of occurrence over any frequency or duration of travel in car
Control	:	C3
Rationale	:	May be required override for danger situation - short time scale to consider appropriate other actions and system not reacting to request
ASIL	:	ASIL D

SAFETY REQUIREMENTS

Safety goal

The Drivers and other road users shall not be exposed to unreasonable risk due to unintended lane change

Safe State

The Vehicle shall remain in the lane in which they intended

Functional goal

Avoid Undemanded Steering

Functional Safety Requirement

System shall detect excessive motor torque

REQUIREMENT QUALITY GATEWAY

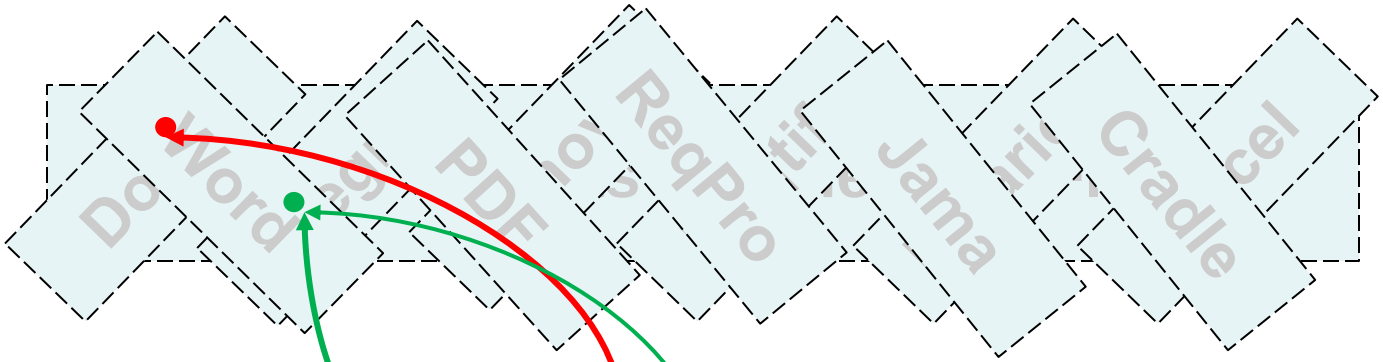
- Requirements are expensive
  - ROI
  - Quality Criteria :
    - Unambiguous
    - Testable (verifiable)
    - Clear (concise, terse, simple, precise)
    - Correct
    - Understandable
    - Feasible (realistic, possible)
    - Independent
    - Atomic
    - Necessary
    - Implementation-free (abstract)

- How do we check for quality
  - Boilerplates
  - Manual inspection (review)
  - model rule checker (if model based)

CONSIDERATIONS

- Requirements stages
- Data management
- Where to store/communicate
- Change management
- Visualisation
- Process/Flow
- Communication
- How to prove

REQUIREMENTS DRIVEN VERIFICATION AND TEST



Test scripts

Integration testing

Manual review

Assertions

Where

Pass?

Metadata?

SOC Simulations

IP1 Simulations

Parameteric testing

Directed testing

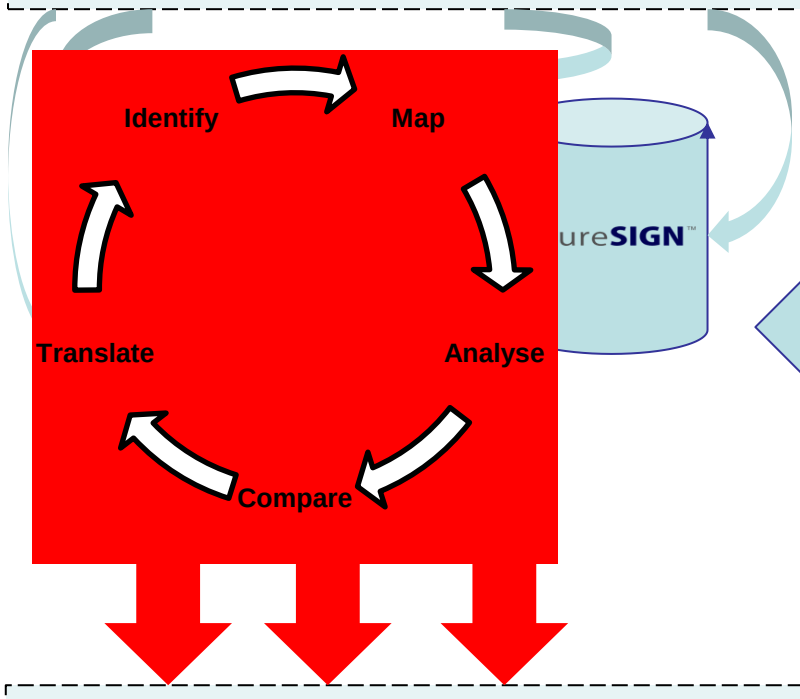
Formal testing

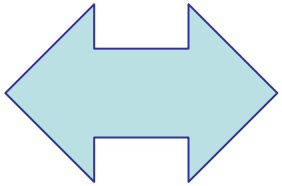
Structural coverage

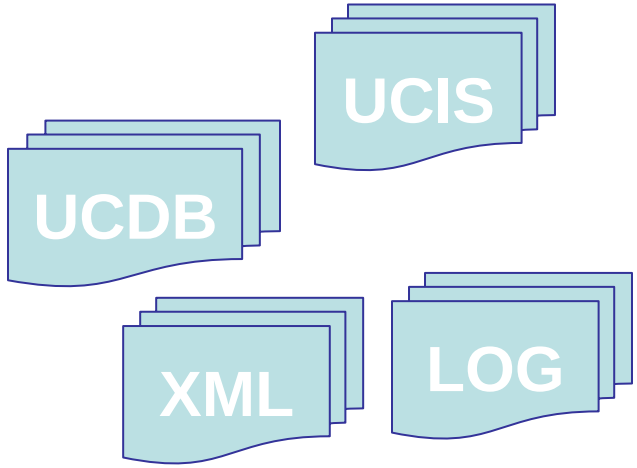
Functional coverage

asureSIGN™ SOLUTION

Requirements Engineering Flow



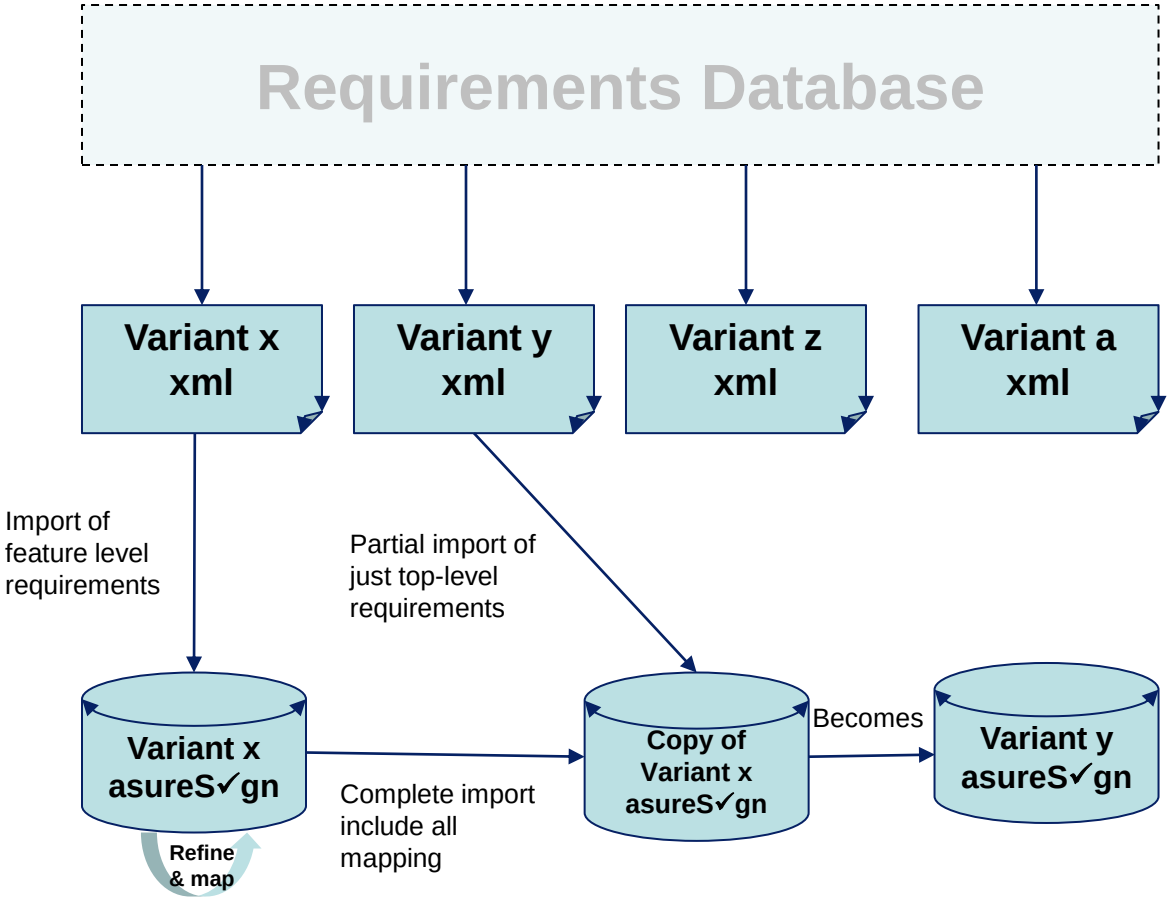




asureVIEW™

Any questions ?

Variant Management



Requirements completeness