Requirements-driven Verification Methodology

for Standards Compliance

Serrie-justine Chapman (TVS)
Mike Bartley (TVS)
Darren Galpin (Infineon)

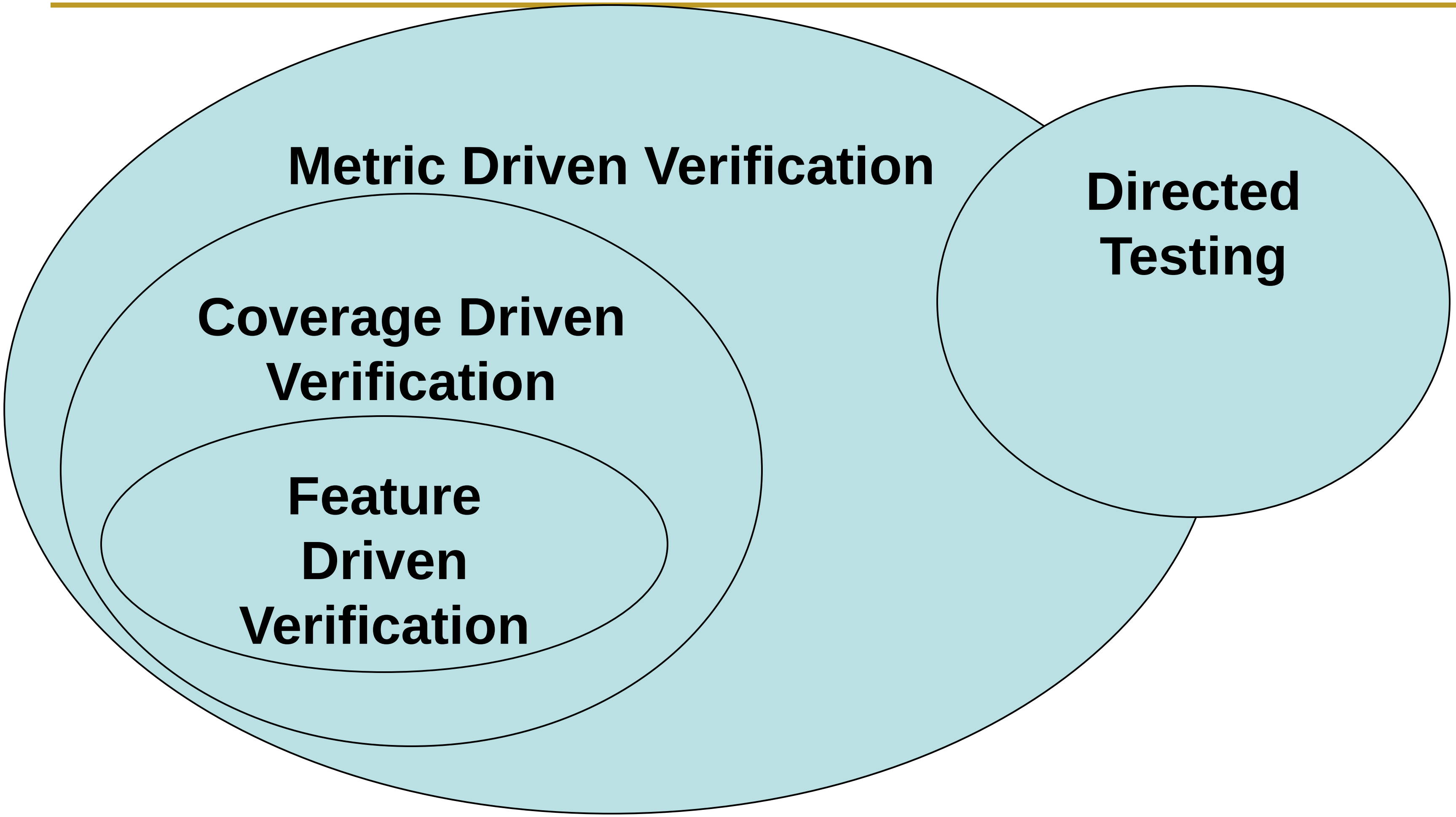
infineon

TVS
Test and Verification Solutions

Agenda

- **Motivation**
  - Why Requirements Driven Verification?
- **Introduction to Safety**
  - The Safety Standards
  - What do we need to do? And deliver?
- **Supporting Requirements Driven Verification with Advanced Verification Techniques**
- **Tool Support**
- **Advantages of Requirements Driven Verification**

An Overview of Verification Approaches


Metric Driven Verification
Directed Testing
Coverage Driven Verification
Feature Driven Verification

- Constrained random verification
- Assertion-based verification.
- Formal property based verification.

Why Requirements Driven Verification?

- **Metric Driven Verification**
  - Allows us to define targets
  - And monitor progress
- **Coverage Driven Verification**
  - Most common metric driven verification approach
  - Code Coverage
  - Functional coverage
    - Might be related to features
- **Feature Driven Verification**
  - Features MIGHT be related to spec
    - Is that relationship captures?
  - Are features related to requirements?

Safety Standards

- **IEC61508:** Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
- **DO254/DO178:** Hardware/Software considerations in airborne systems and equipment certification
- **EN50128:** Software for railway control and protection systems
- **IEC60880:** Software aspects for computer-based systems performing category A functions
- **IEC62304:** Medical device software -- Software life cycle processes
- **ISO26262:** Road vehicles – Functional safety

Introduction to Safety

- **The life cycle processes are identified**
- **Objectives and outputs for each process are described**
  - Objectives are mandatory
  - But vary by Integrity Level
  - For higher Integrity Levels, some Objectives require Independence

Key Elements

- **Plans & Standards**
- **Requirements**
- **Design Specifications**
- **Reviews and Analyses**
- **Testing (against specifications)**
  - At different levels of hierarchy
- **Test Coverage Criteria**
- **Requirements Traceability**
- **Independence**

Key Deliverables

- Hardware Verification Plan
- Validation and Verification Standards
- Hardware Traceability Data
- Hardware Review and Analysis Procedures
- Hardware Review and Analysis Results
- Hardware Test Procedures
- Hardware Test Results
- Hardware Acceptance Test Criteria
- Problem Reports
- Hardware Configuration Management Records
- Hardware Process Assurance Records

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**

*** All Definitions taken from IREB**

REQUIREMENTS ENGINEERING CORE ACTIVITIES

Requirements Engineering is a systematic and disciplined approach to the specification and management of requirements with the following goals:

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

Four core activities :

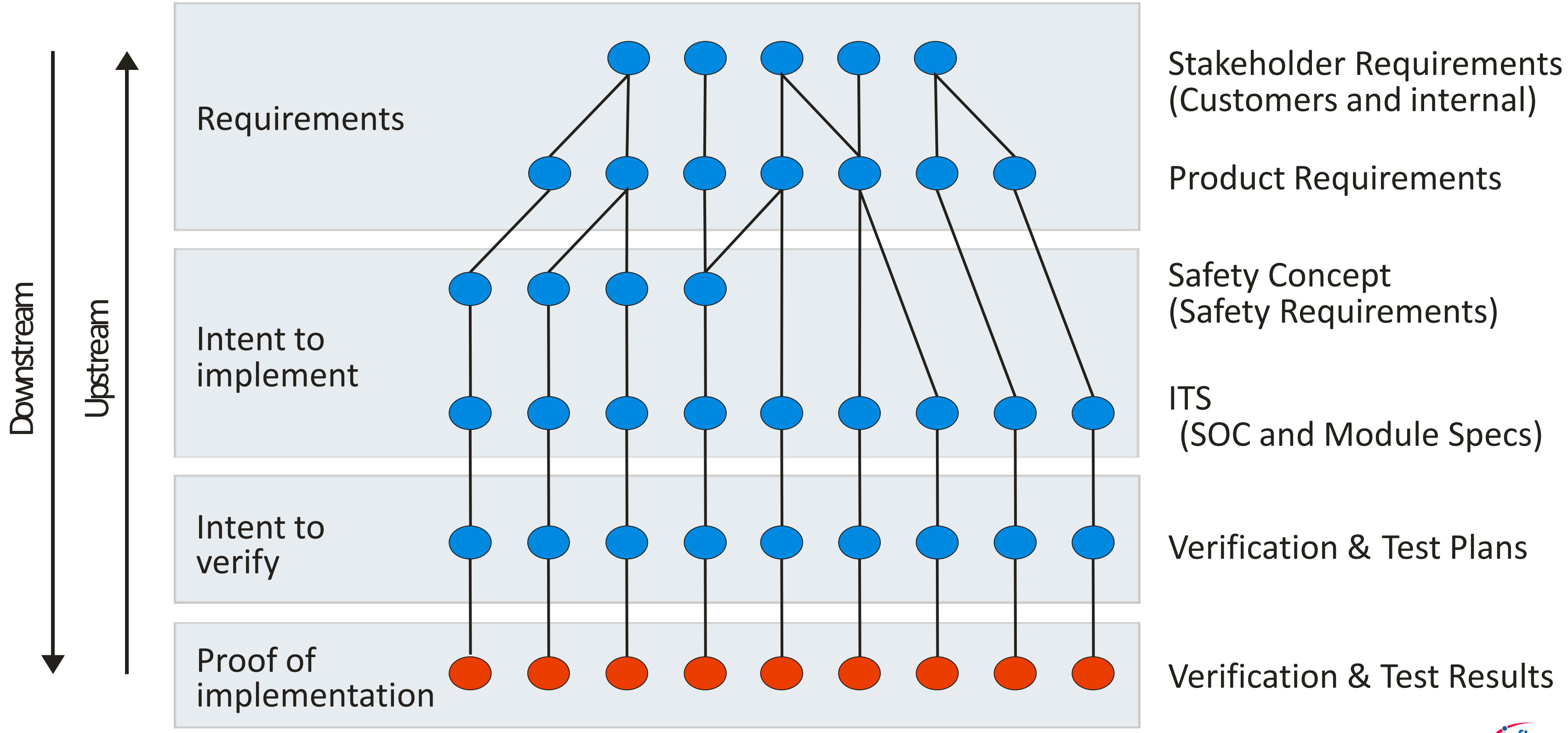
- **Elicitation**
- **Documentation**
- **Validation and negotiation**
- **Management**

Requirements Traceability

- **Documented:**
  - all integrity levels/classes
- **All requirements:**
  - Tested or otherwise verified (Audit trail)
- **Traceable**

"Requirements Traceability =

the ability to follow the life of a requirement, in both a backward and forward direction"

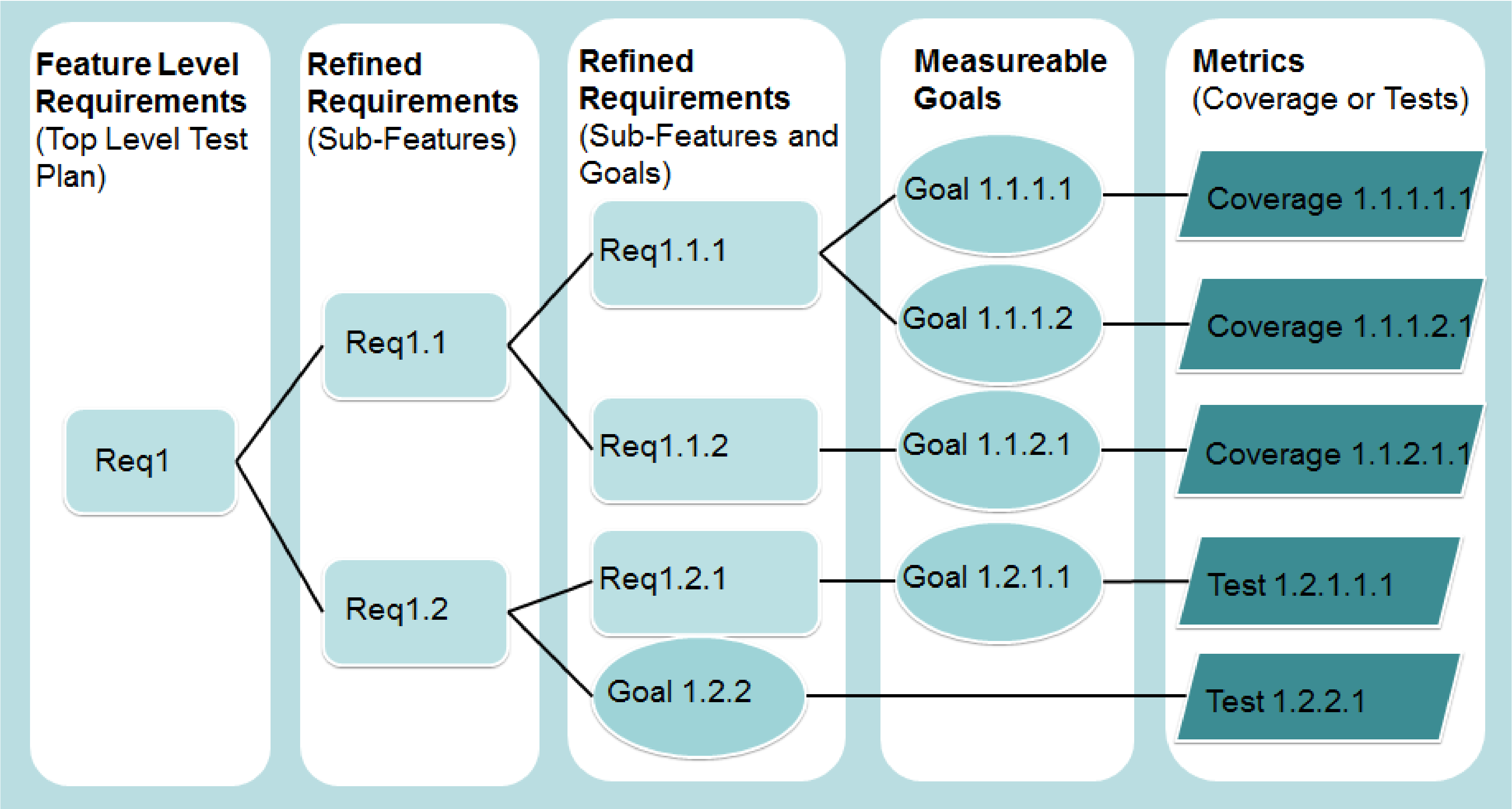


Downstream
Upstream
Requirements
Intent to implement
Intent to verify
Proof of implementation
Stakeholder Requirements (Customers and internal)
Product Requirements
Safety Concept (Safety Requirements)
ITS (SOC and Module Specs)
Verification & Test Plans
Verification & Test Results

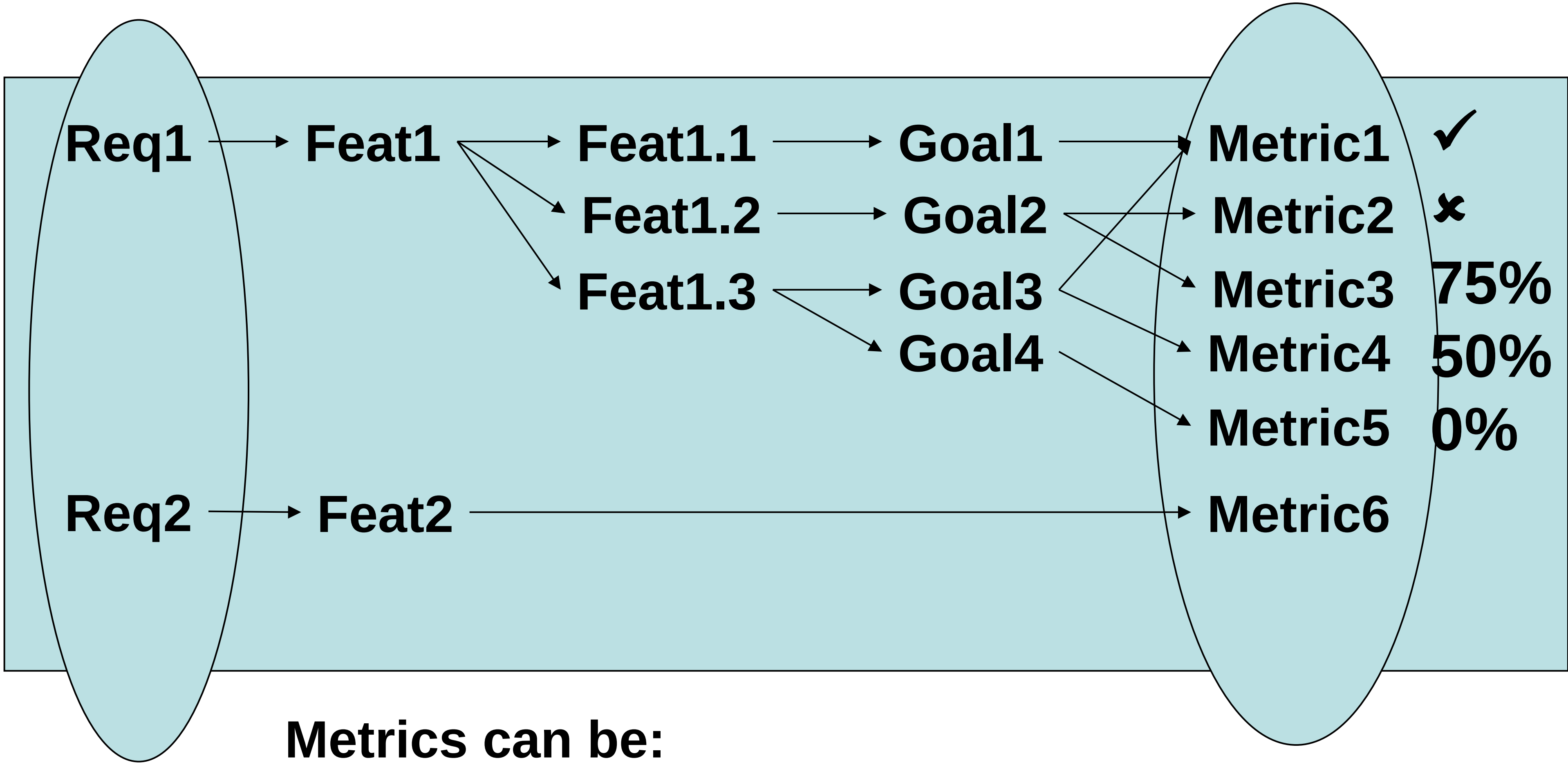
Supporting Advanced Verification

- Constrained random verification with automated checks based on models or scoreboards, etc.
- Coverage driven verification based on functional coverage models and code coverage metrics.
- Assertion-based verification.
- Formal property based verification.

Supporting Advanced Verification



Tracking



Req1 → Feat1 → Feat1.1, Feat1.2, Feat1.3

Feat1.1 → Goal1

Feat1.2 → Goal2

Feat1.3 → Goal3, Goal4

Goal1 → Metric1

Goal2 → Metric2, Metric3

Goal3 → Metric1, Metric4

Goal4 → Metric5

Req2 → Feat2 → Metric6

Metric1 ✓

Metric2 ✗

Metric3 75%

Metric4 50%

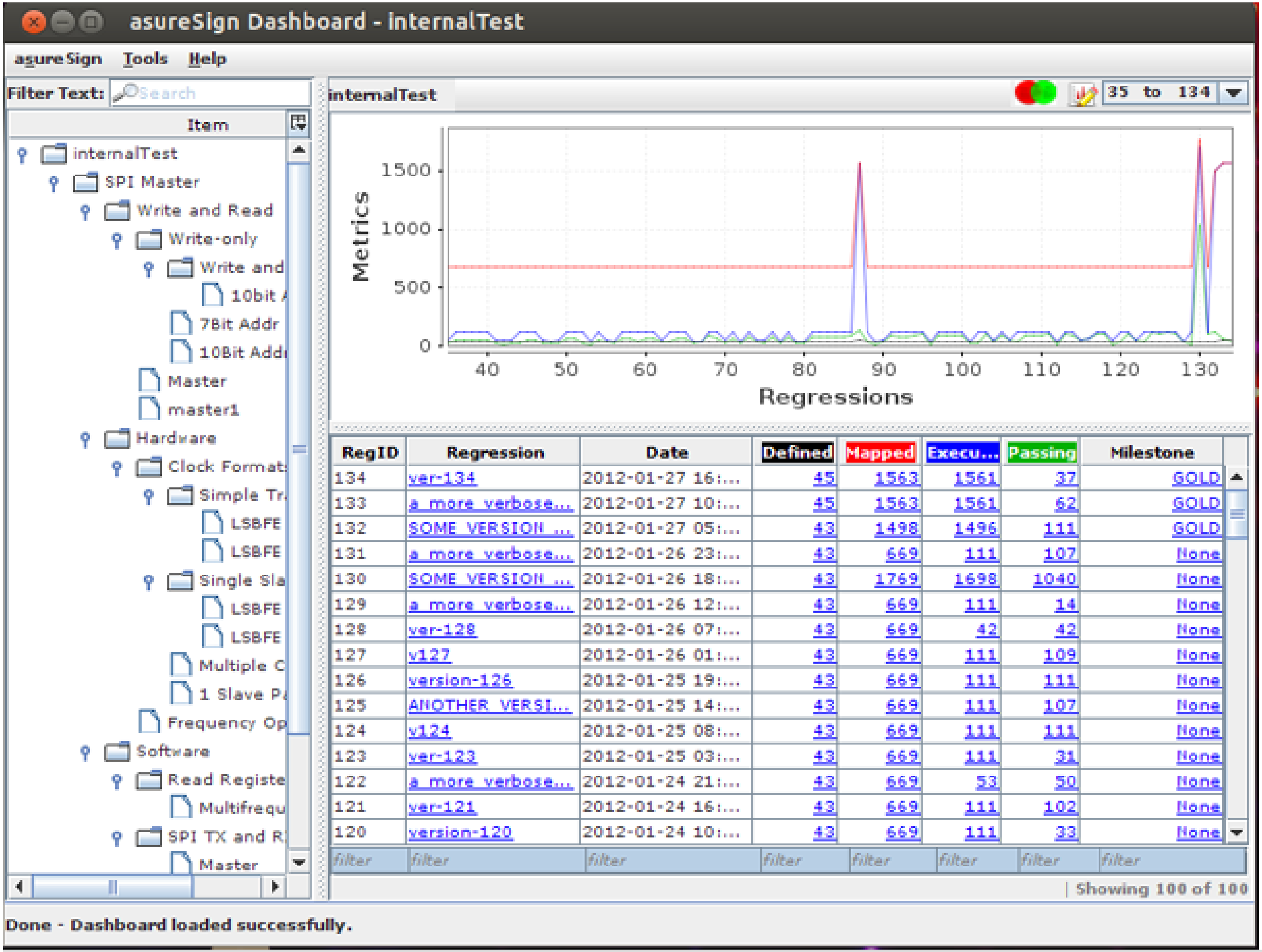
Metric5 0%

Metric6

Metrics can be:

- From HW verification
- From Silicon validation
- From SW testing

Track Progress on Requirements Signoff



RegID	Regression	Date	Defined	Mapped	Execu...	Passing	Milestone
134	ver-134	2012-01-27 16:...	45	1563	1561	37	GOLD
133	a more verbose...	2012-01-27 10:...	45	1563	1561	62	GOLD
132	SOME VERSION ...	2012-01-27 05:...	43	1498	1496	111	GOLD
131	a more verbose...	2012-01-26 23:...	43	669	111	107	None
130	SOME VERSION ...	2012-01-26 18:...	43	1769	1698	1040	None
129	a more verbose...	2012-01-26 12:...	43	669	111	14	None
128	ver-128	2012-01-26 07:...	43	669	42	42	None
127	v127	2012-01-26 01:...	43	669	111	109	None
126	version-126	2012-01-25 19:...	43	669	111	111	None
125	ANOTHER VERSI...	2012-01-25 14:...	43	669	111	107	None
124	v124	2012-01-25 08:...	43	669	111	111	None
123	ver-123	2012-01-25 03:...	43	669	111	31	None
122	a more verbose...	2012-01-24 21:...	43	669	53	50	None
121	ver-121	2012-01-24 16:...	43	669	111	102	None
120	version-120	2012-01-24 10:...	43	669	111	33	None

Showing 100 of 100

Done - Dashboard loaded successfully.

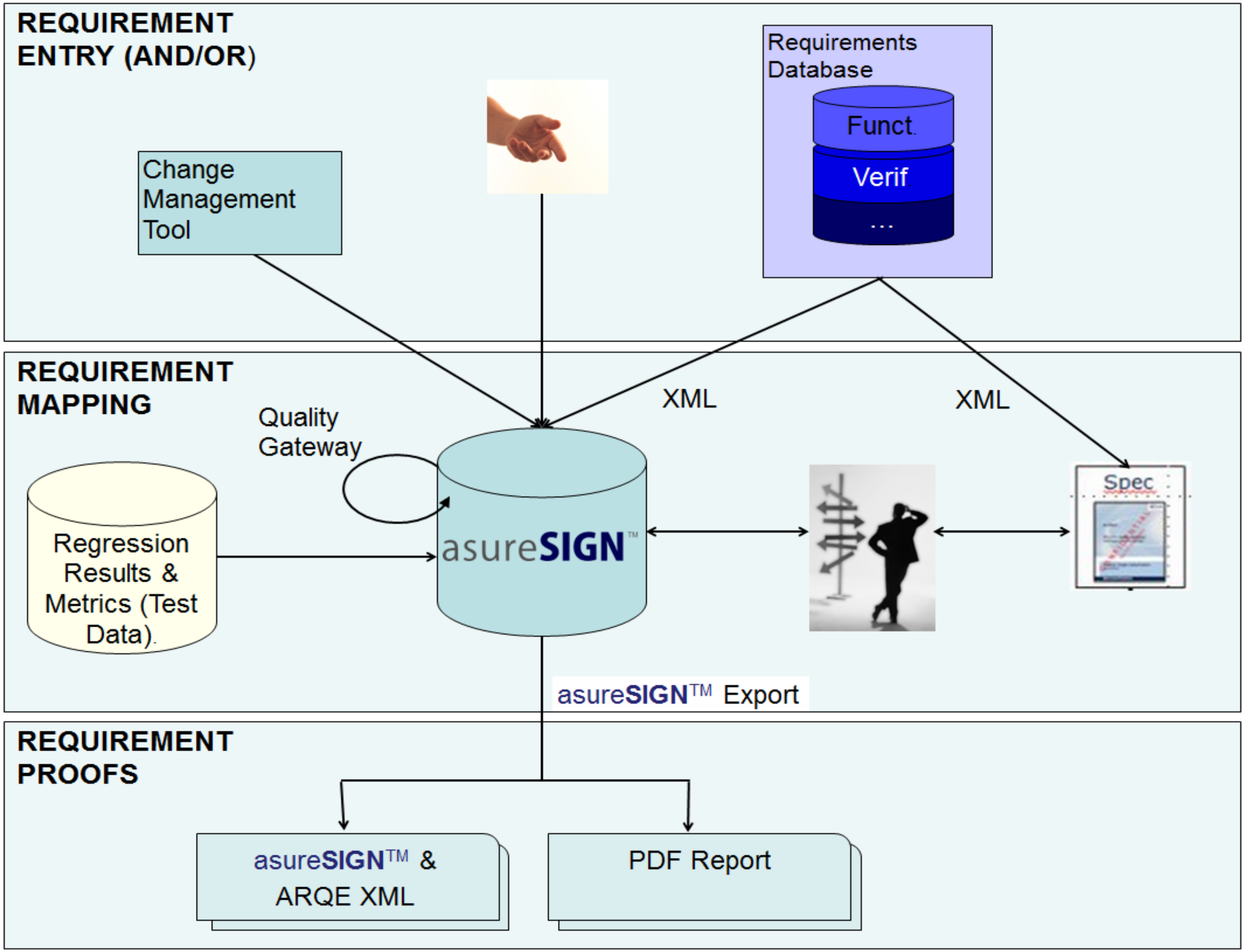
Supporting Hierarchical Verification

- A requirement might be signed off at multiple levels of hierarchy during the hardware development
  - Block
  - Subsystem
  - SoC
  - System
    - Including Software
  - Post Silicon

Tool Support Requirements

- Requirements -> test plan
- Data Integrity, hierarchy, data translation
- Change management – instant update
- Live database -> easy documentation
- Tailored Documented proof
- Allows reviews of implementation document against test plan
- Mapping
- Test management
- Compliance / Audit Management

asureSIGN Dataflow



Advantages of Requirements Driven Verif

- **Requirements Management**
- **Verification Management**
- **Project Management**
- **Impact Analysis**
- **Product Line Engineering**
- **Variant management**
- **Improved Product Sign-Off**

Conclusion

- **Requirements Driven Verification**
  - Needed to support compliance to various hardware (and software) safety standards
  - There are several other advantages
- **Advanced verification techniques can be deployed in Requirements Driven Verification**
  - Tool support required