AST 2016 Conference
Automotive SW Testing Conference

Safer Driving – Standards for Software Testing of Automotive Systems

Stuart Reid PhD, FBCS
STA Consulting Inc.
(stuart@sta.co.kr)

ktl 한국산업기술시험원 STA Global Testing Leader 테스팅컨설팅 KSTQB

Scope

AST 2016 Conference
Automotive SW Testing Conference

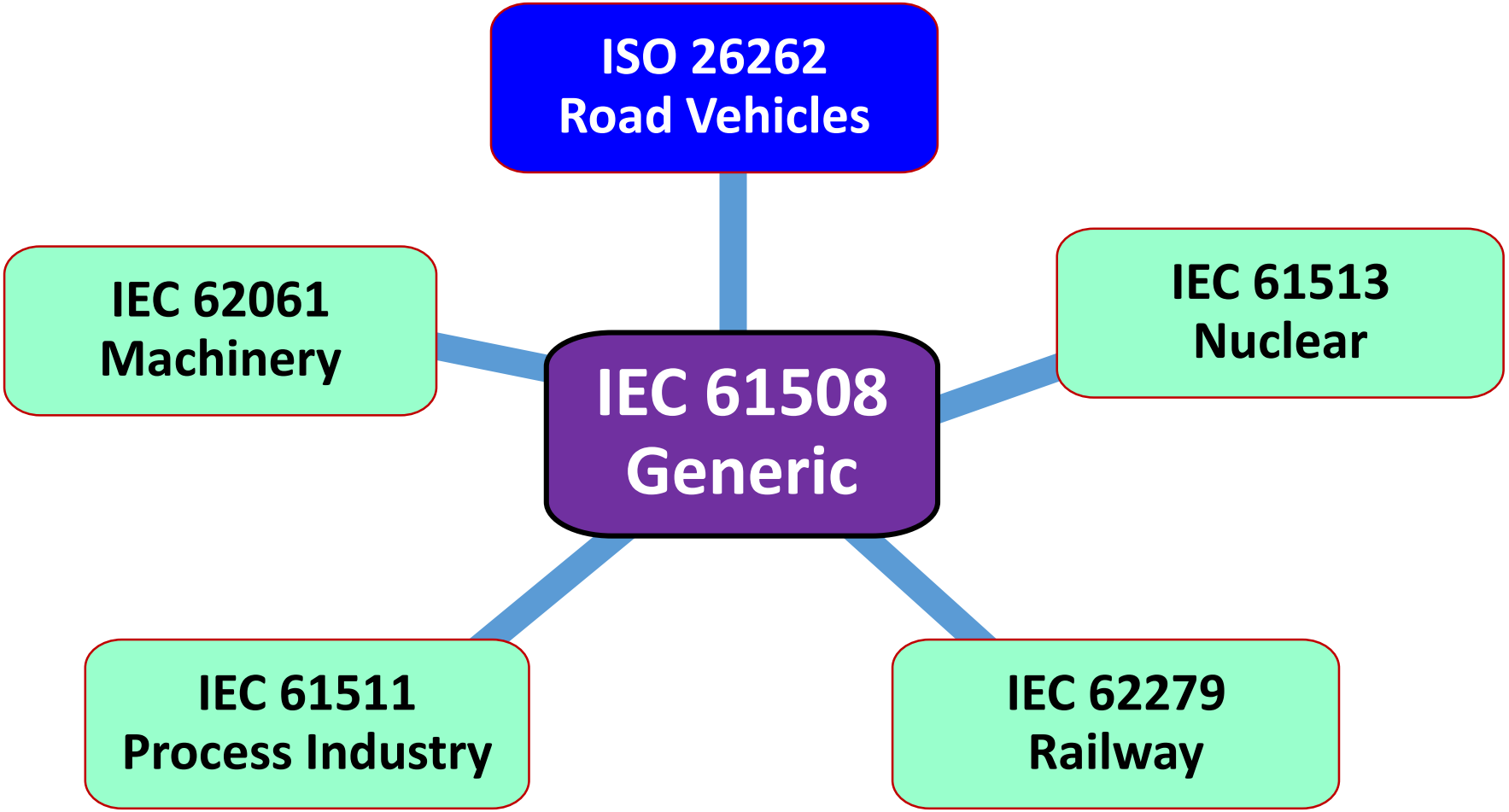
Automotive Safety Standards – ISO 26262

Testing Standards – ISO 29119, ISO 33063 & ISO 20246

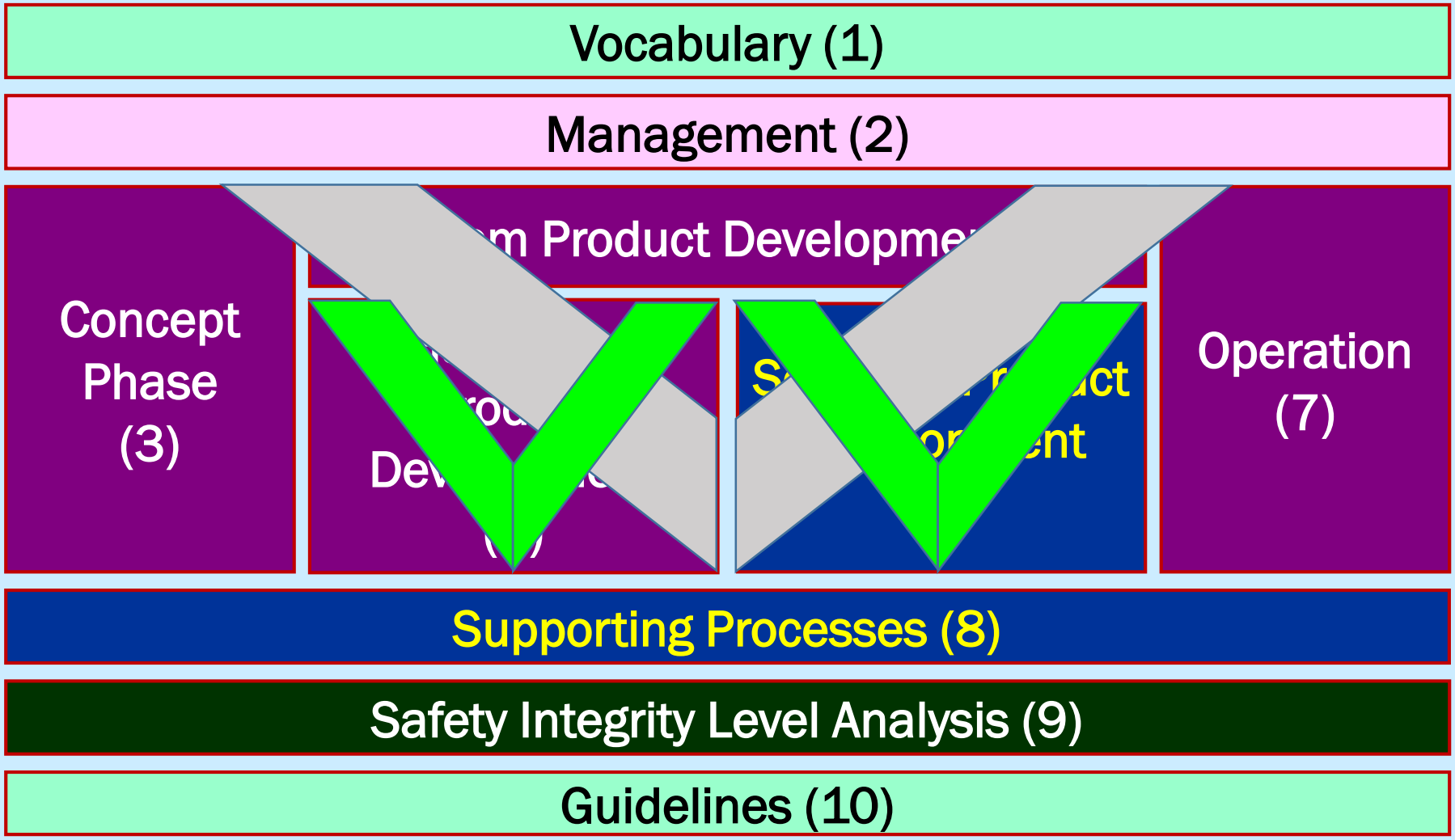
Mappings between ISO 26262 and ISO 29119 – processes, techniques and documentation

A co-ordinated approach – using both ISO 26262 and ISO 29119

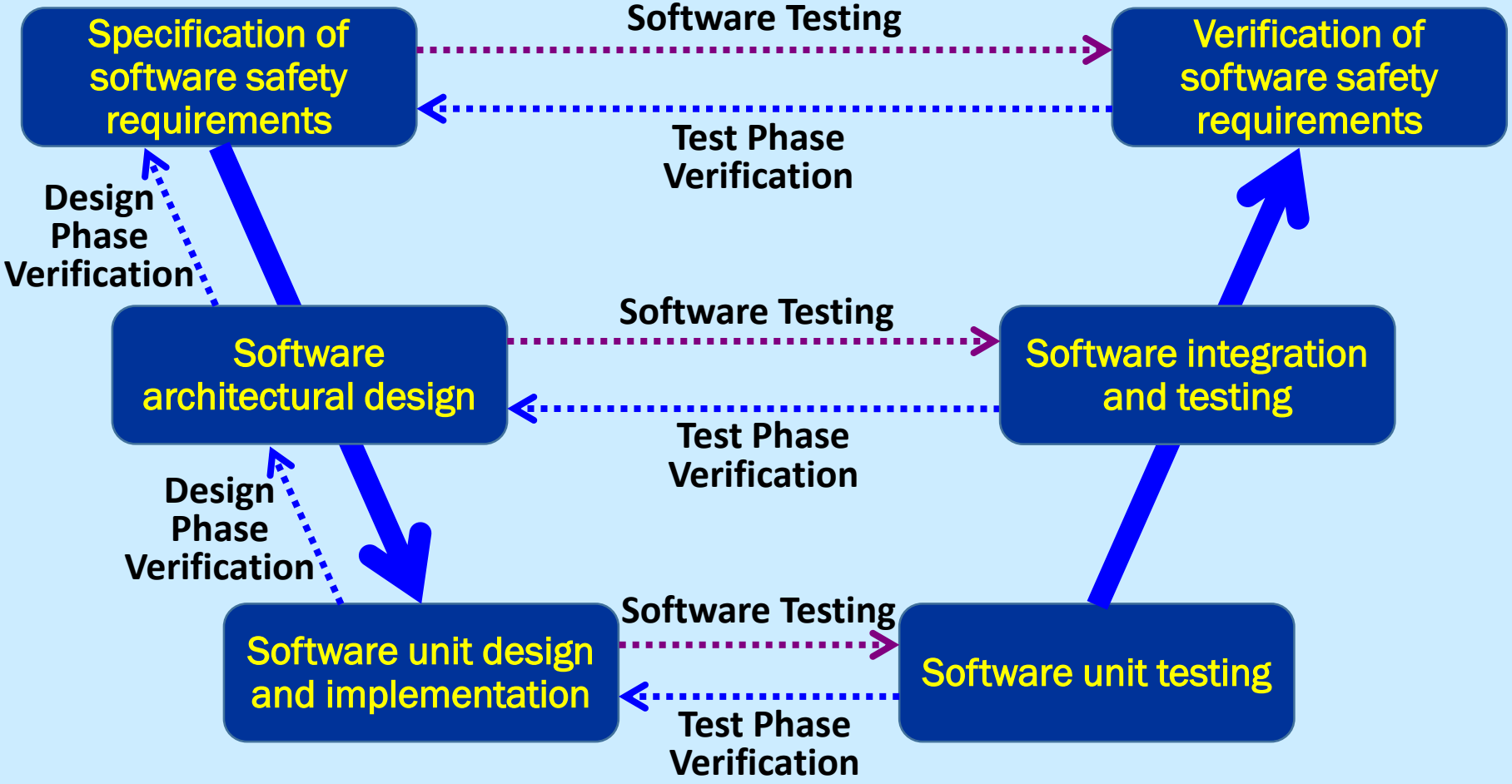
IEC 61508 - Functional safety of systems



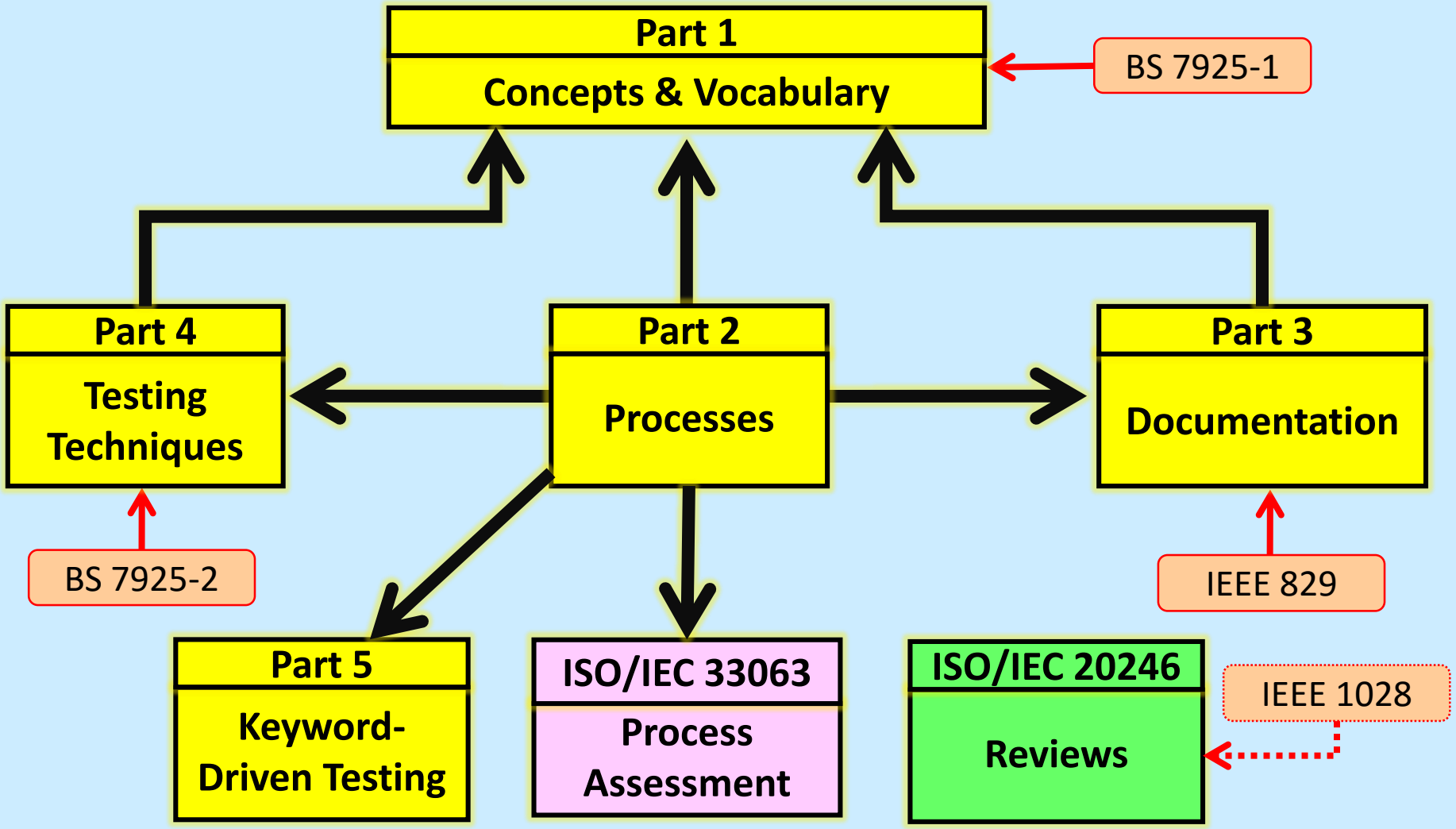
ISO 26262 - Overview



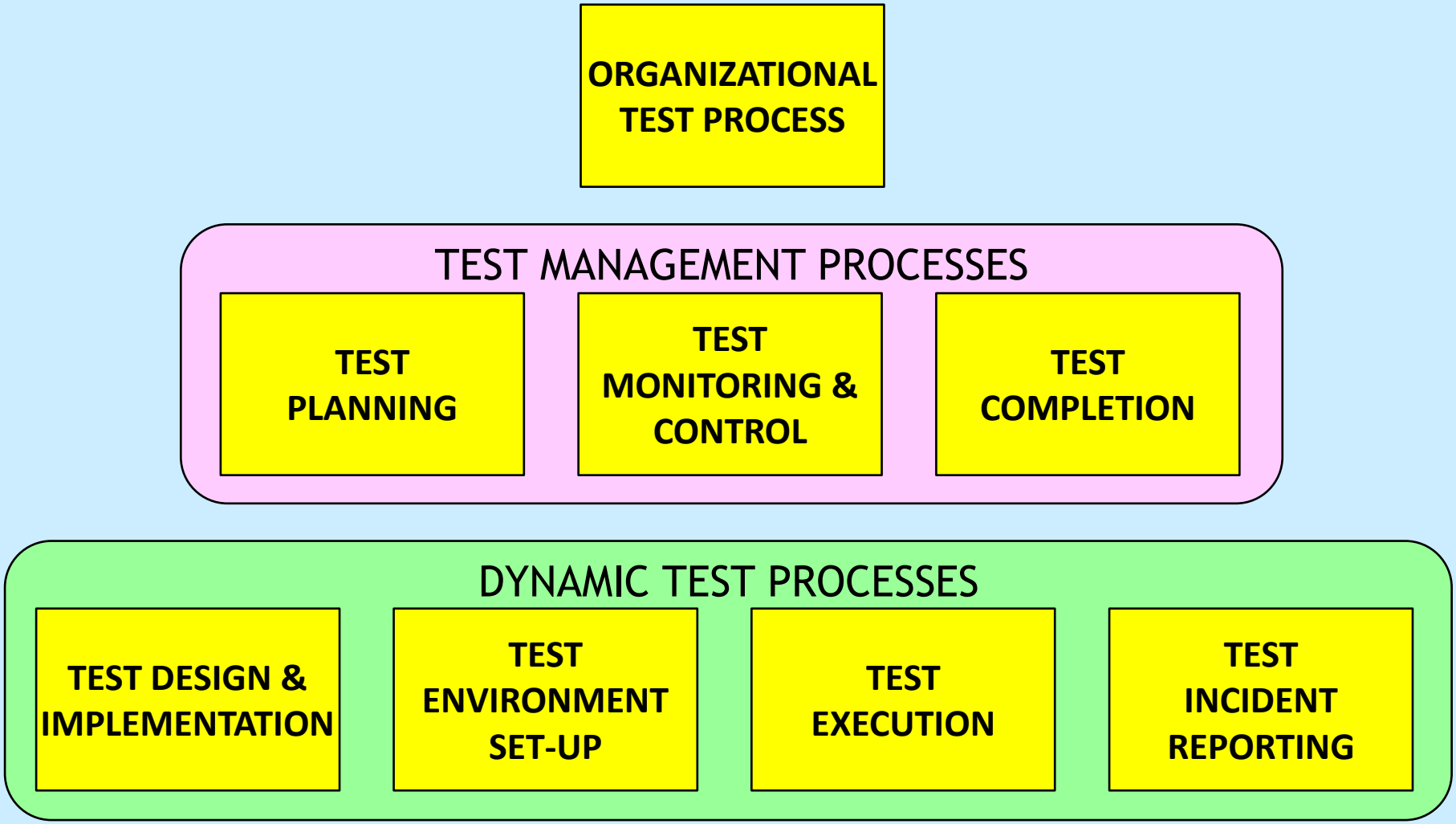
ISO 26262 – Software development process



ISO/IEC/IEEE 29119 – Structure



ISO 29119-2 Test Processes



ISO 26262 – Safety Integrity Level (ASIL)

- **Severity**
  - S1 – light/moderate injuries
  - S2 – severe/life threatening injuries
  - S3 - life threatening/fatal injuries
- **Probability of exposure**
  - E1 – v. low probability
  - E2 – low probability
  - E3 – medium probability
  - E4 – high probability
- **Controllability**
  - C1 – simply controllable
  - C2 – normally controllable
  - C3 – difficult/uncontrollable

Severity	Probability	Controllability		
		C1	C2	C3
S1	E1	ASILs		
	E2			
	E3			
	E4			
S2	E1			
	E2			
	E3			
	E4			
S3	E1			
	E2			
	E3			
	E4			

ISO 26262-6 – Unit Testing

- 9.2 General
  - A procedure for testing the software unit against the software unit design specifications is established, and the tests are carried out in accordance with this procedure.
- 9.4.3
  - The software unit testing methods listed in Table 10 shall be applied…

Table 10 — Methods for software unit testing

Methods		ASIL			
		A	B	C	D
1a	Requirements-based test[a]	++	++	++	++
1b	Interface test	++	++	++	++
1c	Fault injection test[b]	+	+	+	++
1d	Resource usage test[c]	+	+	+	++
1e	Back-to-back comparison test between model and code, if applicable[d]	+	+	++	++

ISO 26262-6 – Software Integration Testing

- 10.2 General
  - In this sub-phase, the particular integration levels and the interfaces between the software elements are tested against the software architectural design.
- 10.4.3
  - The software integration test methods listed in Table 13 shall be applied…

Table 13 — Methods for software integration testing

Methods		ASIL			
		A	B	C	D
1a	Requirements-based test[a]	++	++	++	++
1b	Interface test	++	++	++	++
1c	Fault injection test[b]	+	+	++	++
1d	Resource usage test[cd]	+	+	+	++
1e	Back-to-back comparison test between model and code, if applicable[e]	+	+	++	++

ISO 26262 – Deriving Test Cases

Table 11 — Methods for deriving test cases for software unit testing
Table 14 — Methods for deriving test cases for software integration testing

	Methods	ASIL A	ASIL B	ASIL C	ASIL D
1a	Analysis of requirements	++	++	++	++
1b	Generation and analysis of equivalence classes[a]	+	++	++	++
1c	Analysis of boundary values[b]	+	++	++	++
1d	Error guessing[c]	+	+	+	+

Table 12 — Structural coverage metrics at the software unit level

	Methods	ASIL A	ASIL B	ASIL C	ASIL D
1a	Statement coverage	++	++	+	+
1b	Branch coverage	+	++	++	++
1c	MC/DC (Modified Condition/Decision Coverage)	+	+	+	++

Does not say 100%

Table 15 — Structural coverage metrics at the software architectural level

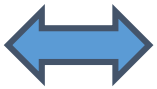
	Methods	ASIL A	ASIL B	ASIL C	ASIL D
1a	Function coverage[a]	+	+	++	++
1b	Call coverage[b]	+	+	++	++

Does not say 100%

ISO 29119-4 Boundary Value Analysis

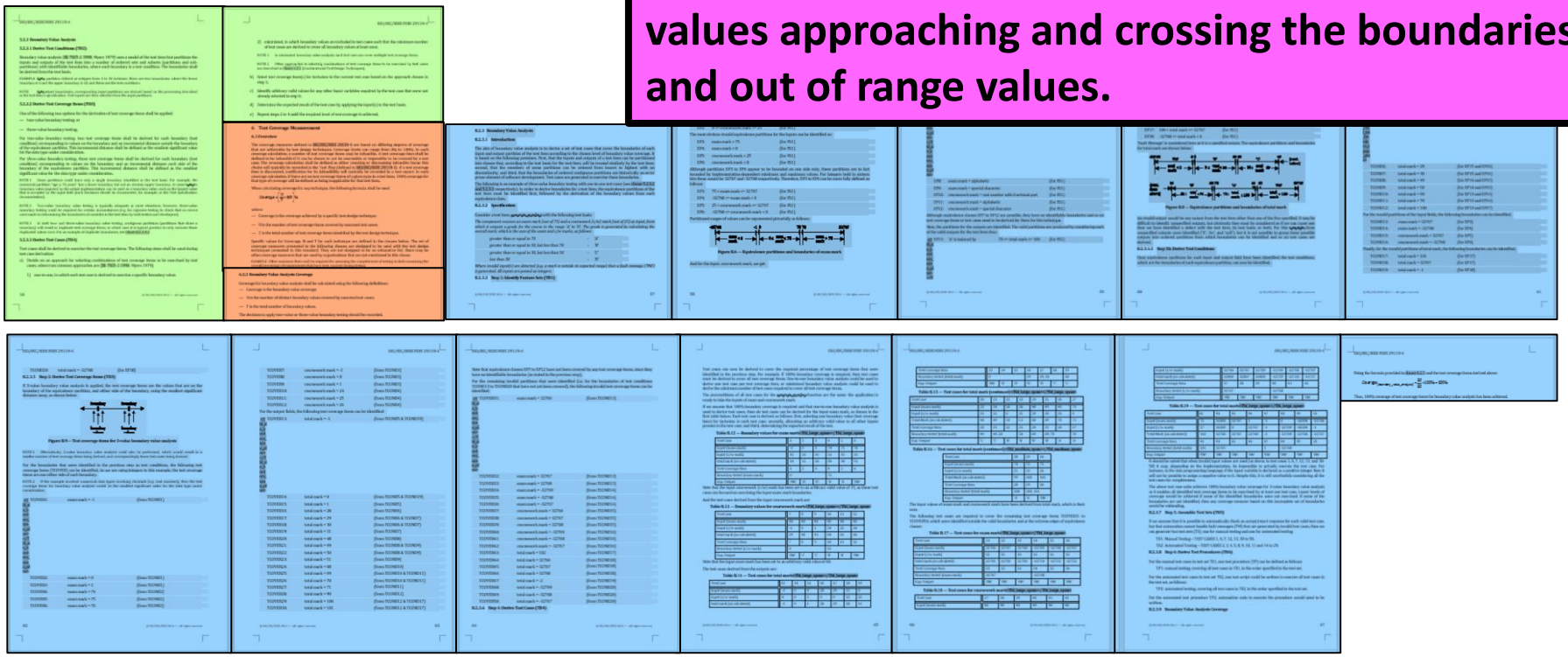
- Test Case Design
- Test Coverage
- Guidelines on Use

ISO 29119
13 pages



ISO 26262
1 sentence

This method applies to parameters or variables, values approaching and crossing the boundaries and out of range values.



ISO 26262-6
Verification software safety requirements

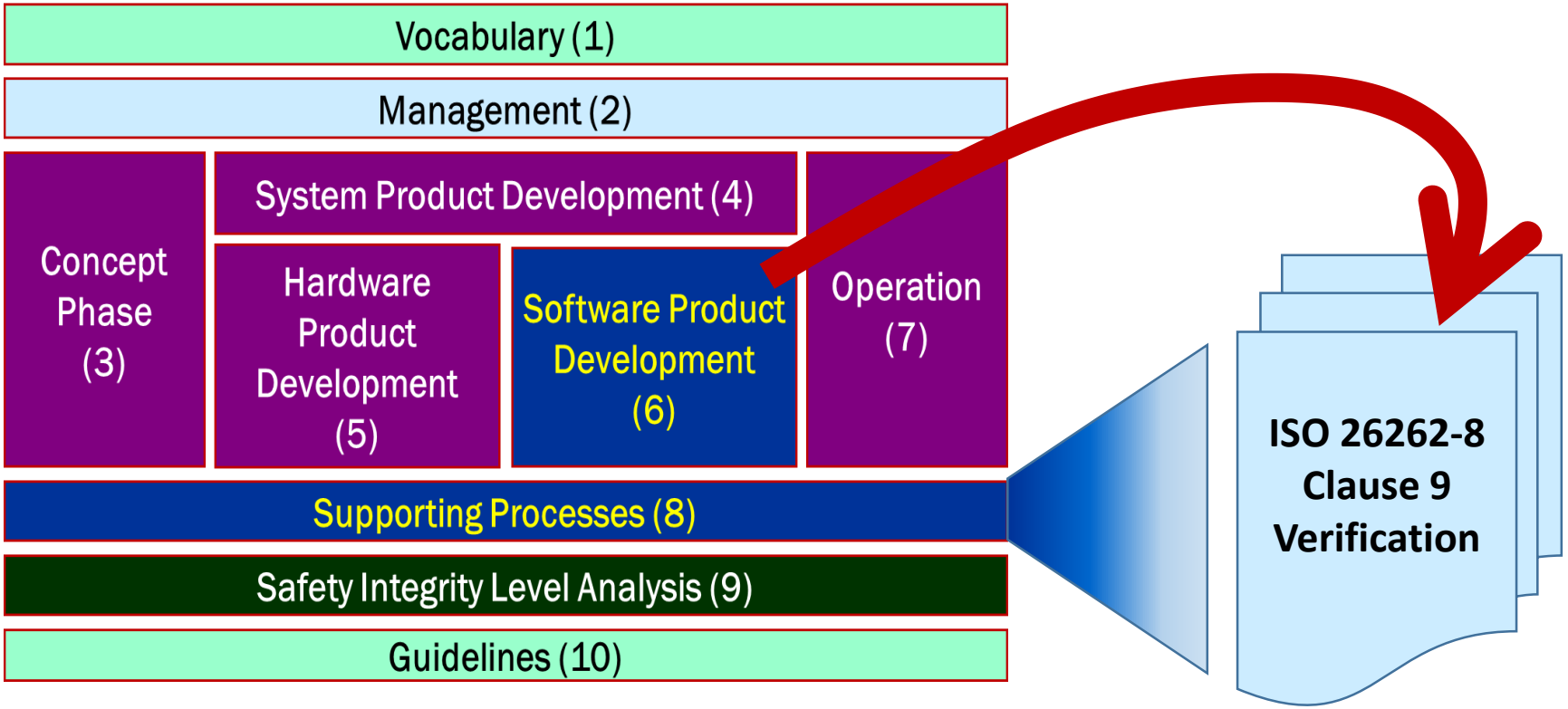
- 11.2 General
  - The purpose … is to demonstrate that the embedded software satisfies its requirements in the target environment.
- 11.4.2
  - To verify that the embedded software fulfils the software safety requirements, tests shall be conducted in the test environments listed in Table 16.

Table 16 — Test environments for conducting the software safety requirements verification

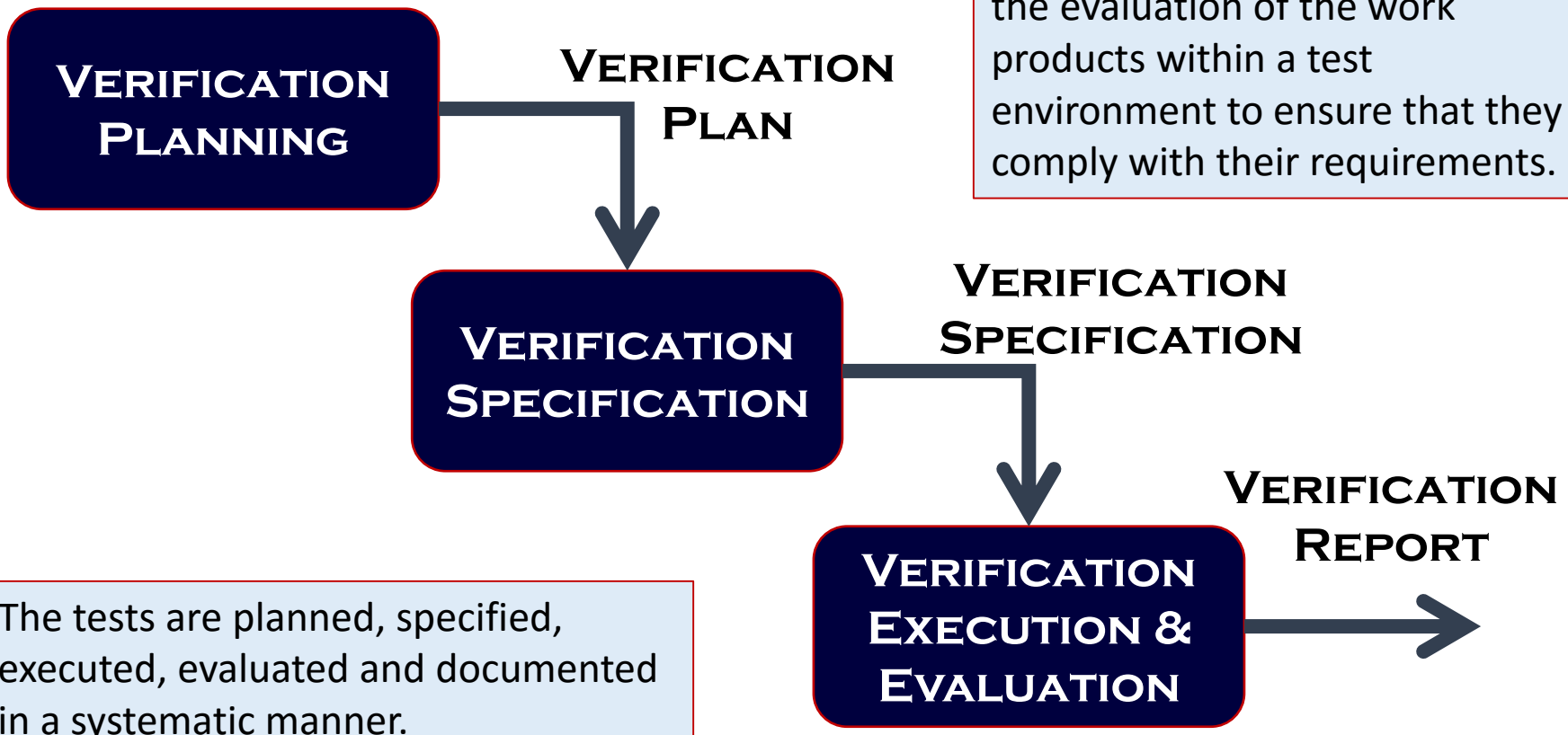
Methods		ASIL			
		A	B	C	D
1a	Hardware-in-the-loop	+	+	++	++
1b	Electronic control unit network environments[a]	++	++	++	++
1c	Vehicles	++	++	++	++

ISO 26262 Verification

9.4.2/10.4.2/11.4.1 Software unit testing/integration testing/verification of software safety requirements shall be planned, specified and executed in accordance with ISO 26262-8:2011, Clause 9.



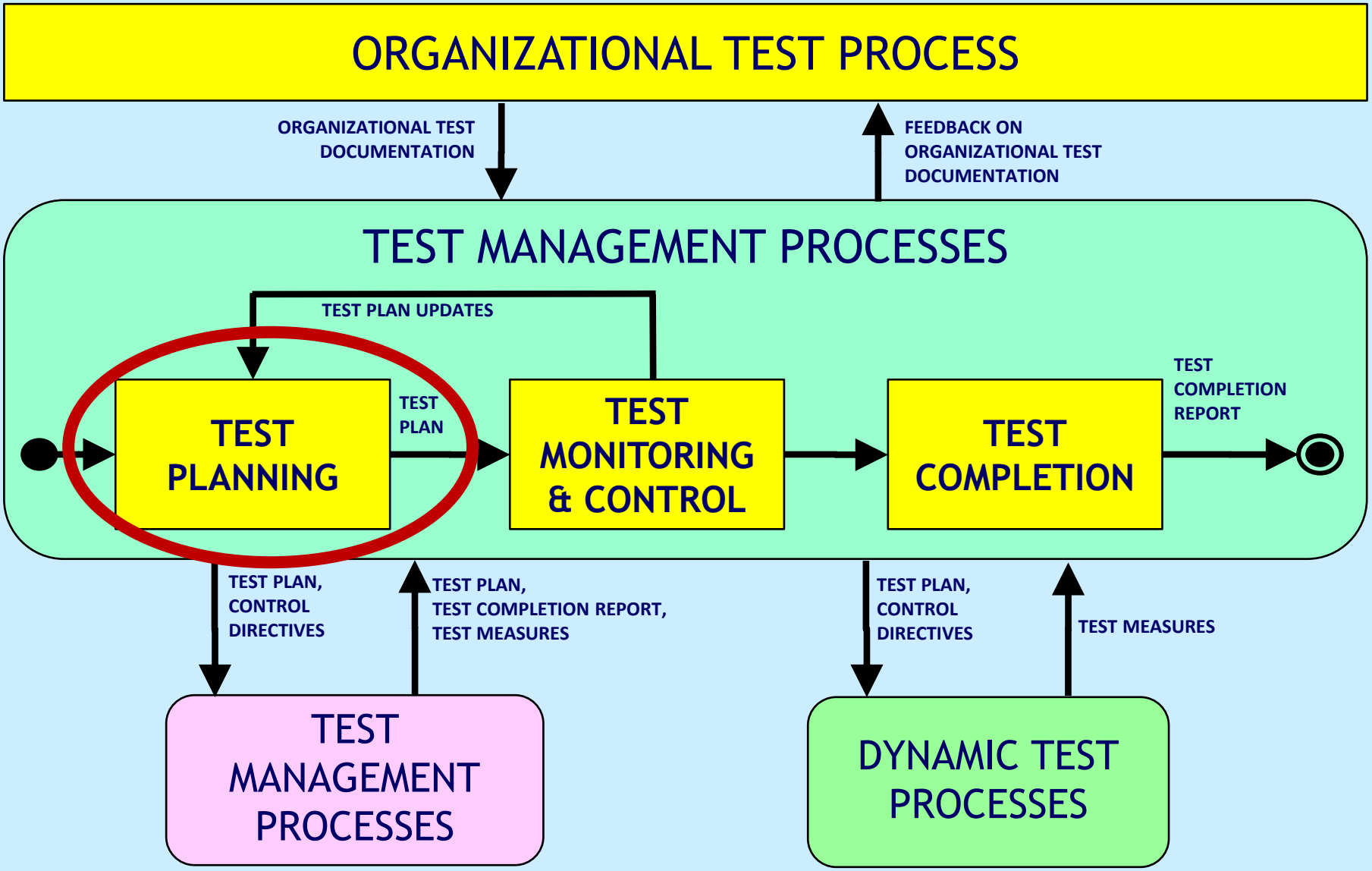
ISO 26262-8 Verification Clause



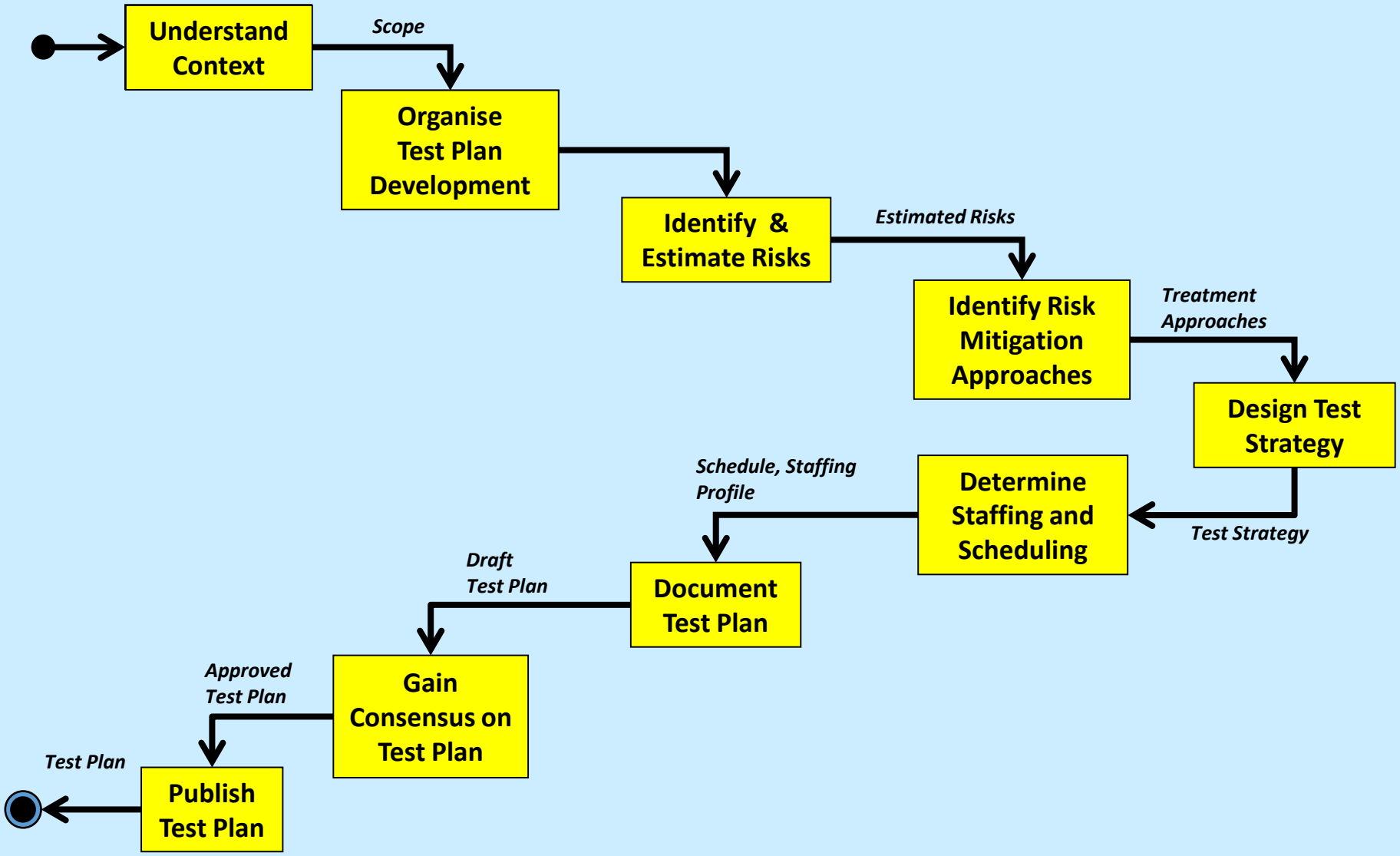
In the test phases, verification is the evaluation of the work products within a test environment to ensure that they comply with their requirements.

The tests are planned, specified, executed, evaluated and documented in a systematic manner.

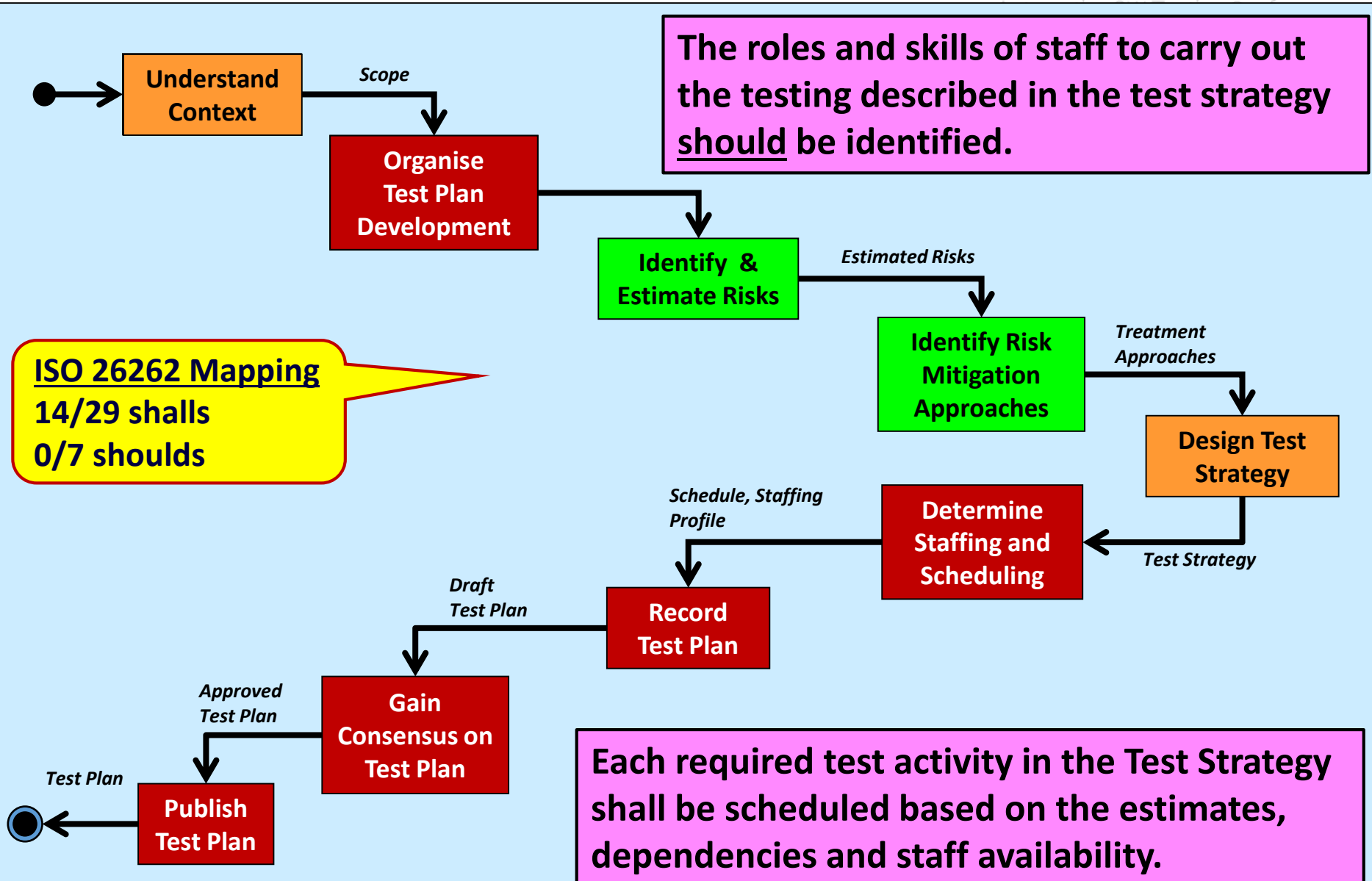
ISO 29119-2 – Test Management Processes



ISO 29119-2 - Test Planning Process

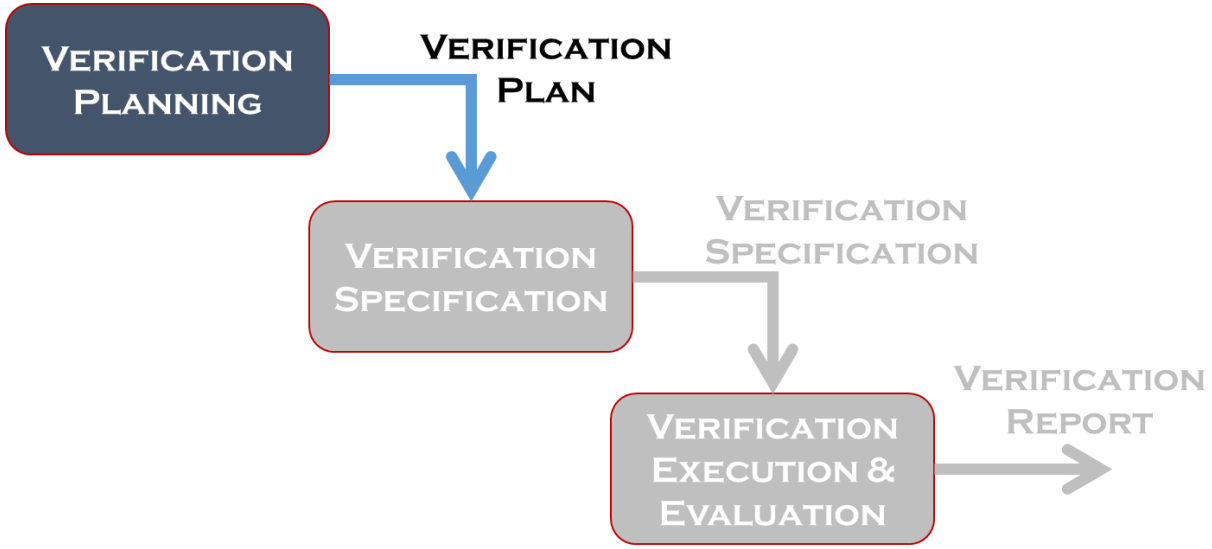


ISO 26262 Mapping to ISO 29119-2 Test Planning Process

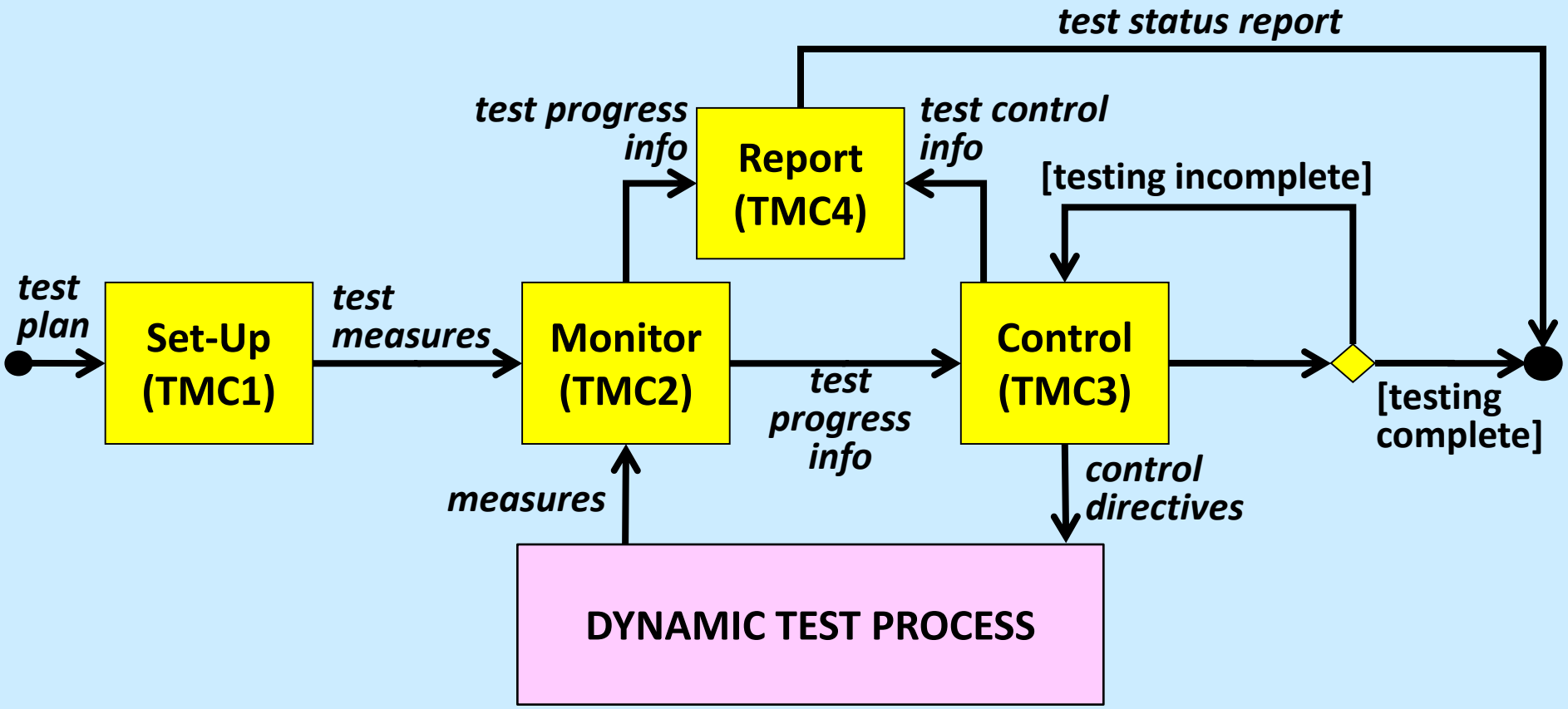


ISO 26262 - Verification Planning

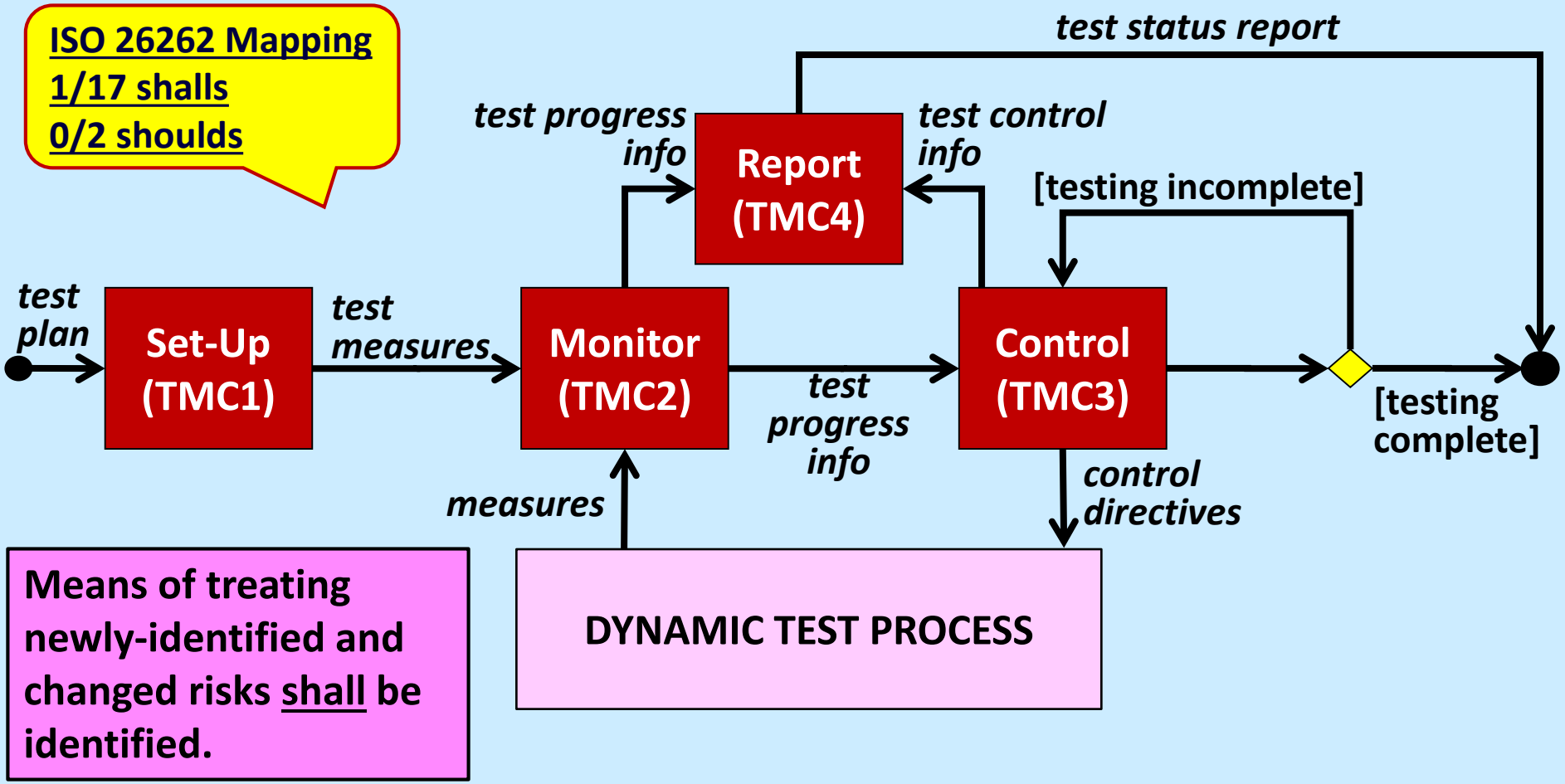
- No consideration of organizational test strategy / test policy
- No coverage of interaction/approval from stakeholders
- Nothing on estimation of required resources
  - no concept of constraints and compromises
- Nothing on staffing or scheduling



ISO 29119-2 –
Test Monitoring & Control Process



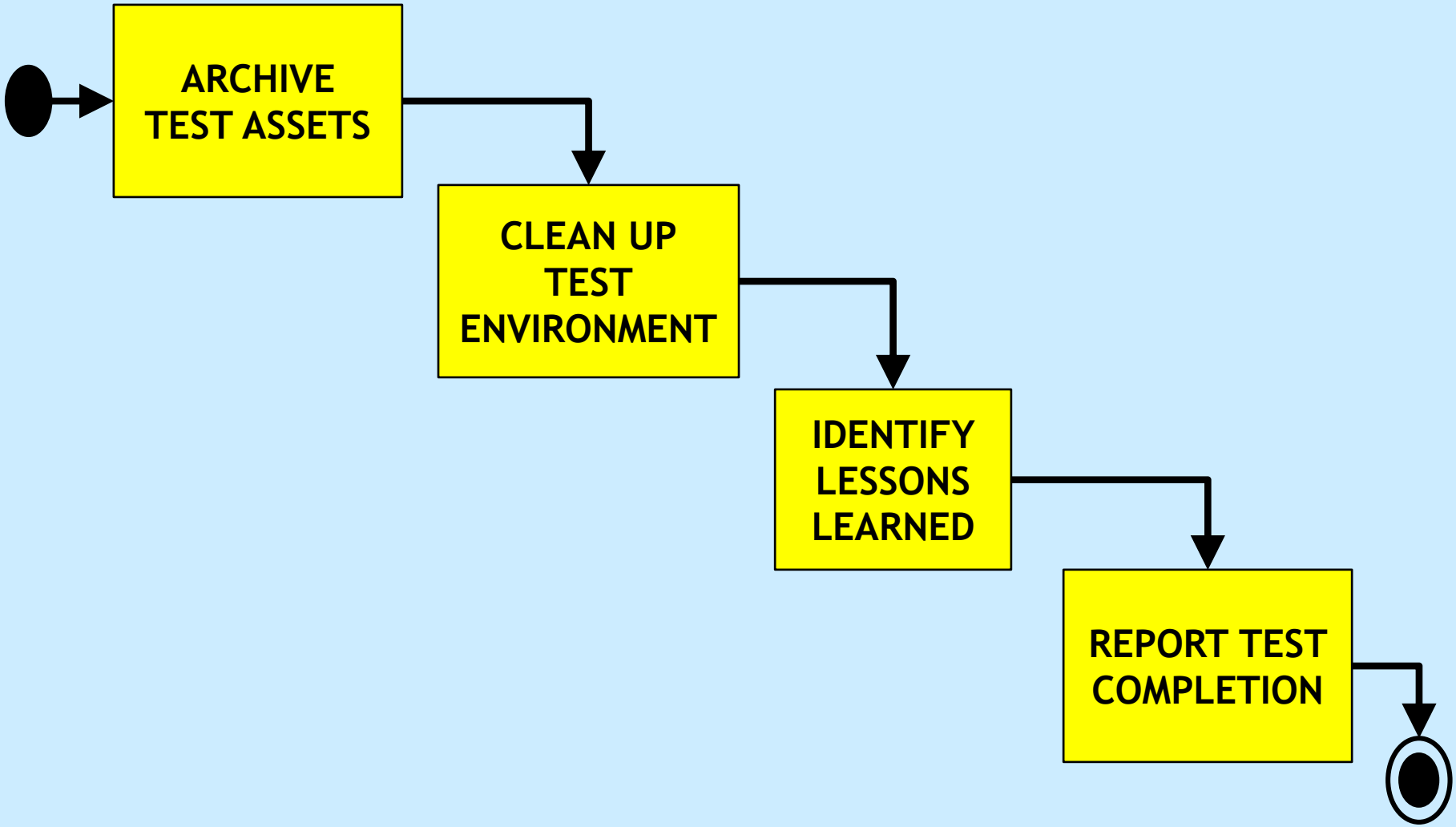
ISO 26262 Mapping to ISO 29119-2 Test Monitoring & Control Process



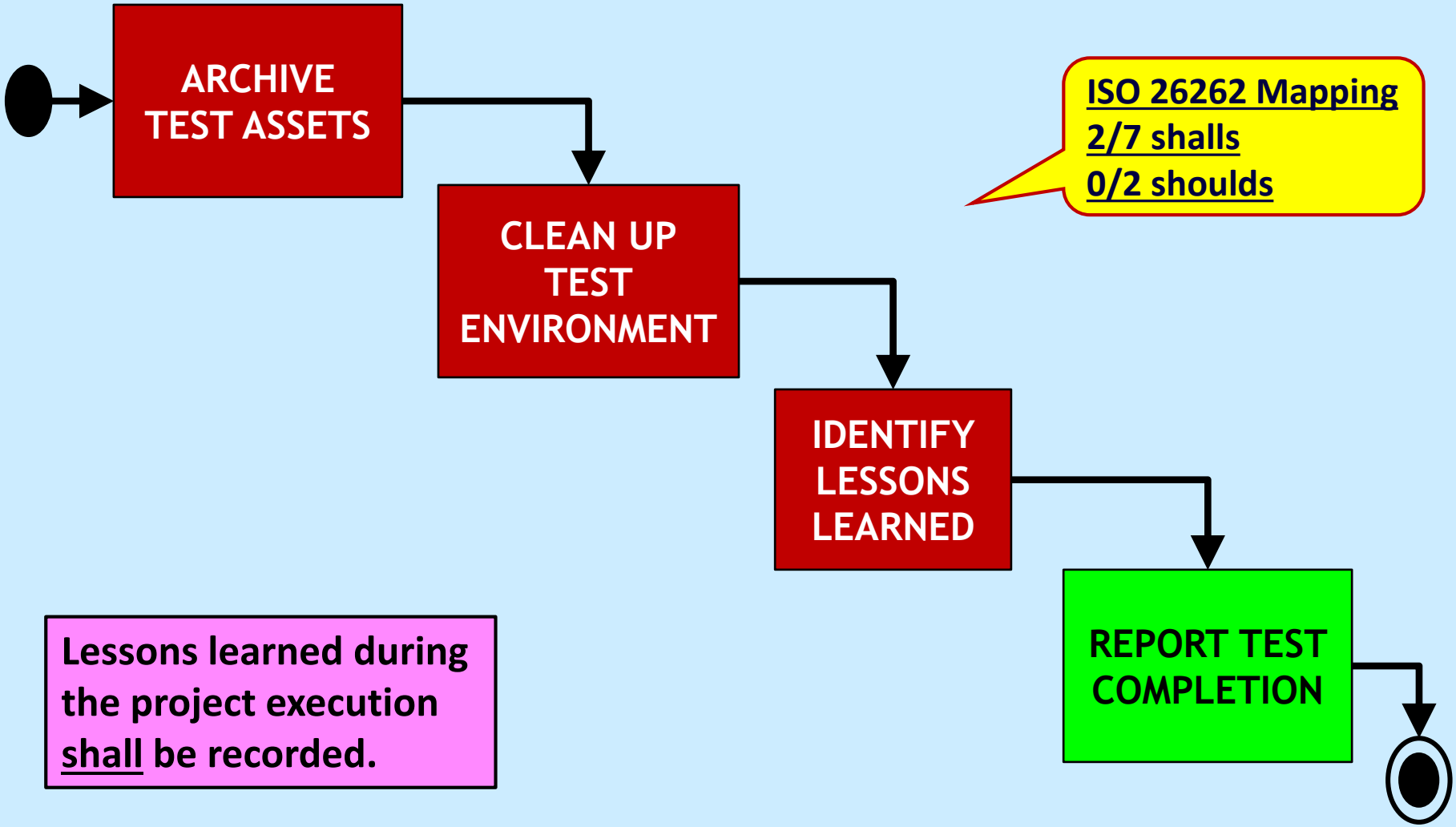
ISO 26262 – Test Management

- Appears to assume that once a plan is specified then testing will simply follow the plan and no so no divergence from the plan is possible
  - does not require new risks to be managed after architectural design
  - there is no requirement for test progress monitoring while testing is being performed
  - there is no requirement for test status reporting while testing is being performed
  - there is no requirement to control the testing
    - so no test management

ISO 29119-2
Test Completion Process



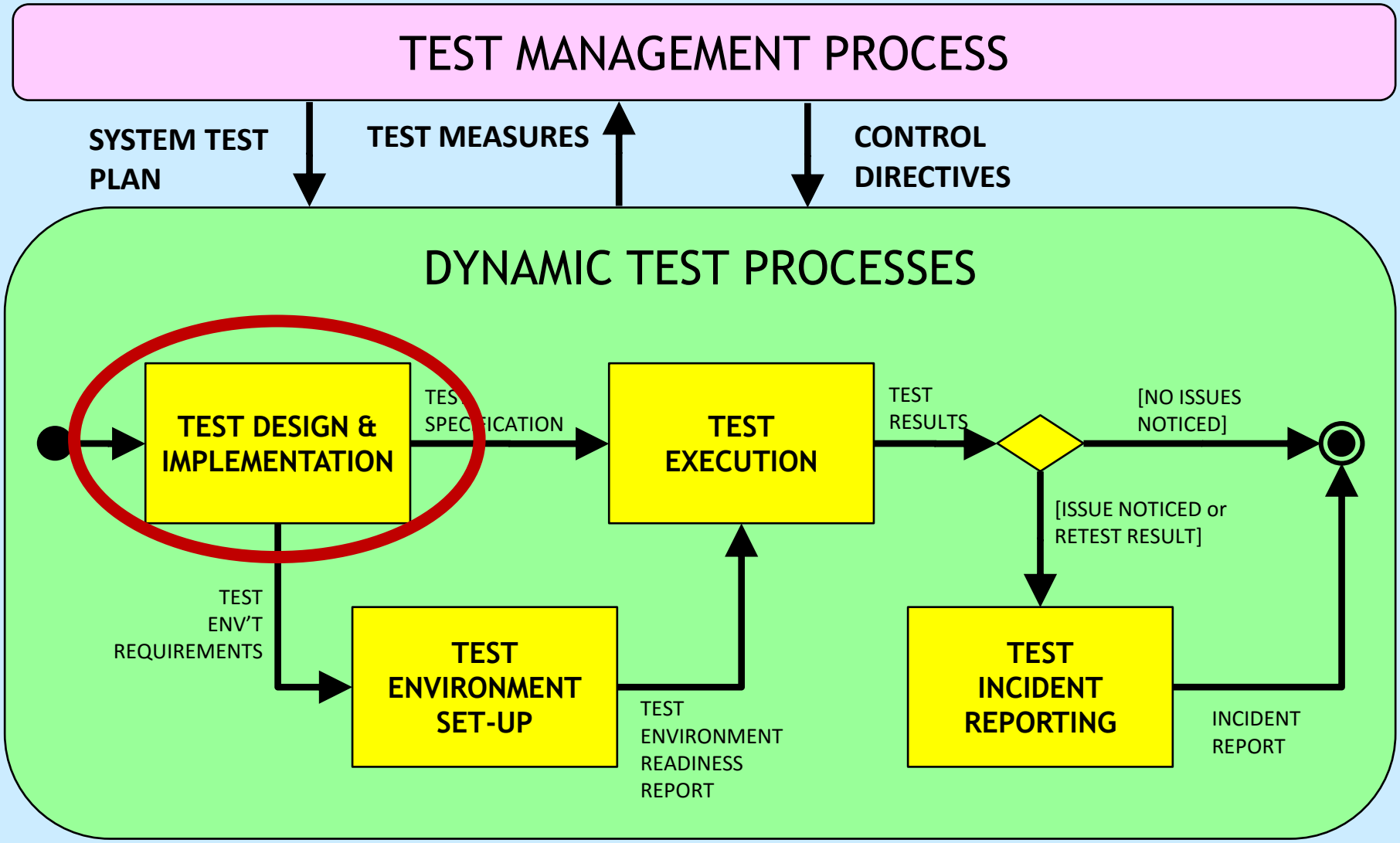
ISO 26262 Mapping to ISO 29119-2 Test Completion Process



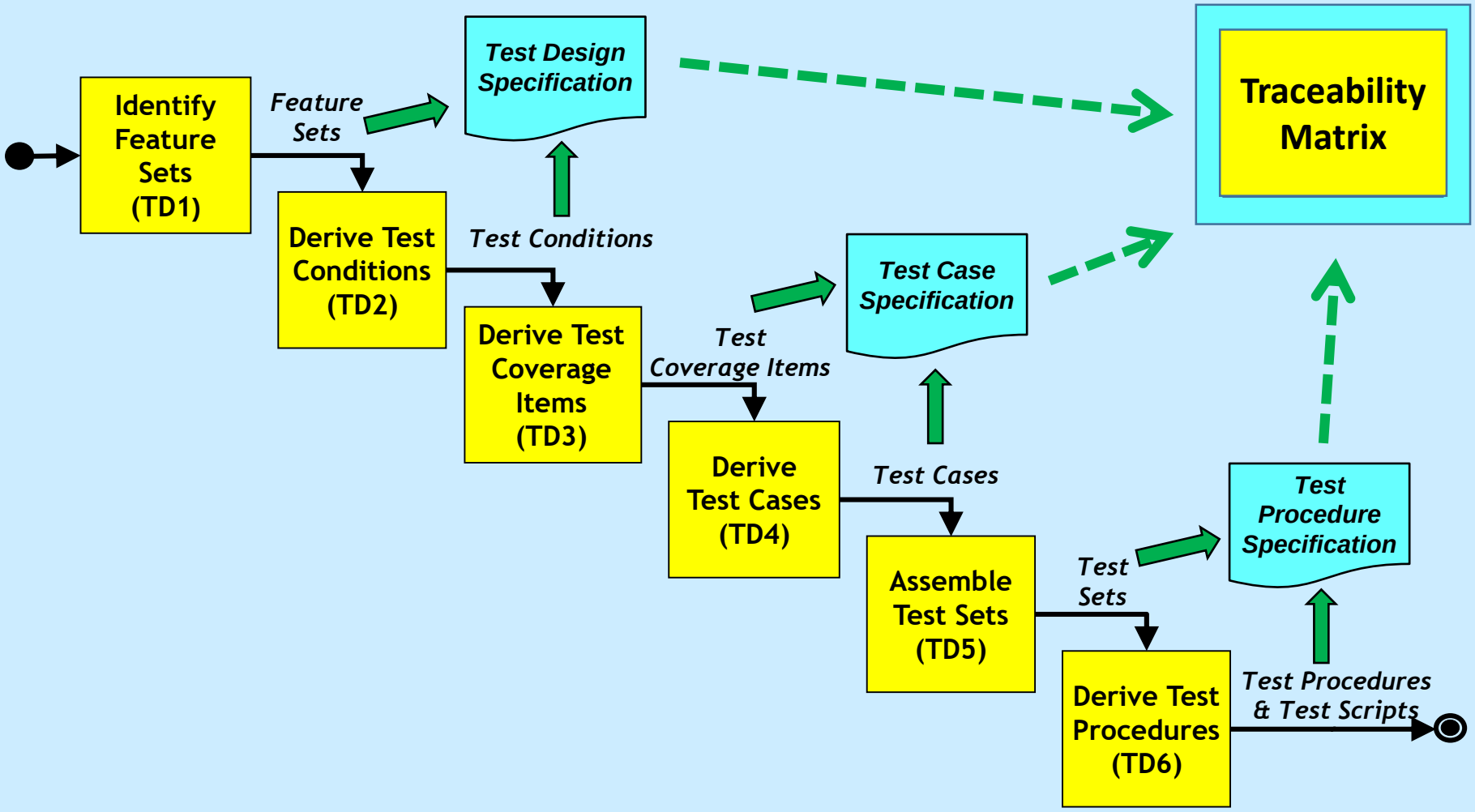
ISO 26262 – Test Completion Process

- No mention of the archiving of test assets at the end of the project
  - e.g. reusable testware
  - e.g. for future regression testing
- No requirement to clean-up the test environment
  - e.g. for future use
  - e.g. for security
- No requirement for lessons learned to improve future testing

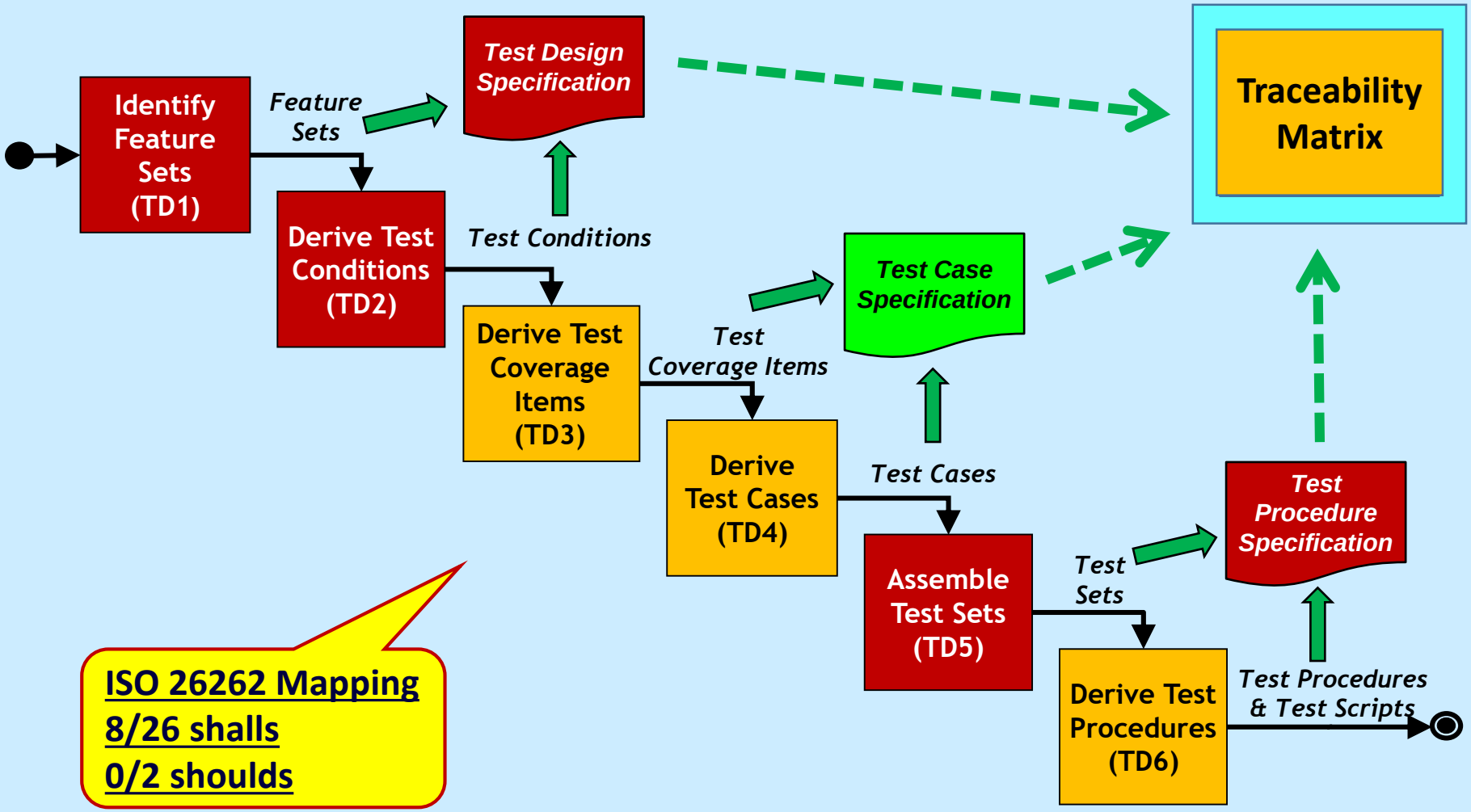
ISO 29119-2 – Dynamic Test Processes



ISO 29119-2 – Test Design & Implementation Process



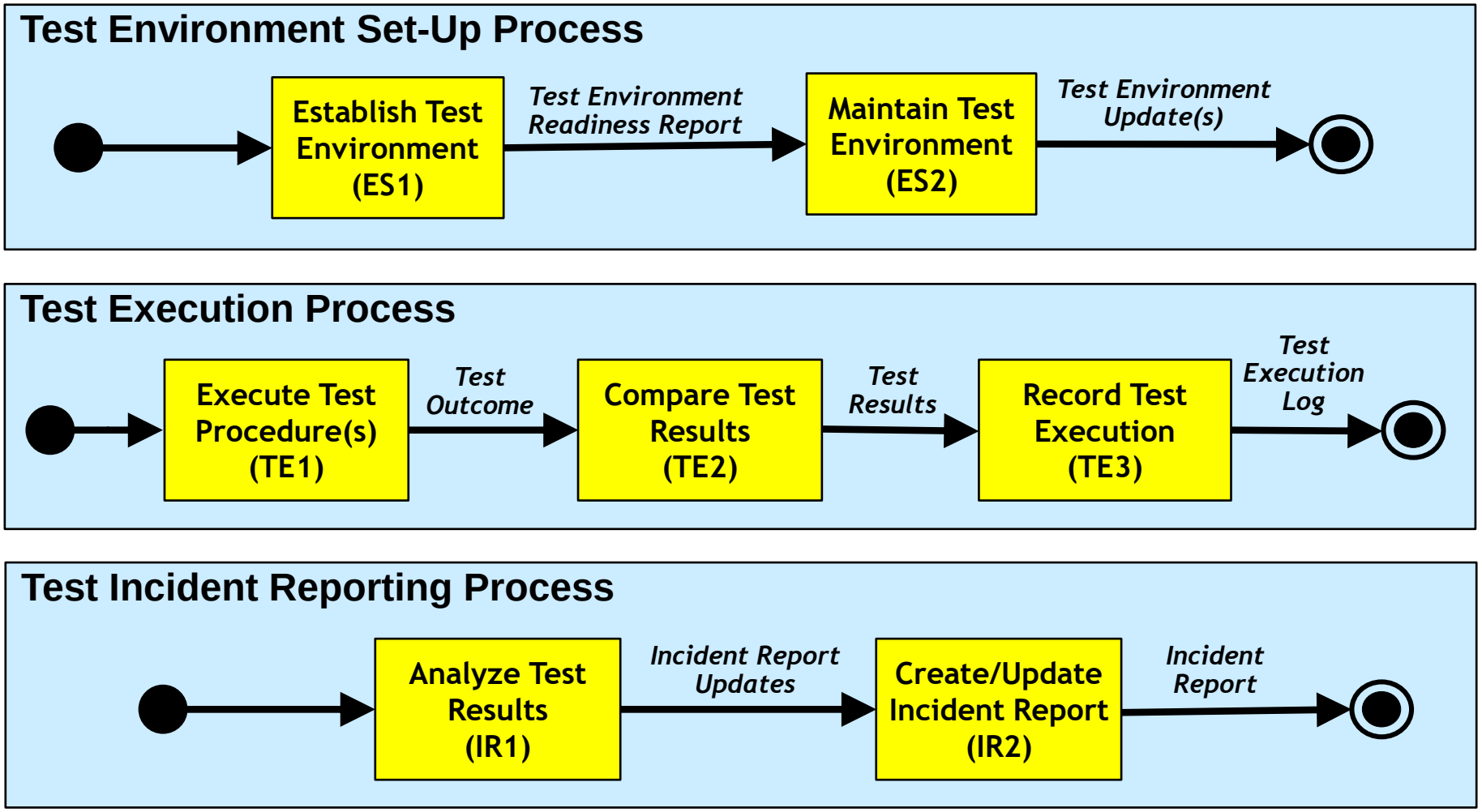
ISO 26262 Mapping to ISO 29119-2 Test Design & Implementation Process



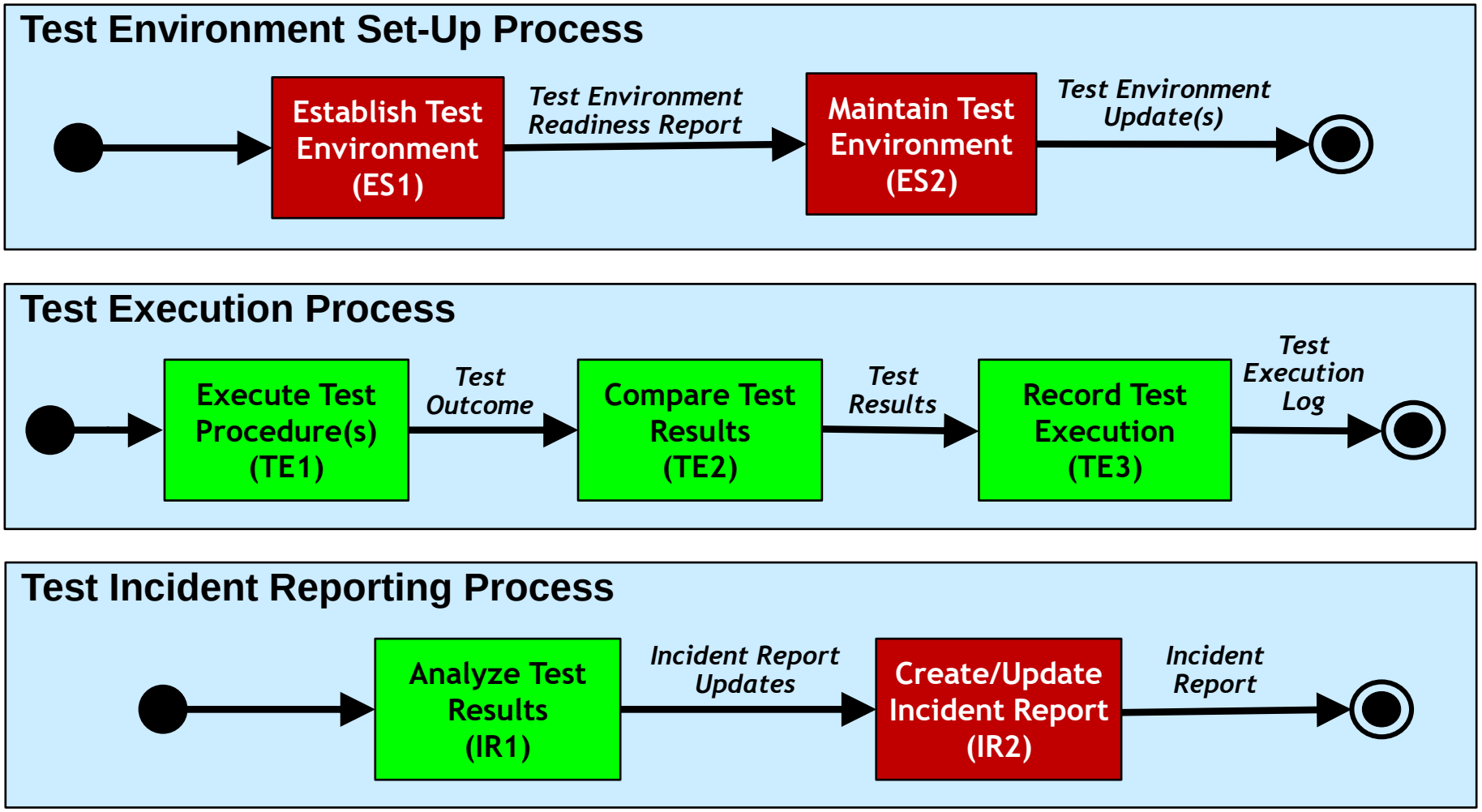
ISO 26262
Test Design & Implementation Process

- No requirement to identify features sets or test conditions
  - already done when assigning ASILs?
- No requirement for the prioritization of tests
  - seems to assume that all planned testing will always occur and no testing will ever get missed – so prioritization is pointless
- No guidance is provided on:
  - how to derive tests by using the required test techniques
    - e.g. Equivalence Partitioning and Boundary Value Analysis
  - how to measure coverage of required test completion criteria
- Requires the grouping of tests by method
  - ISO 29119 suggests grouping tests based on execution constraints

ISO 29119-2
More Dynamic Test Processes



ISO 26262 Mapping to ISO 29119-2
More Dynamic Test Processes

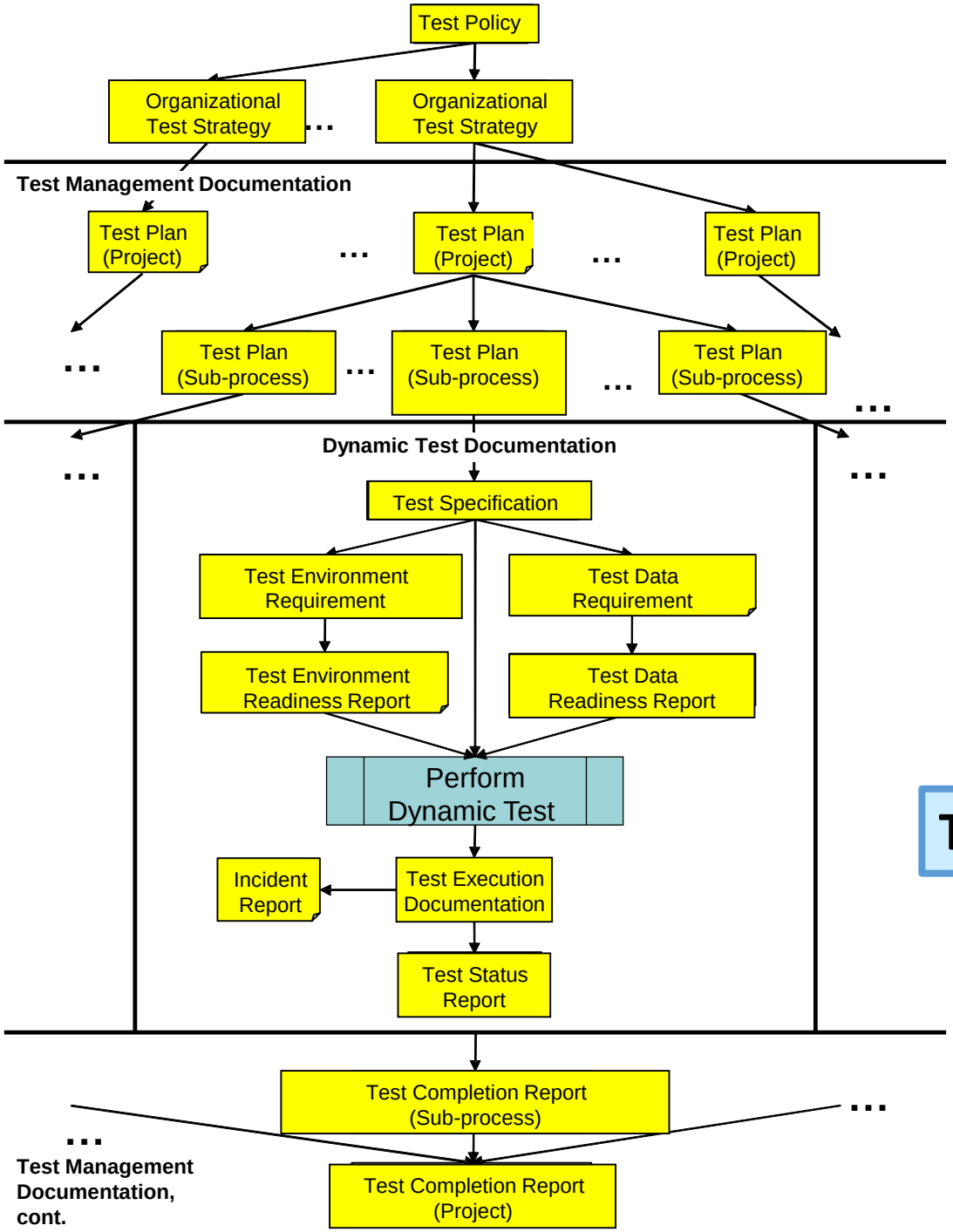


ISO 26262
More Dynamic Processes

- Test Environment Set-Up Process
  - Requirements for the different test environments for the three test phases are specified, BUT
  - no mention of planning, design, configuration management, installation and verification of the test environment
  - nothing on the maintenance of the test environments, nor reporting of their status
- Test Execution Process
  - Nothing requiring that actual results of testing are recorded
    - only level of compliance and test results (pass/fail) need to be documented

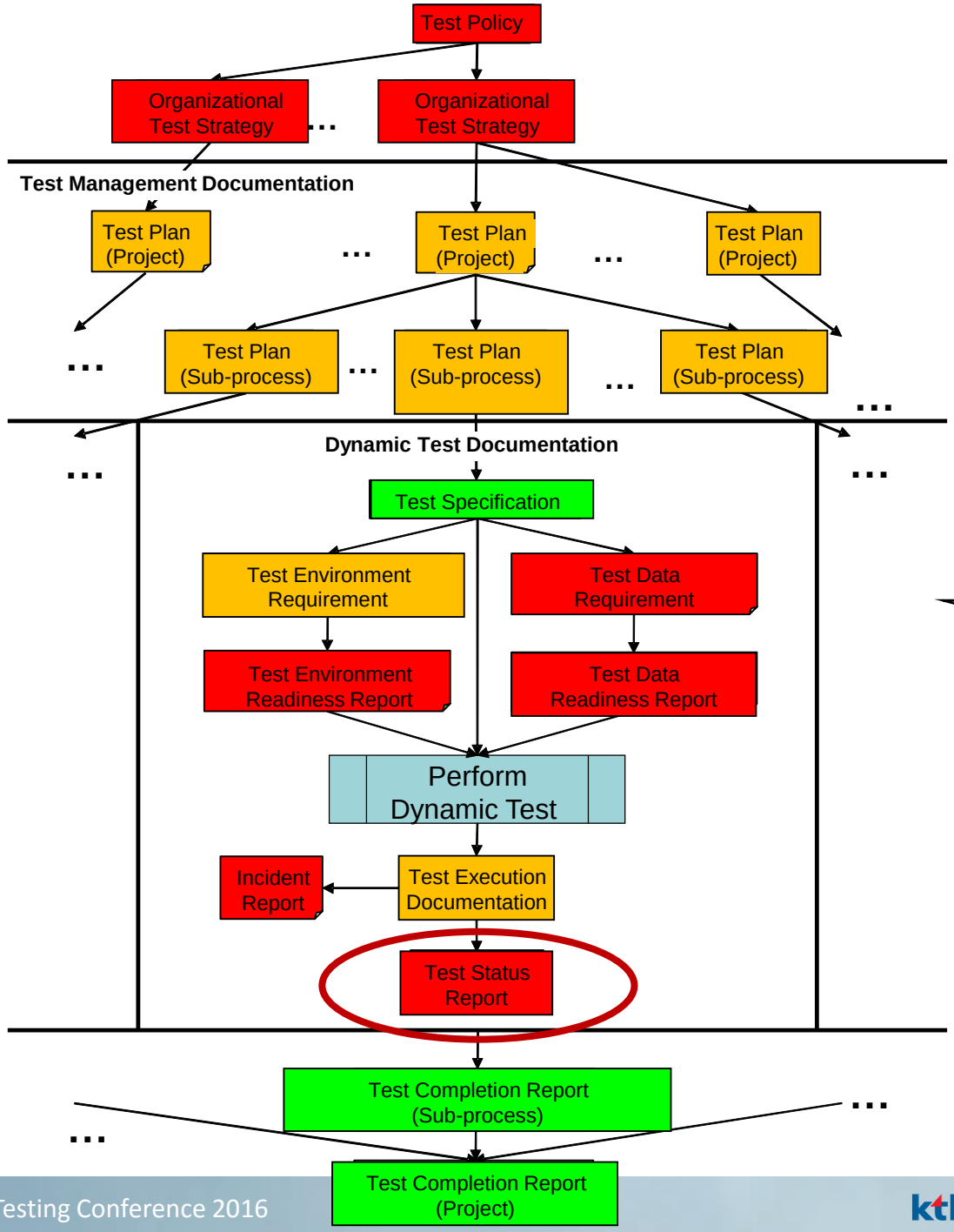
???

- Test Incident Reporting Process
  - Not included – perhaps because this is not testing
  - But for failures requires the rationale for failure and suggestions for changes in the verified work product – this is definitely not testing



29119-3

Test Documentation



AST 2016 Conference
Automotive SW Testing Conference

Verification Documentation

ISO 26262-8

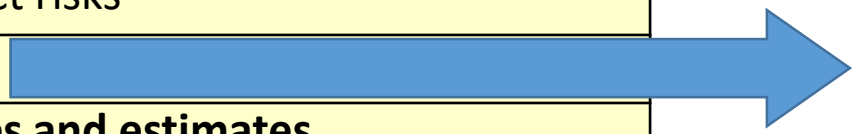
mapping

Test Documentation

ISO 29119-3

ISO 29119-3 Test plan template

Context of the testing:
Project(s)/Test sub-process(es)
Test item(s)
Test scope
Assumptions and constraints
Stakeholders
Testing communication
Risk register:
Product risks
Project risks
Test strategy
Testing activities and estimates
Staffing:
Roles, activities, and responsibilities
Hiring needs
Training needs
Schedule



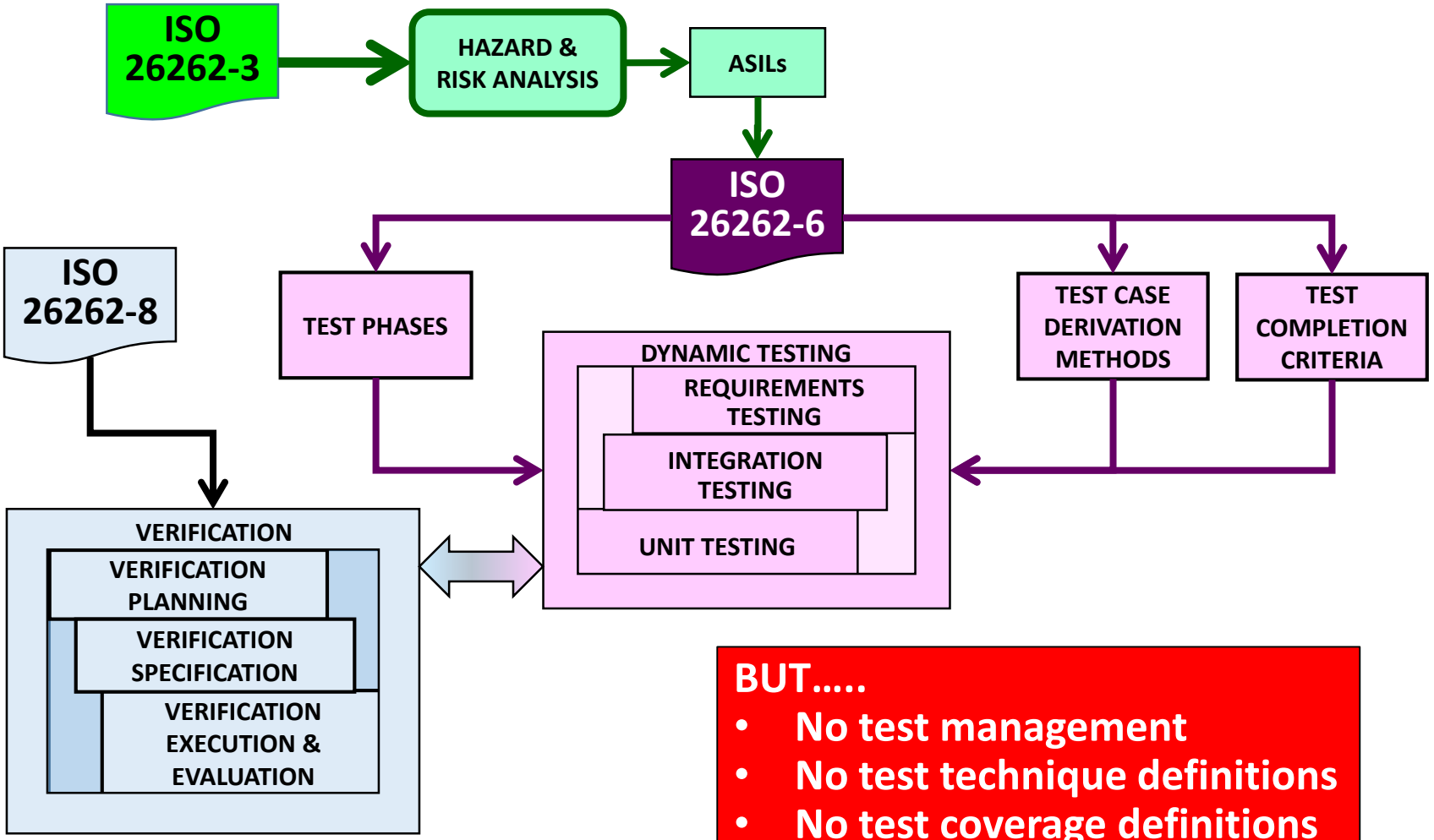
Test strategy:
Test sub-processes
Test deliverables
Test design techniques
Test completion criteria
Metrics to be collected
Test data requirements
Test environment req'ts
Retesting and regression testing
Suspension and resumption criteria
Deviations from the Organizational Test Strategy

ISO 26262 Mapping to ISO 29119-2 Verification/Test Plan

Context of the testing:
Project(s)/Test sub-process(es)
Test item(s)
Test scope
Assumptions and constraints
Stakeholders
Testing communication
Risk register:
Product risks
Project risks
Test strategy
Testing activities and estimates
Staffing:
Roles, activities, and responsibilities
Hiring needs
Training needs
Schedule

Test strategy:
Test sub-processes
Test deliverables
Test design techniques
Test completion criteria
Metrics to be collected
Test data requirements
Test environment req'ts
Retesting and regression testing
Suspension and resumption criteria
Deviations from the Organizational Test Strategy

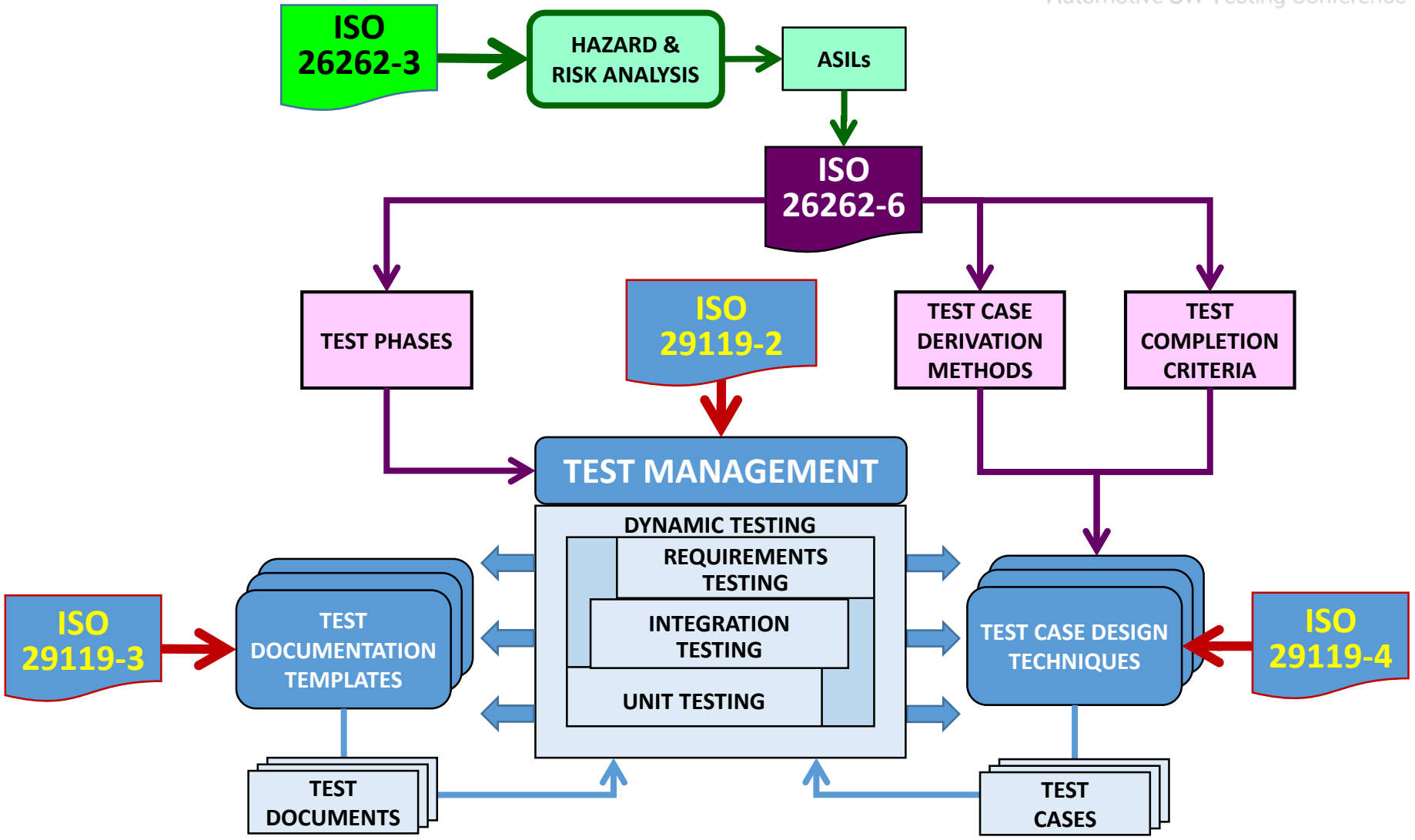
Just ISO 26262 …. OK Software Testing



BUT…..

- No test management
- No test technique definitions
- No test coverage definitions
- Little test documentation

How it should be…Full Software Testing



Conclusions

AST 2016 Conference
Automotive SW Testing Conference

Automotive Safety Standards – ISO 26262

Testing Standards – ISO 29119, ISO 33063 & ISO 20246

Mappings between ISO 26262 and ISO 29119 – processes, techniques and documentation

A co-ordinated approach – using both ISO 26262 and ISO 29119

감사합니다