WInnF'14

DO-178 and Common Criteria

How to combine both design assurance standards

Dr. Rainer Storn, Roger Plieske

2014 March 11-13

ROHDE&SCHWARZ

Demand for Functional Assurance is on the Rise

Avionics



Safety [1)] **Security** [2)]

Design Assurance Standards

1992/2012
DO-178B/C (ED-12B/C),
1999

RTCA
EUROCAE

DO-254
2000

RTCA

Common Criteria

2005 V2.3
2009 V3.1 R3
2012 V3.1 R4

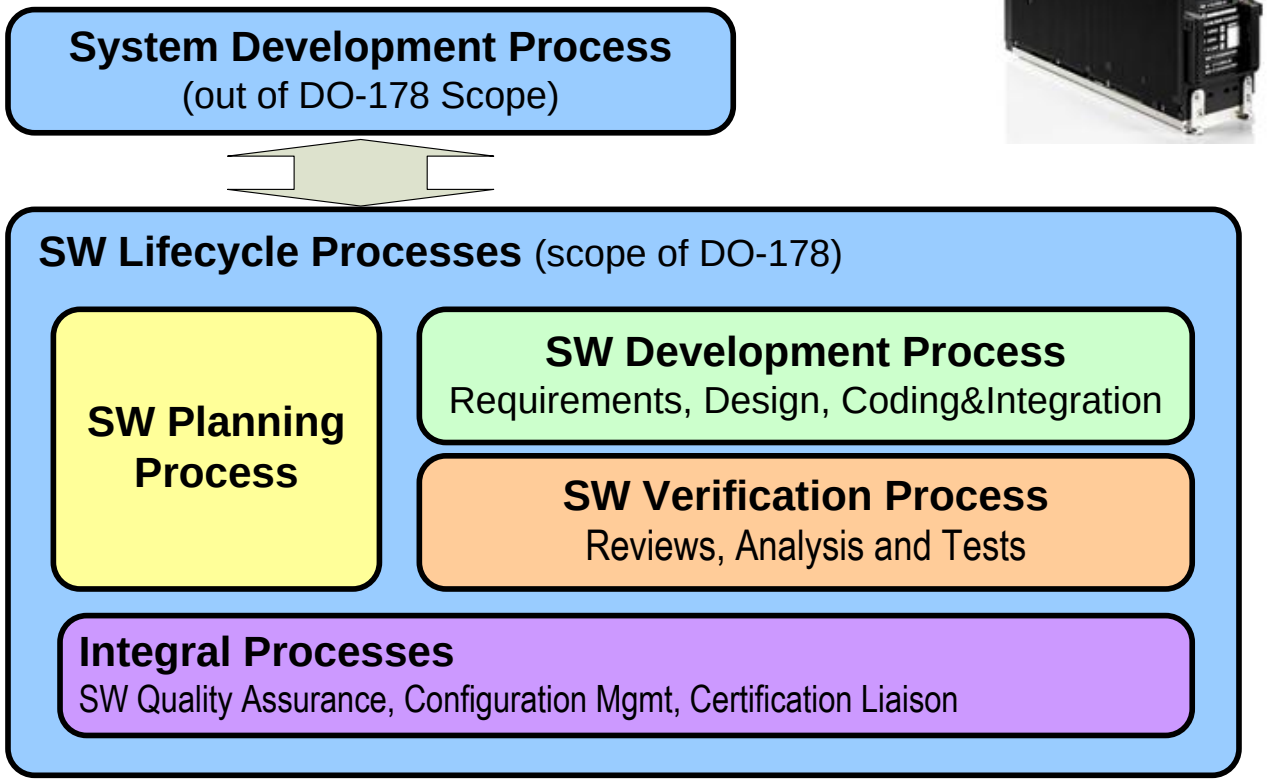
Combine!

[1)] http://www.rtca.org/store_list.asp
[2)] http://www.commoncriteriaportal.org

DO-178B/C (and DO-254) at a Glance

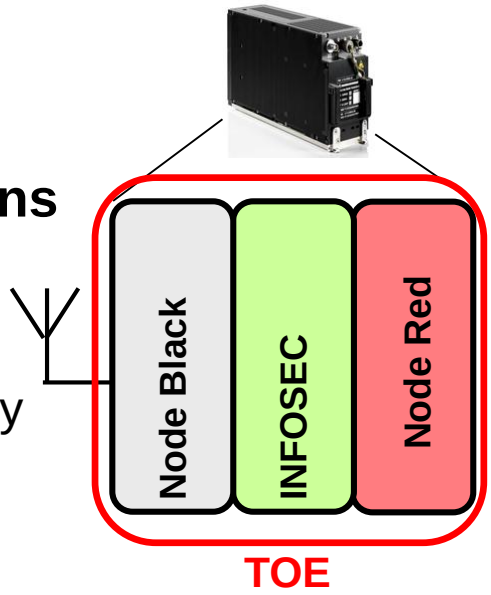
- **Focus on Objectives and Artifacts (DOcuments)**
  - Requirements-based Testing for entire functionality (including security)
  - Functionalities may have different safety impact
  - Structural Coverage Analysis → stopping criterion for testing
  - Traceability

- **Four Key Processes**
- **Definition of documents**
- **DO-standard tells what to do but not how**

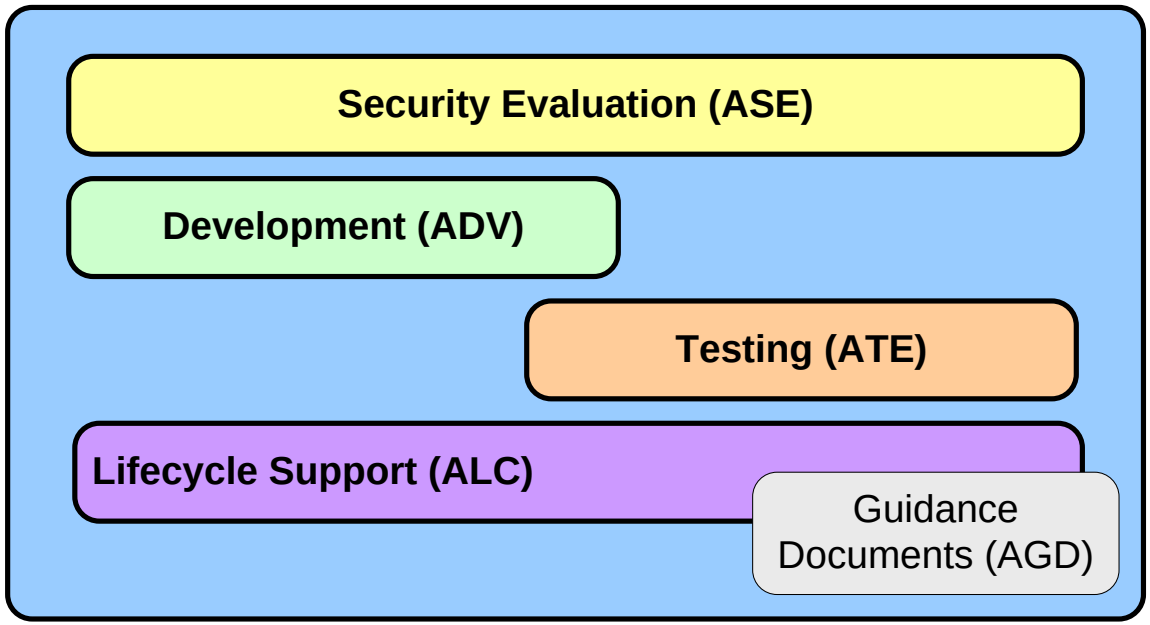


Common Criteria (CC) at a Glance

- **Focus on Design Assurance of Security Functions**
  - By description/analysis of architecture
  - By functional testing
  - Emphasizes tamper-protection and non-bypassability
  - Traceability



- **No process model**
- **No document definition**
- **Security Assurance is structured into assurance classes A<xy>**



DO-178 Assurance Levels → Flight Safety

Level (safety-criticality)	**Failure Description**	**Function**
A (catastrophic)	Failure may cause a crash	Fly by wire controls [1)] Jet Engine control [1)] Auto pilot [1)]
B (hazardous)	Failure has a large negative impact on safety or performance **...**	IFF (friend or foe) [1)] Missile launch [1)]
C (major)	Failure is significant, but has a lesser impact than hazardous failure	Data mining [1)] Communication [2)]
D (minor)	Failure is noticeable, but has a lesser impact than a major failure	Passenger reading lights
E (no effect)	Failure has no impact on safety, aircraft operation, or crew workload	Entertainment System [3)]

[1)] Akos Horvath, Standards in Avionics System Development, Budapest University of Technology and Economics, oct. 2008.

[2)] SAE / ARP 5150, Safety Assessment of Transport Airplanes in Commercial Service, nov. 2003 .

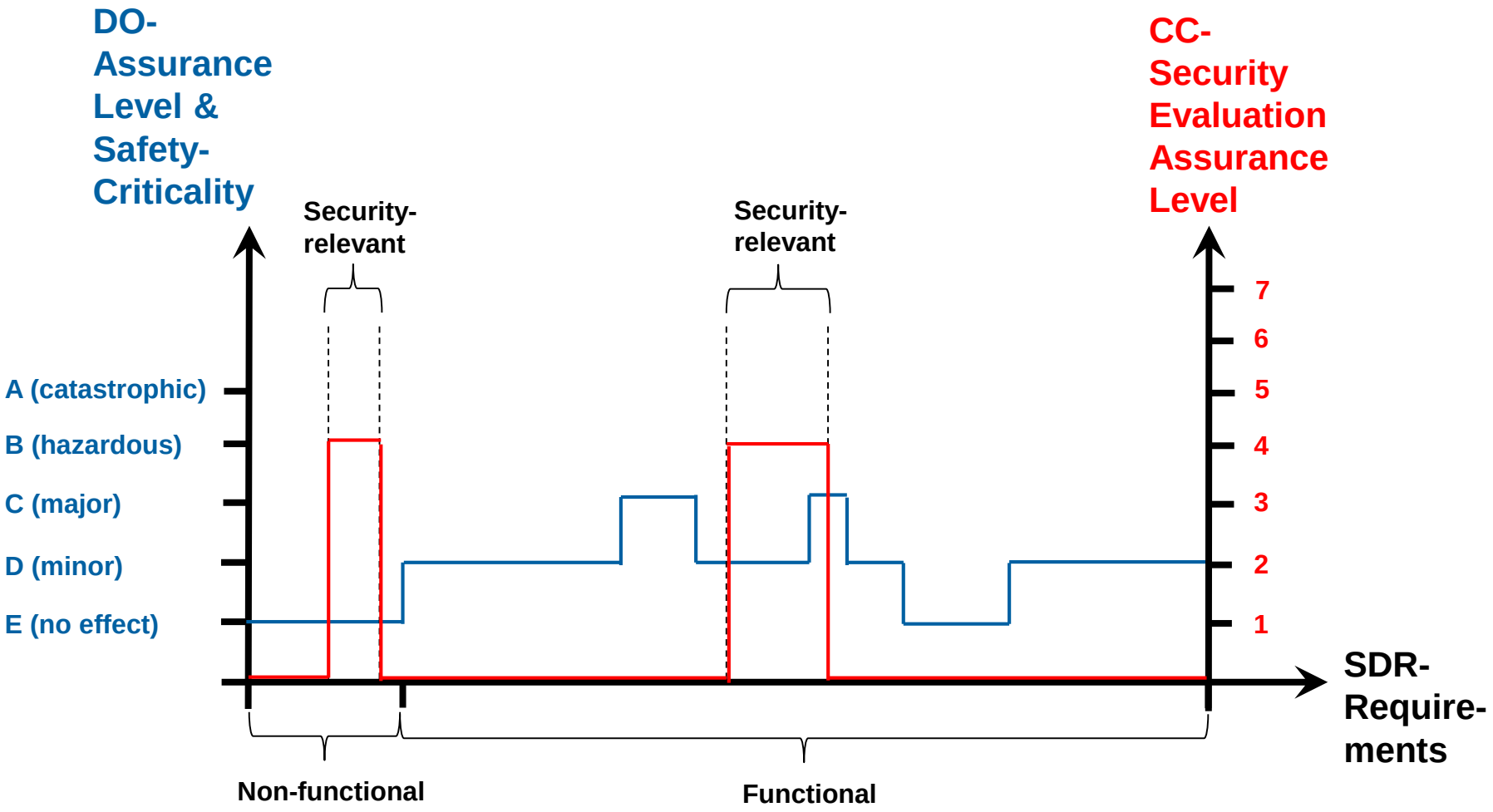
[3)] Uchenick, G.M., and Vanfleet, W.M., Certification Requirements for High Assurance Systems, Systems & SW Techn. Conf., 2007 .

CC Evaluation Assurance Levels [1] → Information Security

Level	Description	Considerations for EAL selection
EAL 7	Formally verified, designed & tested	▪ Value of the assets ▪ Risk of the assets being compromised ▪ Current state of practice in definition and construction of the TOE ▪ Security Environment ▪ Development, evaluation & maintenance costs ▪ Resources of adversaries ▪ Functional requirement dependencies
EAL 6	Semiformally verified, designed & tested	
EAL 5	Semiformally designed & tested	
EAL 4	Methodically designed, tested & reviewed	
EAL 3	Methodically tested & checked	
EAL 2	Structurally tested	
EAL 1	Functionally tested	

[1] http://www.niap-ccevs.org/briefings/rsa_cc_workshop_04.pdf.

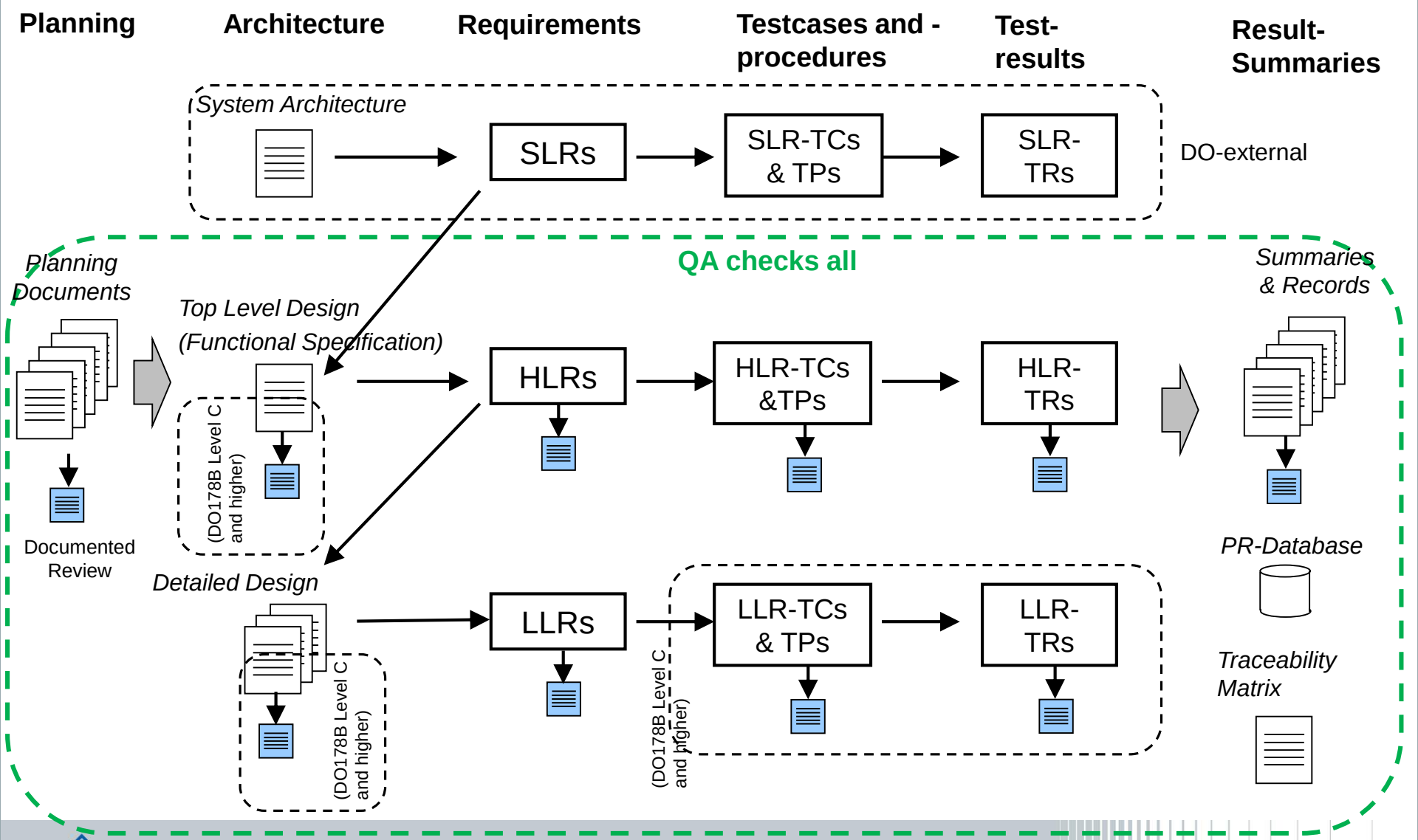
Requirements in an SDR



DO-Artifacts (for the Radio)

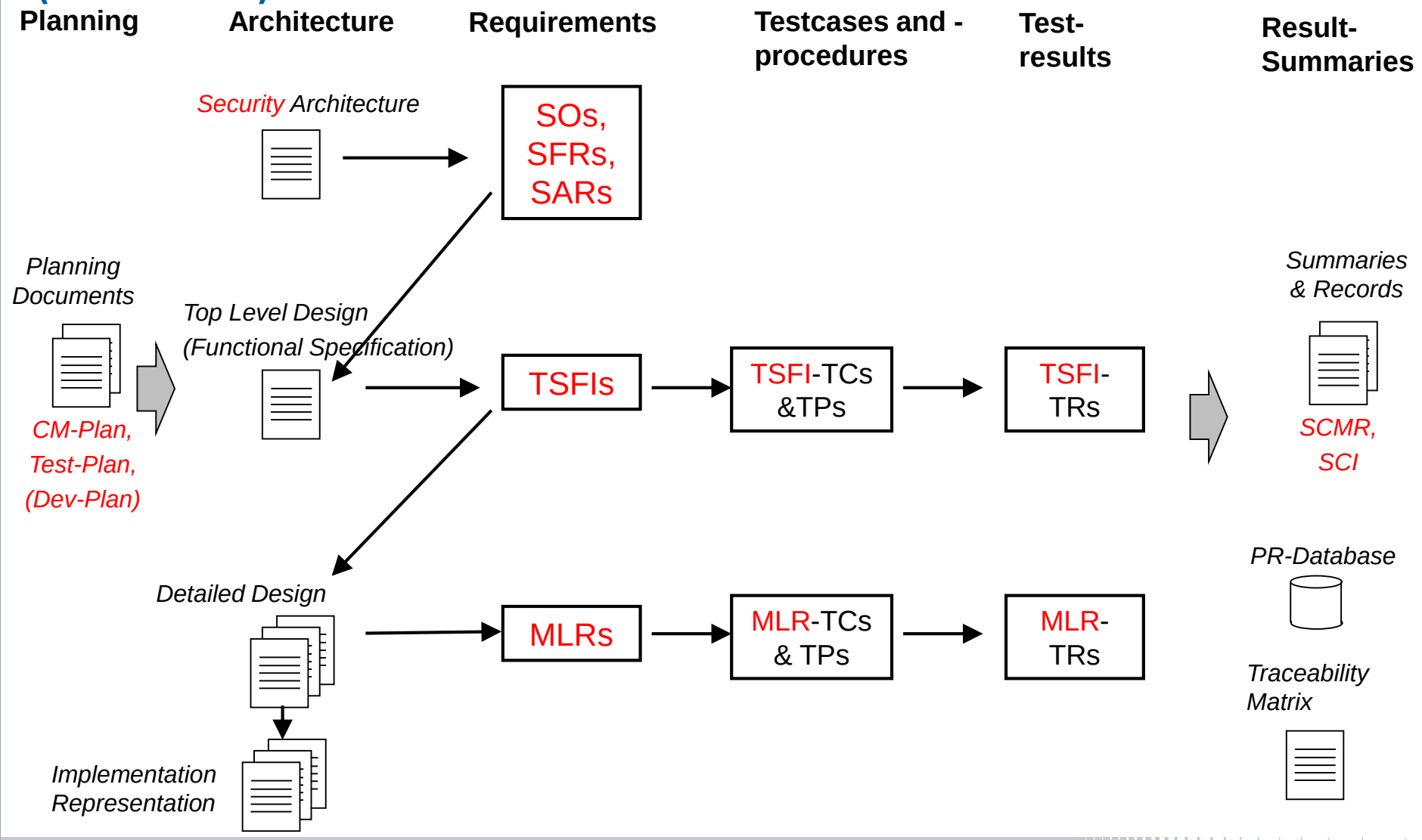
Review sheet

SLR = System Level Requirement
HLR = High Level Requirement
LLR = Low Level Requirement
TC = Testcase
TP = Testprocedure
TR = Testresult
PR = Problem Report



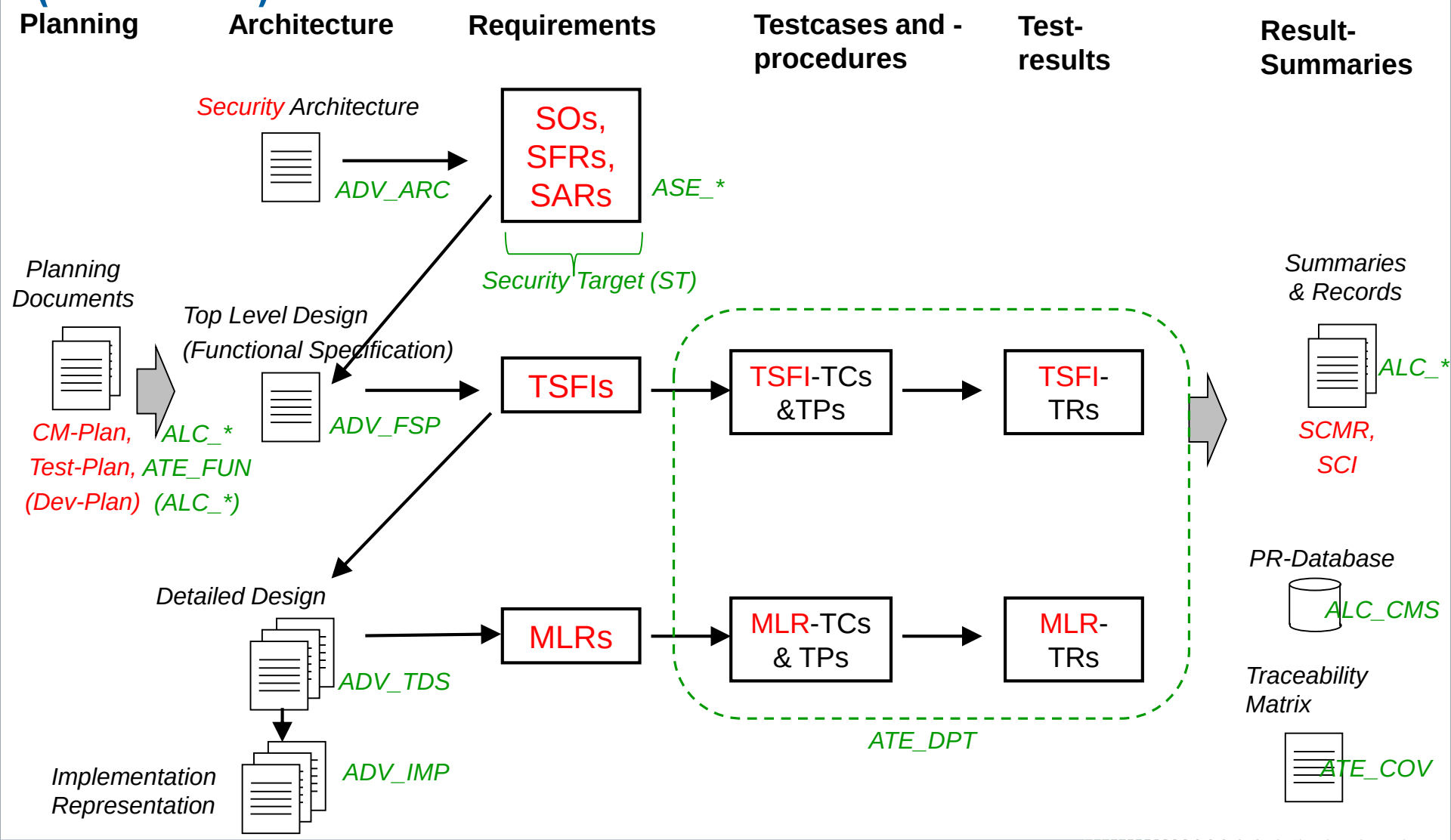
CC-Artifacts (for a TOE)

SFR = Security Functional Req.
SAR = Security Assurance Req.
TSFI = TOE SF Interfaces
TOE = Target of Evaluation
TC = Testcase
CAT = Crypto Acceptance Test
TP = Testprocedure
MLR = Module Level Requirements
SO = Security Objective
PR = Problem Report
TR = Testresult



CC-Artifacts (for a TOE)

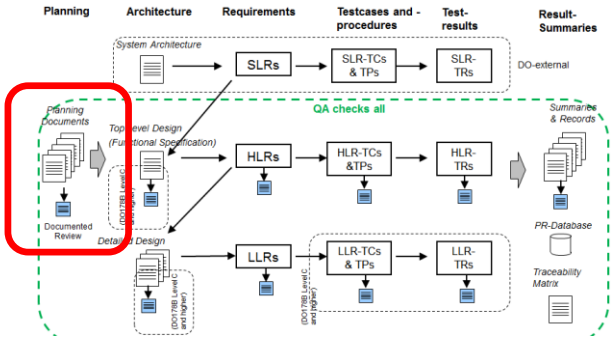
SFR = Security Functional Req.
SAR = Security Assurance Req.
TSFI = TOE SF Interfaces
TOE = Target of Evaluation
TC = Testcase
CAT = Crypto Acceptance Test
TP = Testprocedure
MLR = Module Level Requirements
SO = Security Objective
PR = Problem Report
TR = Testresult



Overall Strategy

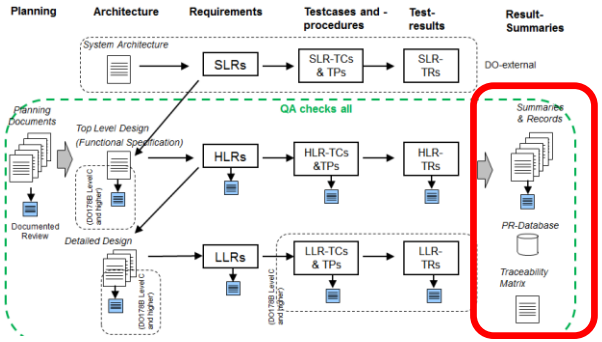
- **Set Framework using DO-Processes and DO-Documents**
- **Augment DO-Documents with CC-Content, labeled with the pertinent assurance class family**
- **Generate DO-only or CC-only documentation separately**
  - For CC: Security Target (ASE_*)
  - For CC: Security Architecture Document (ADV_ARC)
  - For CC: Preparations for independent testing (ATE_IND)
  - For CC: User Guidance Documents (AGD_*)

Planning



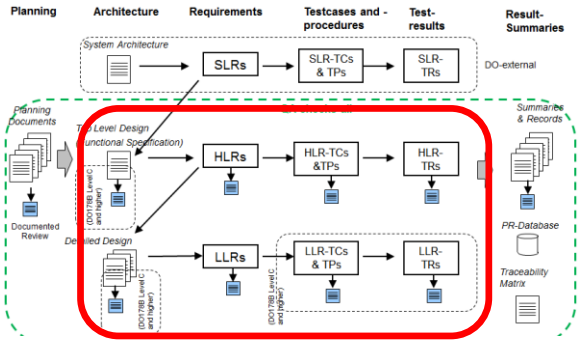
DO-Document	CC-Contribution
Plan for SW-Aspects of Certification (PSAC)	-
SW Development Plan (SDP)	-
SW Verification Plan (SVP)	Yes, mainly ATE_FUN
SW Configuration Management Plan (SCMP)	Yes, ALC_*
SW Quality Assurance Plan (SQAP)	-

Summaries



DO-Document	CC-Contribution
SW Config. Management Records (SCMRs)	Yes, ALC_CMC
SW Configuration Index (SCI)	Yes, ALC_CMC, ALC_CMS
SW Environment Configuration Index (SECI)	Yes, ALC_TAT
SW Quality Assurance Records (SQARs)	-
SW Accomplishment Summary (SAS)	-

Development



DO-Document	CC-Contribution
SW Requirements Document (SRD)	Yes, ADV_FSP
SW Detailed Design (SDD)	Yes, mainly ADV_TDS
Source Code	Yes, ADV_IMP
SW Verfication Cases and Procedures (SVCP)	Yes, mainly ATE_DPT
SW Verification Results (SVR)	Yes, mainly ATE_FUN, ATE_COV

Questions ?

Thank you