Embedded Software: kwaliteitsbewaking door Test en Verificatie

E&A 2023

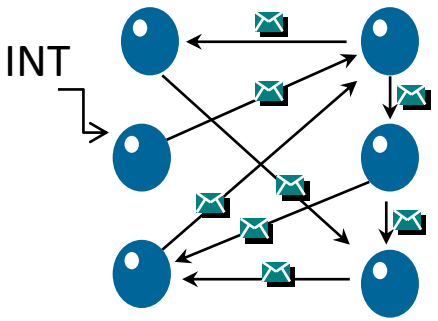
Gerard Fianen

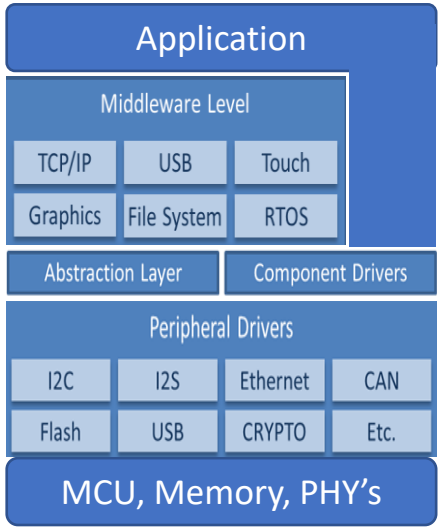
E&A ELECTRONICS APPLICATIONS '23

indes The choice of professionals

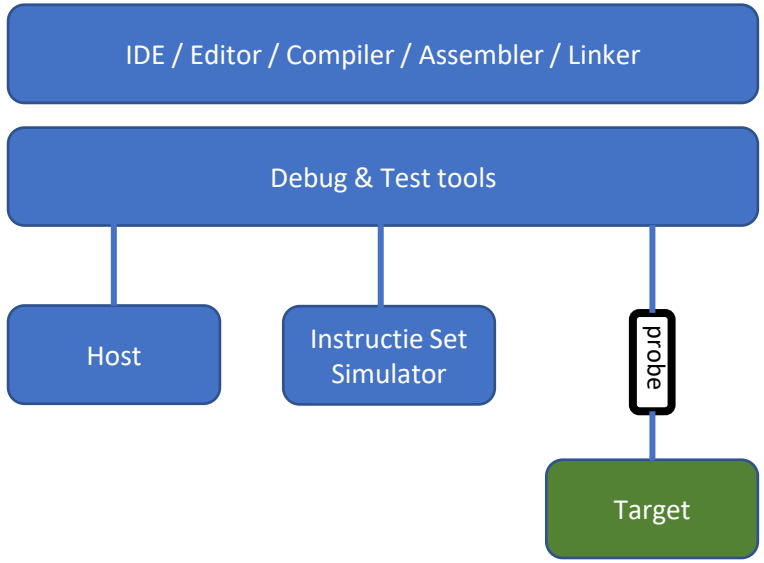
26 T/M 28 SEPTEMBER '23 JAARBEURS UTRECHT

Waarin is Embedded software anders dan ‘gewone’ software ?





- Real-Time gedrag (RTOS), laag stroomverbruik
- Beperkt geheugen, OP = OP
- Low-level / dicht op de hardware
  - Drivers / Flash loader/ verschillende soorten RAM & Flash
- On-target debuggen & testen



- Safety critical / Certificatie ?
- Security & privacy
- Kosten van onderhoud / Firmware updates

Tip: FHI Software cluster bijeenkomsten !

indes The choice of professionals

E&A ELECTRONICS & APPLICATIONS '23

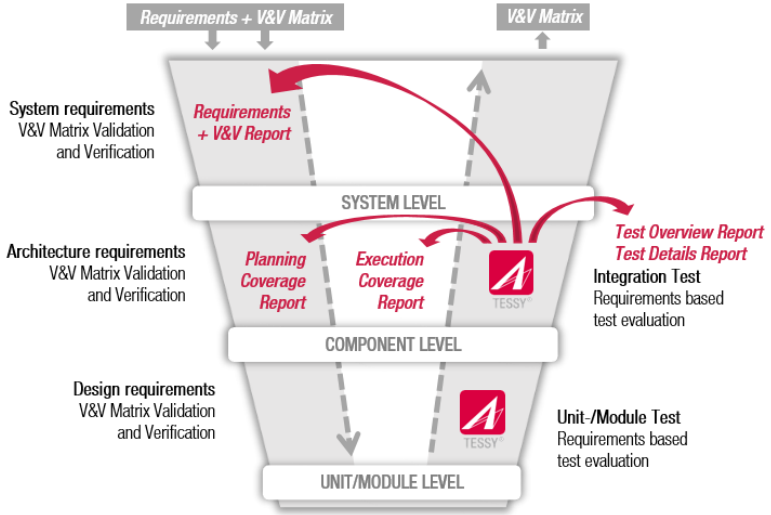
Kwaliteit: Personeel en Proces

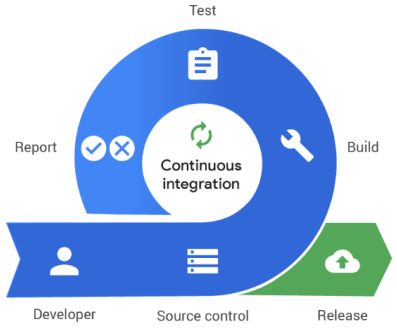
Embedded software vraagt meer van S/W engineers dan ‘gewone’ software
Programmeer taal : C / C++ / Embedded C++ (Python, Rust)

Begeleid de S/W engineers in het volgen van een proces
Kwaliteit, onderhoudbaar en reproduceerbaar

- Begin vanuit de S/W requirements
- Partitioneer S/W in functionele componenten
- Niet te slimme / cryptische code maar leesbare code
- Comments en documentatie
- Programming Standards Verificatie (b.v. MISRA)
- Testen (unit Test / Functionele test)
- Regression Testing

Blijf steeds bewust dat S/W engineers op enig moment het bedrijf verlaten
- Documentatie, documentatie etc

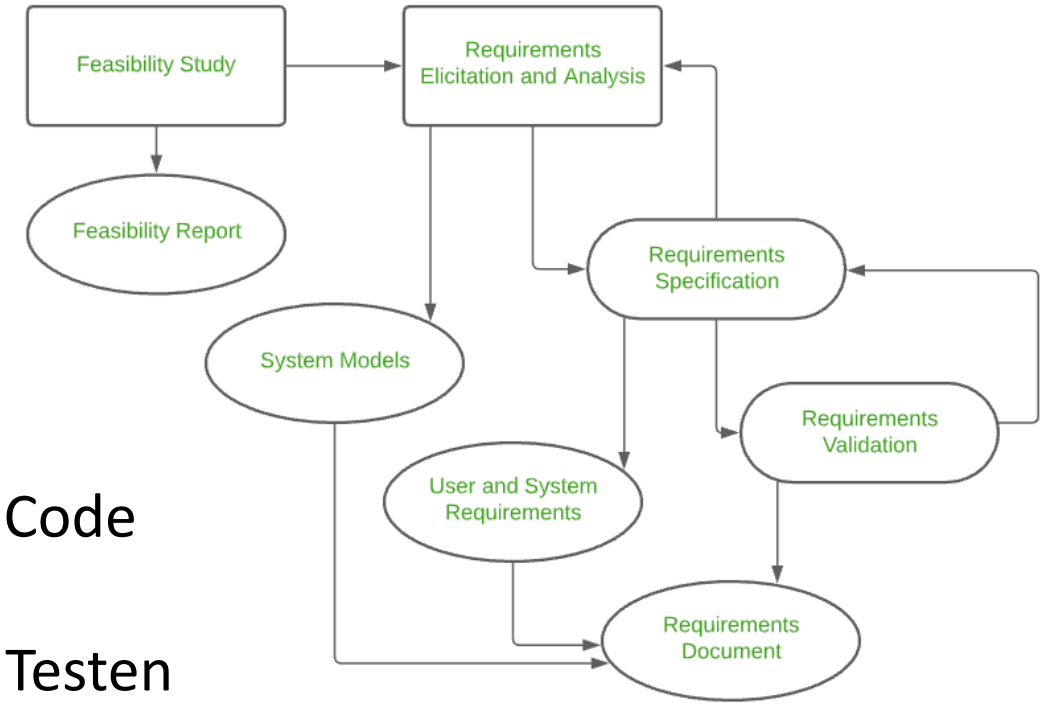




indes
The choice of professionals

E&A
ELECTRONICS & APPLICATIONS '23

Het begint met de Requirements



Functionele Requirements

- Gedrag --> Code
- Verificatie --> Testen

Een goede eerste stap :
Programming Standards Verificatie & Statische Analyse

- Verifieer de sourcecode tegenover een Programming standard (MISRA, CWE, CERT)
- Selecteer een relevante <u>subset</u> van de rule-set
- Static analysis, Code Complexity metrics
- Integratie in de IDE

MISRAC2012-Rule-9.1_b

Synopsis	Read accesses from local buffers were found that are not preceded by writes.
Enabled by default	Yes
Severity/Certainty	High/Medium
Full description	(Mandatory) The value of an object with automatic storage duration shall not be read before it has been set. This check is identical to MISRAC2004-1.2_a, SPC-uninit-arr-all, CERT-EXP33-C_d.
Coding standards	CERT EXP33-C Do not reference uninitialized memory CWE 457 Use of Uninitialized Variable MISRA C:2004 1.2 (Required) No reliance shall be placed on undefined or unspecified behavior. MISRA C:2012 Rule-9.1 (Mandatory) The value of an object with automatic storage duration shall not be read before it has been set
Code examples	The following code example fails the check and will give a warning:

C-STAT Messages

Severity: All Filter: Messages: 3

Message	Check	Severity	File	Line
cstat1.c (2 messages)			cstat1.c	
Function call `function1()' is immediately dereferenc...	PTR-null-fun-pos	High	cstat1.c	14
main			cstat1.c	0
possible_null			cstat1.c	14
Entering into function1			cstat1.c	14
function1			cstat1.c	0
Return NULL			cstat1.c	7
Value assigned to variable `ch' is never used	RED-unused-assign	Low	cstat1.c	17
cstat2.c (1 message)			cstat2.c	
Array `arr' 1st subscript 20 is out of bounds [0,9]	ARR-inv-index	High	cstat2.c	16

Select C-STAT Checks

C-STAT checks Search:

Name	Severity	Used	Synopsis
STDCHECKS		156/221	C-STAT specific checks
ARR		5/6	Array bounds
ARR-inv-index-pos	High		Array access may be out of bou
ARR-inv-index-ptr-...	Medi...		A pointer to an array is potential
ARR-inv-index-ptr	High		A pointer to an array is used out
ARR-inv-index	High		Array access is out of bounds.
ARR-neg-index	High		An array is accessed with a nega
ARR-uninit-index	Medi...		An array is indexed with an unin
ATH		21/22	Arithmetic errors
CAST		None	Type casts

OK Cancel

indes The choice of professionals

E&A ELECTRONICS & APPLICATIONS '23

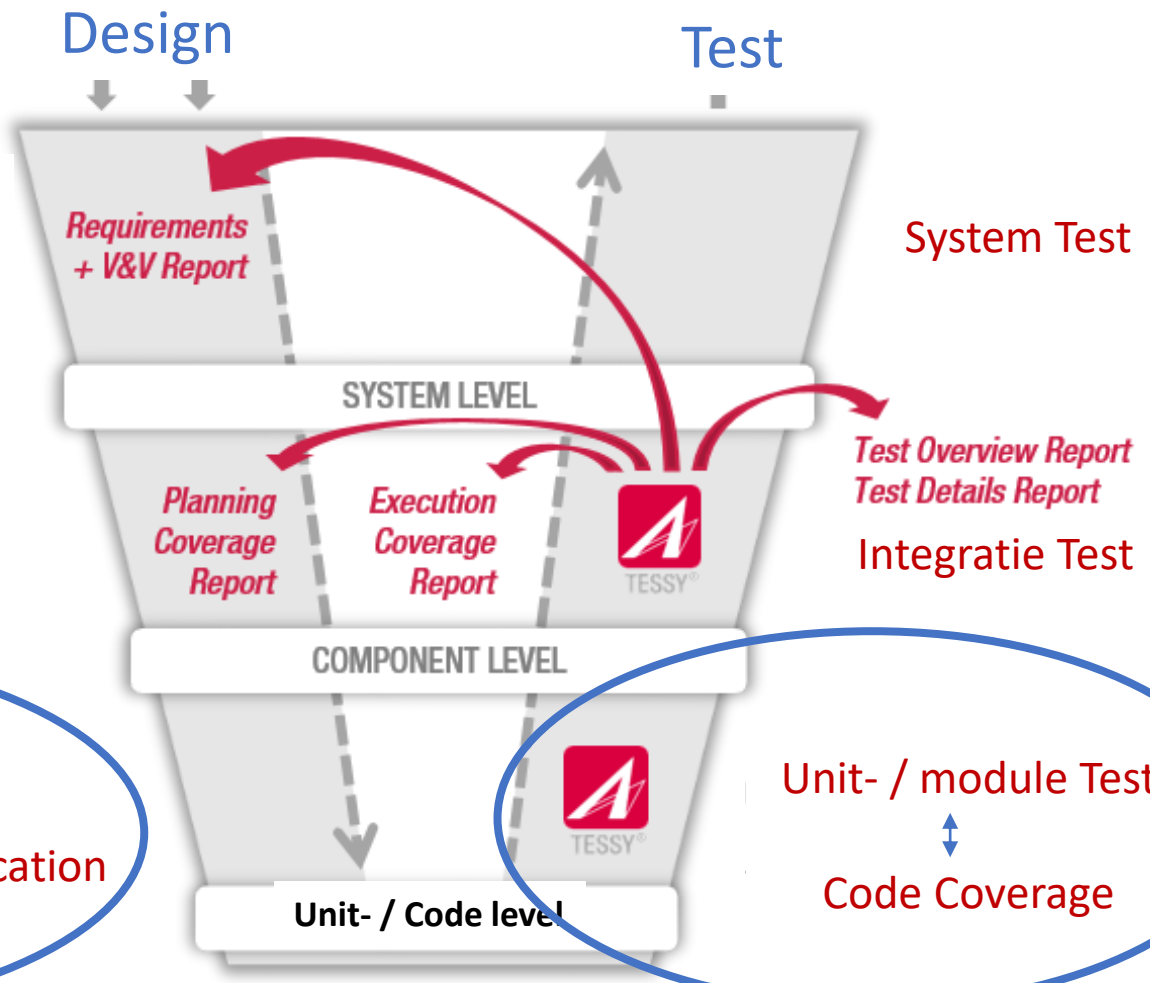
Unit Test en het V-Model

System level
Requirements

Module / subsystem level
Module requirements

Unit - code level

Programming Standard Verification
Static Analysis



System Test

Test Overview Report
Test Details Report

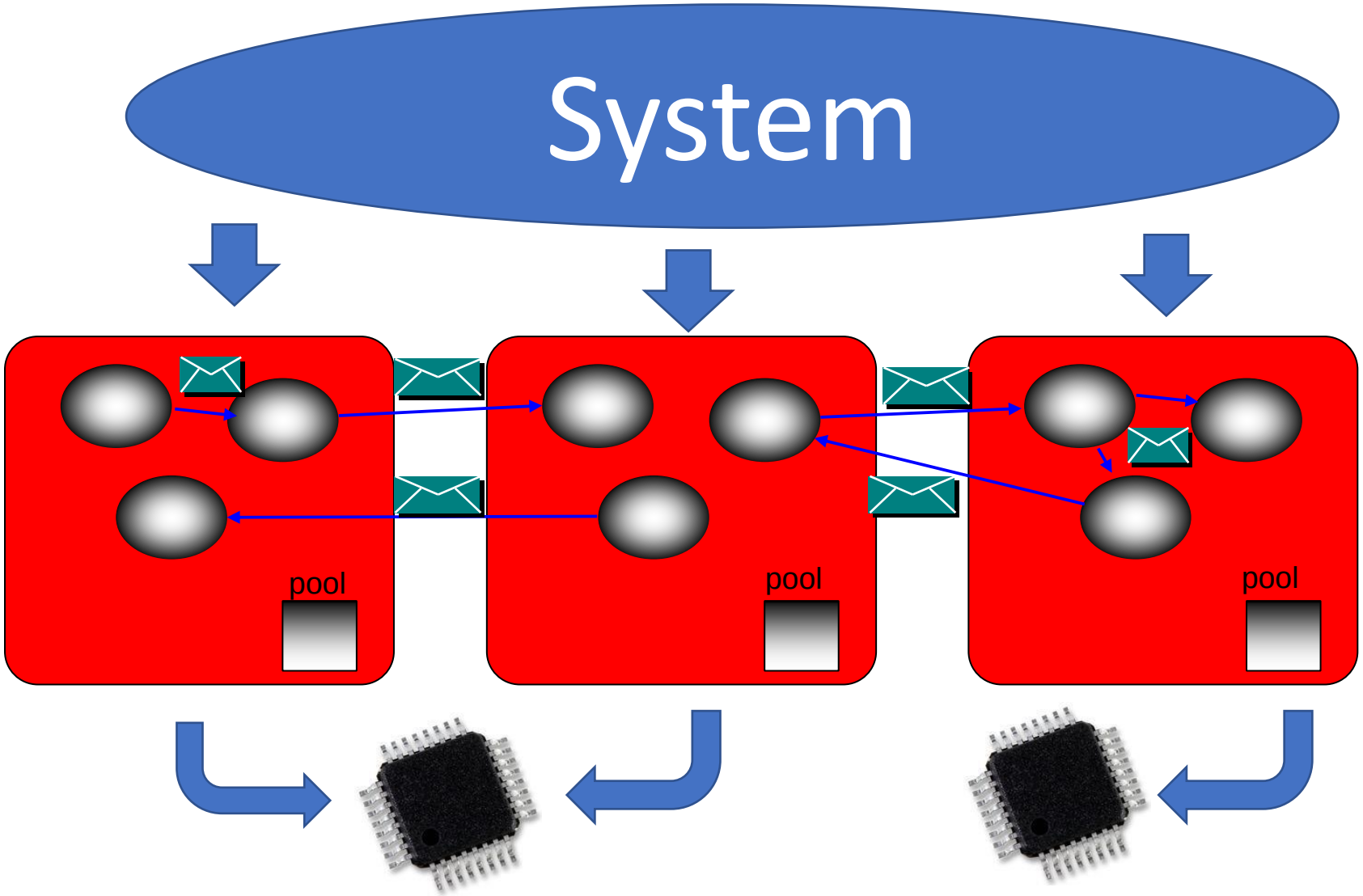
Integratie Test

Unit- / module Test
↕
Code Coverage

indes
The choice of professionals

E&A
ELECTRONICS & APPLICATIONS '23

Top-Down System Design

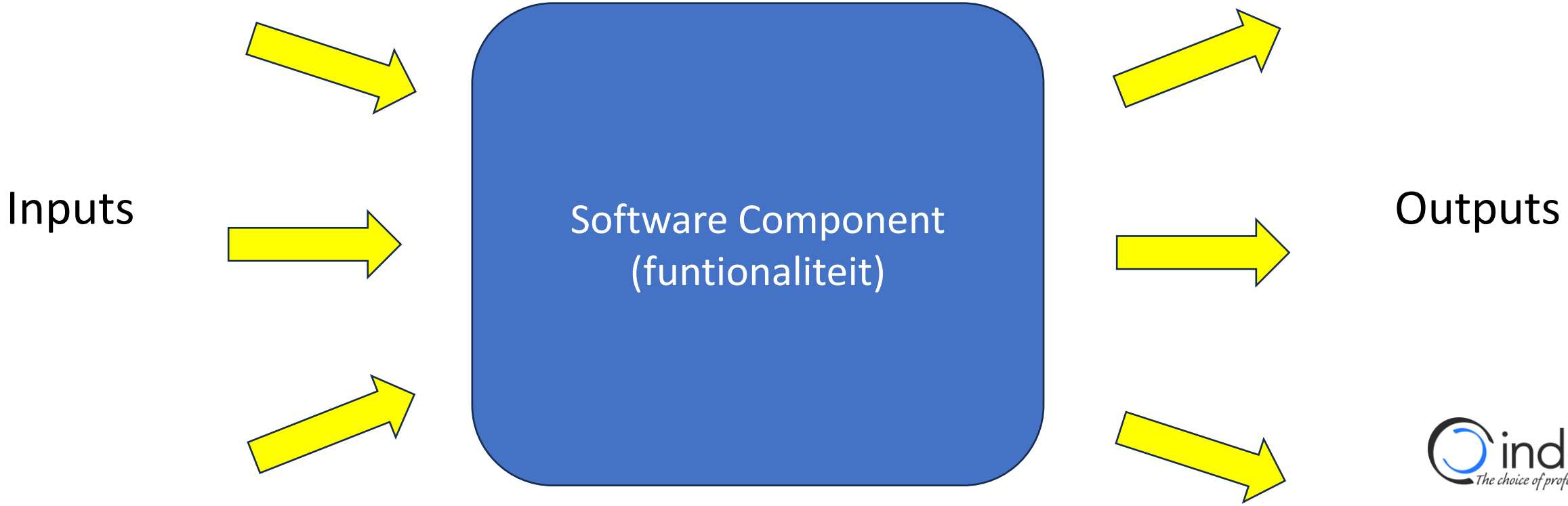


SCIOPTA

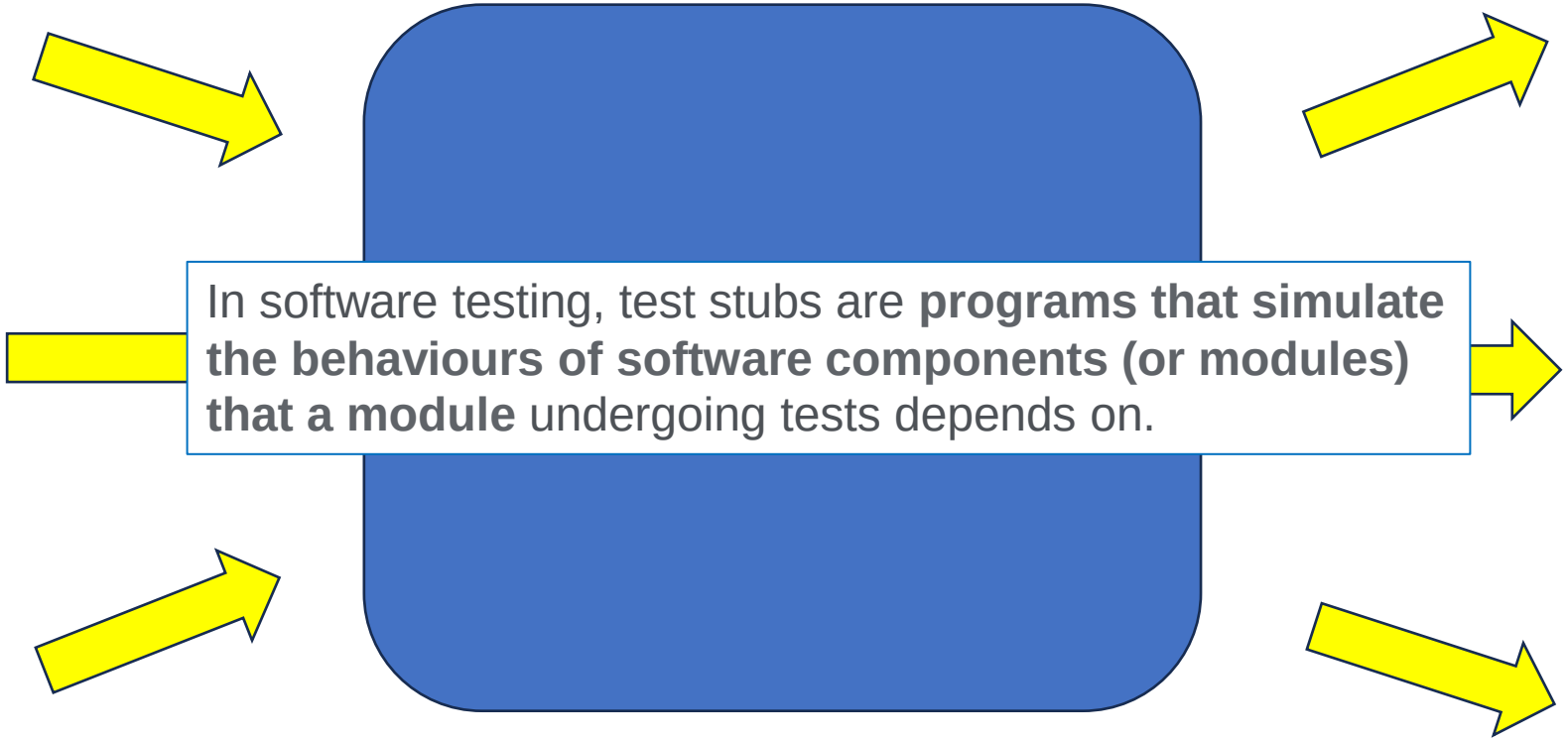
indes
The choice of professionals

E&A
ELECTRONICS & APPLICATIONS '23

Software Componenten & Stubbing



Software Componenten & Stubbing

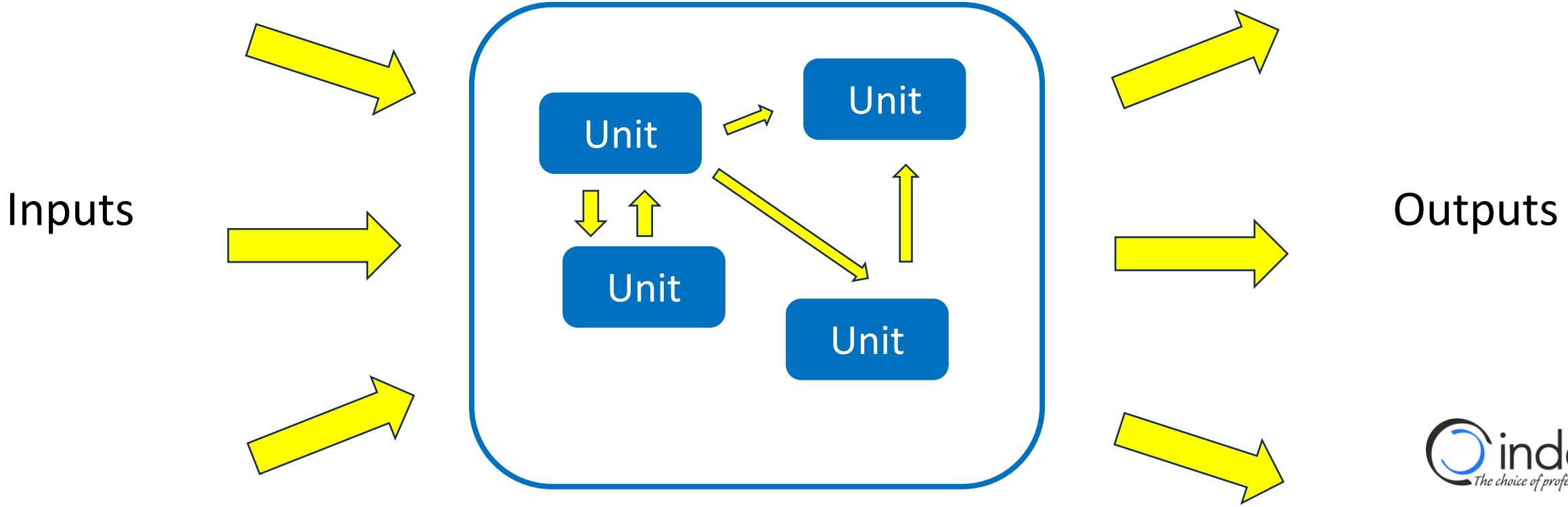


Inputs

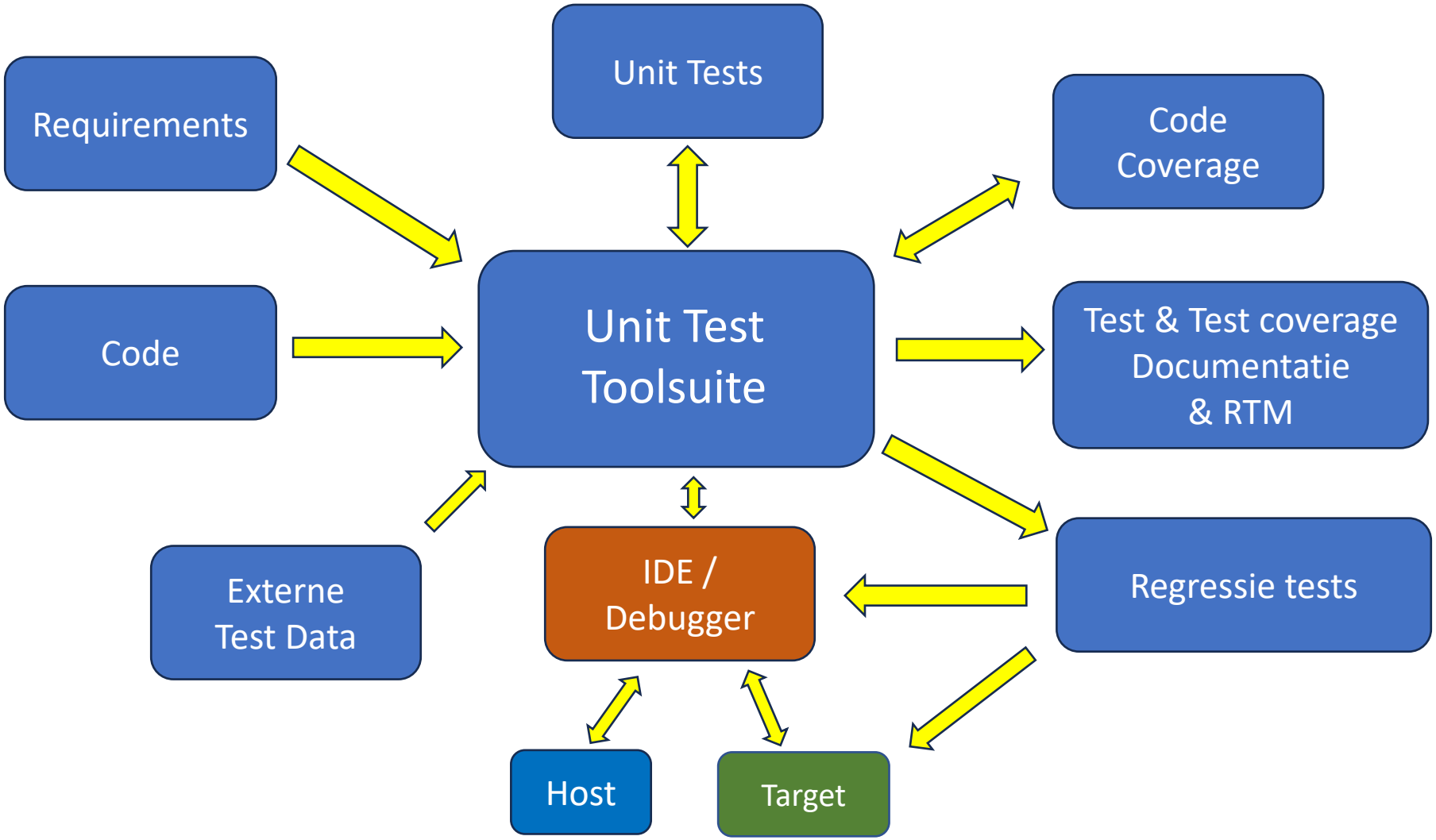
In software testing, test stubs are **programs that simulate the behaviours of software components (or modules) that a module** undergoing tests depends on.

Outputs

Software Units



Unit Test Ecosysteem



Selectie & invoeren van Unit Testing

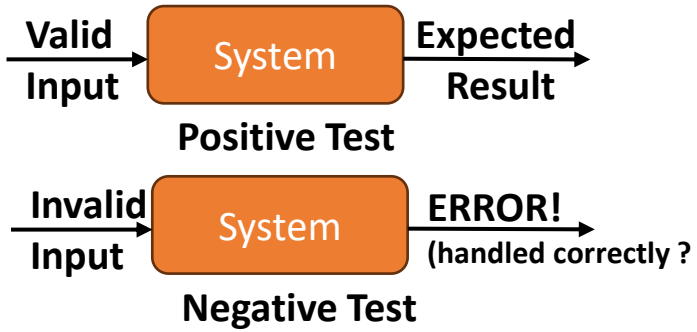
- Tools die specifiek ontwikkeld zijn voor Embedded software

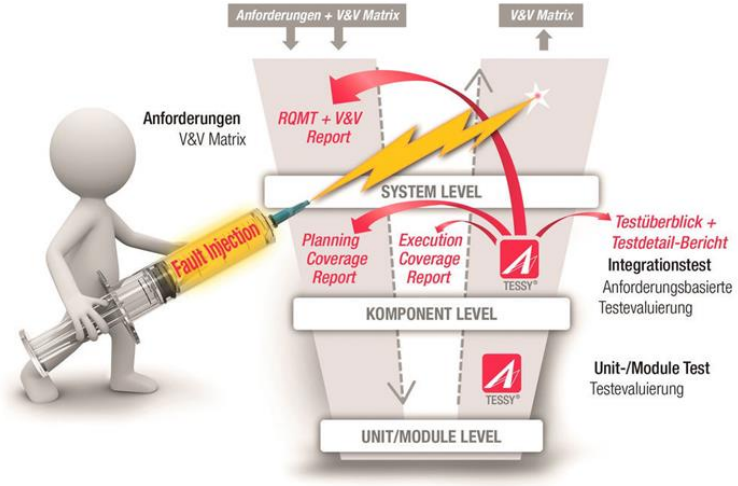
- Selecteer een COMPLETE toolset

- Evaluatie van de tools (assistentie leverancier !)
  - Evalueer geïntegreerd in de uiteindelijke omgeving (IDE, Compiler, on-Target)
  - Doorloop het gehele proces van Req. inlezen tot en met regressie testen
  - Evalueer ook on-target testen
  - Schakel voor assistentie bij deze evaluatie de leverancier in !

- Advanced features : Variant support, Fault injection & Negative testing

- Opleiding / training





indes
The choice of professionals

E&A
ELECTRONICS & APPLICATIONS '23

INDES –
Integrated Development Solutions BV

Cross Compilers, Debuggers, IDE
RTOS, Middleware, Protocol stacks, Security, GUI, EFS
Debug & Trace probes, Emulators
Real-Time Trace, RTOS-Event Trace
Static Analysis, Timing Analysis, Stack Analysis
Unit Test, Code Coverage
(Production) Flash Programming

On-site support
Test-as-a-Service
Verification-as-a-Service

Stand 7F103

www.indes.com info@indes.com

Tel: 0345 - 545.535

26 T/M 28
SEPTEMBER '23
JAARBEURS UTRECHT