hitex

AURIX KNOWLEDGE LAB 2024

Formal methods for unmatched reliability on AURIX/TC4

Rolland DUDEMAINE
J-F POUILLY

TRUST IN SOFT

TrustInSoft In brief

hitex EMBEDDED TOOLS & SOLUTIONS

- Worldwide customers base
- Offices on 3 continents
  - United States
  - Europe
  - Asia

- Spin-off from French Research Agency
- Founded in 2013
- Tools meant for analyzing real-life code

TRUST IN SOFT

- Customer base
  - Safety
  - Security
  - Reliability

Semiconductors, IoT, Telecom

Automotive

Any other Critical

© 2024 TrustInSoft

CHALLENGES OF AUTOMOTIVE SOFTWARE DEVELOPMENT

hitex EMBEDDED TOOLS & SOLUTIONS

Increasing safety and reliability requirements

Increasing cybersecurity threats

Compliance with international standards and regulations (ISO26262 & ISO21434)

Increasing development efforts

More complex, more critical, more regulations

⇨ Higher costs and risks

TRUST IN SOFT

© 2024 TrustInSoft

LET'S BE CONCRETE

hitex
EMBEDDED TOOLS & SOLUTIONS

Example leading to a vehicle recall:

Buffer overflows, variables overflows, which only appear after hours or even days of operation.

For vehicle bus, like CAN or LIN. A communication stack may be overloaded due to a combination of extremely rare load peaks, but that will occur within the 20,000 hours of product life.

Example found during Design Verification test campaign:

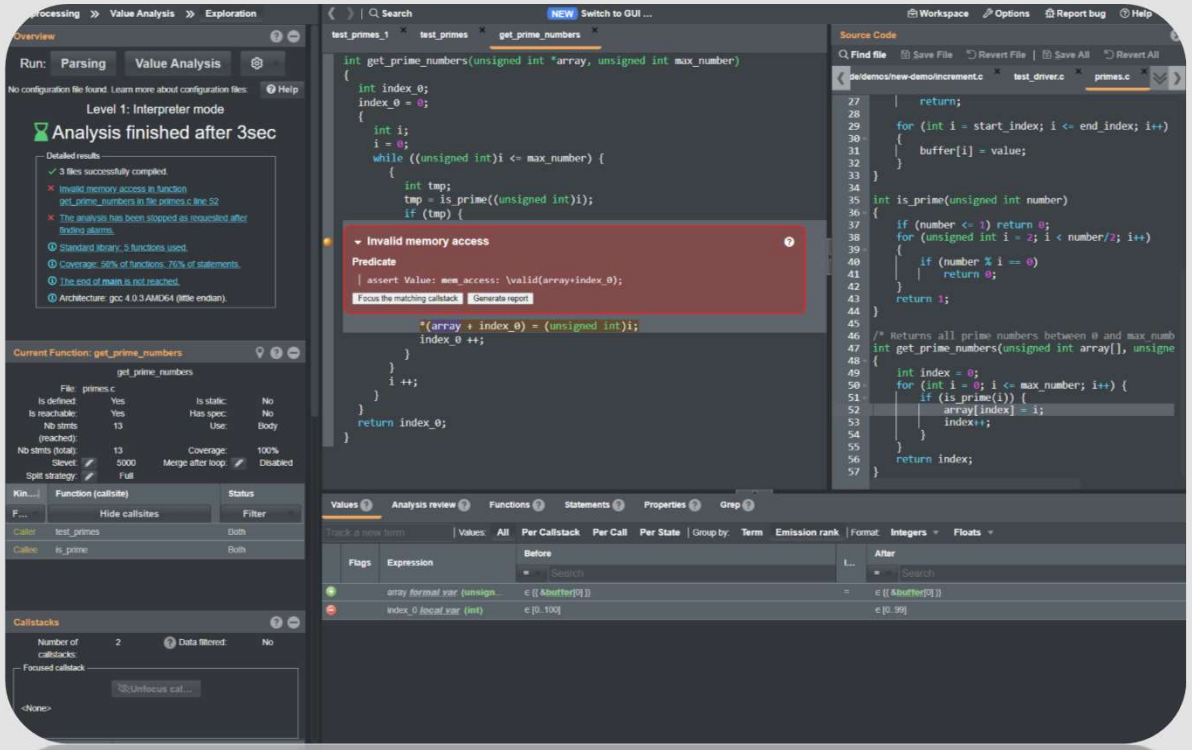
Memory corruption

A function will write a memory area that is almost never used. But when it is used the program will crash. Diagnosing it can take hours, but finding the root cause can take days, weeks.

ROOT CAUSE: C & C++ are not safe languages

© 2024 TrustInSoft

TrustInSoft Root Cause Investigator



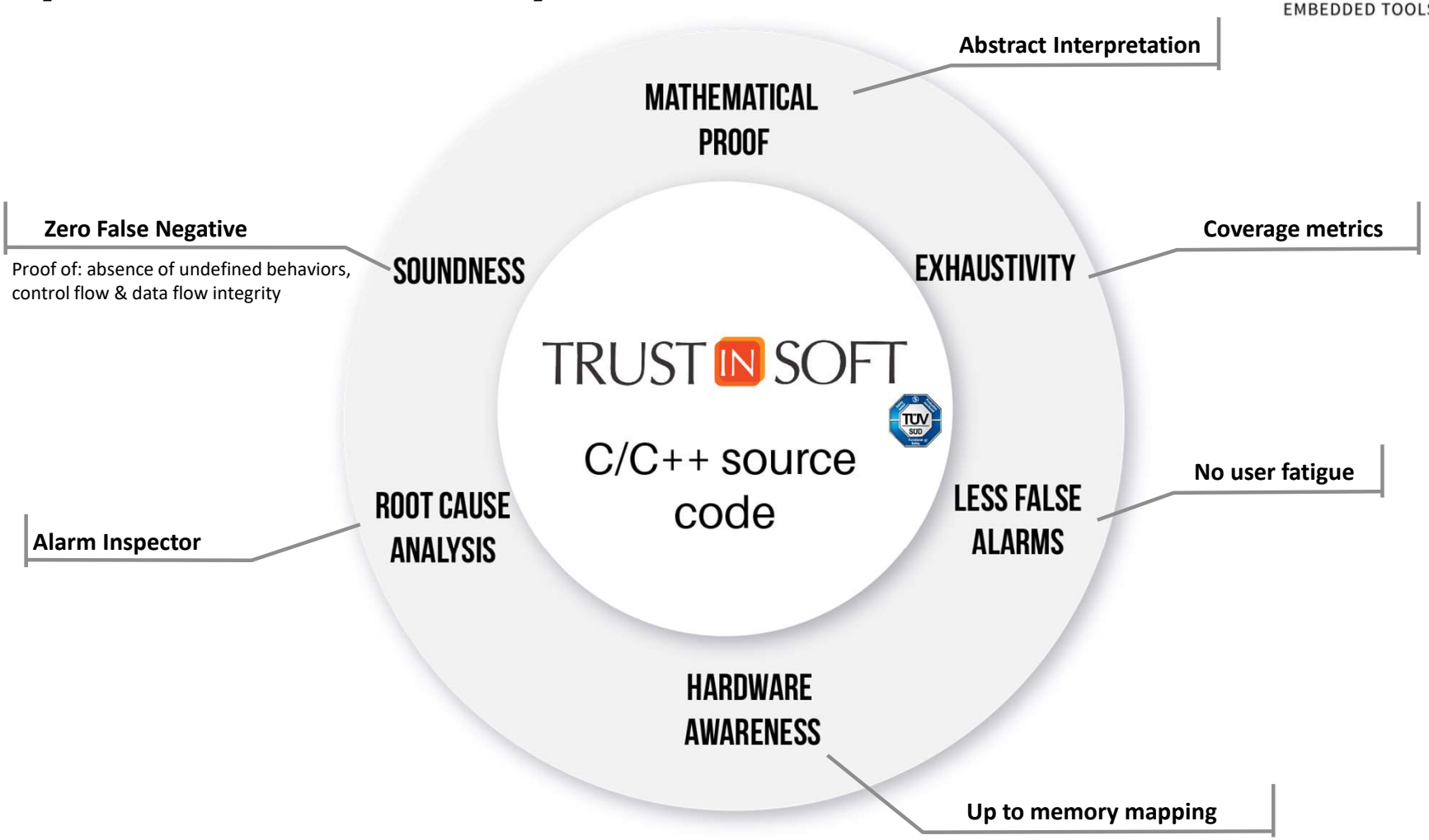
TrustInSoft Analyzer is a Hybrid code Analyzer combining advanced static and dynamic analysis techniques with formal methods.

Value/Data/Code flow using abstract interpretation

Mathematically guarantee C/C++ code quality/security & safety

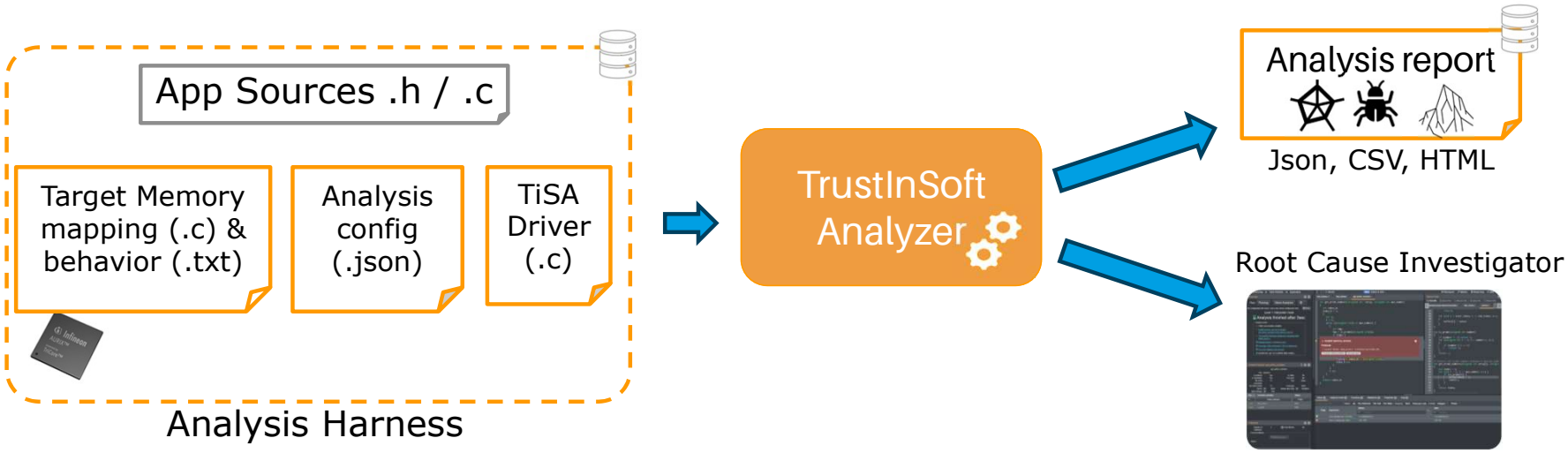
Why is Trustinsoft Analyzer One Of A KIND?

hitex EMBEDDED TOOLS & SOLUTIONS



© 2024 TrustInSoft

TISA PRINCIPLES



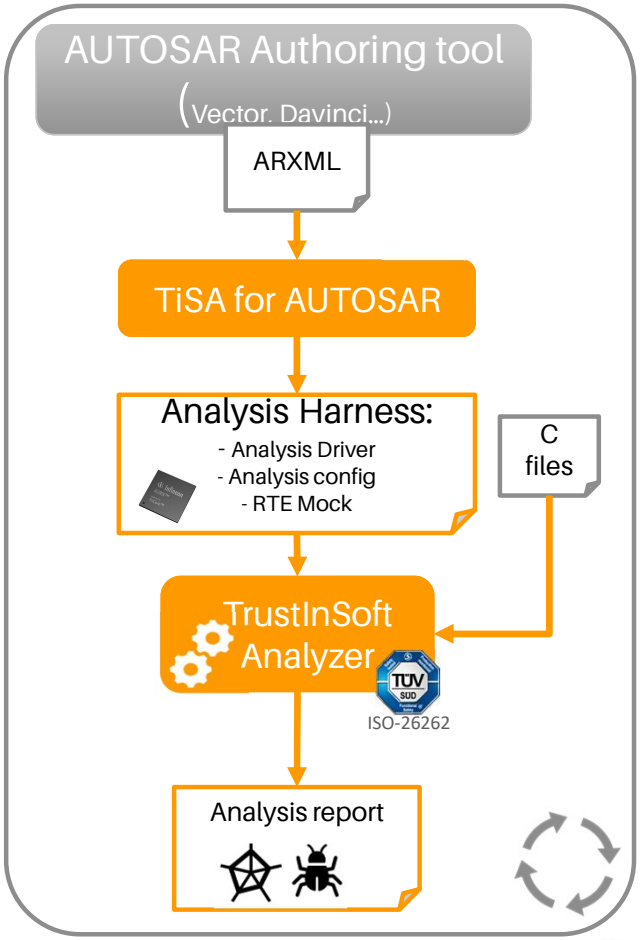
- TISA artefacts (Analysis harness and results) are
  - Fully archivable in Software versioning system
  - Easily integrable in ALM (Application Life Management) and then traceable
  - The traceability facilitates the impact analysis and regression test procedure

© 2024 TrustInSoft

TisA For AUTOSAR Classic

hitex EMBEDDED TOOLS & SOLUTIONS

- Dedicated for AUTOSAR Swc
- Detection of inconsistencies between ARXML and code
- Full automation in CI
- Automatic analysis harness generation
  - RTE Mocks include generalized implementation of RTE API functions
  - Analysis Driver and configuration include invocation of Runnables with generalized input parameters if any (Component Data Structure)
  - Qualified evidence from ASIL QM to D.



TRUST IN SOFT

© 2024 TrustInSoft

AURIX: a concrete case

MEMORY REPRESENTATION

hitex EMBEDDED TOOLS & SOLUTIONS

Table 3 Address Map as seen by Bus Masters on Bus SPB (cont'd)

Address Range from	Address Range to	Size	Unit
$F00E0000_H$	$F00F00FF_H$	64.2 Kbyte	FPI slave interface (I2C1) FPI slave interface (I2C1)
$F00F0100_H$	$F00FFFFF_H$	-	Reserved
$F0100000_H$	$F01FFFFF_H$	1 Mbyte	FPI slave interface (GTM) FPI slave interface (GTM) Mapped RAMs (GTM) Embedded DPLL RAM 2 (GTM)
$F0200000_H$	$F0208FFF_H$	36 Kbyte	RAM Area (CAN0) Register Area (CAN0)
$F0209000_H$	$F020FFFF_H$	-	Reserved
$F0210000_H$	$F0218FFF_H$	36 Kbyte	RAM Area (CAN1) Register Area (CAN1)
$F0219000_H$	$F021FFFF_H$	-	Reserved
$F0220000_H$	$F0228FFF_H$	36 Kbyte	RAM Area (CAN2) Register Area (CAN2)

Extract from https://www.infineon.com/dgdl/Infineon-AURIX_TC39x-UserManual-v02_00-EN.pdf, p24

- Symbol address are abstract by default
- Specific symbols can have an explicit address
- Used for hardware representation
  - Allows hardware fault injection
  - Fixed or volatile contents

```
#define HW_AREA(x) __attribute__((tis_address(x)))
#include "IfxI2c_reg.h"
Ifx_I2C TIS_MODULE_Ifx_I2C1 HW_AREA(0xF00E0000u);
#include "IfxGtm_reg.h"
Ifx_GTM TIS_MODULE_Ifx_GTM  HW_AREA(0xF0100000u);
#include "IfxCan_reg.h"
Ifx_CAN TIS_MODULE_Ifx_CAN0 HW_AREA(0xF0200000u);
Ifx_CAN TIS_MODULE_Ifx_CAN1 HW_AREA(0xF0210000u);
Ifx_CAN TIS_MODULE_Ifx_CAN2 HW_AREA(0xF0220000u);
```

© 2024 TrustInSoft

CORE ARCHITECTURE

hitex EMBEDDED TOOLS & SOLUTIONS

- TIS Analyzer does not need HW platform to work: abstract interpretation & logical simulation
- Need to consider architecture specifics to understand source properly:
  - Basic type sizes (char/int/long, signedness)
  - Endianness
  - Structure and array padding

- TIS Analyzer covers many architectures, 32/64 bits
  - Of course, includes aurix_tricore_le and aurix_tricore_be for Infineon Aurix little and big endian!

TrustInSoft Analyzer Report

Created on Aug 19, 2024, 17:56:03 — Analyzer version 1.47.2

Analyses Summary | Consolidated Alarms | Individual Analyses | Coverage | Metrics | Standards

Analyses Summary

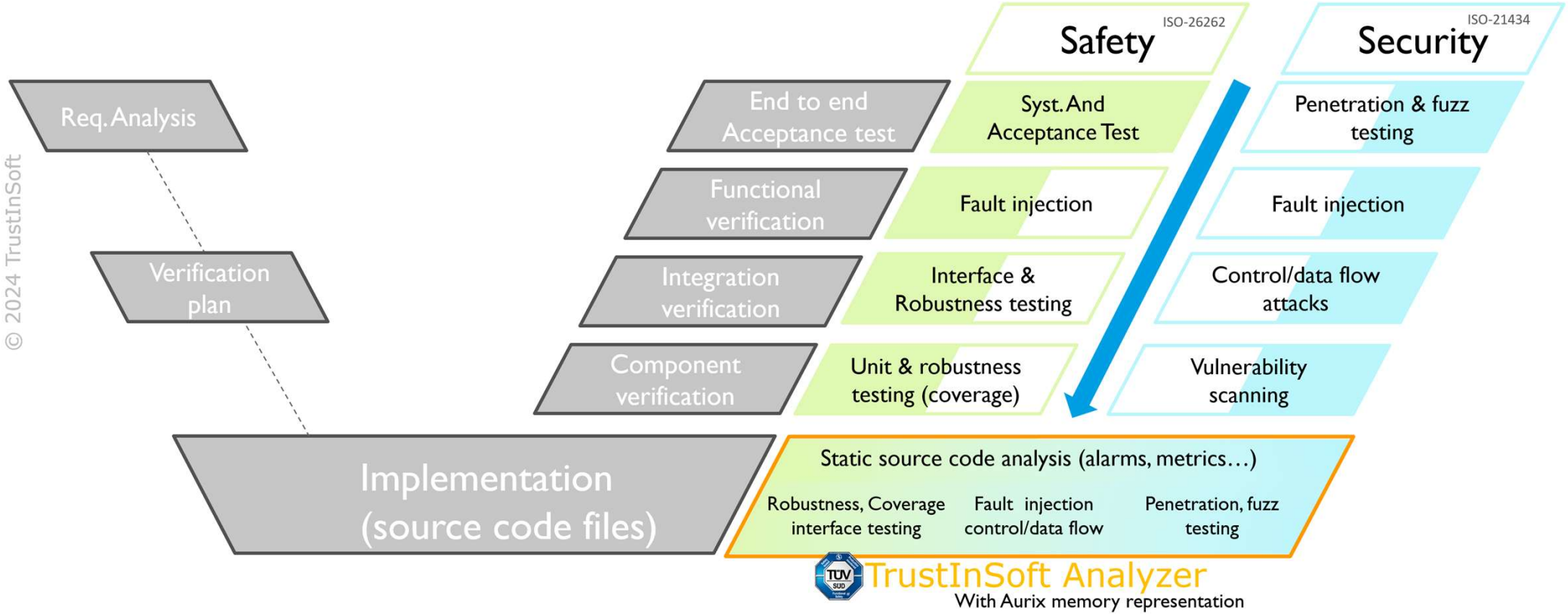
Number of Analyses	14 23 196
Number of Undefined Behaviors	100
Number of Undefined Functions	4
Code Coverage	54 / 67 (80.6%) Functions 3628 / 4294 (84.5%) All Statements 3628 / 3650 (99.4%) Statements in reachable functions 2816 / 3398 (82.9%) All Lines
Architectures	TriCore little-endian - little endian

© 2024 TrustInSoft

Wrap up

TISA: unmatched upstream detection

hitex
EMBEDDED TOOLS & SOLUTIONS



© 2024 TrustInSoft

TRUST IN SOFT

hitex
AURIX KNOWLEDGE LAB 2024
AURIX™ TC4XX
Questions?
eTAS
HIGHTEC
imagimob
An Infineon Technologies Company
infineon
pls
Development Tools
TRUST IN SOFT