

[Complying with international certification standards and guidelines]

Developing reliable embedded systems in compliance with ISO 26262 requirements

TTE Systems Ltd

The safe operation of vehicles on our roads today — whether these are powered by conventional petrol / diesel engines, electric motors or a hybrid arrangement — depends increasingly on embedded processors and associated software. Developing such embedded systems is challenging, and must generally be carried out in line with appropriate international standards.

In this sector, one key new standard is ISO 26262, which is the adaptation of IEC 61508 to comply with the needs of road vehicles. More specifically, ISO 26262 is intended to be applied to safety-related systems that are installed in series production cars with a maximum gross weight of 3,500 kg.

ISO 26262 applies to all activities during the lifecycle of safety-related systems comprised of electrical, electronic and software elements that provide safety-related functions.

This document provides an overview of some of the ways in which TTE Systems may be able to help your organisation to develop reliable embedded systems in compliance with ISO 26262 requirements.

TTE Systems

Developing reliable embedded systems in compliance with ISO 26262 requirements

Recording requirements and designs with RapiDiTty® Designer

UML and SysML have emerged as effective ways of representing requirements and designs for complex embedded systems. Used appropriately, UML / SysML can represent systems in a compact, portable manner which is easy to understand.

RapiDiTty Designer tools provide users with a lightweight, tightly integrated suite of design tools based on UML / SysML standards. RapiDiTty Designer allows users to record requirements and designs (at system, sub-system and component level) and ensure traceability between these different system representations.

RapiDiTty Designer can be provided with a set of matched development processes that are fully customised to meet the needs of the organisation concerned.

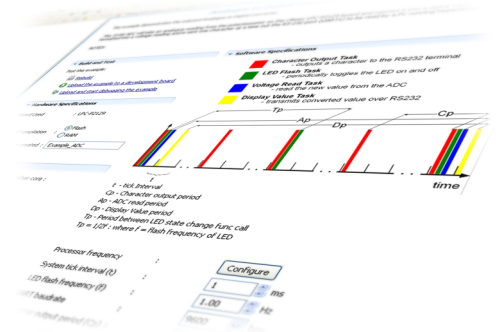
Implementing system software with RapiDiTty® Builder

Once the system requirements and (at least) an initial design have been recorded, work can begin on the system code.

Available in both “off the shelf” and custom formats, RapiDiTty Builder development toolsets provide everything needed to develop software for high-integrity embedded systems that are fully ISO 26262 compliant.

RapiDiTty Builder toolsets include compilers, substantial code libraries, one or more real-time operating systems, and full support for detailed timing analysis.

Members of the RapiDiTty Builder family also support static timing analysis and schedulability analysis, for both single- and multi-core processor targets.



Assessing your complete system with RapiDiTty® Tester

Testing high-integrity embedded systems can be challenging.

In such designs, the system under development must often interact with other equipment (for example, the vehicle wheel in an automotive braking design) and / or with a user (for example, driver control of an adaptive cruise-control system) in a manner which can make it difficult and / or dangerous to test and debug the system. When developing such systems, a “hardware-in-the-loop” (HIL) testbed is often a key part of the development environment.

The RapiDiTty Tester platform provides a flexible means of carrying out such detailed testing at a *system* level.

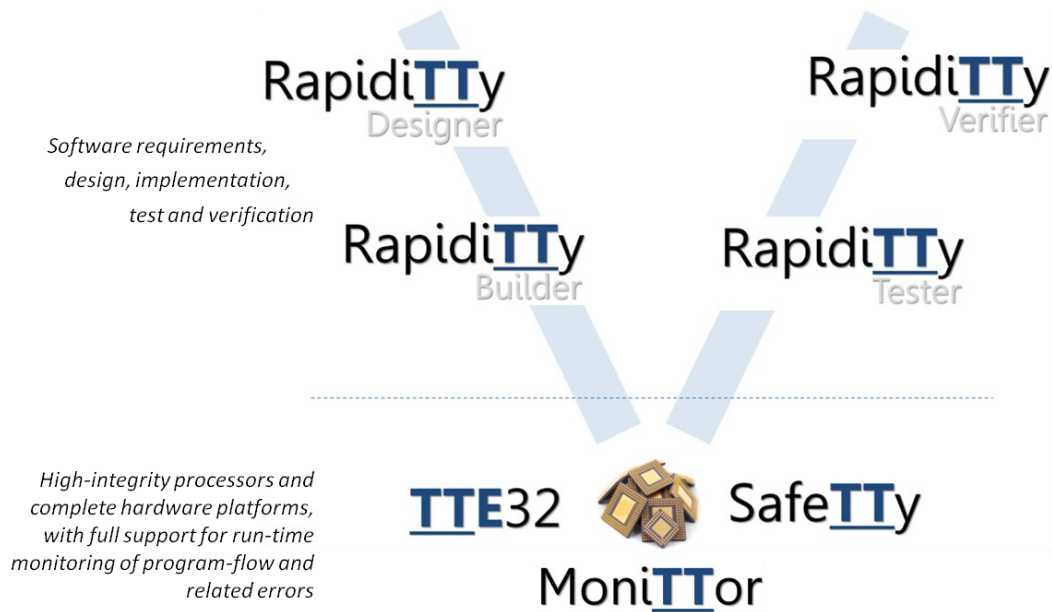
RapiDiTty Tester can be provided in generic forms (where users can create their own detailed test scripts) and — where required — in a fully customised form, to meet the needs of more specialised projects.



Closing the loop with RapiDiTty® Verifier

Verification is the key to the creation of reliable embedded systems. All certification standards — including ISO 26262 — require evidence that (for example) system requirements are fully met by the chosen design, and that, in turn, the design and system code “match up”.

Used in conjunction with other RapiDiTty toolsets, RapiDiTty Verifier provides a highly-effective framework for tracing between design, implementation and test documentation, along with information about design inspections, code reviews and other essential information required to support a case for compliance with ISO 26262.



TTE[®]32 family: High-integrity processors for ISO 26262 systems

TTE32 processors provide a combination of very predictable behaviour, in-built safety mechanisms and comprehensive design documentation that simplifies software development, verification and certification activities for ISO 26262 systems.

The TTE32 family provides the following benefits:

- TTE32 processors are suitable for use in hostile environments, where systems face threats from environmental factors, such as the high levels of EMI which can be associated with electric vehicles;
- TTE32 processors incorporate a task scheduler and error-detection mechanisms in *hardware*: this reduces software complexity, maximises the separation between the scheduler and software tasks, provides extremely fast, fully deterministic, error recovery — and greatly simplifies certification;
- TTE32 processors are available with single-core and fully-deterministic multi-core architectures;
- TTE32 processors are available in standard and custom forms, for both FPGA and ASIC targets.
- TTE32 processors are supplied with a suite of matching RapidITy toolsets;

In many cases, organisations find that switching from off-the-shelf processors and tools to work with high-integrity TTE32 processors and matching RapidITy products provides a significant cost saving.

SafeTTy™ family: Complete hardware platforms for ISO 26262 systems

The SafeTTy family provides complete hardware solutions — TTE32 processors with all required interface electronics — “in a box”. SafeTTy products are supported by matching RapidITy toolsets (including hardware-specific drivers), allowing rapid software development to ISO 26262 standards.

The SafeTTy family provides a perfect platform for the rapid development of high-integrity control units (e.g. ECUs) for use with electric, hybrid and conventional vehicles.

Different members of the SafeTTy family meet the needs of early prototypes, right through to cost-effective volume production. Where required, SafeTTy solutions are available in forms that meet all required electrical and related standards (e.g. IP67).

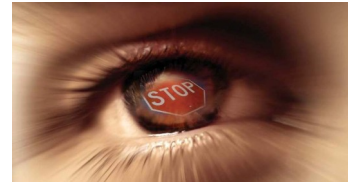
Where required, complete (fully customised) product solutions can be provided, based on SafeTTy platforms. In these circumstances, all (foreground) IP can be assigned to your organisation. You are then free to go into volume production and develop / adapt the design (as required) for future products, subject only to payment of a small royalty fee.



Keeping your system on the road with MoniTTor™ technology

ISO 26262 is a functional safety standard.

Functional safety involves: [i] the detection of a potentially dangerous condition; and [ii] the activation of a protective / corrective device to prevent hazardous events arising, or to provide failure mitigation (to reduce the impact of the hazardous events).



Even when systems are designed with great care, problems may still arise on the road due — for example — to the impact of electromagnetic interference (EMI), “single-event effects” (SEEs), hardware failure, programming errors or even deliberate Stuxnet-like attacks. In modern automotive systems, the impact of such system failures may be serious injury or significant loss of life.

To meet functional-safety requirements, many ISO 26262 designs require the use of an appropriate and independent monitoring device. In such designs, MoniTTor technology can serve as an “intelligent watchdog”, providing a *non-invasive* means of detecting and handling run-time errors.

A solid technology base

TTE Systems provides a range of products and services that can help organisations (large and small) to produce reliable embedded systems. The common factor linking all of TTE’s activities is a rigorous approach to system development, based on the use of *time-triggered* architectures.

Time-triggered architectures have been used for many years in industries such as aerospace and defence, because they have been found to provide significant benefits (including high system reliability and greatly reduced testing costs). Until recently, use of TT architectures has been less common outside these sectors, but this situation is now changing rapidly, as developers in many different organisations experience the benefits of a time-triggered solution.

Further information is available:

<http://www.tte-systems.com/technology>

Certified developers

Creation of certified embedded systems requires the use of appropriate processors, software tools and processes — but it also requires that the development team is both effective and experienced.

Many organisations are now working with TTE Systems to *certify their development teams*, in order to maximise their effectiveness when developing high-integrity embedded systems.

Further information is available:

<http://www.tte-systems.com/services/certification>

Free certification workshops

Organisations based in Europe may wish to send representatives to a one-day workshop on the development of high-integrity embedded systems in compliance with ISO 26262. These free events are organised every 2-3 months. *Attendance requires pre-registration and places are limited.*

Further information is available:

http://www.tte-systems.com/services/training/tte_mira_training_days/26262