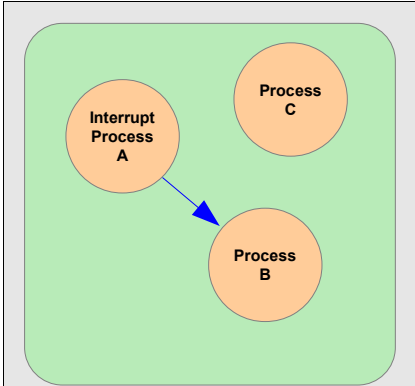
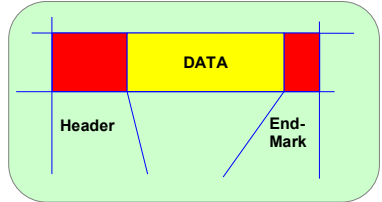
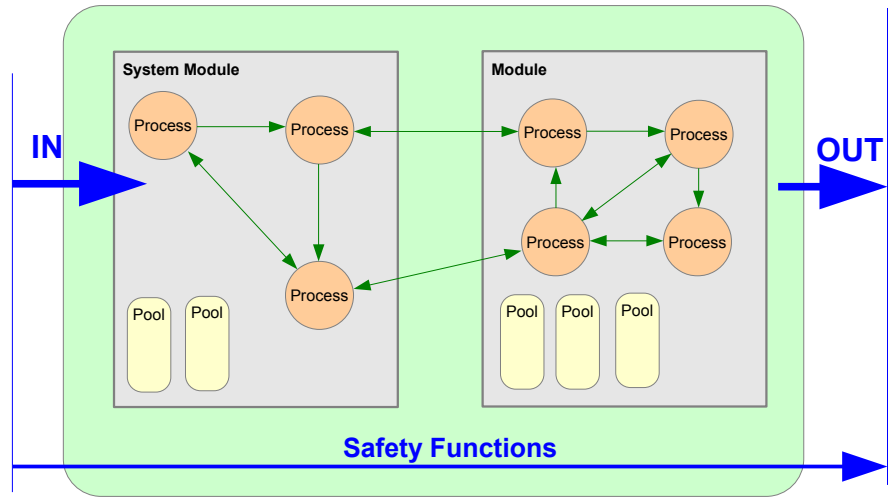


Product Information	Safety-Certified Real-Time Kernels	
<p>Features</p> <ul style="list-style-type: none"> • Message-based Architecture and Methodology. • High performance and low memory footprint. • All data in a SCIOPTA system are encapsulated in messages. • No shared memory and global data. • SCIOPTA messages have identities. • SCIOPTA messages have ownership. Only the owner of a message can access it. Therefore message data is always protected from concurrent access. • Selective receiving of messages. • Unique and efficient memory management of SCIOPTA messages avoids memory fragmentation. • Easier system design and teamwork by the neat message interface. • System level debugger includes message trace, system inspection and message pool analysing. • Centralized error handling. 	<p>Technology</p>	<p>No Shared Memory</p>
<p>Designed for Safety</p>	<p>SCIOPTA is a pre-emptive multi-tasking high performance real-time kernel which includes many built-in safety features.</p> <p>As a direct message-passing kernel, SCIOPTA is very well suited to be used in safety-critical applications.</p> <div data-bbox="587 678 1003 1061" data-label="Diagram">  </div> <p>Direct message-passing in a SCIOPTA system results in a clear, easy to use and secure design.</p> <p>Interrupt Process A allocates a message and sends it to Process B which is waiting for it. As Process B has a higher priority than actual running Process C, the kernel will swap-in Process B which will now receive and free the message.</p>	<p>Shared memory is the standard method for interprocess communication in traditional real-time operating systems. The user is fully responsible to protect shared memory with semaphores and to associate semaphores with data areas and types.</p> <p>There is no need for shared memory in a SCIOPTA system. Direct message passing is safer. All data are encapsulated inside messages and the kernel protects message data by controlling ownership.</p>
<p>Designed for Safety</p>	<p>Safety Certification</p>	<p>Safe Data Transfer</p>
<p>For some SCIOPTA kernels (e.g. PowerPC) there is also data integrity available, covering some requirements for IEC61508 Part 2. These kernels features the following functions:</p> <ul style="list-style-type: none"> • All kernel data (control blocks and list) is stored twice where one copy is inverted. • Safe data types (e.g. safe integer) also doubly inverse stored. • Program flow control. • Plausibility check on message passing gives safe interprocess communication. • Safe Memory Management System gives the possibility to have safety-related systems and non-safety related systems on the same CPU. • The safety kernel provides functions to ensure protection of internal and external data. Safety critical data are validated at every read and write operation. All kernel data are doubly stored. 	<p>SCIOPTA is certified by TÜV Süd Munich</p> <p>to IEC 61508 SIL3, EN50128 SIL3/4 and ISO 26262 ASIL-D.</p> <p>SCIOPTA safety documentation includes the TÜV Certificate, the TÜV Certification Report and the Safety Manual.</p> <p>The safety manual provides guidance on how to safely use SCIOPTA.</p> <p>This will include information about which features and functions can and can't be used safely as well as any procedures that must be put in place to ensure safety.</p>	<p>SCIOPTA messages are exclusively used for inter-process communication and coordination. The direct message-passing together with many built-in error checks results in easy to design and safe data transfer between processes.</p> <div data-bbox="1086 1111 1469 1312" data-label="Diagram">  </div> <p>The SCIOPTA message consists of a header including the process ID of the sender, owner and addressee, a data area of any size and an end-mark which is checked by the kernel.</p>
<p>Designed for Safety</p>	<p>Safety Certification</p>	<p>Easy to Use</p>
<p>Designed for Safety</p>	<p>Safety Certification</p>	<p>The SCIOPTA message-passing interprocess communication can be handled by using only four powerful system calls:</p> <div data-bbox="1110 1749 1430 1854" data-label="List-Group"> <ul style="list-style-type: none"> sc_msgAlloc sc_msgFree sc_msgTX sc_msgRx </div>

Safety Related Systems

The SCIOPTA development methods and Life-Cycle activities are certified to IEC 61508 SIL3, EN50128 SIL3/4 and ISO 26262 ASIL-D.

This allows to use the safety certified SCIOPTA in multi-channel (multi-CPU) systems.

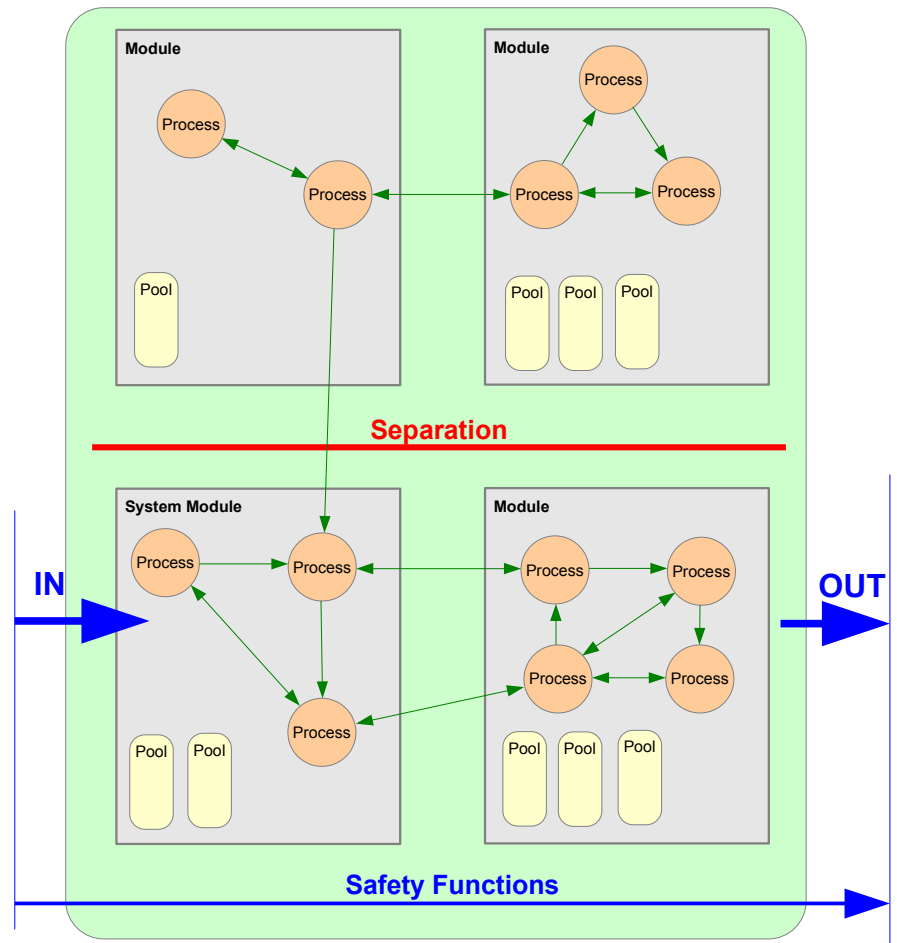


Implementing Safety and Non-Safety Functions

IEC61508-2 (7.4.2.3) says:

"Where an E/E/PE safety-related system is to implement both safety and non-safety functions, then all the hardware and software shall be treated as safety-related unless it can be shown that the implementation of the safety and non-safety functions is sufficiently independent (i.e. that the failure of any non-safety-related functions does not cause a dangerous failure of the safety-related functions). Wherever practicable, the safety-related functions should be separated from the non-safety-related functions".

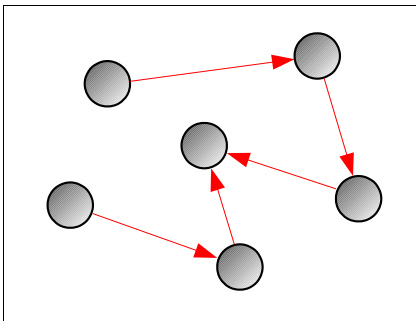
The specific safety functions such as duplicated data storage, program-flow control, stack check, crc-functions, safe-data types and CPU-checks together with the SCIOPTA Memory Management Systems helps you to meet above requirements.



Safe Process Flow

The safety kernel provides internal and external safety functions to insure correctness of the process flow or to detect incorrect process flow.

Logical program flow supervision for one or multiple parallel flows is supported.



Execution Control

In a SCIOPTA system the user can include own functions called Hooks at specific system events.

For example the message transmit hook, the message receive hook and the process swap hook allow the user to realize an execution control which can be an important safety function in a certified system.

Centralized Error Handling

Centralized error handling is an important safety feature of SCIOPTA. All errors will call a centralized error handling function called Error Hook.

The SCIOPTA kernel does not simply return an error code to the user, which is the typical method in traditional real-time operating systems and leaves the responsibility of error handling to the user.

Safe Memory Management

Processes can be grouped together into SCIOPTA modules. Each module can have up to 128 pools to hold SCIOPTA messages.

SCIOPTA supports a module friend concept. Friendship between modules can be defined and configured by the user. This friendship setting defines if messages are copied or not when they are crossing module boundaries.

Modules and pools can be located in the same or in different memory segments. With the SCIOPTA Memory Management System (SMMS) and a Memory Management Unit (MMU) full memory protection can be achieved.

Message Protection

The safety kernel provides protection of SCIOPTA messages and provides functions to check and update the integrity information of message data.

The message internal data are plausibility checked by the kernel.

All checks are performed at message-passing.

Code Protection

The safety kernel provides CRC-functions to be used for code protection.

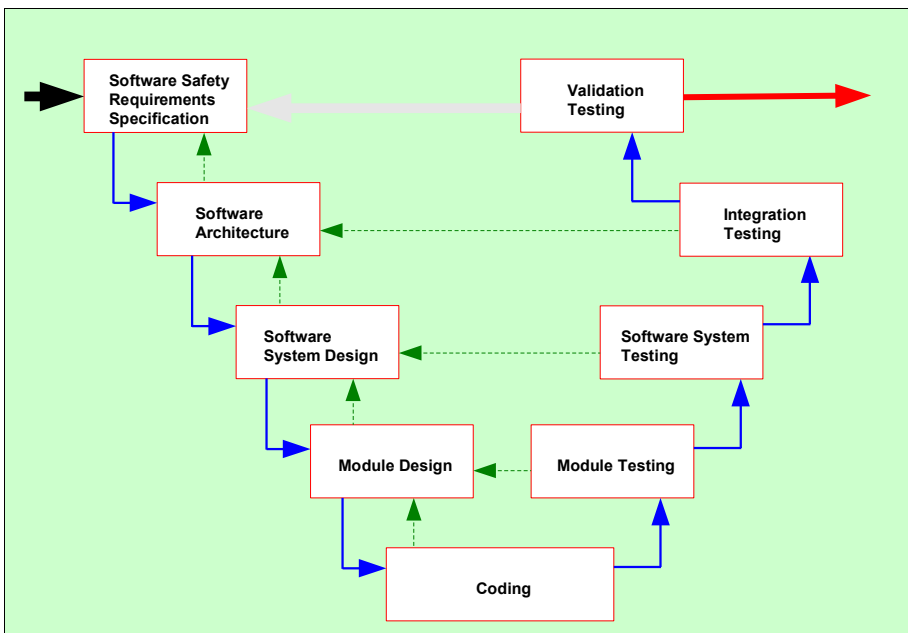
The code protection of the kernel is part of the overall code protection of the project.

Safety Life-Cycle

IEC 61508 is based on a safety life-cycle approach which identifies requirements and activities based on it.

The SCIOPTA life-cycle activities and methods have been certified by TÜV to IEC 61508 SIL3, EN50128 SIL3/4 and ISO 26262 ASIL-D.

Life Cycle



EU Headquarters
 SCIOPTA Systems GmbH
 Hauptstrasse 293
 79576 Weil am Rhein
 Germany

Tel. +49 7621 940 919 0
 Fax +49 7621 940 919 19

Headquarters
 SCIOPTA Systems AG
 Fiechthagstrasse 19
 4103 Bottmingen/Basel
 Switzerland

Tel. +41 61 423 10 62
 Fax +41 61 423 10 63

www.sciopta.com
sales@sciopta.com