

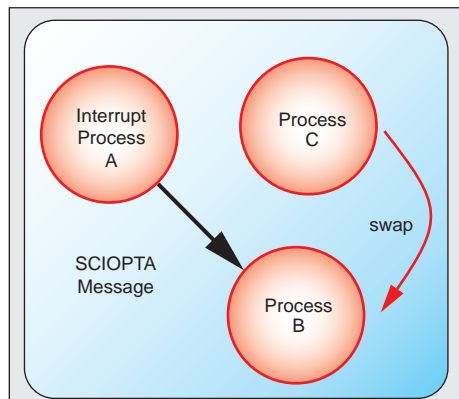
**Product Information** IEC61508 Safety-Certified Real-Time Kernels

**Features** **Technology** **No Shared Memory**

- Message-based Architecture and Methodology.
- Low memory footprint allows single-chip and SoC applications.
- High performance.
- 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 analyzing.
- Centralized error handling.

SCIOPTA 61508 is a pre-emptive multi-tasking high performance real-time kernel which includes many built-in safety features.

As a direct message-passing kernel, SCIOPTA is very well suited to be used in safety-critical applications.



**Direct message-passing** in a SCIOPTA system results in a clear, easy to use and secure design.

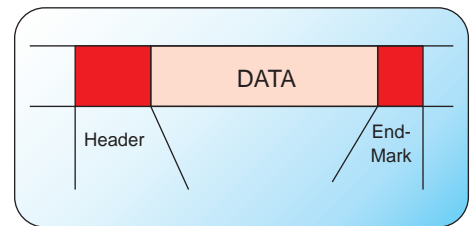
**Interrupt Process A** allocates a message and sends it to **Process B** which is waiting for it. As **Process B** has a higher priority than actual running **Process C**, the kernel will swap-in **Process B** which will now receive and free the message.

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.

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.

**Safe Data Transfer**

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.



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.

**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.

**IEC 61508 Certification**

SCIOPTA is in the final stages of certification by TÜV to the IEC 61508 standard which allows to build SIL3 (Safety Integrity Level 3) systems.

SCIOPTA safety documentation is extensive and includes the Safety Manual.

All other certification documents such as Safety Requirement Specification, Design Specifications, Test Specifications, Safety, Validation and Verifications Plans are available upon request.

IEC61508 is the international standard focusing on safety-related systems that incorporate electrical, electronic and/or programmable electronic (E/E/PE) instruments and devices.

Initially mainly used in the automation and process control industry, IEC61508 is more and more accepted for applications in other industries including automotive and medical where safety and reliability are paramount.

## SCIOPTA IEC61508 Kernels

SCIOPTA offers two versions of IEC61508 Safety-Certified Real-Time Kernels

### SCIOPTA IEC61508-P3 Kernels

SCIOPTA Safety-Certified Kernel according to IEC61508 Part 3

**IEC 61508 Part 3  
Functional Safety of  
E/E/PESystems  
Software  
Requirements**

The SCIOPTA IEC61508-P3 Kernels allow the user to develop and certify safety application up to a level of SIL3.

The kernel is certified according to part 3 of the standard.

Please consult:

**Internation Standard IEC 61508-3**

Please Note:

The user is responsible to include and certify data integrity for the safe system up to the desired SIL following the rules and recommendation of the standard and the SCIOPTA safety manual. Using the SCIOPTA IEC61508-P3 kernel is not sufficient to comply with IEC 61508 Part 2.

### SCIOPTA IEC61508-I Kernels

SCIOPTA Safety-Certified Kernel according to IEC61508 Part 2 and Part 3 with included data integrity

**IEC 61508 Part 2  
Functional Safety of  
E/E/PESystems  
Requirements for  
E/E/PESystems**

**IEC 61508 Part 3  
Functional Safety of  
E/E/PESystems  
Software  
Requirements**

The SCIOPTA IEC61508-I Kernels allow the user to develop and certify safety application up to a level of SIL3.

Additionally this kernel is fully certified **with data integrity** to SIL2 with a Safe Failure Fraction of 90%.

The kernel is certified according to part 2 and part 3 of the standard.

Please consult:

**Internation Standard IEC 61508-2  
Internation Standard IEC 61508-3**

Please Note:

The user is responsible to include and certify data integrity for the safe system for SIL3 following the rules and recommendation of the standard and the SCIOPTA safety manual.

Some of the safety data integrity functions:

#### Critical Data Protection

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.

The kernel provides safe data type system calls.

Stack data are protected while process is not running.

To allow critical data protection a hazop of all kernel data have been performed.

#### Message Protection

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

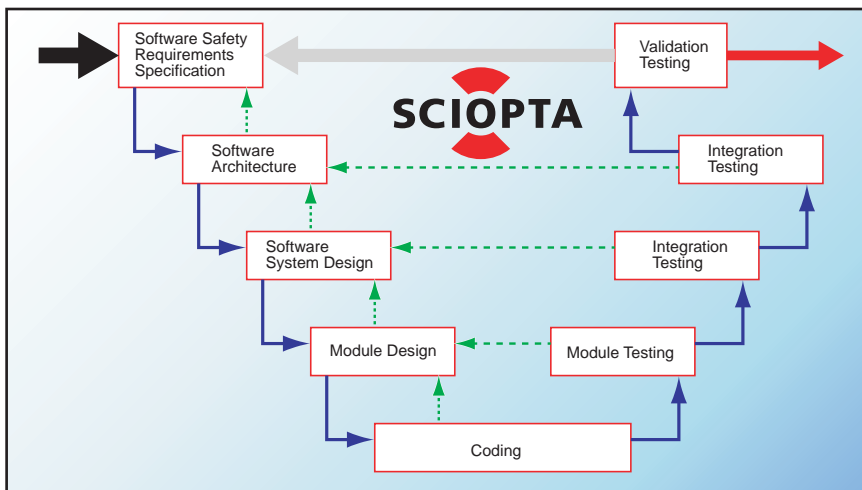
The message internal data are plausibility checked by the kernel.

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.



### 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.

### Safety Library

Selected safety functions are made available to the user by a specific safety library.

### Execution Control

In a SCIOPTA system the user can include own functions called **Hooks** at specific system events. For example the message transmitt 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.

### Easy to Use

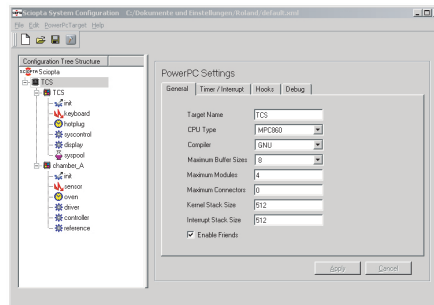
The SCIOPTA message-passing interprocess communication can be handled by using only four powerful system calls:

**sc\_msgAlloc**

**sc\_msgFree**

**sc\_msgTx**

**sc\_msgRx**



For the static system configuration (modules, processes, pools etc.) a graphic configuration tool is available.

### Supported CPUs

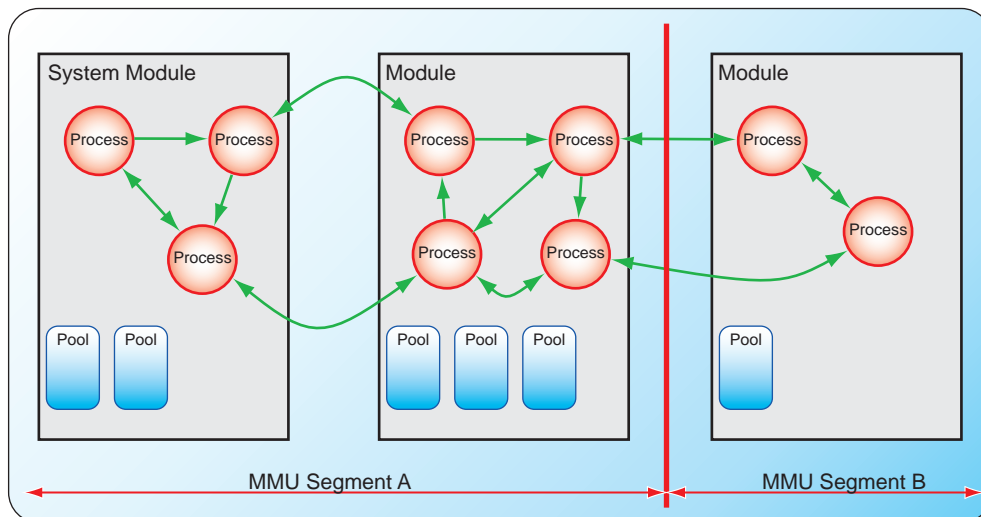
Initially certified for the ARM7/9 family, SCIOPTA IEC61508 will be available for all popular CPUs supported by SCIOPTA.

- ARM7/9, including ATMEL AT91SAM, NXP LPC2000, Sharp, STMicroelectronics STR7/9 and others
  - Freescale ColdFire
  - Freescale PowerPC MPC500
  - Freescale PowerPC MPC55xx
  - Freescale PowerPC MPC5200
  - Freescale PowerPC MPC8xx
  - Freescale PowerPC MPC82xx
  - Marvell XScale
  - 16-Bit CPUs:
    - Freescale HCS12
    - Renesas M16C/M32C
- Please ask for other CPUs

### 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.



### Contact

Headquarters:  
 SCIOPTA Systems AG  
 Fiechthagstrasse 19  
 4103 Bottmingen/Basel  
 Switzerland  
 Tel. +41 61 423 10 62  
 Fax +41 61 423 10 63

Engineering and German Office:  
 SCIOPTA Systems GmbH  
 Hauptstrasse 293  
 79576 Weil am Rhein  
 Germany  
 Tel. +49 7621 940 919 0  
 Fax +49 7621 940 919 19

sales@sciopta.com  
[www.sciopta.com](http://www.sciopta.com)