Importance of the Failure Mode Effect and Diagnostics Analysis when Designing Safety Critical Applications

Introduction

Author: Jacob Lunn Lassen, Microchip Technology Inc.

Note: If you already have experience with designing safety-critical systems, you may want to skip this document and rather download Microchip's FMEDA and Safety Manual sample documents, or request the documents for the microcontroller you want to use.

While the different functional safety standards have a slightly different approach on how to comply with the specific standard, they all have the same purpose: To reduce the likelihood of injuries caused by a failure of the electronic systems to an acceptable level.

It is important to understand that safety-critical systems must comply with and be certified to a safety standard on a system level. There is no single component that can make a system safety compliant. Compliance is reached through rigorous specification, design, implementation, and test of the system as a whole. Still, a component in the system may implement one of many safety features, and it is imperative to assess how to maintain the intended operation of each safety feature. For that reason, it is relevant to understand the correct use of each component in a safety context. The required information is beyond what is described in the data sheet of the components and is typically offered as separate documentation by serious suppliers in the safety market.

This white paper describes one of the key tools that Microchip offers to designers of safety-critical systems for free, namely the Failure Mode Effect and Diagnostics Analysis (FMEDA). This document is essential to determine and quantify the failure rate and diagnostics coverage, as well as to understand the failure modes and effects on a chip level for the PIC®, AVR®, and SAM microcontrollers (MCUs) and dsPIC33 Digital Signal Controllers (DSCs). The FMEDA is defined by the automotive standard, ISO 26262, but can also be applied to other safety-critical designs that must comply with standards such as IEC 60730 for household appliances, IEC 61508 for industrial applications and IEC 62304 for medical applications.

Microchip also offers other documents, such as safety manuals, which supplement the FMEDA, but they are outside the scope of this white paper.

Table of Contents

1. A Simplified Description of the Safety Design Process

In safety designs, it is common, and in some cases mandatory, to use the so-called V-model design method. It describes the phases and steps of a robust and reliable design process, including the definition of the system's safety requirements, and track these all the way through design, implementation, test, and validation, to ensure that they are correctly and sufficiently covered in the final product.

In the specification phase, it is required to identify all *hazards* of the safety-critical system (or sub-system). Let us consider a gas boiler. Since gas is flammable, gas leakage is the *hazard*. The specification, therefore, describes that a gas leakage must be detected within a certain duration to prevent fires and explosions. At the design level, specify one or more *safety features* that can reduce the likelihood of the *hazard*. This could be a gas sensor or a position sensor on the gas valve to determine if it is closed. Now, the element that differs from non-safety applications is that the *safety features* must be verified to operate as intended at run-time. This is what is referred to as *functional safety*. In other words, that the safety mechanism is functional. The designer also referred to as the *system integrator*, ensures that the gas sensor and valve position sensors are operating as intended, by applying the appropriate *diagnostics mechanisms* (self-test): If a *fault* is detected by the *diagnostics,* the system must enter a *safe state* to avoid the *hazard*. The safe state may, in this case, be to close a secondary closing valve, enable a ventilation system, or sound an alarm to indicate the safety mechanism is not working.

The mentioned safety standards also focus on failures occurring in the electronics, even on a smaller scale, in the silicon-based components, such as the microcontrollers in the system.

A general misconception is that the objective of functional safety is to avoid the fault, which is incorrect, partly because the probability of a fault is never zero. The correct way to understand functional safety is that a safety-critical system must detect and respond to faults in a safe way within a defined time interval, referred to as the fault tolerance time interval (FTTI). As an example, for a gas boiler that uses a gas sensor to determine if there is a gas leakage (a safety feature), it must be possible to verify that the gas sensor is operating as intended and can detect leaking gas. It might be reasonable to tolerate a leakage for 10 ms since it does not represent a hazard, but it is not likely that the leakage can be allowed for tens of seconds as the amount of gas leaked then represents a hazard.

The objective is to understand the hazards and the faults - and how to reliably detect them.

2. The Failure Mode Effect and Diagnostics Analysis (FMEDA)

Each safety standard operates with slightly different safety levels. For IEC 61508, these are referred to as safety integrity levels (SIL), ranging from SIL 1 to SIL 3. The automotive ISO 26262 standard uses the automotive safety integrity level (ASIL), from ASIL A to ASIL D[1]. The IEC 60730 uses Class A to Class C.

Since the FMEDA originated from the ISO 26262 standard, we will stick to the definition from this standard for the remaining part of this document for simplicity, and refer to ASIL.

2.1 FMEDA - Failure In Time (FIT)

To meet a certain ASIL level, the failure in time (FIT) rate must be below a given limit. The FIT rate is the number of expected failures per one billion hours of operation, so a statistical representation for the probability of failure. Typically, the microcontroller (MCU) is allotted a certain amount of the total allowed FIT for the entire electronics module in a safety-critical application, e.g., 10%. This can be adjusted from application to application based on the rest of the design. The ASIL level and thereby the acceptable FIT limit is a result of the impact of the hazard, which is expressed as the product of the severity, exposure, and controllability of the hazard (refer to the ISO 26262 standard for further details). An ASIL D application, which is associated with a more severe risk of injury, therefore requires a lower FIT than an ASIL A, B or C application.

In ISO 26262, 100 FITs are allowed for ASIL B and ASIL C, and 10 FITs for ASIL D. In Microchip's FMEDA, the MCU is by default allocated 10%, and the allowed FIT for the MCU is therefore 10 FIT for ASIL B and ASIL C, and 1 FIT for ASIL D applications.

Figure 2-1. FIT Limits for Various ASIL Levels

ISO 26262 ASIL Level	ASIL A	ASIL B	ASIL C	ASIL D
Allowable PMHF budget for this item	10 %	10 %	10 %	10 %
- Actual PMHF limit	None	< 10 FIT	< 10 FIT	< 1 FIT
PMHF - Probabilistic Metric for random Hardware Failures [1/hr]:	1.05	1.05	1.05	1.05
SPFM - Single Point Fault Metric [%]:	98.9%	98.9%	98.9%	98.9%
LFM - Latent Fault Metric [%]:	99.5%	99.5%	99.5%	99.5%

The base FIT rate of the MCU in Microchip's FMEDAs is determined using the Siemens SN29500 model, which calculates the FIT rate based on the number of logic gates in the design, the size of the die, the voltage and current, temperature profile, and several other parameters. The base FIT rate applies if the entire device is considered safety-critical, all features are used, and no diagnostics mechanisms are applied to detect failures (and safely handle them). The FMEDA is used as a tool to identify the portions of the die that are not safety-relevant and to assign diagnostics to detect failures in the portion of the die that is safety-relevant, which results in a much lower residual FIT rate that must be less than the required ASIL based FIT rate. The residual FIT rate represents the undetectable failures of the safety-critical functions of the MCU after diagnostics have been applied, which is what the ASIL levels dictate limits for. We will get back to the failure modes and diagnostics shortly.

2.2 Diagnostics Coverage

In addition to the FIT rate, it is also necessary to evaluate and comply with the diagnostics coverage requirements. The diagnostics coverage is given as a percentage and describes how well the modules required for the safety features are monitored, and how reliably a fault can be detected. The coverage for any given type of diagnostic is defined by the standard and can be low (60%), medium (90%), or high (99%). The higher the ASIL level, the higher the weighted average test coverage must be. The weighted average is based on the physical size of the MCU module, so a larger module, such as the flash memory, contributes relatively more than, e.g., a small timer. This is because the failures considered by ISO 26262 are primarily related to random hardware failures, for which the probability is a function of the area of the die, or in this case, the area of the module.

[1] ISO 26262 also uses Quality Managed (QM), which is the least strict level that indicates a general process conformance rather than a safety level.

Figure 2-2. Diagnostics Coverage for Various ASIL Levels

ISO 26262 ASIL Level	ASIL A	ASIL B	ASIL C	ASIL D
Allowable PMHF budget for this item	10 %	10 %	10 %	10 %
- Actual PMHF limit	None	< 10 FIT	< 10 FIT	< 1 FIT
PMHF - Probabilistic Metric for random Hardware Failures [1/hr]:	**1.05**	1.05	1.05	1.05
SPFM - Single Point Fault Metric [%]:	**98.9%**	**98.9%**	**98.9%**	**98.9%**
LFM - Latent Fault Metric [%]:	**99.5%**	**99.5%**	**99.5%**	**99.5%**

Two criteria are used to assess what ASIL compliance can be achieved, Single Point Failure Metric (SPFM) and Latent Failure Metric (LFM). A single point failure is when a single module (function) in the MCU fails, causing a safety feature to not operate as intended[2]. A single point failure can be that an I/O pin is not set high when the software tries to set it high. A latent failure is when a function, that can indirectly affect the intended operation of the system, fails. In other words, when a hardware monitoring/diagnostics mechanism in the MCU fails. This can be more easily understood with an example: In most MCU based safety-critical systems, the CPU itself is a primary function, in which faults will violate the safety requirements and are therefore single point faults. For that reason, the Watchdog Timer is used to ensure that the MCU is reset (safe state) if the program flow timing changes, which is an indication that there is a fault in the CPU. If, however, there is a fault in the Watchdog Timer, it will not cause the system to fail: The CPU continues to operate normally, and the WDT failure remains latent (silent). Then if the CPU also fails, the WDT is unable to detect the irregular program flow timing changes, and instead of switching to a safe state, continues operating in a likely unsafe way. It is, therefore, required to verify that the Watchdog Timer operates as intended so that its failures are not latent failures in the system. In other words, safety mechanisms implemented in hardware are great, and they reduce the need for periodic testing and thereby reduce the load on the CPU, but you must still verify that they work as intended.

2.3 MCU Failure Mode Effects and Diagnostics

With a fundamental understanding of what we try to achieve, it is time to look at the FMEDA as a tool. To determine the residual FIT and Diagnostics Coverage, the FMEDA must be filled out by the system integrator. To do this, it is required that the system integrator has identified the hazards of the system and have a good understanding of how the system will be implemented on a hardware/mechanical level. Let us look at the (simplified) gas boiler system again and focus on the gas valve only. This is a constructed example for explaining the purpose of the FMEDA only.

The gas valve is used to shut off the gas flow. The position of the valve is controlled by a digital signal and has a digital position sensor that provides information about whether the valve is open or closed. From a microcontroller perspective, the safety-relevant feature is the control signal to the gas valve, so an output pin/signal and input pins to read the sensor feedback signal from the valve position sensors. Let us, for simplicity, assume that it is a perfect valve which cannot fail, and focus on the MCU. We have determined the safety-relevant feature, and now we need to consider the failure modes of the modules involved to ensure the correct operation of the safety feature. The CPU, flash, SRAM, and clock are always critical, and in this case, the General Purpose I/O (GPIO) as well. The section of the FMEDA describing the GPIO is shown below.

[2] This is in contrast to Multi-Point Failures, where the combination of two or more simultaneous faults cause a safety feature to not operate as intended. Since the probability of a single failure is small, the simultaneous occurrence of two faults is very small (assuming that they are independent), and for that reason, it is considered acceptable to primarily focus on Single-Point Failures.

Figure 2-3. Section of the FMEDA Showing the General-Purpose I/O Pins Failure Mode, Effect and Diagnostics

Failure Mode	Effect	FIT Split	FIT rate component	Internal Diagnostics for Single Point Failure
I/O pin stuck	Wrong output value	20%	1,6926%	(H) IO_PORTS_INPUT_COMPARISON (H) IO_PORTS_OUTPUT_MONITOR
No output	High impedance	20%	1,6926%	(H) IO_PORTS_OUTPUT_MONITOR
Pin pullup not working	Floating pin	13%	1,1002%	(H) IO_PORTS_OUTPUT_MONITOR
Pin invert output not working	Wrong output value	2%	0,1693%	(H) IO_PORTS_OUTPUT_MONITOR
Input sense not working	Incorrect operation	11%	0,9309%	(H) IO_PORTS_INPUT_COMPARISON
Hardware read/modify/write modifies wrong pin	Wrong pin direction/value	11%	0,9309%	(H) IO_PORTS_OUTPUT_MONITOR
Hardware read/modify/write does not update intended pin		11%	0,9309%	(H) IO_PORTS_OUTPUT_MONITOR
Virtual ports not working		5%	0,4231%	(H) IO_REGISTER_RESET_STATE_CHECK & IO_REGISTER_BLOCK_REPLICATION & IO_REGISTER_WRITE_READ_TEST
No event to EVSYS	Incorrect operation	2%	0,1693%	(M) EVENT_ROUTING_CHECK
No PORT interrupt		2%	0,1693%	(M) IO_PORTS_CHANGE_NOTIFICATION_TEST
PORT interrupt cannot be cleared		2%	0,1693%	(M) IO_PORTS_CHANGE_NOTIFICATION_TEST
Register failure		1%	0,0846%	(H) IO_REGISTER_RESET_STATE_CHECK & IO_REGISTER_BLOCK_REPLICATION & IO_REGISTER_WRITE_READ_TEST

The “Failure Mode” column describes the type of failure, the “Effect” column describes the direct result of the failure, and the two following FIT columns describe the relative and absolution contribution to the FIT rate (total for all pins). The last column is the reference name to a potential diagnostic, which is described in more detail in the Safety Manual. Looking at the first line, the failure described is that an I/O pin can be stuck, which may result in outputting the wrong output value. The contribution to the FIT rate is 1.69% for all pins in total (each pin, therefore, contributes significantly less).

Consider the output pin that controls the gas valve's position. The FMEDA describes several ways it may fail. It may be stuck high or low, floating (not driving the line), and several other faults. This gives the system integrator a good understanding of what to consider to ensure that the intended operation can be maintained if required. It may not be necessary to detect all possible faults. If for example, an input pin that is stuck low creates an invalid determination that the valve is open and unsafe, and therefore the application unnecessarily goes into a safe state, is by definition safe and does not need to be detected or prevented and is not counted in the single point fault or residual FIT rate. In some situations, it is sufficient to monitor the output pin by reading it back using its input buffer, and if it does not go high or low as expected, the MCU can reset itself[3], which will always cause the MCU to release all I/O lines. This is function of the IO_PORT_OUTPUT_MONITOR diagnostics (described in the Safety Manual). Another solution could be to combine two output pins so that both must be in a given state for the valve to open, and if either pin is not in the open-state, the valve will remain closed. This mechanism uses redundancy to detect and prevent a Single-Point Failure.

For the input required to read the position sensor, the IO_PORT_INPUT_COMPARISON diagnostics is listed as a suitable mechanism. This diagnostic uses two input pins that are both connected to the sensor. If the input read by these do not match, one is concluded to have failed, and the system is placed in a safe state.

[3] The Reset state must always be a safety state, as this is an expected state for the MCU during start-up. External hardware, such as pull-up resistors, must ensure that all lines have a well-defined and safe state.

Depending on what diagnostics methods that are selected in the FMEDA, low, medium, or high single point diagnostics coverage can be achieved. The figure below shows the selection (in the implemented diagnostics column) and the corresponding coverage to the right of it.

Figure 2-4. Available Diagnostics for General Purpose I/O, Implemented Diagnostics and Resulting Diagnostics Coverage

Internal Diagnostics for Single Point Failure	Implemented Diagnostics	Single Point Fault Diagnostic Coverage (High = 99%, Medium = 90%, and Low = 60%) Per ISO 26262-5;2018, Table D.1
(H) IO_PORTS_INPUT_COMPARISON (H) IO_PORTS_OUTPUT_MONITOR	IO_PORTS_OUTPUT_MONITOR	99%
(H) IO_PORTS_OUTPUT_MONITOR	IO_PORTS_OUTPUT_MONITOR	99%
(H) IO_PORTS_OUTPUT_MONITOR	IO_PORTS_OUTPUT_MONITOR	99%
(H) IO_PORTS_OUTPUT_MONITOR	IO_PORTS_OUTPUT_MONITOR	99%
(H) IO_PORTS_INPUT_COMPARISON	IO_PORTS_INPUT_COMPARISON	99%
(H) IO_PORTS_OUTPUT_MONITOR	IO_PORTS_OUTPUT_MONITOR	99%
(H) IO_PORTS_OUTPUT_MONITOR	IO_PORTS_OUTPUT_MONITOR	99%
(H) IO_REGISTER_RESET_STATE_CHECK & IO_REGISTER_BLOCK_REPLICATION & IO_REGISTER_WRITE_READ_TEST	IO_REGISTER_RESET_STATE_CHECK & IO_REGISTER_BLOCK_REPLICATION & IO_REGISTER_WRITE_READ_TEST	99%
(M) EVENT_ROUTING_CHECK	NONE	0%
(M) IO_PORTS_CHANGE_NOTIFICATION_TEST	NONE	0%
(M) IO_PORTS_CHANGE_NOTIFICATION_TEST	NONE	0%
(H) IO_REGISTER_RESET_STATE_CHECK & IO_REGISTER_BLOCK_REPLICATION & IO_REGISTER_WRITE_READ_TEST	IO_REGISTER_RESET_STATE_CHECK & IO_REGISTER_BLOCK_REPLICATION & IO_REGISTER_WRITE_READ_TEST	99%

The exercise is repeated for all functions of the MCU that are deemed to affect the safety features, so for the CPU, memories, clocks, and potentially timers and communications modules. All can be found in the FMEDA.

As seen from the FMEDA sections, the FMEDA is a very compact format with limited information. Keep in mind that an FMEDA report is a tool to assess the required diagnostics and calculate the unsafe FIT rate and Diagnostics Coverage. The details to understand the failures and the diagnostics mechanisms are described in the Safety Manual, which is, like the FMEDA, available on request.

3. Select a Functional Safety Ready Microcontroller

Learning how to design safety-critical system can seem like a tough challenge, but working with the right suppliers and involving the right expertise early in the design process will help you reach your goal. Microchip is committed to helping designers of safety-critical systems to succeed on their mission to make their products safe to use and to comply with the various safety standards, and for that reason, Microchip offers FMEDAs and Safety Manuals for all PIC, AVR, and SAM MCUs and dsPIC33 DSCs. Combining these valuable documents with Microchip's MPLAB® X development tools for safety applications and the help from our local experts and partners will save you time and money - and will help you reach safety compliance faster.

Look for Microchip's Functional Safety Ready logo to know that you can get everything you need for your safety-critical design:

4. Revision History

Doc. Rev.	Date	Comments
A	09/2020	Initial document release

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Product Change Notification Service

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods being used in attempts to breach the code protection features of the Microchip devices. We believe that these methods require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Attempts to breach these code protection features, most likely, cannot be accomplished without violating Microchip's intellectual property rights.
- Microchip is willing to work with any customer who is concerned about the integrity of its code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable." Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Trademarks

ISBN: 978-1-5224-6673-4

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: www.microchip.com/support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Australia - Sydney** Tel: 61-2-9868-6733 **China - Beijing** Tel: 86-10-8569-7000 **China - Chengdu** Tel: 86-28-8665-5511 **China - Chongqing** Tel: 86-23-8980-9588 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 **China - Hong Kong SAR** Tel: 852-2943-5100 **China - Nanjing** Tel: 86-25-8473-2460 **China - Qingdao** Tel: 86-532-8502-7355 **China - Shanghai** Tel: 86-21-3326-8000 **China - Shenyang** Tel: 86-24-2334-2829 **China - Shenzhen** Tel: 86-755-8864-2200 **China - Suzhou** Tel: 86-186-6233-1526 **China - Wuhan** Tel: 86-27-5980-5300 **China - Xian** Tel: 86-29-8833-7252 **China - Xiamen** Tel: 86-592-2388138 **China - Zhuhai** Tel: 86-756-3210040	**India - Bangalore** Tel: 91-80-3090-4444 **India - New Delhi** Tel: 91-11-4160-8631 **India - Pune** Tel: 91-20-4121-0141 **Japan - Osaka** Tel: 81-6-6152-7160 **Japan - Tokyo** Tel: 81-3-6880- 3770 **Korea - Daegu** Tel: 82-53-744-4301 **Korea - Seoul** Tel: 82-2-554-7200 **Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906 **Malaysia - Penang** Tel: 60-4-227-8870 **Philippines - Manila** Tel: 63-2-634-9065 **Singapore** Tel: 65-6334-8870 **Taiwan - Hsin Chu** Tel: 886-3-577-8366 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 **Thailand - Bangkok** Tel: 66-2-694-1351 **Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4485-5910 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-72400 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-72884388 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820