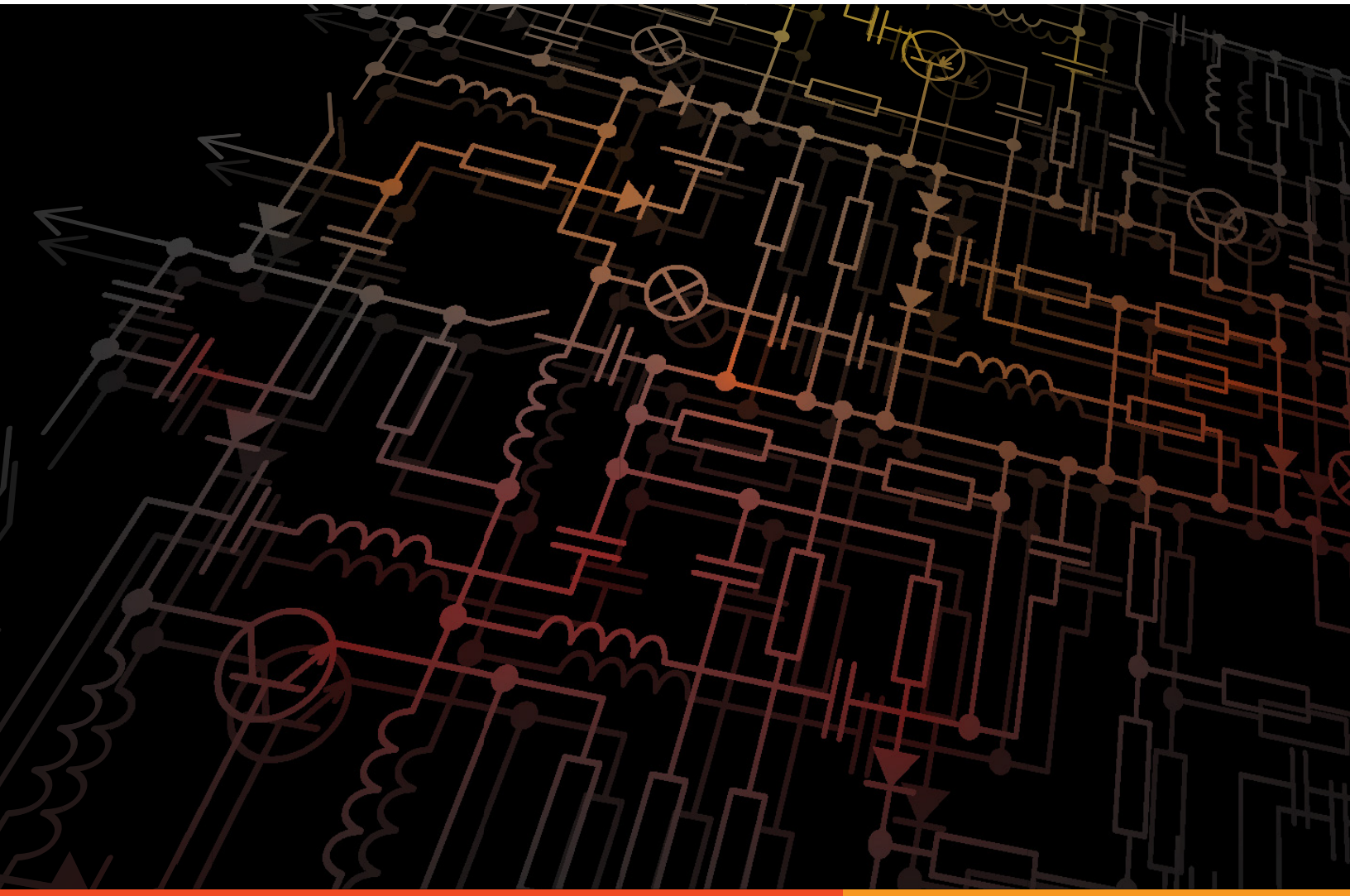
FMEDAx



Design next Generation Safety into Next Generation Automation Products

The goal of all safety critical devices is that they perform their intended function correctly (reliability) and that the system fails in a predictable and safe manner (safety). Failure Modes, Effects, and Diagnostics Analysis **(FMEDA)** is the most commonly used quantitative analysis technique for predicting safety and reliability of a product. It calculates the reliability performance metrics that are needed for compliance with the **IEC 61508** family of performance-based standards (IEC 61511, IEC 62061, ISO 13849, ISO 26262, etc.) and which are required by product users to perform safety calculations (like **PFDavg**).

Example Reliability Performance Metrics:

- Safe Detected (SD) Failure Rate
- Safe Undetected (SU) Failure Rate
- Dangerous Detected (DD) Failure Rate
- Dangerous Undetected (DU) Failure Rate
- Proof test effectiveness / coverage
- Annunciation Failure Rate
- Useful life

FMEDAx

From First Generation to Next Generation

The FMEDA technique, which was developed in the late 1980's by engineers now working for exida, is a staple of functional safety engineering because of its effectiveness predicting product safety and reliability metrics. It was created from a need to be able to account for the impact of diagnostics on safety and reliability performance.

The FMEDAx tool from exida embeds 30+ years of real-world experience and expertise from the team that pioneered the technique, to provide the world's most accurate tool for safety & reliability predictions. It can support detailed hardware design of automation systems in a variety of applications (process industry, industrial equipment / machinery, robotics, medical devices, railway, mining, automotive, etc.).

FMEDAx can take you from schematic to identification of design weaknesses and accurate / defendable failure rate predictions quicker than conventional FMEDA tools; this reduces cost and enables new products to be brought to market faster.

Why Accurate Failure Rate Predictions Are Important

Being able to accurately predict product and system failure rates impacts development cost, design complexity, time to market, and the Cost of Poor Quality (COPQ). Having accurate FMEDA results is critical to be able to make effective decisions during the product design & development lifecycle in areas such as:

- Assessing whether product marketing reliability targets can be achieved
- Understanding the susceptibility of a design to random failures
- Evaluating design alternatives (trading off cost, reliability, weight, size, etc.)
- Establishing objectives for reliability tests (e.g., fault injection testing)
- Planning logistic and life-cycle support strategies
- Providing data for system reliability and availability analysis by customers
- Detecting and controlling failures to ensure predictable failure modes that are safe

The FMEDA Process

The FMEDA process consists of the following steps.

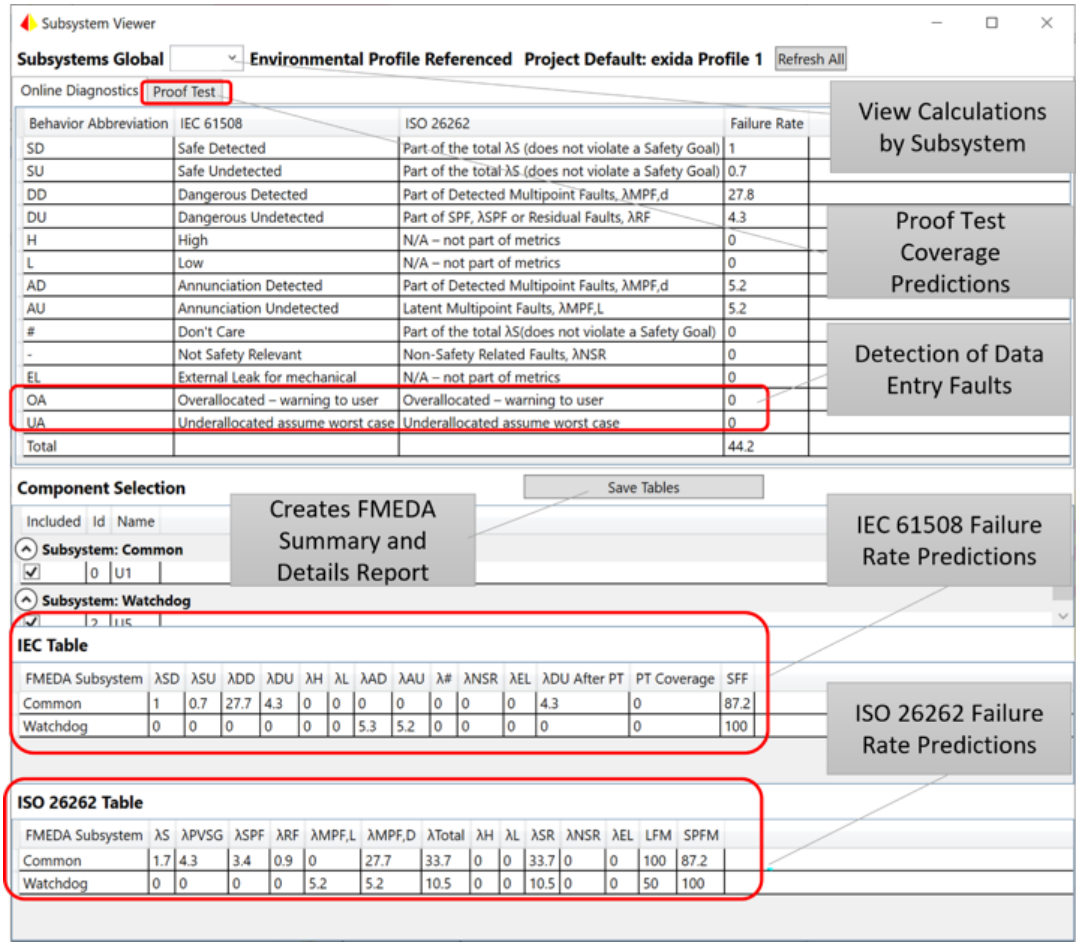
1. All components from a subsystem (on a schematic) are identified with stress levels for the given application (based on design parameters and operating environment).
2. Component failure rates and failure mode distributions are provided from a database / handbook, and diagnostic / proof test methods are chosen if applicable.
3. The failure rates, failure modes, diagnostic coverage, useful life, and proof test coverage for the entire subsystem is calculated (predicted).
4. Subsystem failure rates are combined at the product level and then compared to target requirements.
5. If requirements are not met, the activity is repeated (iterative).

Failure Modes Flow Down from FMEA to FMEDA

A mature design process goes from FMEA (Failure Modes and Effects Analysis) to FMEDA and back. FMEDA analysis uses failure mode and mitigation information from an FMEA about the existence and effectiveness of diagnostics. The FMEDAx tool allows FMEA information to flow down automatically from ARCHx, an integrated FMEA tool, to minimize engineering time. The tool also allows entire subsystems or smaller to be cloned to speed up completion of the product level FMEDA.

Unified Approach to Failure Rate Predictions for Different Markets

Quantitative failure rate predictions are required by the IEC 61508 and ISO 26262 performance-based standards. Different failure rate metrics are prescribed by each standard. FMEDAx takes a unified approach to failure predictions by calculating and presenting both IEC 61508 and ISO26262 metrics, using a single FMEDA. To assist in design evaluation and decision-making, FMEDAx calculates additional metrics beyond the minimum required set (e.g., AD, AU, NSR, H, L, EL). Failure rate predictions can be viewed for the entire assembly or by individual subsystem and can be compared to values that have been allocated as part of high-level design (failure rate budget).



Behavior Abbreviation	IEC 61508	ISO 26262	Failure Rate
SD	Safe Detected	Part of the total λS (does not violate a Safety Goal)	1
SU	Safe Undetected	Part of the total λS (does not violate a Safety Goal)	0.7
DD	Dangerous Detected	Part of Detected Multipoint Faults, λMPF,d	27.8
DU	Dangerous Undetected	Part of SPF, λSPF or Residual Faults, λRF	4.3
H	High	N/A – not part of metrics	0
L	Low	N/A – not part of metrics	0
AD	Annunciation Detected	Part of Detected Multipoint Faults, λMPF,d	5.2
AU	Annunciation Undetected	Latent Multipoint Faults, λMPF,L	5.2
#	Don't Care	Part of the total λS(does not violate a Safety Goal)	0
-	Not Safety Relevant	Non-Safety Related Faults, λNSR	0
EL	External Leak for mechanical	N/A – not part of metrics	0
OA	Overallocated – warning to user	Overallocated – warning to user	0
UA	Underallocated assume worst case	Underallocated assume worst case	0
Total			44.2

FMEDA Subsystem	λSD	λSU	λDD	λDU	λH	λL	λAD	λAU	λ#	λNSR	λEL	λDU After PT	PT Coverage	SFF
Common	1	0.7	27.7	4.3	0	0	0	0	0	0	0	4.3	0	87.2
Watchdog	0	0	0	0	0	0	5.3	5.2	0	0	0	0	0	100

FMEDA Subsystem	λS	λPVSG	λSPF	λRF	λMPF,L	λMPF,D	λTotal	λH	λL	λSR	λNSR	λEL	LFM	SPFM
Common	1.7	4.3	3.4	0.9	0	27.7	33.7	0	0	33.7	0	0	100	87.2
Watchdog	0	0	0	0	5.2	5.2	10.5	0	0	10.5	0	0	50	100

FMEDAx Failure Rate Predictions (Unified View presenting IEC 61508 and ISO 26262 Results)

(Reliability) Data is King

Experienced engineers know that that FMEDA results are only as good as the failure data that is used to create them. If the database does not contain all necessary failure rate information (based on operating environment, failure modes / distributions, or useful life), then assumptions will need to be made. Unfortunately, bad assumptions typically lead to bad results. Without useful life information a designer could select a component with a 5-year useful life for a product with a 20-year mission time. This could lead to premature failures and product "quality" issues. Missed failure modes can lead to product recalls or safety issues (including loss of life). Incorrectly predicting which components are most likely to fail (design weakness) could lead to unnecessary design changes, increased complexity, and cost overruns.

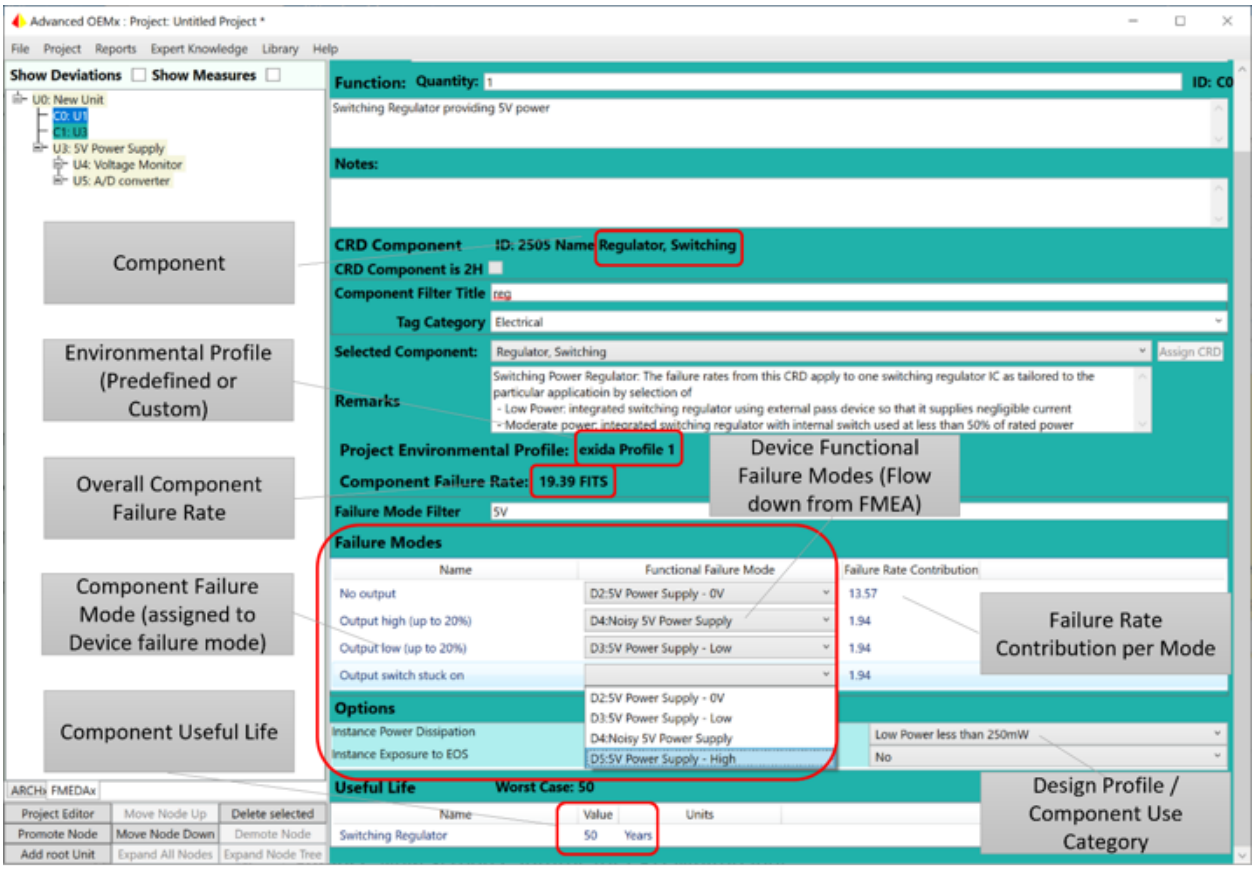
CRD

COMPONENT RELIABILITY DATABASE

Much of the benefit of using FMEDAx comes from its integration with the exida Component Reliability Database (CRD)™. The exida CRD is the most comprehensive and complete reliability database for performing FMEDAs, fulfilling the following criteria:

1. Contains data for all components used in the product design
2. Documents component failure modes and distributions (not just 50%/50% assumptions)
3. Documents component useful life
4. Provides failure rates for various design profiles and operating environments
5. Is updated on a regular basis to keep up with changes in technology (impact of Moore's Law)
6. Supports IEC 61508 Route 2H architectural constraints
7. Includes the impact of analog drift in components
8. Includes the impact of integrated circuit soft error rates (SER)
9. Is calibrated against field failure data for accuracy

Data from the exida CRD is loaded automatically into FMEDAx minimizing the chance of human error and reducing the time it takes to perform the calculations.



Typical View of Component Reliability Data from the exida CRD

Comprehensive Reliability Database that Stays Up-to-Date with New Technology

We know that if the database does not contain all the components used in your design, then engineers will need to search the internet for the missing information, ending up with data of questionable pedigree and burning design hours. The need for this is alleviated with a comprehensive reliability database such as the exida CRD, which gets updated on a regular basis (typically every 6 months) to address new products and technology.

Incorporating regular updates is particularly important for semiconductors. As stated in ISO26262:2019 “As semiconductor technology is rapidly evolving, It is difficult for published recognized industry sources for failure rates to keep pace with the state of the art, particularly for deep submicron process technologies.”

Accounting for Operating Environment

A common issue with Reliability handbooks is that they don't provide failure rates for different operating environments, which leads to inaccurate results. The exida CRD provides pre-defined environmental profiles (temperature, humidity, vibration, mechanical shock, etc); six for process industry applications and two for automotive. Custom profiles can also be defined so that the provided component failure rates are determined for the specific design environment. Different environments can be applied to each subsystem. For an automotive application there might be a different profile for roof mounted sensors, bumper level sensors, backend processors in the trunk, engine compartment, and passenger compartment.

Calibration vs. Field Failure Data Ensures Accurate FMEDA Predictions

Field failure rate data is used to "calibrate" the CRD and FMEDA results using a combination of root cause analysis and closed loop comparison of FMEDA predictions to estimated failure rates from quality field failure data. The comparisons between FMEDA predictions and field failure estimations should show the same results. When a discrepancy exists, exida determines the root cause of the discrepancy and takes corrective action. This ensures that the failure rate predictions provided by FMEDAx are as accurate as possible.

exida has analyzed over 400 billion operating hours of field failure data to calibrate its component reliability data and FMEDAx tool in order to deliver the most accurate and realistic predictions for use in the development of IEC 61508 / ISO 26262 – compliant products.

ARCHx

Part of an Integrated Product Development Process with ARCHx™

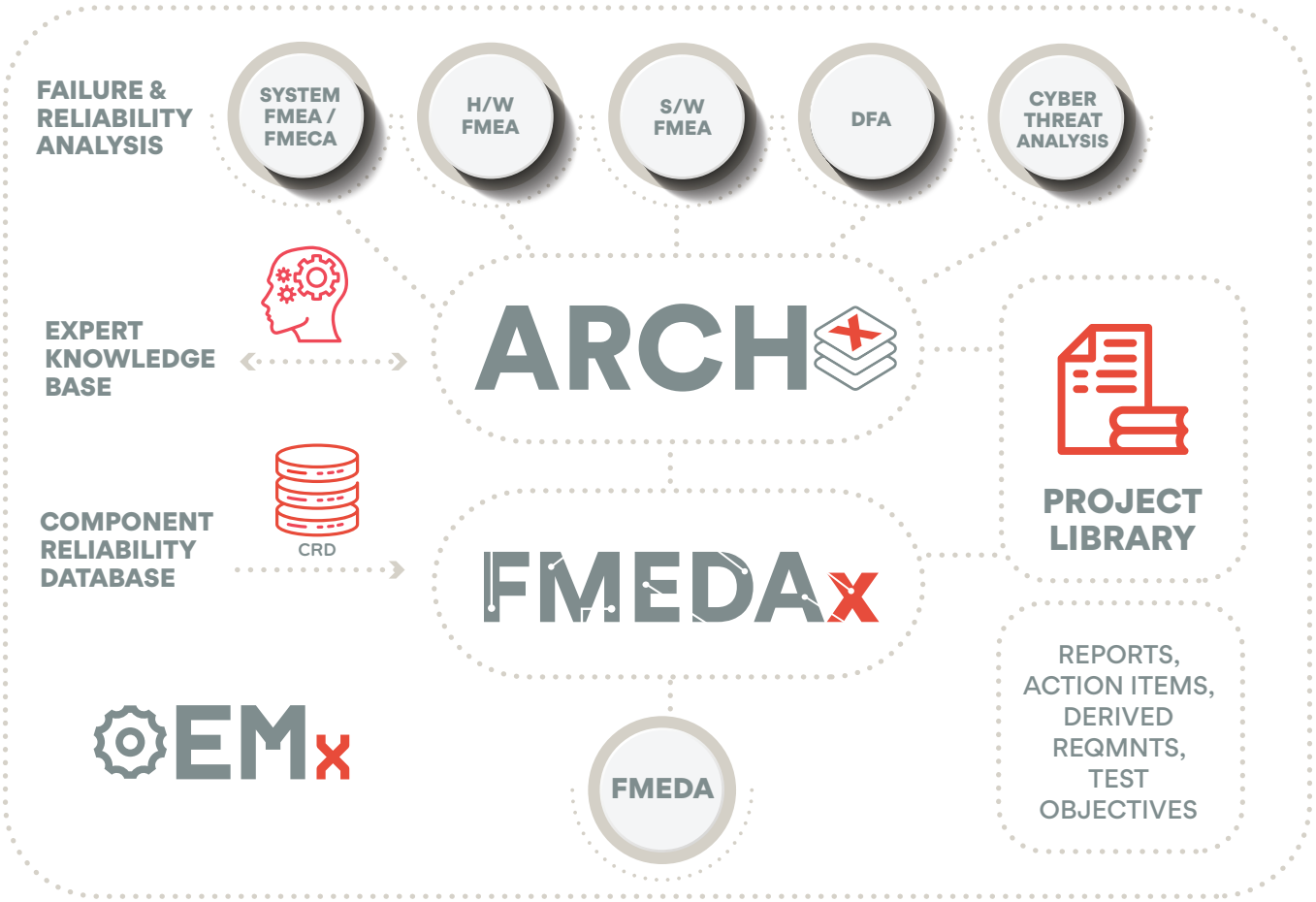
To deliver new products to market in the shortest period of time, the Hardware Detailed Design stage (where FMEDAs are used) should be tightly integrated into the rest of the product development process. A thorough FMEDA can identify design changes / clarifications, additional failure modes, new mitigation measures, or other derived safety requirements. When used with ARCHx™, the information surfaced by FMEDAx can be propagated seamlessly to other design stages - updating FMEA results, Integration / Validation testing goals, system and subsystem requirements, project action item lists, etc.

Verifying Predicted Design Performance matches Real-life Results

Typically, fault injection testing is performed on a prototype or pre-production assembly, after the FMEDA is completed, to verify the design and to discover unforeseen problems. It involves simulating specific component failures as highlighted by the FMEDA. The detailed results provided by FMEDAx arm you with the information needed to confirm your design and its expected behavior; verifying that the predicted “effects” occurred, that the diagnostic coverage was effective at detecting failures, and that the mitigation measures worked as designed.

Support for Functional Safety Certification

Customers and regulatory bodies are demanding the use of products that have been certified to functional safety standards such as IEC 61508 and ISO 26262. The failure rate predictions generated by FMEDAx provide clear requirements traceability and documentation to support the functional safety certification process.



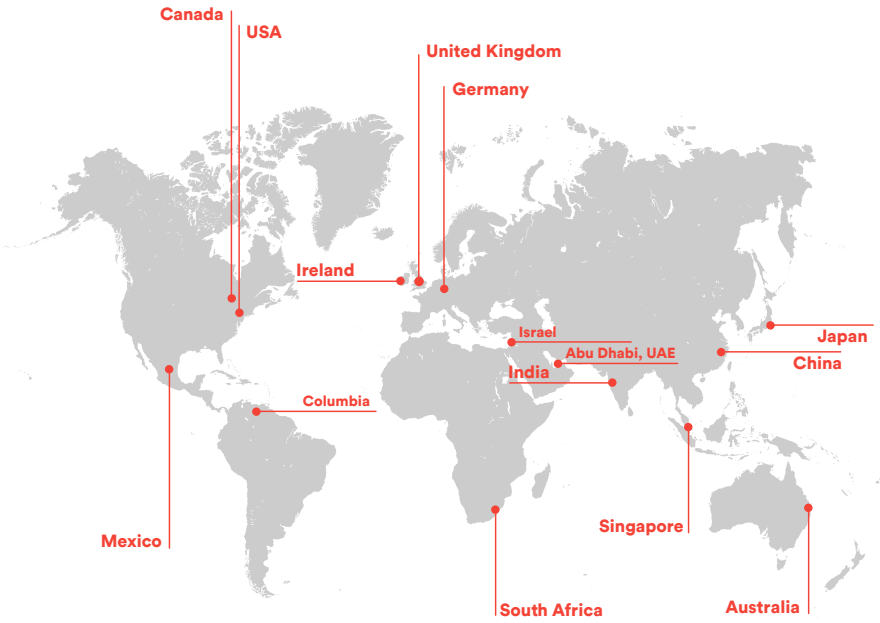
The OEMx Product Line

OEMx provides a common set of tools to support hardware, software, and cybersecurity reliability and safety analysis for automation systems and critical safety devices.

FMEDAx™, part of the OEMx™ product line from exida, can be used to analyze the impact of component failure modes and perform quantitative analysis of products and subsystems to predict safety and reliability performance metrics as required by the IEC 61508 family of standards.

ARCHx™, part of the OEMx™ product line from exida, can be used to perform system / subsystem / product architecture analysis to document the design, evaluate the impact of potential design faults in hardware and/or software (FMEA), identify potential cybersecurity vulnerabilities, and document methods to avoid design faults.

www.exida.com/oemx



exida has offices all over the world.

North America

USA

80 North Main Street
Sellersville, PA 18960
United States

Phone:+1-215-453-1720

Mexico

Amores 1029 – 201
Col. Del Valle Centro
CDMX, México
CP 03100

Phone:+ 52-55-7572-4870,
+52-55-7572-4871

Canada

452 Aqua Drive
Mississauga, Ontario L5G 2B6
Canada

Phone:+1-215-453-1720

Europe

Germany

Birkensteinstr. 53
83730 Fischbachau
Germany

Phone:+49-89-49000547

United Kingdom

Lake View House
Tournament Fields
Warwick
CV34 6RG
UK

Phone: +44 (0) 19-266-76125

Ireland

Gateway Hub, Suite 13
Shannon Airport House
Shannon Free Zone
Co. Clare Ireland V14 E370

Phone:+353 61 513 009

Asia

Singapore

51 Goldhill Plaza
#21-08/09
Singapore 308900

Phone:+65 6222-5160

India

Workwise Solutions, LEVEL 14,
Lotus Business Park, Off New Link Road,
Andheri West, Mumbai - 400053
India

Phone: +91-99-30-250-104

Japan

Shin-machi 1-31-10
Ome, Tokyo, 198-0024
Japan

Phone: +81 50-5539-9507

Africa

South Africa

2 Brendon Lane,
Westville,
3629,
Durban,
Kwa-Zulu Natal,
South Africa

Phone:+27 31 2671564

www.exida.com

© 2021 exida