ARCH

Next Generation Architecture Analysis Tool for Next Generation Automation Products

Optimizing the design engineering process for new automation systems and safety critical devices involves balancing goals that normally conflict – time to market, development cost, safety & reliability.

OEMx , from exida, changes this by seamlessly taking you from safety-critical product requirements to high-level architecture, to detailed hardware and software design (FMEA and FMEDA), to accurate and defendable safety & reliability predictions more quickly; reducing development cost, time to market, and supporting compliance with the IEC 61508 family of safety standards. ARCHx™ enhances the hierarchical architecture design process. It supports design of automation systems in a variety of applications (process industry, industrial equipment / machinery, robotics, medical devices, railway, mining, automotive, etc.).

ARCHx

From First Generation to Next Generation

exida is a knowledge company specializing in high reliability and high safety automation systems. To advance the state of the art, we regularly perform research on high reliability and safety systems, sharing the results with the world via papers, journal articles, webinars, training courses, tools, and books (we have written more books on functional safety than any other company). The engineers at exida have pioneered and developed many safety and reliability analysis techniques, including the Failure Modes, Effects and Diagnostics Analysis (FMEDA) in the late 1980's. exida is an internationally-accredited body for functional safety and cybersecurity certification.

From this fertile environment comes the ARCHx tool. ARCHx includes an expert knowledge base embedding 30+ years of accumulated experience in the design and analysis of hardware, software, FPGAs, semiconductors and automation cybersecurity. Use of the expert knowledge base with functional failure modes and proven solutions on a project reduces engineering time, increases design rigor, improves the accuracy of the results, and sets up an organization for a successful certification pursuit.

ARCHx also allows your experts to add to the knowledge base structure with company-specific design expertise. This enhances the ability to make application-specific design assistance available to new designers when they need it, driving efficiency, consistency and improving traceability.

ARCHx Expert Knowledge Bases

- Electronic Hardware incl. Microcontrollers
- Software
- FPGA / ASICs
- Mechanical Hardware
- Dependent Failure Analysis
- Cybersecurity

Failure & Reliability Analysis Tools at Your Fingertips

The goal of all critical safety devices is that they perform their intended function correctly (reliability) and that the system fails in a predictable and safe manner (safety). ARCHx provides multiple Failure & Reliability Analysis tools so that you can select the right tool for the task:

» System FMEA / FMECA
» Hardware FMEA
» Software FMEA
» Dependent Failure Analysis (DFA)
» Cyber Threat Analysis / TARA
» FMEDA export

Integrated Toolset for Safety & Reliability analysis of Hardware, Software, and Cybersecurity

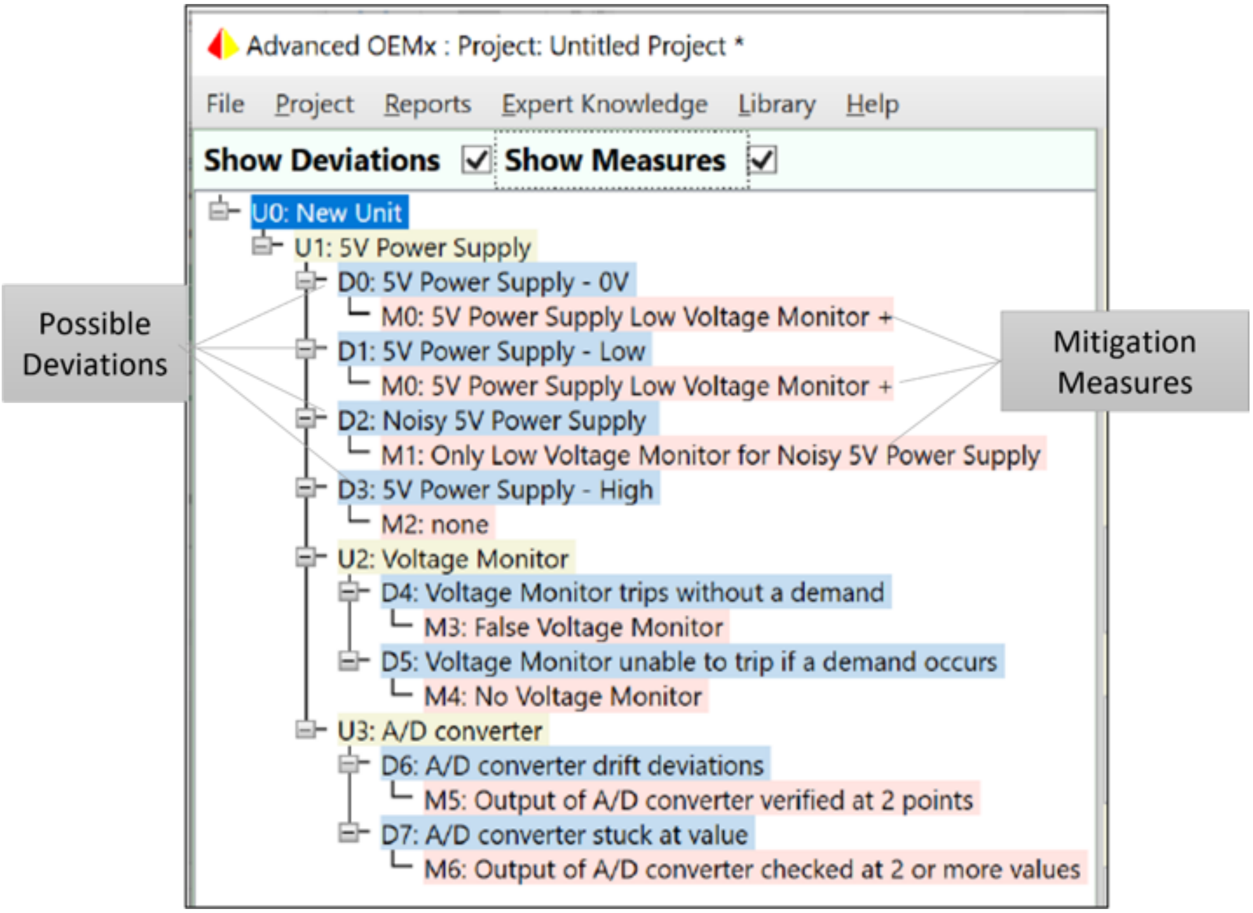
The integrated Failure Modes and Effects Analysis (FMEA) tool in ARCHx helps you document each block in your system architecture, decomposing into subsystems, and lower-level subsystems as necessary so that functional requirements can be allocated to the appropriate part of the design. This allows you to model and analyze the entire architecture from the system level down to the hardware chip level, using the same tool for analysis of hardware, software, and cybersecurity threats.

The FMEA tool helps you to determine and document the following:

- subsystem criticality
- interactions between subsystems
- possible deviations from expected operation due to hardware or software faults and cybersecurity intrusions
- the impact of identified deviations (functional failure modes)
- potential mitigation measures to address the deviation (fault avoidance, fault control, interference free, fault tolerance)
- which portions of the design are safety critical, safety related, and interference free.

Guiding You to Make the Best Decisions with Expert Knowledge

As part of the FMEA process when you define a subsystem or unit (such as a 5V power supply), the expert knowledge base in ARCHx will suggest relevant functional failure modes to be considered (shown highlighted in Blue in the figure below), including criticality level. For each failure mode, ARCHx will then suggest relevant mitigation measures (highlighted in peach in the figure below), including level of effectiveness (Low, Medium, High). These recommended mitigation measures can be reviewed, accepted, deleted, or modified by the designer. or by individual subsystem and can be compared to values that have been allocated as part of high-level design.



Show Deviations ☑ Show Measures ☑

- U0: New Unit
  - U1: 5V Power Supply
    - D0: 5V Power Supply - 0V
      - M0: 5V Power Supply Low Voltage Monitor +
    - D1: 5V Power Supply - Low
      - M0: 5V Power Supply Low Voltage Monitor +
    - D2: Noisy 5V Power Supply
      - M1: Only Low Voltage Monitor for Noisy 5V Power Supply
    - D3: 5V Power Supply - High
      - M2: none
    - U2: Voltage Monitor
      - D4: Voltage Monitor trips without a demand
        - M3: False Voltage Monitor
      - D5: Voltage Monitor unable to trip if a demand occurs
        - M4: No Voltage Monitor
    - U3: A/D converter
      - D6: A/D converter drift deviations
        - M5: Output of A/D converter verified at 2 points
      - D7: A/D converter stuck at value
        - M6: Output of A/D converter checked at 2 or more values

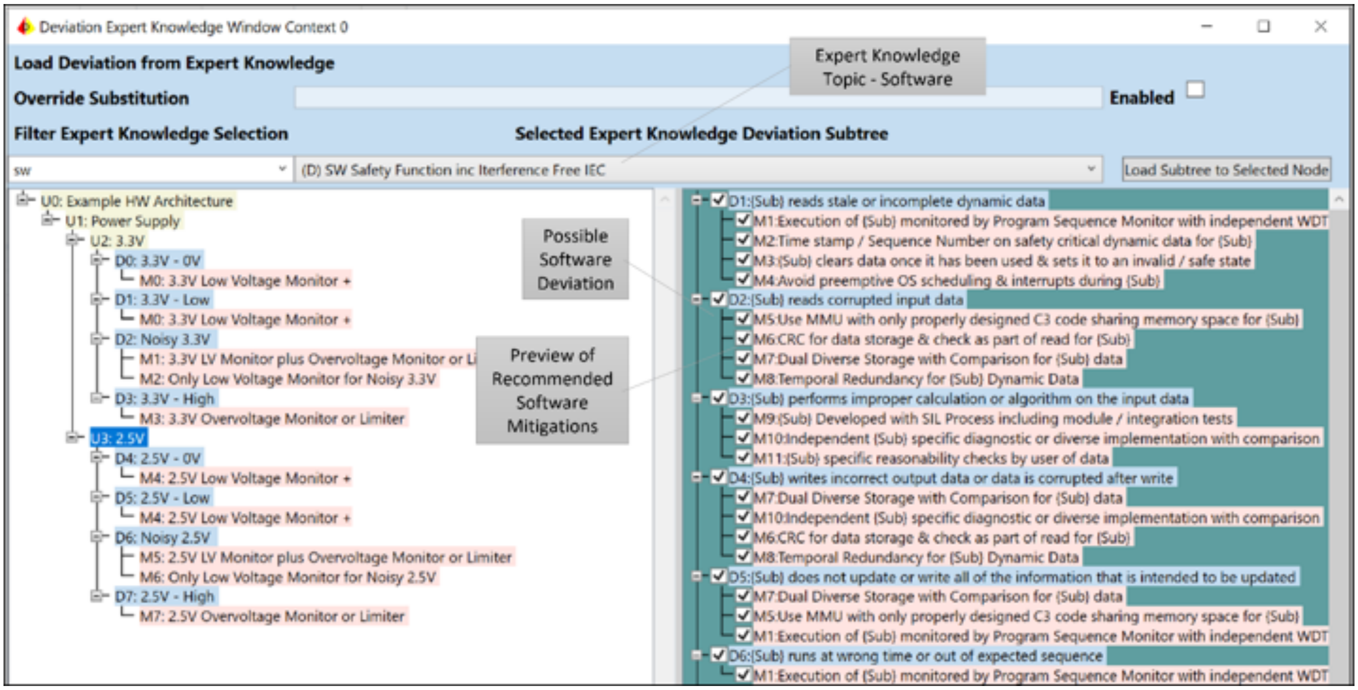
Architecture Analysis Showing Deviations and Mitigation Measures

The suggested failure modes and recommended mitigation measures can be previewed before adding to the design. This allows the user to consider design alternatives as part of the work process (What if analysis) and to rank / evaluate potential mitigation measures to choose what will be most effective. Diagnostic mitigations provide advice on the typical level of effectiveness that can be claimed based on interpretation of the safety standards. Once mitigation measures have been selected, derived functional requirements can be generated automatically and integration / validation test plan objectives created automatically to verify mitigation effectiveness.

For cyber analysis potential mitigations are typically more closely associated with the type of threat or method of attack than the deviation or failure mode.

Rigorous Analysis of Software Design

ARCHx supports analysis of software via FMEA, an improvement on more traditional software HAZOPs. Software HAZOPs, which make use of guidewords to help teams discover potential functional failure modes, are reliant on the expertise of the team to be successful. To overcome this limitation, S/W FMEA provides an extensive set of known software failure modes discovered by exida experts during their long history of performing S/W HAZOPs on similar software modules. Guidewords can still be used within the S/W FMEA for novel topics that have not been well-characterized.


Expert Knowledge Topic - Software
Possible Software Deviation
Preview of Recommended Software Mitigations

Deviation Expert Knowledge Window Context 0

Load Deviation from Expert Knowledge

Override Substitution **Enabled** □

Filter Expert Knowledge Selection: sw

Selected Expert Knowledge Deviation Subtree: (D) SW Safety Function inc Iterference Free IEC

Load Subtree to Selected Node

- U0: Example HW Architecture
  - U1: Power Supply
    - U2: 3.3V
      - D0: 3.3V - 0V
        - M0: 3.3V Low Voltage Monitor +
      - D1: 3.3V - Low
        - M0: 3.3V Low Voltage Monitor +
      - D2: Noisy 3.3V
        - M1: 3.3V LV Monitor plus Overvoltage Monitor or Li
        - M2: Only Low Voltage Monitor for Noisy 3.3V
      - D3: 3.3V - High
        - M3: 3.3V Overvoltage Monitor or Limiter
    - U3: 2.5V
      - D4: 2.5V - 0V
        - M4: 2.5V Low Voltage Monitor +
      - D5: 2.5V - Low
        - M4: 2.5V Low Voltage Monitor +
      - D6: Noisy 2.5V
        - M5: 2.5V LV Monitor plus Overvoltage Monitor or Limiter
        - M6: Only Low Voltage Monitor for Noisy 2.5V
      - D7: 2.5V - High
        - M7: 2.5V Overvoltage Monitor or Limiter

- ☑ D1:(Sub) reads stale or incomplete dynamic data
  - ☑ M1:Execution of (Sub) monitored by Program Sequence Monitor with independent WDT
  - ☑ M2:Time stamp / Sequence Number on safety critical dynamic data for (Sub)
  - ☑ M3:(Sub) clears data once it has been used & sets it to an invalid / safe state
  - ☑ M4:Avoid preemptive OS scheduling & interrupts during (Sub)
- ☑ D2:(Sub) reads corrupted input data
  - ☑ M5:Use MMU with only properly designed C3 code sharing memory space for (Sub)
  - ☑ M6:CRC for data storage & check as part of read for (Sub)
  - ☑ M7:Dual Diverse Storage with Comparison for (Sub) data
  - ☑ M8:Temporal Redundancy for (Sub) Dynamic Data
- ☑ D3:(Sub) performs improper calculation or algorithm on the input data
  - ☑ M9:(Sub) Developed with SIL Process including module / integration tests
  - ☑ M10:Independent (Sub) specific diagnostic or diverse implementation with comparison
  - ☑ M11:(Sub) specific reasonability checks by user of data
- ☑ D4:(Sub) writes incorrect output data or data is corrupted after write
  - ☑ M7:Dual Diverse Storage with Comparison for (Sub) data
  - ☑ M10:Independent (Sub) specific diagnostic or diverse implementation with comparison
  - ☑ M6:CRC for data storage & check as part of read for (Sub)
  - ☑ M8:Temporal Redundancy for (Sub) Dynamic Data
- ☑ D5:(Sub) does not update or write all of the information that is intended to be updated
  - ☑ M7:Dual Diverse Storage with Comparison for (Sub) data
  - ☑ M5:Use MMU with only properly designed C3 code sharing memory space for (Sub)
  - ☑ M1:Execution of (Sub) monitored by Program Sequence Monitor with independent WDT
- ☑ D6:(Sub) runs at wrong time or out of expected sequence
  - ☑ M1:Execution of (Sub) monitored by Program Sequence Monitor with independent WDT

Deviation Expert Knowledge Preview of Software Expert Knowledge

Adding Your Company Design Standards to the Expert Knowledge Base

The flexibility of ARCHx makes it suitable for use across a wide range of applications and industries with differing requirements. User-specific data fields can be added (Groups) so that you can define specific information needed for your application, or workflow, and following your terminology.

The expert knowledge base can be supplemented with company-specific design information. This allows you to add your own reusable design templates and safety design patterns. For example, you could define your own architectural unit templates with associated deviations and potential mitigation measures based on lessons learned from past projects, or to document tribal knowledge. Use of the knowledge base drives design consistency, reduces the probability of design errors, and allows you to leverage your company's intellectual property.

From High Level Architecture to Detailed Design and Back

A mature design process goes from FMEA (Failure Modes and Effects Analysis) to FMEDA and back. ARCHx allows you to start from the beginning, by documenting and allocating high-level safety concepts or known high level requirements. The failure mode and mitigation information defined during the FMEA, along with the diagnostics, flows down automatically from ARCHx to the FMEDA tool within FMEDAx. FMEDAx produces safety & reliability predictions that can be compared to those defined in the high-level product requirements. During the detailed FMEDA it is not unusual to discover additional failure modes. Design changes made based on the FMEDA results are propagated back automatically to the FMEA, keeping the architecture in sync with the design details. This saves time and eliminates potential design discrepancies. No development process proceeds in a straight line, so the ability to deal quickly and easily with design iterations, keeping design information consistent, minimizes cost and time to market.

Optimizing Safety & Reliability

Not all designs need the same level of safety and reliability; often these two factors tradeoff against each other. ARCHx provides feedback on high-level design more quickly so that system designers can address harmful deviations early in the design, giving them an opportunity to evaluate alternatives that may provide safety with less impact on availability. Safety measures added later in the design cycle often improve safety at the expense of availability since there is a more limited set of feasible options.

There are often multiple potential diagnostic techniques that can be employed, each with its own level of effectiveness and fit based on project-specific considerations (such as SIL or ASIL level). The expert knowledge base seeds the design discussion by providing a starter set of information for evaluation and review, helping you get to a better design, quicker with less time and effort.

A Good FMEA Tool Should Do More than Just Find Design Errors

Compared to conventional FMEA and HAZOP tools, ARCHx captures more information in a more structured easy to reuse format that supports a seamless and traceable transition to subsequent stages of the development process. ARCHx packages project information automatically to support detailed design and verification steps:

- creation of required integration / verification test cases
- generation of derived requirements for fault control diagnostics and functional failure mode tables for use in FMEDA
- generating reports to verify that the design meets its requirements and complies with the planned architecture
- capturing and tracking of action items that can not be solved at the time of the analysis.

Automatically Generate Design Documentation

ARCHx organizes and structures the information captured during the design and analysis process so that it can be output via a common set of pre-defined reports, including the following:

- **Action Item Report** –provides documentation of Action Items organized by Type
- **FMEA Summary Report** – provides the key information in a condensed traditional FMEA style format for both hardware and software analysis
- **Safety Manual Content** – provides information that was identified as important to be documented in the Safety Manual
- **Standard Report** – provides all the relevant details captured in the ARCHx architecture analysis including a summary of the action items at the end of the report
- **Test Report** – provides a full list of test objectives defined during the FMEA process including Integration Tests and Validation Tests

Action items surfaced during the design can be documented, categorized by purpose (such as “discuss during design review”, “open design issue”, “missing requirement”, or “include in safety manual”), assigned to a responsible party, and connected to any architectural building block (unit), deviation, or mitigation in the design hierarchy. Action item status can be updated and tracked to completion to support project management.

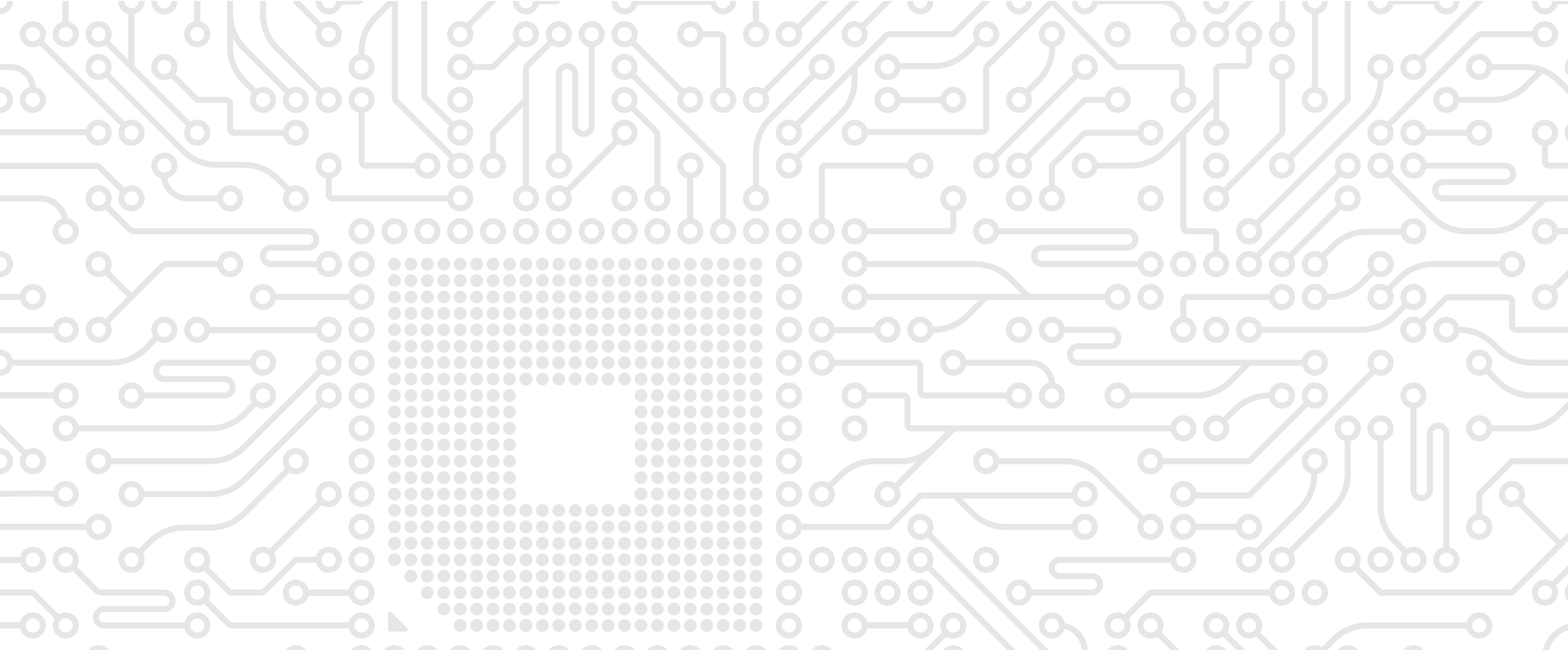
Reduce Engineering Time and Improve Efficiency

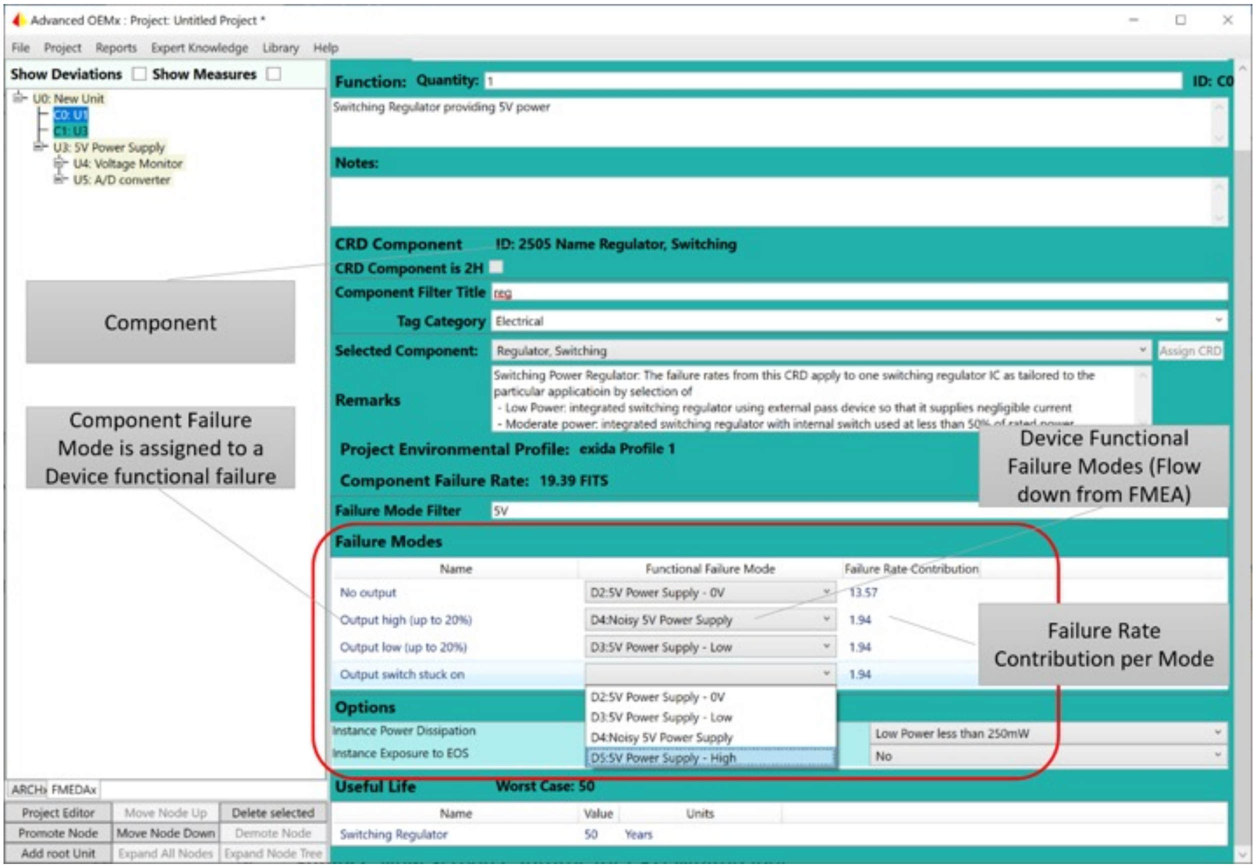
In addition to supporting a streamlined product development process, ARCHx also contains many features that minimize engineering time.

- **An integrated spell-checker** helps capture information completely and correctly the first time. This ensures that your design documentation is free of spelling errors so that you don't have to go back to edit details after the fact to get the final design deliverables in order.
- **Smart renaming** ensures that when descriptions are changed at a higher level, the update propagates automatically to lower levels in the tree structure.
- **Re-indexing** allows units, deviations, and mitigations to be renumbered automatically (in sequence) to clean up a design that has evolved in a piecemeal fashion.
- **Reusable templates** can be created for entire subsystems or smaller units to speed up FMEA completion.

Part of an Integrated Product Development Process with FMEDAx

To deliver new products to market in the shortest period of time, the architecture analysis, high-level design, and analysis of failure modes and effects via FMEA should be tightly integrated into the rest of the product development process. The information documented in ARCHx can be propagated seamlessly to other design stages - Integration / Validation testing, system and subsystem requirements, project action item lists, etc. Failure modes & effects tables are passed down automatically to the FMEDAx™ tool for quantitative prediction of safety and reliability. Design changes resulting from the FMEDA analysis (such as the identification of new failure modes) are propagated seamlessly back to ARCHx, updating architecture layouts, derived requirements, and FMEA analysis.





Function: Quantity: 1 ID: C0

Switching Regulator providing 5V power

Notes:

CRD Component ID: 2505 Name Regulator, Switching

CRD Component is 2H □

Component Filter Title reg

Tag Category Electrical

Selected Component: Regulator, Switching

Remarks Switching Power Regulator: The failure rates from this CRD apply to one switching regulator IC as tailored to the particular applicatioin by selection of
- Low Power: integrated switching regulator using external pass device so that it supplies negligible current
- Moderate power: integrated switching regulator with internal switch used at less than 50% of rated power

Project Environmental Profile: exida Profile 1

Component Failure Rate: 19.39 FITS

Failure Mode Filter 5V

Failure Modes

Name	Functional Failure Mode	Failure Rate Contribution
No output	D2:5V Power Supply - 0V	13.57
Output high (up to 20%)	D4:Noisy 5V Power Supply	1.94
Output low (up to 20%)	D3:5V Power Supply - Low	1.94
Output switch stuck on		1.94

D2:5V Power Supply - 0V
D3:5V Power Supply - Low
D4:Noisy 5V Power Supply
D5:5V Power Supply - High

Options

Instance Power Dissipation	Low Power less than 250mW
Instance Exposure to EOS	No

Useful Life Worst Case: 50

Name	Value	Units
Switching Regulator	50	Years

Flowdown of Failure Mode Information from FMEA to FMEDAx

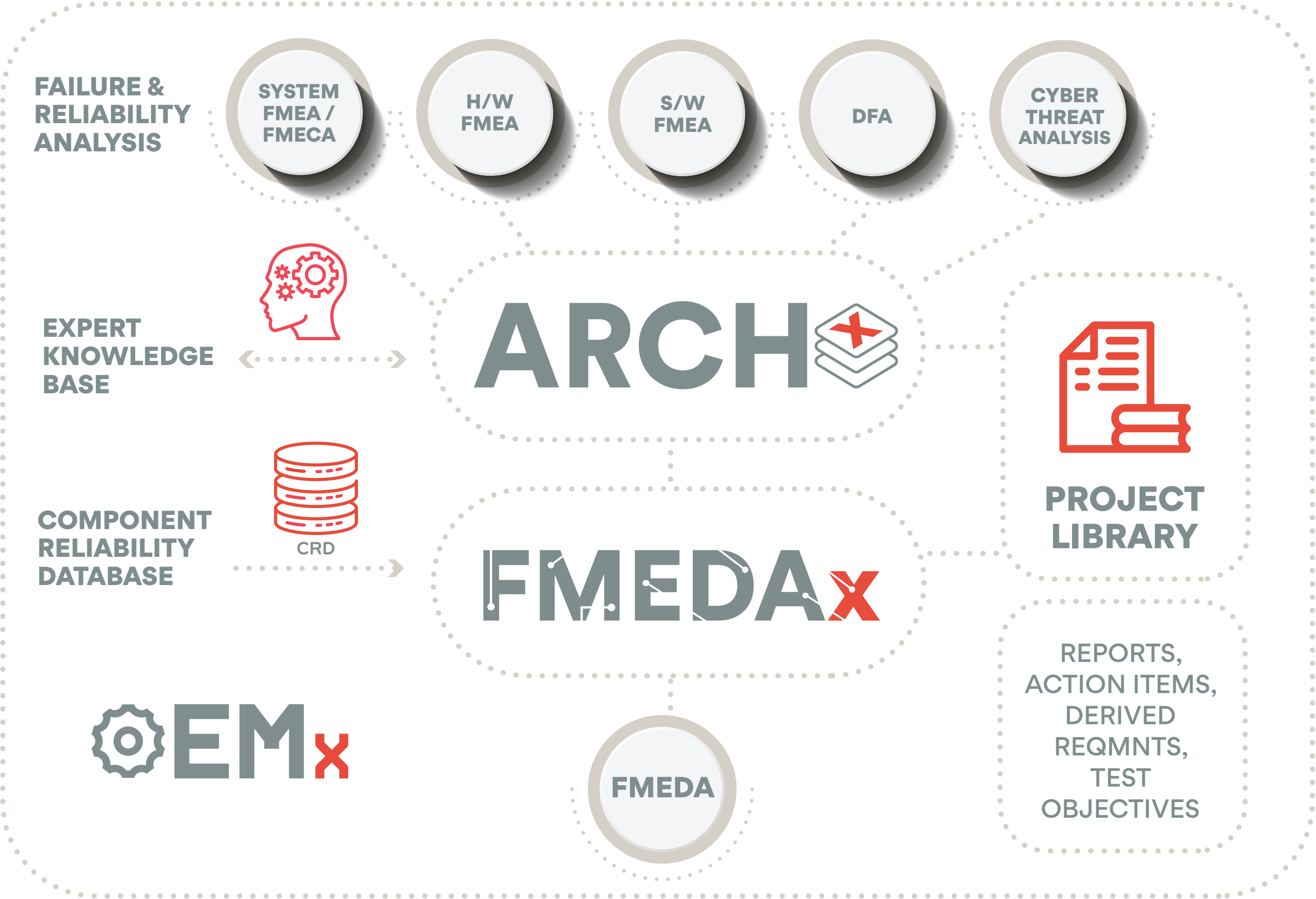
Project Library may contain All Design Artifacts

The project library allows all types of documentation, reference material, design and analysis data, as well as ARCHx objects (such as a 5V power supply), to be stored, archived, and managed from a central location. Library objects (such as a schematic) can be attached to the appropriate nodes in the design hierarchy via drag and drop. Object templates can be updated centrally from the library and changes propagated throughout the design automatically.

The library provides a way to view inter-project linkages and to manage the Units, Deviations, and Mitigation Measures that have been defined within the project. "Where used" (list of objects that reference the mitigation) and "number of instances" information is compiled automatically. This allows one to assess, for example, the number of times a specific fault control mechanism is used in the design. The association between objects can be documented using a Type field, which supports an extensive set of categories (such as "Executes" to indicate particular S/W units that are executed by a H/W element, or "Derived from" for traceability to higher level requirements).

Reduces Preparation Time for Functional Safety Certification

The project library gathers and categorizes relevant design documentation in a common location so that relevant artifacts can be quickly pulled together and supplied to support safety case documentation as part of certification to IEC 61508 or ISO 26262.



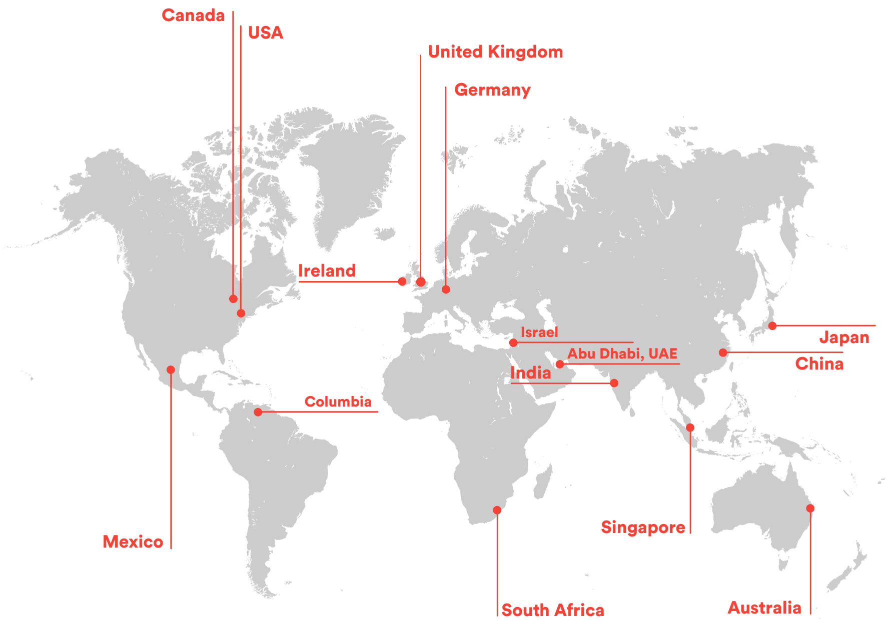
The OEMx Product Line

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