ITEA 3

**ITEA Office**
High Tech Campus 69 - 3
5656 AG Eindhoven
The Netherlands

T + 31 88 003 6136
E info@itea3.org
W www.itea3.org

*ITEA 3 is a EUREKA strategic ICT cluster programme*

# Data sheets

## 10039 SAFE

### Project details

| | |
|---|---|
| Project leader: | Dr. Stefan Voget |
| Email: | Stefan.voget@continental-corporation.com |
| Website: | www.safe-project.eu |

| Name: Architecture Description Language | | |
|---|---|---|
| Input(s): | Main feature(s) | Output(s): |
| ▪ EAST-ADL<br>▪ AUTOSAR | ▪ model based development processes that integrate functional as well as safety development lifecycle compliant to functional safety norm ISO26262<br>▪ exchange format compliant with the existing standards and enriched with the SAFE meta-model formats<br>▪ encloses concepts for safety goals modelling, architecture modelling, and methods for safety analysis, variant management and safety code generation have been developed. | ▪ SAFE meta-model |

| | |
|---|---|
| Unique Selling Proposition(s): | ▪ First worldwide realization of ISO26262 in a standardized ADL<br>▪ Seamless ADL from requirements down to HW/SW design |
| Integration constraint(s): | ▪ Metamodel is documented in Enterprise Architect<br>▪ Associated tool platform is based on Eclipse |
| Intended user(s): | ▪ Tool vendors that provide architecture tooling for the automotive industry<br>▪ Architects of embedded automotive system, SW and HW<br>▪ Researchers that develop ADLs and processes for the automotive industry |
| Provider: | ▪ www.safe-project.eu |
| Condition(s) for reuse: | ▪ Free for use and change<br>▪ Available at website |

| Name: Process Description | | |
|---|---|---|
| Input(s): | Main feature(s) | Output(s): |
| ▪ EASIS<br>▪ EAST-ADL<br>▪ AUTOSAR | ▪ model based development processes that integrate functional as well as safety development lifecycle compliant to functional safety norm ISO26262<br>▪ exchange format compliant with the existing standards and enriched with the SAFE meta-model formats<br>▪ gives hints about how to use the concepts for safety goals modelling, architecture modelling, and methods for safety analysis, variant management and safety code generation have been developed. | ▪ SAFE process model<br>▪ SAFE assessment model<br>▪ SAFE guideline |
| Unique Selling Proposition(s): | ▪ SAFE guidelines provide an interpretation of the ISO26262 norm to the market. It is seamless from requirements down to HW/SW implementation<br>▪ | |
| Integration constraint(s): | ▪ Based on existing development lifecycle processes (existing modelling languages EAST-ADL and AUTOSAR)<br>▪ Associated tool platform is based on Eclipse | |
| Intended user(s): | ▪ Tool vendors that provide architecture tooling for the automotive industry<br>▪ Process responsible of embedded automotive system, SW and HW<br>▪ Researchers that develop ADLs and processes for the automotive industry | |
| Provider: | ▪ www.safe-project.eu | |
| Condition(s) for reuse: | ▪ Free for use and change<br>▪ Available at website | |

| Name: Safety Designer | | |
|---|---|---|
| Input(s): | Main feature(s) | Output(s): |
| ▪ Requirements | ▪ Dysfunctional models compatible with ISO26262 including the definition of safety goals and the derivation of safety requirements.<br>▪ Simulation of systems with fault injection. | ▪ Architecture model<br>▪ Behavior model<br>▪ Safety analysis |

| Name: Safety Designer | |
|---|---|
| | ▪ Capability to model both SW and HW.<br>▪ Major breakthroughs in performance of algorithms for safety analysis have been reached, which is a key issue in large scale industrial models.<br>▪ Automatic calculation of hardware metrics based on Altarica and requirements in Safety Designer connected to Reqtify<br>▪ Safety code generation in Autosar Builder |
| Unique Selling Proposition(s): | ▪ Exploration of complex architectures with high safety constraints<br>▪ Simulation of system behavior with multiple fault injection<br>▪ Model-based safety assessment<br>▪ Automated metrics computations<br>▪ Generation of cut-sets at high order<br>▪ Exact computation of fault trees |
| Integration constraint(s): | ▪ Microsoft Windows 7 (64-bit).<br>▪ SW requirements<br>○ JDK 1.7 (32-bit).<br>○ In case of use of an Oracle database instance (version 9i, 10g or 11g), you must install the Oracle JDBC Drivers package (version 11.1 and above) on the client workstation by using Oracle Universal Installer. Then you can connect to Oracle server 11.2.0, 11.1.0, 10.2.0, 10.1.0, 9.2.0, and 9.0.1. For more information, refer to http://www.oracle.com/technetwork/database/enterprise-edition/jdbc-faq-090281.html<br>○ Access 2010 runtime: If you have installed Microsoft Office 2010 (64-bit edition), then you already have this component. Otherwise, you can download it from: http://www.microsoft.com/en-us/download/details.aspx?id=10910<br>○ C compiler: Before installing Safety Designer, you must install the C compiler from MinGW (Minimalist GNU for Windows). Download the GNU compiler collection (GCC) from: http://sourceforge.net/projects/mingw/<br>▪ HW requirements<br>○ 1 GHz 64-bit (x86-64) processor<br>○ Hard disk space: 20 MB |

| Name: Safety Designer | |
|---|---|
| | ○ RAM: 1 GB<br>○ Screen resolution: 1024 x 768 pixels, 65536 colors. |
| Intended user(s): | ▪ Safety engineers |
| Provider: | ▪ Dassault Systèmes |
| Condition(s) for reuse: | ▪ Commercial license from Dassault Systèmes |

| Name: PREEvision | | |
|---|---|---|
| Input(s): | Main feature(s) | Output(s): |
| ▪ Requirements<br>▪ | ▪ Vector Informatik implemented a model based qualitative safety analysis method FMEA and added malfunction modelling capabilities in their PREEvision tool.<br>▪ model-based safety analysis and evaluation of electric-/electronic vehicle architectures to ensure support for the application of ISO 26262 early in the development process<br>▪ Focusing on reliability in context of random hardware failures, seamless safety evaluations of hardware designs at the level of architectural designs and electronic schematics can be iteratively performed in a model-based approach, supported by analysis methods such as FMEA and FTA.<br>▪ The architecture modeling and optimization tool PREEvision was extended to provide integrated tool support for engineers to efficiently develop safe vehicles. | ▪ Architecture model<br>▪ Safety analysis |
| Unique Selling Proposition(s): | ▪<br>▪ | |
| Integration constraint(s): | ▪ PREEvision Client 6.5.0 or later<br>▪ | |

| Name: PREEvision | |
|---|---|
| Intended user(s): | ▪ |
| Provider: | ▪ Vektor Informatik |
| Condition(s) for reuse: | ▪ Commercial end user license agreement for Vector tools |

| Name: pure::variants | | |
|---|---|---|
| Input(s): | Main feature(s) | Output(s): |
| ▪ Architecture model<br>▪ | ▪ pure::systems realised a seamless integration of pure::variants into the SAFE platform. Therewith, the variant management capabilities of pure::variants are enabled for contexts having safety related assets.<br>▪ Functionality of the seamless integration plugin:<br>○ a. Associating SAFE model elements with features using rules<br>○ b. Coloring related elements<br>○ c. Assign a Variant Description Model<br>○ d. Show realization view of a Variant<br>○ e. Show transformation, meaning materialization of variants | ▪ Architecture Model enriched with variant information<br>▪ Family model<br>▪ Variant model<br>▪ Variant specific Architecture Model |
| Unique Selling Proposition(s): | ▪ Support enriching of architecture models with variant information<br>▪ Previewing and transforming of variants from such models<br>▪ Delta analysis showing the impact of reconfigurations<br>▪ Exploiting pure::variants simple constraint language to ensure the configuration of just safe variants | |
| Integration constraint(s): | ▪ pure::variants<br>○ Eclipse 3.5 or later<br>○ Java 1.5 or later | |

| Name: pure::variants | |
|---|---|
| | ▪ pure::variants seamless integration plugin for SAFE platform<br>○ Sphinx (an Eclipse project)<br>○ EATOP (an Eclipse project)<br>▪ ARTOP (www.artop.org) |
| Intended user(s): | ▪ Practitioners and Researchers that experiment with automotive architecture and safety |
| Provider: | ▪ Pure::systems |
| Condition(s) for reuse: | ▪ The plugin as well as pure::variants are made available and may be used under the terms of the "pure-systems Electronic End User License Agreement" |

| Name: SAFE technology platform | | |
|---|---|---|
| Input(s): | Main feature(s) | Output(s): |
| ▪ EAST-ADL model<br>▪ | ▪ Reference implementation of the SAFE meta-model<br>▪ Basic explorer and editor functionality to work with models based on SAFE meta-model<br>▪ Integration of EAST-ADL, AUTOSAR and SAFE meta-models in one Eclipse environment<br>▪ Based on Sphinx (an Eclipse project) technology | ▪ SAFE model including references to EAST-ADL and AUTOSAR<br>▪ |

| | |
|---|---|
| Unique Selling Proposition(s): | ▪ Unique implementation of SAFE meta-model in a seamless tool platform<br>▪ |
| Integration constraint(s): | ▪ Eclipse<br>▪ Sphinx (an Eclipse project)<br>▪ EATOP (an Eclipse project)<br>▪ ARTOP (www.artop.org) |
| Intended user(s): | ▪ Researchers that experiment with automotive architecture and safety |
| Provider: | ▪ www.safe-project.eu |
| Condition(s) for reuse: | ▪ Open Source license based on Eclipse EPL (Eclipse public license) available at internet page of SAFE |

| Name: Safety analysis platform | | |
|---|---|---|
| Input(s): | Main feature(s) | Output(s): |
| ▪<br>▪ | ▪ OFFIS enhanced the safety analysis platform, which was originally developed during the projects ESACS and ISAAC, by implementation of a novel approach for model-based safety analysis (MBSA).<br>▪ A fault injection technique is used to enrich these models with the dysfunctional behaviour specifications that enable the tool chain to systematically evaluate each fault and determine its potential impact on the system.<br>▪ See SAFE deliverable SAFE_D4.2.3.c at the ITEA community page | ▪ Different safety analysis techniques like FTA and FMEA<br>▪ |

| | |
|---|---|
| Unique Selling Proposition(s): | ▪ Support for failure injection in Matlab/Stateflow models<br>▪ Analysis-based cut set generation<br>▪ SAFE platform integration |
| Integration constraint(s): | ▪ Windows 7<br>▪ Java JRE 7 (32 Bit)<br>▪ MATLAB/SIMULINK/STATEFLOW (2011b - 2013a) |
| Intended user(s): | ▪ Researcher<br>▪ Safety experts in the automotive industry that apply safety analysis |
| Provider: | ▪ OFFIS |
| Condition(s) for reuse: | ▪ The tools in this bundle use a personalized license mechanism. The tools are not useable without a license. To obtain a license, please send a request to techsupport@safe.offis.de. |