Functional Safety of Road Vehicles

By Dr. Jürgen Klarmann and Stefan Kriso, Robert Bosch GmbH, and Markus Gebhardt, ETAS

The long-anticipated functional safety standard, ISO 26262, is edging closer to replacing the generic standard for the functional safety of electronic systems, IEC 61508, as the binding standard for road vehicles. Published as Draft International Standard (DIS) in July 2009, ISO/DIS 26262 was approved on the international level in December 2009. It appears as if the automotive community does not expect any major changes in terms of requirements prior to the publication of the final standard, which is anticipated by mid-2011. Robert Bosch GmbH pursues the objective of releasing all of their products, both in hardware and software development, in conformance with the new safety standard, relevant with its coming into effect. In light of the foregoing, and as an integral part of the company's development processes, Bosch has already begun with the qualification of the company's development tools as per ISO 26262. With support by ETAS, the tools belonging to the ASCET, RTA, and INCA product families, all of which are deployed in software development, are being classified and qualified for their particular deployment.

To be allowed to participate in road traffic, road vehicles must conform to the state of the art in terms of scientific and technological maturity. The prevention of product liability claims requires, at minimum, adherence to applicable standards. Subsequent to the publication date of the ISO 26262 standard, all products being introduced to the market should have been developed in accordance with that standard.

Software tools

As defined in ISO/DIS 26262, a “software tool” is any tool comprised of software. Aside from the tools used in software development, the term also describes application programs used in hardware development, ECUs, calibration, or deployed at the system level, e.g., for requirements management.

As its objective, the qualification of software tools is aimed at preventing faults that could find their way into a product by maintaining quality assurance for certain tools and their utilization. To this end, the standard provides for the following measures: On the one hand, appropriate measures can be introduced during the product development phases that keep a tool from generating faults in and of itself. On the other hand, faults generated by a tool can be identified and eliminated in a subsequent process step or by means of organizational measures. To ensure conformity with ISO 26262, all software tools deployed in the development of a safety-relevant electronic product must be reviewed with regard to the specific development process of said product. It is instructive to note that, independent of the use case of a given tool, the standard itself precludes any assurance of across-the-board “ISO 26262” tool conformity. Even the frequently used qualification by means of so-called “sample processes” fails to achieve this objective as applied to the specific development process of a given software tool. That being said, it may still be possible to exploit the reusability of results to establish a useful advance qualification of tools for standard applications, provided that the deployment of said tools throughout the development process can be derived from a standard configuration. Such early qualification, in conjunction with the proper interpretation – a case in point being the IEC 61508 certification of the ETAS ASCET-SE code generator – greatly facilitates the tool's qualification as part of an ISO 26262-conformant process.

Tool classification

The first step in the qualification process addresses the classification of all use cases for which a given tool is deployed during the development process. For example, if a text processing application used for documentation purposes changes its font style upon saving a file, this is not considered safety-relevant. It is a different matter, however, if file saving causes the falsification of relevant information. In the former case, because the tool does not influence the result contents, no further qualification measures are required. The latter case calls for an investigation into the degree of probability with which faulty contents issued by the tool in a subsequent development step may be discovered, e.g., through reviews or testing.

To be allowed to participate in road traffic, road vehicles must conform to the state of the art in terms of scientific and technological maturity. The prevention of product liability claims requires, at minimum, adherence to applicable standards. Subsequent to the publication date of the ISO 26262 standard, all products being introduced to the market should have been developed in accordance with that standard.

Software tools

As defined in ISO/DIS 26262, a “software tool” is any tool comprised of software. Aside from the tools used in software development, the term also describes application programs used in hardware development, ECUs, calibration, or deployed at the system level, e.g., for requirements management.

As its objective, the qualification of software tools is aimed at preventing faults that could find their way into a product by maintaining quality assurance for certain tools and their utilization. To this end, the standard provides for the following measures: On the one hand, appropriate measures can be introduced during the product development phases that keep a tool from generating faults in and of itself. On the other hand, faults generated by a tool can be identified and eliminated in a subsequent process step or by means of organizational measures. To ensure conformity with ISO 26262, all software tools deployed in the development of a safety-relevant electronic product must be reviewed with regard to the specific development process of said product. It is instructive to note that, independent of the use case of a given tool, the standard itself precludes any assurance of across-the-board “ISO 26262” tool conformity. Even the frequently used qualification by means of so-called “sample processes” fails to achieve this objective as applied to the specific development process of a given software tool. That being said, it may still be possible to exploit the reusability of results to establish a useful advance qualification of tools for standard applications, provided that the deployment of said tools throughout the development process can be derived from a standard configuration. Such early qualification, in conjunction with the proper interpretation – a case in point being the IEC 61508 certification of the ETAS ASCET-SE code generator – greatly facilitates the tool's qualification as part of an ISO 26262-conformant process.

Tool classification

The first step in the qualification process addresses the classification of all use cases for which a given tool is deployed during the development process. For example, if a text processing application used for documentation purposes changes its font style upon saving a file, this is not considered safety-relevant. It is a different matter, however, if file saving causes the falsification of relevant information. In the former case, because the tool does not influence the result contents, no further qualification measures are required. The latter case calls for an investigation into the degree of probability with which faulty contents issued by the tool in a subsequent development step may be discovered, e.g., through reviews or testing.

Qualification of development tools as per ISO 26262

The long-anticipated functional safety standard, ISO 26262, is edging closer to replacing the generic standard for the functional safety of electronic systems, IEC 61508, as the binding standard for road vehicles. Published as Draft International Standard (DIS) in July 2009, ISO/DIS 26262 was approved on the international level in December 2009. It appears as if the automotive community does not expect any major changes in terms of requirements prior to the publication of the final standard, which is anticipated by mid-2011. Robert Bosch GmbH pursues the objective of releasing all of their new E/E systems in conformance with the new safety standard, relevant with its coming into effect. In light of the foregoing, and as an integral part of the company's development processes, Bosch has already begun with the qualification of the company's development tools as per ISO 26262. With support by ETAS, the tools belonging to the ASCET, RTA, and INCA product families, all of which are deployed in software development, are being classified and qualified for their particular deployment.

To be allowed to participate in road traffic, road vehicles must conform to the state of the art in terms of scientific and technological maturity. The prevention of product liability claims requires, at minimum, adherence to applicable standards. Subsequent to the publication date of the ISO 26262 standard, all products being introduced to the market should have been developed in accordance with that standard.

Software tools

As defined in ISO/DIS 26262, a “software tool” is any tool comprised of software. Aside from the tools used in software development, the term also describes application programs used in hardware development, ECUs, calibration, or deployed at the system level, e.g., for requirements management.

As its objective, the qualification of software tools is aimed at preventing faults that could find their way into a product by maintaining quality assurance for certain tools and their utilization. To this end, the standard provides for the following measures: On the one hand, appropriate measures can be introduced during the product development phases that keep a tool from generating faults in and of itself. On the other hand, faults generated by a tool can be identified and eliminated in a subsequent process step or by means of organizational measures. To ensure conformity with ISO 26262, all software tools deployed in the development of a safety-relevant electronic product must be reviewed with regard to the specific development process of said product. It is instructive to note that, independent of the use case of a given tool, the standard itself precludes any assurance of across-the-board “ISO 26262” tool conformity. Even the frequently used qualification by means of so-called “sample processes” fails to achieve this objective as applied to the specific development process of a given software tool. That being said, it may still be possible to exploit the reusability of results to establish a useful advance qualification of tools for standard applications, provided that the deployment of said tools throughout the development process can be derived from a standard configuration. Such early qualification, in conjunction with the proper interpretation – a case in point being the IEC 61508 certification of the ETAS ASCET-SE code generator – greatly facilitates the tool's qualification as part of an ISO 26262-conformant process.

Tool classification

The first step in the qualification process addresses the classification of all use cases for which a given tool is deployed during the development process. For example, if a text processing application used for documentation purposes changes its font style upon saving a file, this is not considered safety-relevant. It is a different matter, however, if file saving causes the falsification of relevant information. In the former case, because the tool does not influence the result contents, no further qualification measures are required. The latter case calls for an investigation into the degree of probability with which faulty contents issued by the tool in a subsequent development step may be discovered, e.g., through reviews or testing.
Maserati service network banks on VCI

Back in April 2009, Maserati service shops started phasing in a new solution for vehicle diagnostics. An essential component of the package is the ETAS supplied MDVCI interface module, which handles communications with the vehicle. The new diagnostic system has a modular structure:

For connection with the diagnostic laptop, the MDVCI module is Bluetooth enabled.

Essential factors in Maserati’s decision in favor of the VCI by ETAS were the system’s performance and its modular architecture. The flexibility offered by optional bus interfaces, wireless connectivities, and memory extensions facilitates the configuration of several device variants.

The MDVCI module for Maserati is based on the E6520 Vehicle Communication Interface platform and was developed by the engineers at Vetronix in Santa Barbara, CA, in a scant eight months. With the aid of prototypes, Vetronix developers had evaluated the MDVCI’s core functions, i.e., communications with scan tool and vehicle, jointly with the customer at Vetronix in Santa Barbara,” stated Claudio Buccafurri from Maserati. Communications with the diagnostic software normally use the Protocol Data Unit API, whereas special cases call for the UDS4 diagnostic hardware interface.

The new diagnostic solution has been readily accepted by the Maserati service facilities. “Maserati project staff were very pleased not only with the MDVCI’s entire development process but also with the excellent support provided by the experts at Vetronix in Santa Barbara,” stated Claudio Buccafurri from Maserati.

THE CHALLENGE
ISO 26262 will replace the generic standard IEC 61508 for the functional safety of electronic systems as the binding standard for road vehicles. Robert Bosch GmbH pursues the objective of conforming all of their new E/E systems in accordance with ISO 26262. With support by ETAS, the tools belonging to the company’s development tools as per ISO 26262. ETAS supplies the MDVCI interface module, which handles communications with the vehicle. The new diagnostic system has a modular structure:

For connection with the diagnostic laptop, the MDVCI module is Bluetooth enabled.

THE SOLUTION
ETAS supplies the MDVCI interface module, which handles communications with the vehicle. The new diagnostic system has a modular structure:

For connection with the diagnostic laptop, the MDVCI module is Bluetooth enabled.

THE BENEFIT
The flexibility offered by optional bus interfaces, wireless connectivities, and memory extensions facilitates the configuration of several device variants.

Vehicle Diagnostics

By Dr. Ulrich Lauff and Uwe Maier, ETAS

Maserati service network banks on VCI

Back in April 2009, Maserati service shops started phasing in a new solution for vehicle diagnostics. An essential component of the package is the ETAS supplied MDVCI interface module, which handles communications with the vehicle. The new diagnostic system has a modular structure:

For connection with the diagnostic laptop, the MDVCI module is Bluetooth enabled.

Essential factors in Maserati’s decision in favor of the VCI by ETAS were the system’s performance and its modular architecture. The flexibility offered by optional bus interfaces, wireless connectivities, and memory extensions facilitates the configuration of several device variants.

The MDVCI module for Maserati is based on the E6520 Vehicle Communication Interface platform and was developed by the engineers at Vetronix in Santa Barbara, CA, in a scant eight months. With the aid of prototypes, Vetronix developers had evaluated the MDVCI’s core functions, i.e., communications with scan tool and vehicle, jointly with the customer at Vetronix in Santa Barbara,” stated Claudio Buccafurri from Maserati. Communications with the diagnostic software normally use the Protocol Data Unit API, whereas special cases call for the UDS4 diagnostic hardware interface.

The new diagnostic solution has been readily accepted by the Maserati service facilities. “Maserati project staff were very pleased not only with the MDVCI’s entire development process but also with the excellent support provided by the experts at Vetronix in Santa Barbara,” stated Claudio Buccafurri from Maserati.

THE CHALLENGE
ISO 26262 will replace the generic standard IEC 61508 for the functional safety of electronic systems as the binding standard for road vehicles. Robert Bosch GmbH pursues the objective of conforming all of their new E/E systems in accordance with ISO 26262. With support by ETAS, the tools belonging to the company’s development tools as per ISO 26262. ETAS supplies the MDVCI interface module, which handles communications with the vehicle. The new diagnostic system has a modular structure:

For connection with the diagnostic laptop, the MDVCI module is Bluetooth enabled.

THE SOLUTION
ETAS supplies the MDVCI interface module, which handles communications with the vehicle. The new diagnostic system has a modular structure:

For connection with the diagnostic laptop, the MDVCI module is Bluetooth enabled.

THE BENEFIT
The flexibility offered by optional bus interfaces, wireless connectivities, and memory extensions facilitates the configuration of several device variants.