CHARTER

Critical and High Assurance Requirements Transformed through Engineering Rigoure

ARTEMIS

COMPLETED
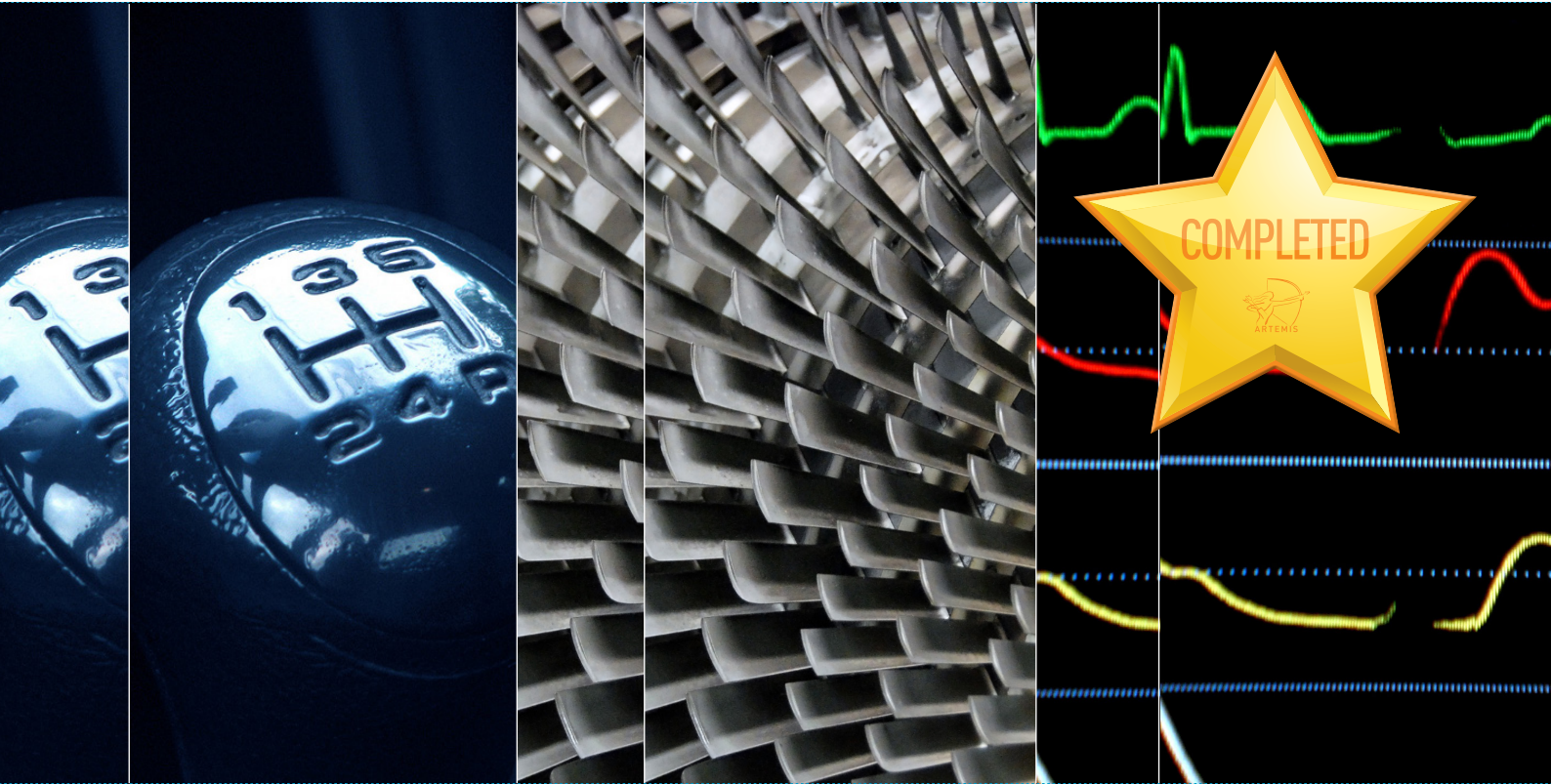
EXECUTIVE *summary*

CHARTER will develop concepts, methods and tools for embedded system design and deployment that will enable EU developers to master the complexity and substantially improve the development, verification and certification of critical embedded systems. The project will ease, accelerate and reduce the cost of verification and certification of critical embedded systems as safe and reliable in compliance with regulatory requirements, and will contribute to the overall safety and security of citizens that rely on embedded technologies.

CONTRIBUTION *to SRA*

Critical embedded software systems assist, accelerate and control various aspects of European society and are common in cars, aircraft, medical instruments and major industrial and utility plants. These systems are critical to human life and must be subject to the highest standards of performance through formal certification procedures. With human life becoming increasingly dependent on embedded software and our society needing protection from the severity of the risks, more and more software will be subject to governmental regulations and require verification. The costly and time-consuming procedures employed today to verify new software will be unable to meet future formal verification demands. The CHARTER project technologies will enable new methods of verification and certification that will streamline the process for certification of crucial embedded systems through the use of higher level languages and model-driven development methods and tools.

MARKET INNOVATION *& impact*

CHARTER will improve the productivity of EU embedded systems developers by making it practical to use high-level language technology in high assurance and safety-critical embedded systems. High-level languages provide a richer and more advanced development environment that speeds the design and development process while allowing application developers to use and adapt existing code more easily and in less time. These benefits have yet to be realised for critical applications in the aviation, medical, automotive and surveillance markets due to stringent and complex requirements for certification. CHARTER technologies will enable European companies relying on safety-critical embedded systems for their products to be more competitive through reduced costs and shorter time to market. Costs of re-certification for product releases will also be reduced, making EU companies more receptive and competitive.

RELEVANCE & CONTRIBUTIONS *to Call 2008 Objectives*

CHARTER seeks to increase the productivity of system development and enable the modular assembly of systems. Getting embedded applications correct first time generates a significant payback, especially in safety-critical embedded systems. A typical system has several stages of development: requirements, design, modelling, coding, test, deployment. At each stage, the cost of repairing an error is roughly an order of magnitude higher than in the previous stage.

By giving the developer tools to help ensure that errors are not introduced throughout the process and to ensure consistent requirements from the start, considerable time and costs can be saved over the lifetime of the embedded system.

Today this level of rigour can only be afforded for the most critical systems like aviation, but with the introduction of CHARTER technologies higher standards of safety and reliability will be affordable and applicable to a wide array of systems beyond aviation and enable more complex systems to be certified at the highest safety levels.

R&D INNOVATION *and technical excellence*

Advanced requirements for engineering processes will be developed to address deductive formal verification and requirements-driven test generation that will streamline regulatory compliant verification and certification procedures. Hyperlinked traceability evidence containing baseline artefacts, their certification evidence, including verification traces, and their traceability relationships will be provided.

Extra-functional properties of critical embedded systems that are an essential part of verification will be addressed through Automatic Test Case Generation methods, while a lightweight, portable, repository independent graph rewriting tool that is retargetable to different languages and metamodels will be developed. These innovations will be the basis of new technology for the certification of model-driven development that translates partial models to more complete models, models to source code and source code to binary code, complemented by rule-driven compilation techniques that are able to demonstrate the correctness of the code.

Together these technologies will be assembled in a complete tool chain and methodology for safety-critical software development that will reduce design costs, shorten the overall design cycle, leverage pre-existing tools and help manage project complexity by providing developers with more powerful tools.

PROJECT *partners*

ARTEMIS
www.artemis.eu

CHARTER