SAFETY CRITICAL SYSTEMS

SAFETY AND SECURITY THE HIGH-TECH WAY

Despite the gloom and doom of the daily news, Europe has arguably never been a safer and more comfortable place to live. Although we are constantly under threat, cutting-edge technology protects our critical infrastructures from disastrous malfunction. Europe continues to invest in the development of ICT for safety critical systems and controls so that society can enjoy its freedom long into the future.

'Brace!' barks the warning over the plane's intercom. The passengers tuck their heads to their knees as the captain continues. 'Ladies and gentleman, it appears that we have a software bug in our flight controls and we are now unable to control our engines...'

It is hardly what you want to hear when you are high above the clouds. Fortunately you can continue to fly without fear — thanks to years of research and some clever technologies.

ICT systems and controls will keep you safe. Aeroplanes, along with cars, nuclear power stations and other vital infrastructure, all have one thing in common: they are 'safety critical'. In other words, the consequences of a malfunction could be disastrous.

You only have to look back to Chernobyl or the 2010 oil spill in the Gulf of Mexico to appreciate the awful loss of human life and environmental damage that can occur when safety critical or control systems actually go wrong.

We now live in an age where the safety of citizens and the smooth running of our economies are under constant threat from terrorism, natural disaster and the long-term effects of climate change. So the EU takes the protection of its citizens and critical infrastructure extremely seriously, while respecting privacy and personal data.

By the summer of 2010, nine projects had received more than EUR 17 million following a joint call between the ICT and security themes of FP7. The projects are investigating new ICT-based methods to protect critical infrastructures in the EU, from banking networks to offshore wind farms.

The importance that the EU places on security and safety is evident in the number of initiatives and funding programmes it has supported in the past decade, including the 'European programme for critical infrastructure protection' (EPCIP) and the current EUR 140 million 'Specific programme for prevention, preparedness and consequence management of terrorism and other security related risks' (CIPS).

ICT INSIDE

ICT is found in almost every safety system that has been developed or tested in the past 15 or more years. ICT can deliver the three essential elements for safety control: detection using sensors, rapid data analysis and preventative actions.

The EU has supported R & D in all these areas, from microscopic gyroscopes that pick up sudden deceleration to complex algorithms and real-time data mining techniques that spot the first tell-tale signs of a problem from within vast quantities of complex monitoring data. Many of the technologies and prototypes tested by past European projects are now finding their way into commercial products and going live in real safety systems.

»

SAFETY CRITICAL SYSTEMS

Scientists funded through FP7 are also developing hardware and software that could help to improve the safety features of so-called complex systems that do not behave in predictable ways.

One exciting area that the EU is giving particular attention is in the use of embedded electronics for active safety monitoring. Microchips are so cheap and small that it is possible to embed electronic sensors and actuators with wireless connectivity into machinery, engine parts, building structures and industrial plants.

However, these chips — and any electronics within safety critical systems — must be robust and extremely reliable; several projects have been launched to improve the dependability of such embedded safety devices.

The Artemis joint undertaking , an EU-supported public-private partnership for R & D in embedded systems, is also placing a strong emphasis on the safety and security of embedded systems within its own research funding programme.

With the current research effort, catastrophic accidents and system failures should become even rarer than they are today. So even when the captain shouts 'Brace!', your hope of landing alive will not be in vain. ■

PROJECTS IN FOCUS

Since the 1990s Europe has made considerable advances in its development of ICT-based safety and security systems and controls. This R & D investment is beginning to pay dividends; European safety solutions and products have a worldwide reputation and are finding their way into commercial products.

ROBUST SECURITY, JUST IN TIME

An innovative EU-funded technology called time-triggered architecture (TTA) provides highly reliable electronic systems where safety issues are critical, such as in transport or energy engineering.

These systems are particularly robust and dependable when data and commands must be processed with extraordinary precision and speed. Any errors that may occur are contained within a single subsystem and are not allowed to spread to other parts of the network.

The first major commercial success for TTA was achieved in 2002 when Airbus announced that it had chosen TTA technology for the cabin pressure system of the new A380. It is also now widely used in the automotive sector.

The TTA technology was developed over 25 years and an investment of more than EUR 60 million. A series of EU-funded projects including NEXT TTA, PDCS and X-by-Wire contributed to the research effort.

A spin-off (TTTech) of the Technical University of Vienna has commercialised the technology, selling products to the automotive, aerospace and automation industries, as well as manufacturers of off-road vehicles and industrial plants.

»

SAFETY CRITICAL SYSTEMS

STEALING AN ADVANCE ON SAFETY SYSTEMS

Prevention is better than cure, they say, but preventative action relies on advanced warning. That is why the MICIE project is eager to establish a 'Critical infrastructure warning information network' (CIWIN).

MICIE is building an alert system that identifies, in real time, the level of possible threats induced on a given critical infrastructure (CI) by 'undesired' internal or external events. Whenever such events occur, the MICIE alert system will support the CI operators, providing them with a real-time risk level estimate (for example, green, yellow, red).

Similarly, the Viking project, approved in the FP7 ICT/security joint call, looks at the security of the ICT control systems in the electric power infrastructure. Keeping these systems secure and resilient to external attacks, as well as to internal operational errors, is vital for uninterrupted service.

However, this is challenging since the control systems are extremely complex and need to respond in real time. Viking researchers are looking to develop more secure and robust industrial control systems for power generators and the grids that carry the power.

COPING WITH COMPLEXITY, SELFHEALING SOFTWARE

Has your PC crashed again? At least you can just reboot — not an option for a pilot or nuclear power operator.

The Shadows project has developed tools to spot software bugs and even heal dodgy code. Today, the software and algorithms running everything from air conditioning in shopping centres to power grids and water purification plants, have become so complex that programmers can no longer cope. EU researchers are learning that some of the best security and safety systems and controls are those that automatically detect and repair faults.

In 2009, the Selfman project delivered the potential of self-configuration, -tuning, -healing and -protection. The Modelplex project went a step further and created a development platform that will enable applications to tackle the enormous and increasing complexity of modern computer science. It promises better quality at a lower price. While the Momocs project released a prototype software engineering platform that could help organisations save time, money and energy as they scramble to upgrade complex IT systems. ■

EUROPEAN COMMISSION