Eingebettete Systeme sind inzwischen in nahezu allen Bereichen des Alltags präsent, auch in Flugzeugen: Autobahn bei Frankfurt am Main.
Nowadays, embedded systems can be found virtually everywhere — also in aeroplanes: Highway near Frankfurt/Main.

„Dialog muss schnellstens beginnen“

Werner Damm

Eingebettete Systeme gelten als extrem marktrelevant: Schon jetzt gibt es kaum ein Produkt, das ohne die Technologie entwickelt wird. Doch während immer neue Forschungsallianzen und Unternehmensstrategien zu ihrer Förderung entstehen, sucht man eine fundierte Gefahrenabschätzung über ihren Einsatz vergebens. Eine solche Analyse ist dringend nötig – und kann nur aus interdisziplinärer Perspektive gelingen.

Es gibt Dinge, die sind überall und trotzdem nimmt man sie kaum wahr. So ist es auch mit den Eingebetteten Systemen – jene Querschnittstechnologie, die aus bloßer Mechanik wahrnehmende, ja handelnde Größen macht. Wenn im stockenden Verkehr eine Person am Steuer einschläft und die Kontrolle über ihr Fahrzeug verliert, kann eine fatale Kettenreaktion die Folge sein. Beherbergt das Auto jedoch Eingebettete Systeme, passiert gar nichts.

Denn ein Müdigkeitssensor hat längst gemerkt, dass die Augenlider des übermüdeten Fahrers in einer charakteristischen Frequenz das Weggleiten in den Kurzschlaf andeuten. Er hat die sich verändernde Körperhaltung registriert. Und gibt der Schaltzentrale das Kommando, das Fahrzeug selbstständig sicher zu führen. Über 70 Steuergeräte befinden sich heute in einem Auto – von Prozessoren über Speicher bis hin zu Schnittstellen zur Kommunikation durch sogenannte Bussysteme.

Für eine Fahrzeugfunktion wie etwa „Übernehme Längs- und Querführung des Fahrzeuges, wenn Fahrer einschläft“ wird an einem Steuergerät das aktuelle Wissen über den Zustand des eigenen Fahrzeuges mit dem ermittelten Fahrerzustand sowie der Fahrzeugumgebung zusammengeführt. Der Wagen übernimmt auf Grund des inneren Bildes von seiner Umgebung Längs- und Querführung selbst: eine Maschine, die durch sich selbst zu existieren scheint.

Es ist, als seien die Fahrzeuge mit eigenen Sinnen ausgestattet. Sie werden sehend: Durch Überlagerung von Informationen aus verschiedensten Sensorquellen wie Videokameras, Laserscanner, Radar und über Funk bauen sie ein genügend genaues Bild der realen Fahrzeugumgebung auf und nehmen Lageeinschätzungen vor. So ist der „Müdigkeitssensor“ mitnichten ein mit dem Fahrer verbundenes Messgerät, sondern wird aus der Bewertung der Abfolge von Videobildern gewonnen – durch Algorithmen, die darauf programmiert sind, auf Muster von Augenlidbewegungen und Körperhaltung zu achten und daraus einen geschätzten Fahrerzustand wie etwa „ist dabei einzuschlafen“ zu gewinnen. Die Fahrzeuge werden auf diese Weise handelnd: Rechtzeitig leiten sie im autonomen Fahrmodus

“Dialogue is Imperative”

Embedded systems are perceived to have extreme market potential. Nowadays, hardly any products are developed without this technology. However, whereas new research alliances and corporate strategies are emerging everywhere to support the development of such systems, one searches in vain for a grounded evaluation of the risks attached to their application. There is a pressing need for such an analysis, though, and it can only be successful from an interdisciplinary perspective.

Some things can be found all around us, although we hardly take any notice of them being there. It is no different in the case of embedded systems – a cross-sectional technology capable of transforming simple mechanics into sensing and even autonomously acting agents. To give an example: When a truck driver succumbs to tiredness at the wheel and loses control over his vehicle, the result could trigger a chain reaction with fatal consequences. If the vehicle is fitted with appropriate embedded systems, though, maybe an accident can be averted.

Vehicles equipped with driver-fatigue sensors automatically register when the driver’s eyelids close with a frequency characteristic of falling into a sleepy state. Sensors also register any change in body posture and, if alerted, pass a command to the control centre to switch to automatic pilot and take over the guidance of the vehicle. A typical modern automobile is equipped with upwards of 70 control devices – from processors, through data memory, up to communication interfaces via so-called bus systems.

In the case of a safety function like “Take over longitudinal and lateral guidance of vehicle when driver falls asleep”, for instance, a control device is fed with real-time data encompassing the status of the vehicle in question, the driver’s condition, and the immediate environment. On the basis of all this processed information the vehicle is enabled to safely guide itself: A machine with an apparent life of its own.

It is almost as though the vehicle is equipped with its own senses. The various devices enable it to see: By overlaying the information gathered from various sensor sources like video cameras, laser scanner, radar and radio, it is able to build up an exact picture of its real surroundings and carry out predictions. It is not necessary for a “driver-fatigue sensor” to be attached to the driver in any way; rather, the assessment is arrived at on the basis of video images – by means of algorithms programmed to register certain patterns of eye-lid movement and body posture and, hence, to arrive at an assessment of the driver’s status like “is about to fall asleep”. In this way, vehicles become actors: In autonomous drive mode, the control centre triggers actuators to regulate the correct braking pressure to be applied in an emergency stop, for instance, to avoid colliding with the vehicle in front.

See, analyze, decide, act: There are very few fields of application that can do without these capabilities, and hence extremely few products that can be developed without embedded systems. The significance of this technology for Germany as a location for industry is enormous. More than three million high-tech jobs depend on it. Every year the automobile industry, together with the mechanical and plant engineering branches, and the sector of medical engineering invest some 15 billion euros in related research and development – and generate turnover in excess of 550 billion euros annually.

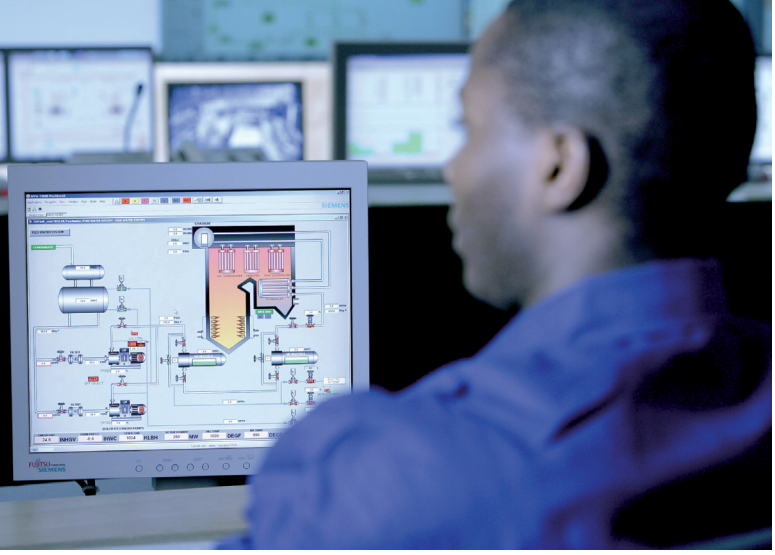
Uncharted territory on the research landscape

One could describe the phase the technology currently finds itself in as a hype. The enthusiasm is great, and lots of things are being eagerly tried out. It seems almost as if there is no end to possible applications, and the enormously high market potential continues to fuel the research machinery, which is adopting and being shaped by

Der Autor The author

Prof. Dr. Werner Damm studierte Informatik und Mathematik in Bonn und promovierte anschließend mit Auszeichnung 1981 in Aachen auf dem Gebiet der Informatik. Nach seiner Habilitation wurde er 1987 auf die Professur „Rechnerarchitekturen“ der Universität Oldenburg berufen, wo er seit 2002 die Abteilung Sicherheitskritische Eingebettete Systeme leitet. Damm arbeitet eng mit Partnern aus der Luftfahrt- und der Automobilindustrie sowie des Schienenverkehrs zusammen. Er hat den Forschungs- und Entwicklungsbereich Verkehr am An-Institut OFFIS - Institut für Informatik – etabliert, wo er als Vorstandsmitglied tätig ist. Außerdem ist er Vorstandsvorsitzender des Kompetenz-Clusters SafeTRANS - Safety in Transportation Systems -, Sprecher des Sonderforschungsbereichs/Transregio 14 AVACS, Sprecher des Steuerkreises National Roadmap Embedded Systems sowie Direktor des Forschungszentrums Sicherheitskritische Systeme.

Prof. Dr. Werner Damm studied computer science and mathematics in Bonn. He was awarded summa cum laude for a doctoral dissertation in the field of computer science in Aachen in 1981. After completing his post-doctoral dissertation in 1987, he was appointed full professor of computer architecture at the University of Oldenburg, where since 2002 he has been holding the Chair for Safety-Critical Embedded Systems. Prof. Damm practices applied research and cooperates closely with industrial partners in automotive, avionics, and train systems. He established the research and development area transportation at the OFFIS Institute for Computer Science, an affiliated institute of the University of Oldenburg, where he is also member of the board of Directors. Moreover, he is Chairman of the SafeTRANS competence cluster - Safety in Transportation Systems -, he is Scientific Director of the Transregional Collaborative Research Center Transregio 14 AVACS, speaker of the National Roadmap Embedded Systems Steering Board as well as Director of the Research Center Safety-Critical Embedded Systems.



Arbeit mit Eingebetteten Systemen: In Forschung und Entwicklung der Technologie investieren die Branchen Automobilbau, Maschinen- und Anlagenbau sowie Medizintechnik jedes Jahr etwa 15 Milliarden Euro.
Working with embedded systems: The manufacturing sector of the economy, especially the automobile branch, as well as the sectors of mechanical, plant and medical engineering, invest some 15 billion euros in research and development every year.

über so genannte Aktuatoren wie etwa die Ansteuerung des Bremsdruckes eine Vollbremsung ein, wenn in der Kolonne plötzlich eine Stausituation eintritt.
Sehen, Analysieren, Entscheiden, Handeln: Es gibt kaum ein Anwendungsgebiet, in dem diese Fähigkeiten nicht gefragt sind, und kaum ein Produkt, das ohne Eingebettete Systeme entwickelt würde. Die Bedeutung der Technologie für den Wirtschaftsstandort Deutschland ist enorm: Mehr als drei Millionen High-Tech Arbeitsplätze hängen von ihr ab. Die Branchen Automobilbau, Maschinen- und Anlagenbau und Medizintechnik investieren jedes Jahr etwa 15 Milliarden Euro in ihre Forschung und Entwicklung – und erwirtschaften damit Gesamtumsätze von mehr als 500 Milliarden Euro jährlich.

Weißer Fleck in Forschungslandschaft

Als „Hype“ könnte man die Phase bezeichnen, in der sich die Technologie derzeit befindet. Groß ist die Begeisterung, und vieles wird erst einmal munter ausprobiert. Scheinbar beliebig steigerbar ist ihre Einsetzbarkeit, und die extrem hohe Marktrelevanz heizt eine Forschungsmaschinerie beständig an, die in Termini von Unternehmensstrategien, Roadmaps, Joint Undertakings und Innovationsallianzen Gestalt gewinnt.
Doch so hilfreich Eingebettete Systeme sind, so risikobehaftet ist auch ihr Einsatz. Buchstäblich alles kann bei ihrem Einsatz schief gehen: Sensoren können ausfallen, die Situationsanalyse kann zu einem falschen Bild der Lage kommen. Handlungsentscheidungen können nicht oder falsch umgesetzt werden. Möglich, dass die Bildanalyse von Videodaten eine Mülltonne irrtümlich für ein spielendes Kind hält und die resultierende Vollbremsung zu einem Auffahrunfall führt. Und dass die Situationsanalyse eine Aschewolke einfach nicht kennt und deswegen das Flugzeug blind in eine scheinbar gefahrenfreie Zone fliegt.
Nun handelt es sich hier um Beispiele aus verkehrstechnischen Anwendungen – und gerade diese Branchen sind vorbildhaft in der Risikoforschung. Kein Flugzeug fliegt, kein Stellwerk der Bahn wird aktiviert, ohne dass nicht eine von unabhängigen Agenturen abgenommene Risikoprüfung vorgenommen worden ist, die internationale Sicherheitsstandards einhält – ähnliche Standards gelten im Automobilbereich, der Automatisierungstechnik und der Medizintechnik.
In vielen anderen Anwendungsgebieten von Eingebetteten Systemen sieht Risikoforschung aber ganz anders aus. Besser gesagt: Sie ist nicht vorhanden, man kann geradezu von einem weißen Fleck in der Forschungslandschaft sprechen. Was passiert, wenn für eine flächendeckende Gesundheitsversorgung in starkem Maße auf die dezentrale Erfassung von Vitalparametern in der ambulanten Nachversorgung gesetzt wird – und keine Krankenschwester, sondern ein Eingebettetes System den Patientenstatus überwacht?
Die Risiken der Technologie scheinen hier offensichtlich: Falsch oder nicht übertragene Vitalparameter, eine Situationsbewertung, in der die Messdaten bewusst oder irrtümlich mit falschen Patientenstammdaten verknüpft werden, eine daraus resultierende falsche Einschätzung eines kritischen Gesundheitszustandes, eine durch Fehlfunktion erfolgende Überdosis eines automatisch verabreichten Medikamentes. Das Besondere an diesem Szenario: Es sprengt die Grenzen eines einzelnen Produktes – denn erst durch die Vernetzung von am Körper erfassten Sensordaten mit Patientendaten und ärztlichen Versorgungszentren, in den sogenannten „Systems of Systems“, können neuartige Lösungen für gesellschaftliche Fragestellungen – hier die Sicherung der ärztlichen Versorgung – geschaffen werden.

Handlungsvollmacht der Systeme

Und gerade für solche systemübergreifenden Lösungen fehlt es an klaren Regelungen zur Risikoanalyse. Oft werden Teilsysteme miteinander vernetzt, die für sich zwar einschlägigen Bestimmungen genügen – doch eine kanonische Organisation für Risiken, die aus der Vernetzung entstehen, sucht man vergebens. Dabei sind Systems of Systems aufgrund ihrer notwendigen Vernetzung allen Risiken ausgesetzt, die wir aus dem Internet kennen: Angriffen, die in das „Nervensystem“ des Eingebetteten Systems eindringen, beispielsweise um Patientendaten zu gewinnen. Oder um bewusst ein System zu schädigen und Fahrzeuge auf Kollisionskurs zu bringen.
Dieses Fehlen einer systematischen Risikoanalyse ist beunruhigend, zumal der Mensch zunehmend immer mehr Bestandteil eines vernetzten Systems von Systemen wird – ob auf dem Feld der Energie, des Verkehrs oder der Gesundheit. Er wird zum Einsprengsel in digitalen Lagekarten, ein Bewertungsparameter in automatisierten Entscheidungsprozessen, Subjekt von Handlungen, die autonom in der Schaltzentrale des Systems of Systems veranlasst werden. Und es ist noch nicht absehbar, welche Gefahren entstehen, wenn wir im Treiben nach neuen Lösungen unsere Handlungsvollmacht zu Gunsten autonom „für uns“ handelnder Systeme verlieren.
Denn während die eingangs beschriebenen Assistenzsysteme im Auto darauf angelegt sind, dem Menschen zu helfen, ihm gewissermaßen als freundlicher Berater zur Seite zu stehen, verändert sich die Rolle des Menschen im Systems of Systems Kontext schlagartig. Eine Systems of Systems-Flugsicherung, die bei der Aschewolke je nach Land oder sogar Flughafen bei objektiv gleichen Randbedingungen mal eine Anflugerlaubnis erteilt, mal versagt, veranschaulicht die Kernproblematik: Inwieweit wird die Interessenlage eines einzelnen Menschen in einem Gesamtgeflecht von hunderten oder tausenden Systemen in der Entscheidungsfindung tatsächlich berücksichtigt? Und wer liefert die Werteskala, um zu sagen, wann Allgemeininteressen wichtiger als Einzelinteressen sind?
Die Folgen berühren grundlegende Fragen des Interessensausgleichs. Dies umso mehr, als Eingebettete Systeme zunehmend unser Denken, Handeln und Fühlen unterwandern. Nur in einer interdisziplinären Perspektive kann es gelingen, den Menschen nicht aus den Augen zu verlieren und eine Gefahrenabschätzung vorzunehmen. Systems of Systems werden wie lebende Organismen sein, die aufgrund ihrer zahlreichen Interaktionsformen selbst neue Verhaltensweisen ausprägen – die zu ihrer Entwurfszeit überhaupt nicht voraussehbar waren. Kein Zweifel, wir brauchen einen fächerübergreifenden Dialog. Und der sollte schnellstens beginnen.

Polar-Express: In verkehrstechnischen Anwendungen ist die Risikoforschung vorbildhaft – in anderen Anwendungsgebieten ist sie noch ein weißer Fleck.
Polar Express: Risk research concerning applications in the area of passenger transport are exemplary – in other fields of application, though, it is a blank spot on the research landscape.

terms like "corporate strategies", "roadmaps", "joint undertakings" and "innovation alliances". But as helpful as embedded systems may be, their application is fraught with risks. Literally everything can go wrong: Sensors can malfunction, the situation analysis can arrive at a false assessment of the situation. Decisions to act may be falsely interpreted, or even not implemented at all. It is possible that the analysis of image data mistakes a dustbin for a child playing, and the subsequent emergency stop causes a rear-end collision, or the situation analysis fails to recognize an ash cloud so that an aeroplane flies into an apparently danger-free zone.

Admittedly, the above examples are of applications in air and land traffic – and these branches above all are exemplary in their approach to risk research. No plane is able to take off and no rail interlocking system can be put into operation before being put through rigorous tests on the part of independent agents under observance of international safety standards – similar standards are also to be found in the automobile branch, automation engineering as well as medical engineering.

In many other areas where embedded systems are applied, though, it is quite a different story. Or, better said, there is no risk evaluation at all: It is uncharted territory on the research landscape. What would happen if it were to be decided to rely nation-wide on the decentralized capture of vital parameters for the aftercare of outpatients – completely in the absence of nurses and relying entirely on embedded systems?

The risks attached to the technology are obvious in this case: Failure to transmit or falsely transmitted vital parameters, a situation assessment in which the measuring data is either consciously or erroneously linked with wrong patient master-data, the subsequently resulting false evaluation of a critical health state, leading to an overdose of an automatically administered medication. What's so special about this particular scenario: It exceeds the boundaries of a single product – for only the crosslinking of sensor data obtained directly from the patient's body with patient master data and medical care centres in the so-called system of systems will be able to provide innovative solutions for societal issues – here the provision of medical treatment.

Authority of Systems

And it is precisely in the case of such system-of-system solutions that we can constitute a lack of clear rules and guidelines for risk analysis. Though often appropriate safety standards exist for the individual systems in such a system-of-system context, one searches in vain for any canonical organisation of the risks arising from cross-linkages in general. And this despite the fact that systems of systems, due to their necessary crosslinking, are prone to all the risks that we already know from the internet: Attacks on the "nerve centre" of the embedded system in order to steal patients' data, for instance, or to consciously damage a system in order to cause accidents.

This lack of systematic risk analysis is disturbing, particularly in view of the fact that we are all increasingly becoming components of a universally crosslinked system of systems – whether in the areas of energy, road traffic, or the health system. We are reduced to tiny dots on digital tactical maps, an evaluation parameter in automated decision processes, subjects of actions which are triggered autonomously in the control centre of the system of systems. And it is entirely unforeseeable what dangers will materialize when, driven by the ever-pressing search for new solutions, we lose our power of negotiation to autonomously acting systems which are acting "for us".

For whereas the above-described assistance systems in automobiles have been designed to help people, much in the way of offering friendly support, the role of man undergoes an abrupt change within the context of the system of systems. The core problem is illustrated by a system-of-systems air traffic control, for instance, which in the event of an ash cloud and objectively same framework conditions sometimes grants permission to land and sometimes doesn't, depending on the country, or even the airport, in question. To what extent are the interests of the individual drawn into the decision-making process and taken into account in an overall constellation of hundreds or even thousands of systems? And who is to provide the values scale which determines when the public interest is more important than that of the individual?

The consequences touch upon fundamental questions of balancing interests. And this even more so as embedded systems increasingly infiltrate our thinking, actions and emotions. Only in an interdisciplinary perspective can we be successful in not losing sight of man as the main actor and in carrying out an appropriate evaluation of the risks. Systems of systems will be like living organisms which, due to their manifold forms of interaction, develop new manners of behaviour by themselves – forms which at the time they were conceived were utterly inconceivable. Let there be no doubt, we urgently need a cross-disciplinary dialogue. And the sooner that gets underway, the better.