Importance of Certification for Embedded Real-Time Systems

G Motet, J.-P Seuma Vidal

Session 1A: Certification

Title: Importance of Certification for Embedded Real-Time Systems

Authors:

Pr. G. Motet, LESIA / INSA, 135, avenue de Rangueil, 31077 Toulouse cedex 4, France. Tel. +33 (5) 61 55 98 18, Fax +33 (5) 61 55 98 00, gilles.motet@insa-tlse.fr

Brief biography: Gilles Motet, Professor at the National Institute of Applied Sciences, is the head of the LESIA research laboratory. He works in the team Systems Dependability on fault prevention and certification of embedded real-time systems. He participates to various organisations including National Research Centre in Technology for Avionics and Space, French Standardisation AFNOR and the European Institute of Research on Electronics Systems for Transportation. He is co-author of 3 books on Systems Dependability (Prentice Hall, Kluwer Academic Publisher, InterEdition).

J.-P. Seuma Vidal, LESIA / INSA, 135, avenue de Rangueil, 31077 Toulouse cedex 4, France. Tel. +33 (5) 61 55 98 02, Fax +33 (5) 61 55 98 00, jpseuma@insa-tlse.fr

Brief biography: Jean-Pierre Seuma Vidal is Ph. D. student in the team Systems Dependability of the LESIA laboratory. His thesis deals with the use of UML to develop systems which must be certified: assessment of the modelling language features and guidelines to use them.

Keywords: certification, safety, real-time systems

1. Statement: Increasing of embedded real-time systems responsibilities

1.1 Quantitative increasing

Embedded real-time systems are now integrated in numerous products used everyday: transportation vehicles (aircrafts, cars, trains, etc.), communication means (phones, switchboards, satellites, etc.), medical devices (tele-echography, pacemakers, etc.), systems producing energy (nuclear plants, etc.), consumer goods (robots, etc.) or services (cash dispensers, etc.).

The increasing of the number of such systems is correlated with the increasing of the number of the services they offer. This is mainly due to the software technology which, at first, allowed the improvement of the former functionalities replacing other technologies for implementation. Software is now used to offer functionalities to compensate for inadequacies of the capacities of users or other products, taking charge of new responsibilities. Finally, embedded real-time systems are now completely integrated in global systems and cannot be considered as independent elements. In the following sub-sections, these new characteristics and roles of software technology included in real-time embedded systems are analysed to highlight their consequences.

summary previous next

1.2 Improvement of performance and functionalities

The increasing of software technology in real-time embedded systems is at first due to the clients who require more reliability. Indeed, this technology is not prone to ageing. Thus, the electronics systems embedded in cars were developed to manage the ignition of sparks. The executed program takes into account the position of the piston deduced from the position of the driving shaft. This substitution of a software technology for an hardware technology initially allows the ignition system reliability to be increased: no more contact points to be changed or tuned.

Then, the software technology was used as it allows to implement sophistic functions, that is, functions whose behaviour is complex and adaptable to the changing of the environment parameters values. Thus, the functional flexibility offered by the software realisation permits to control dynamically the spark ignition depending on the values of various parameters such as the engine temperature or speed, in order to reduce the consumption, for instance thanks to the ignition advance. The valve opening controlled by a computer instead of a camshaft also increased the engine capabilities (horsepower) taking the environmental characteristics (engine temperature, etc.) into account. Therefore, the software technology improves the performance of functionalities previously offered.

As software allows complex behaviours to be expressed, new services were offered afterwards. The air conditioning control considering inside and outside temperatures, the adaptation of the power steering considering the car speed, or the changing of the shock absorber laws taking the driving style into account are three examples.

However, in all cases, these functionalities provide more comfortable cars but are not absolutely necessary.

These new functionalities were largely distributed thanks to the low production cost but also the relatively low development cost offered by the software technology: implementation is made easier by compilers, prototypes can be quickly designed, etc. These characteristics associated with the flexibility of this technology encouraged designer to imagine new products.

1.3 Take charge of shortcomings

More recently but with an increasing importance, embedded real-time systems implemented with software technology aim at overcoming shortcomings not due to these systems but to other elements in their environment. Thus, more and more responsibilities are transferred to these systems.

1.3.1 Responsibilities to take charge of bad use

At first, a part of the responsibilities previously taken by users is now delegated to these systems. In particular, the requirement of the absence of unacceptable effects due to a bad use

of the system, is transferred from the user to the system. Hereafter, we mention some examples coming from automotive domain.

The excessive emission is an unacceptable harm which may be due to a bad driving. Such a situation occurs if the driver steps too much on the accelerator when the car climbs up a hill. To handle this bad behaviour of the user, a device analyses the exhaust gas and the accelerator cable is replaced by a numeric transmission allowing the engine control system to limit the pollution, reducing the injected fuel despite the driver action on the accelerator. Thus, the actual engine acceleration is not only due to the driver but partially delegated to the computerised system.

Injuries or deaths due to accidents are a second type of harms. Their prevention is now partially delegated to embedded real-time software applications. For instance, the ESP (Electronic Skid Prevention) prevents skids, maintaining the car on its trajectory when a car is entering a bend too fast. So, this system is a palliative device to a bad driving. The system which pressurises the hydraulic braking circuit when the driver removes quickly his/her foot from the accelerator, or the ABS avoiding the blocking of the wheels are other systems preventing accidents when car speed is too high. The systems controlling the airbags are useful to reduce the effects of these accidents.

1.3.2 Responsibilities to take charge of inadequacies of other technologies

Besides they have to overcome the user failures, the embedded real-time software applications now have to take charge of unacceptable effects of the other technologies used in the product. These effects are due to characteristics of hardware technologies such as the ageing. For instance, the software application has to adapt its behaviour to the deteriorated states, or sometimes the failures, of the external hardware components. For example, to respect acceptable emission levels, embedded programs have to take into account the change of the surrounding elements: deteriorated states of mechanical parts, of the hydraulic circuits, blocking of valves such as the EGR (Exhaust Gaz Recirculation).

1.3.3 Responsibilities to take charge of design faults of other components

To complete this list of new responsibilities, we must mention the fact that embedded software now has to handle design faults of surrounding elements. For instance, a car manufacturer added an ABS with an electronic braking distributor to prevent harms for a car mechanically unstable at braking time.

1.3.4 Responsibilities to act and to take decisions

Thus, more and more responsibilities are transferred to embedded real-time software applications. These delegated responsibilities at first concerned the realisation of actions decided by humans or external devices. Now, certain applications take decisions. In automotive domain, the ABS may release the hydraulic pressure to avoid the blocking of the wheels, despite the action of the driver on the brake pedal.

The complete autonomy to take decision and to realise the associated action is illustrated by the systems opening and controlling the airbags. The preservation of the directional stability of the car is another role delegated to real-time software, previously played by the driver.

1.4 Integration

A last significant changing for embedded real-time software concerns the progressive integration of these systems in products. Previously, these software applications were isolated, providing specific and independent functions. Then, they were associated with other elements of a product at first by service relationships (a master using fonctionalities offered by software applications) and finally by cooperation relationships (exchanging data). Therefore, complex interactions now exist with humans, mechanical devices or other real-time software applications.

Again, real-time systems embedded in cars provide numerous examples. They interact with the driver and the environment using sensors (temperature, pressure, position of the drive shaft or of the steering wheel, etc.) and actuators (injector or valve opening, hydraulic braking circuit, etc.). They also interact together exchanging data on the CAN bus. For instance, the system controlling the braking interacts with the engine control system, the power steering control system, the absorber control system, etc., to prevent a car to skid or to overturn. Indeed, it needs to reduce the speed, to modify the wheel direction and to harden the absorbers.

This strong coupling between an embedded real-time application and other components increases the harms caused by a failure of this application due to the contamination effects.

2. Requirements: Assurance of absence of risk

2.1 Increase in risks to increase the benefits

As described, the embedded real-time systems now have more and more responsibilities. This assignment aims at increasing the benefits thanks to software technology. In automotive domain, these benefits concern the decreasing of the pollution rate, of the accident probability or severity, and of the production costs. Everybody accepts these benefits but also has to wonder about negative effects of the potential failures of these systems.

For instance, nowadays, the steering shaft transmits the rotation of the steering wheel to the wheels. This shaft is at the origin of numerous sever injuries when an impact occurs. The replacement of this mechanical device by a software program detecting the steering wheel movement and acting on the wheels could avoid such harms. It also offers numerous other advantages as the possibility to adapt the effect on the wheels of the orientation of the steering wheel depending on the car speed, making easier the driving in cities. Unfortunately, we also can imagine the harms caused by a dysfunction of such a system, particularly when the car is running fast.

The increasing of the benefits provided by embedded real-time software also implies a harms' severity increasing if a failure occurs.

The harms concern the human injuries but also the trade. In particular, the confidence of the consumers in products may decrease strongly and may court actions against firms.

2.2 Requirements for more guarantees

The increasing of the responsibilities transferred to embedded software and the complexity of their coupling with other systems lead the citizens but also the firms, the engineers and the authorities to wonder about the confidence they can attribute to these applications, that is about the absence of the harms they can cause.

2.2.1 The citizens

The citizens use everyday products integrating embedded real-time software. They are bothered by their dysfunction and are worried about the potential harms they can cause on their health, money, etc.

Their confidence in the products realised with conventional technologies is based on a recognised know-how of the manufacturers. For instance, a client buys a car of a given trademark because the reliability of its engine was tested by previously produced models and progressively improved, or because the trademark capabilities in creating new cars are well-known. Such a situation does not exist for complex real-time software embedded in these products and the previous experiences justify the existing suspicion (car recalls for instance).

2.2.2 The firms

Firms and engineers perceived the benefits which are provided by the software technology: implementation of complex functionalities, reduced costs, etc. They are also aware of the harms which can be caused by the computing systems integrating their products: physical harms to the users and their environment but also trade harms particularly on the brand image of the firm, and financial risks due to high penalities or damages to be paid to displeased clients.

The financial proceedings against Toyota due to a failure of an embedded real-time software have to be studied as they provide a typical example. Coming from USA, we may imagine similar lawsuits in Europe in the near. Beforehand, let us specify that similar issues occurred to other/all manufacturers. However, they were generally not promoted through media. On the contrary, the problems met by Toyota were at the origin of numerous communications.

On September 1998, the ARB (Air Resources Board) of California required of Toyota the recall of 330 000 cars sold in California. The electronic system checking emissions (on-board diagnostic system) may not detect a too important gas emission and so does not signal such a situation to the driver [CEPA, 1998]. This system provides one more time an illustration of the transfer of responsibilities previously mentioned: the exceeding rate of emission has to be detected by a system and not by the car owner. The cost to repair was 250$ per car. Thus, the global cost reached more than 82 millions $. This is probably one of the reasons of the Toyota refusal to recall the cars. Moreover, the firm signalled that the involved systems received an agreement. The case was transmitted to the court of California (Sacramento).

In July 1999, at the US Environmental Protection Agency request, the US Department of Justice repeats the demand at federal level [USDJ, 1999] [OLSON, 1999]. The court records that the failure affects 2.2 millions of cars sold in USA between 1996 and 1998. It also mentions that the failure comes from a program design fault and claims more than 58 Billions $ of civil fine for the harms caused to the environment (pollution) and citizens. Finally, it requires the recall of the cars. The comments of the judgement show that the court considered the transfer of responsibilities from the driver to the software and consequently to the designer: "Companies that take shortcuts with their vehicle pollution-control systems shortchange the consumer and our environment. [...] We will hold them accountable" (Lois Schiffer, Assistant Attorney General for Environmental affairs).

2.2.3 The engineers

Engineers have a quite low confidence in the software they produce. This is shown by the huge duration spent to test their programs (often 40 to 50 % of the total development duration). This duration is, on one hand, due to the time needed to diagnose and to correct detected faults, but also, on the other hand, aims at increasing the assurance that they want to have on the product behaviour correction.

The engineers are aware of the harms which can be caused to the users but also to themselves as the user harms may have strong impacts on their careers. Indeed, the harm caused by the system is often due to a failure of its behaviour. The fault in the program generally comes from a human error of the engineers activities.

2.2.4 The authorities

The highlighted issues also concern the national or international authorities. They are faced with a dilemma.

- The demand of assurance from citizens is very high as the harms caused by embedded software failures may affect the society (pollution, health, transportation, etc.).

- The very high expenditure necessary to provide such assurance may increase the prices of the products whereas a strong concurrency exists. Some court orders may also put a brake on the development of embedded software technology.

Moreover, the non respect for assurance given to the citizens has an important political impact.

3. Solution: Certification

The Toyota issues show that, even if the harms due to embedded software failures affect each person (respiratory troubles, etc.), they have to be handled by the authorities. They must

- determine the harms and their origins to start legal proceedings against the firm, but also

- prevent these harms providing a high level of guarantee to the citizens.

This guarantee is obtained by the certification of these systems. Certification is defined as [EN4502, 1993] the procedure by which a third-party gives written assurance that a product, process, or service conforms to specified requirement. The requirement may concern various points of view. In this paper, they deal with safety, that is the absence of unacceptable risk [ISO51, 1999].

The product user is the first person interested in certification as he/she is the first affected by the harms caused by these products. Moreover, thanks to the existence of a certificate, he/she does not have to assess him/herself the potential damages these systems can provoke.

For the firms or the designers, the certification does not only provide a trade advantage. It provokes a transfer of a part of their responsibilities to the certification authority. One more time, the legal proceedings against Toyota illustrate this assertion. From 1999, Toyota signals that its failing on-board diagnosis system received a certificate from the Californian Air Resources Board, after experiments in their laboratories. Thus, Jim Orson from Toyota headquarters said in July 1999: "We [...] firmly believe our vehicules comply with the testing procedures as originally written" [OLSON, 1999]. This argument was accepted by the Californian court which decided the 24 February 2000 that the California Air Resources could not require a global recall of the 337 000 cars concerned in California [APSA, 2000]. Implicitly, this decision considered ARB as partially responsible of the pollution due to the oversight of their verification. At the same period, the federal ERA (Environmental Protection Agency) required a national recall.

Finally, in California, a settlement was signed the 7 march 2002. Toyota accepted to pay 7.9 millions $ to finance projects on environment and to increase the duration of the guarantee of their embedded systems from 3 to 14 years or from 50 000 miles to 15 000 miles. Moreover, the court does not require the callback of the 33 000 cars specifying that ARB certified the system but Toyota did not provided certain pieces of information useful to the certification process [USDT, 2002] [CEPA, 2002].

An equivalent settlement occurs at the federal court on the 7 march 2003. Toyota will spent 34 millions $ including 20 millions $ to reduce the emission of 3000 public vehicles (scholar buses, etc.) and was fined 500 000 $ [USDJ, 2003]. This amount is far from the initial 58 billions $ and the recall of 2.2 millions of vehicles required [ARB 2003]. This moderated judgement is due to the obtained certificate. However, it does not minimise the responsibilities of systems designers. Indeed, the judgement also announces clearly the future consequences if these responsibilities are not taken. Thomas L. Sansonetti of the Environment and National resources Division wrote: "Vehicule manufacturers must make all required disclosures so that EPA [Environmental Protection Agency] can carry out its responsibilities to ensure clean air. [...] This settlement makes clear that we will enforce these requirements vigorously".

4. Problem handling

The transfer of responsibilities from the user to embedded real-time software applications or the

attribution of new responsibilities to these systems, correlated with the assurance required by users may have severe consequences.

- For the designers, these features may reduce innovation: even if the benefits of software technology is well-known, the potential damages also exist. In particular, the use of recent technologies such as Object-Oriented languages arouses suspicions.

- For the firms, these features may strongly increase the cost of the products to provide the required assurance.

- For the certification authorities, these features may increase their requirements and the duration spent to attribute a certificate, to obtain more and more guarantees. This will increase the cost of the products and delayed their availability on the market.

To prevent these drawbacks, most of the proposed solutions

- concern separated domains (avionics, space, medical systems, transportation, etc.) whereas the problems are generic,

- mainly study the implementation technologies whereas numerous issues concern the system design.

The research activities started in the framework of the project "UML & Certification" aim at

- going back to the basic requirements of certification proposing a generic approach based on risk management [IS073, 2002],

- studying the risks associated with the UML modelling technology,

- examining how the risks associated with each embedded real-time software application can be expressed and handled using UML,

in order to provide to the user, the designer and the authorities assurance of the absence of risk of unacceptable harms.

5. References

[ARB 2003] Air Resources Board, "Report of enforcement activities for January 1 – December 31, 2002", July 2003.

[APSA, 2000] APSA (Automotive Parts and Service Alliance), "California Toyota Recall Overturned", Capital Report, vol. 2, n° 2, March 2000.

[CEPA, 1998] California Environmental Protection Agency, "ARB orders repair plan for 330,000 Toyota and Lexus", News Release, Air Resources Board, 2 September 1998.

[CEPA, 2002] California Environmental Protection Agency, "Toyota agrees to pay $7.9 Million settlement", News Release, Air Resource Board, 2 march 2002.

[EN4502, 1993] EN 4502, "General terms and definitions concerning standardization and related activities", CEN, Brussels, 1993.

[ISO51, 1999] ISO, "Guide 51. Safety Aspects. Guidelines for their inclusion in standards", International Standardization Organization, 1999.

[ISO73, 2002] ISO, "Guide 73. Risk Management. Vocabulary. Guidelines for their use in standards", International Standardization Organization, 2002.

[OLSON, 1999] CNN Web site, "Government suit alleges faulty emissions computers seek $58.5B", http://money.cnn.com/1999/07/12/home_auto/toyota/, 12 July 1999.

[USDJ, 1999] US Department of Justice, "U.S. sues Toyota for clean air act violation claims 2.2 millions cars have illegal emission control monitoring systems", Washington DC, 12 July 1999.

[USDJ, 2003] US Department of Justice, "United States settles clean air act cases against Toyota", Washington DC, 7 march 2003.

[USDT, 2002] US Department of Transportation, "Toyota CARB reach OBD settlement", Federal Highway Administration, 20 march 2002.