ELECTRONIC AUTOMOTIVE REQUIREMENT DESIGN SPACE
A Bird's Eye View of a Strategic Requirement Design Space Exploration

Liliana Díaz-Olavarrieta, David Báez-López
Fundación UDLA. Puebla, Dept. Electronics and Communications, 100 Sta.Catarina Mártir, San Andrés, Puebla, Mexico

Keywords: Automotive Requirements Specification Design Space, Strategic Consistency, Specification Completeness, Distributed Systems, Real-time Systems, Communications & Control Automotive Networks, Fault Tolerance, Time-triggered protocols, Event-triggered protocols, Safety Critical Applications, User-centered.

Abstract: The purpose of this article is to make a holistic compilation of many different types of requirements for an automotive electronic communications / control network (though the framework is in itself more generally applicable), and organize them into an easily reusable framework. Requirements have to be correct, consistent and complete. The issue of correctness of the specification should be dealt with formal validation models. The issue of consistency can be handled through domain expert specification reviews. The completeness issue can be dealt with by comparison with a reference, and this paper proposes a metamodel to help with the completeness and strategic consistency issues in the requirement specification process. The requirements framework proposed in this paper aims to answer the question: "What is the requirements design space for an automotive electronic communications network?", and help in the completeness of the requirements specification through a holistic, multi-perspective, Bird's Eye View. The main perspectives that will be examined in this requirements design space exploration are four: a) The "Nature of the User" perspective, b) The "Nature of the Application" perspective: Distributed, Real time, Safety-Critical applications, and Resource Constraints requirements, c) The "Nature of the Process Development" perspective, in particular, the component based development (CBD) process of Electronic Subsystem Design within Automotive Companies: component *architecting*, component *assembly* and component *provisioning*, and d) The "Nature of the Industry" is given by the competitive environment: Suppliers, Substitute Products, Substitute Technologies, Competitors, Potential Industy Entrants, the Company and its Clients.

1 INTRODUCTION

The global demand for vehicle electronics – which are distributed, heterogeneous, real time systems- is forecast to reach nearly $75 billion by 2005, and the percentage of automotive electronics cost in 2010 will grow from 12 % to 30 % of a mid-range car's total cost (Mayer, 2005). The design and implementation of heterogeneous, real-time, distributed systems is a complex, knowledge intensive, problem. The design of embedded electronic distributed real-time systems for automotive applications, even more so. The complexity comes not only from the electronics, but from all the non-electronic automotive parts which interact with, and constrain, the electronic systems.

The automotive electronic control applications range from non-critical comfort level functions such as doors, lights, mirrors, window and seat control, to critical-safety applications (where human life is at risk if the electronic system fails) or image-critical functions, such as being able to get into a locked car through the door. In critical activities, generically *X-by-wire* applications, (Kopetz,1995), taking their name from the first "Fly-by-Wire" (FBW) Aircraft systems, fault-tolerance has to be guaranteed. The first all digital FBW application without mechanical backup was the F-8 military aircraft (1972), while the first commercial aircraft, which entered service in 1988 with Fly-by-Wire technology, was the A320. At Boeing, research on FBW prototypes began in 1986 led by GE & Allied Signal, and the first full FBW civil commercial aircraft was the Boeing 777 (1995), and used the fault-tolerant SafeBus™ protocol (Rushby, 2001), and had 3 primary flight computers, 3 completely redundant physically and electrically separate ARINC 629 Databuses, 4

Díaz-Olavarrieta L. and Báez-López D. (2005).
ELECTRONIC AUTOMOTIVE REQUIREMENT DESIGN SPACE - A Bird's Eye View of a Strategic Requirement Design Space Exploration.
In *Proceedings of the Second International Conference on Informatics in Control, Automation and Robotics*, pages 147-153
DOI: 10.5220/0001191001470153

Actuator *ECUs*, Sensors, and an Airplane Information Managemtent System (Ong, 2003).

In contrast, a high-end automobile today has more electronic functionality than a fault-tolerant aircraft had a decade ago: a BMW Mini Cooper, has between 7 and 23 *ECUs* (Electronic Control Units) depending on the configuration, with a higher degree of integration (Mayer, 2005), used for both critical and non-critical applications. As there are opportunities for electronic design functionality increase in the automobile, there are also completeness specification challenges and questions:
How does one ensure the requirements' completeness, consistency and correctness?
What are the user's expectations and service trends that one should consider?
How can one produce a "strategically consistent" automotive requirement?
What is the best way to categorize *non-critical*, or *Y-critical* applications? (Y= safety, image, cost with the highest priority).
What automotive electronic requirements are derived from external (to the company)/ internal perspective analysis?
How can one make a probabilistic, context-customizable, priority-based decision?
What communications protocol subset is appropriate to comply with the specification, among the automotive protocols available?
This paper attempts to give answers to the first three questions above, while the remaining issues will be addressed in other papers.

The requirements framework Bird's Eye View meta-model proposed in this paper aims to answer the question 1) What is the requirements design space (taken from different perspectives) for an automotive electronic communications network?

This is the first phase in the design of an application, and the problem of matching a subset of protocol communications to a given probabilistic, priority oriented, context customizable requirement specification.

The paper is organized as follows: *Section 2* presents Requirements Analysis: Perspectives and Design Space Exploration; *Section 3* will present a brief overview of In-Vehicle Networks, Standard and safety-critical automotive protocols; *Section 4* presents the USER requirements perspective; *Section 5* presents the APPLICATION requirements. *Section 6* presents the (CBD) Company Development Process perspective and finally, *Section 7* presents the INDUSTRY perspective. In *Section 8* we present Conclusions, *Section 9* are the Acknwoledgements and Section 10 includes the Bibliography used.

2 REQUIREMENTS ANALYSIS: PERSPECTIVES AND DESIGN SPACE EXPLORATION

The analysis of requirements will be done through a user-guided perspective kaleidoscope, with the high level bird's view perspective inspired from competitive business analysis (Porter, 1988), and the lower requirements perspective driven from safety critical and non-critical applications. The four main requirements perspectives to examine are:
1) USER: Requirements derived from the Client himself/herself, or Market Specific User Resource Constraints (i.e. Selling Cost, Speed Limits, Market Trends, Financing, Re-configurability);
2) APPLICATION: Requirements derived from the Nature of the Application: Distributed, Real time, Safety-Critical, Resource Constraints (Standards, Regulations, Supplier Offerings);
3) COMPANY Requirements derived from the *CBD*-based (CBDP, 2005) Automotive Component based DESIGN & DEVELOPMENT PROCESSES.
4) INDUSTRY: Requirements derived from the automotive industry competitive environment according to Michael Porter's Competitive Strategy model (Porter, 1988).

The exploration of the *requirements design space* is the first step to design user oriented electronic automotive control applications. The design of a specification requirement for an application is the second step, and once the requirement specification has been decided upon, a designer must match the application requirements to a small subset of communications protocols, to implement the *IVN*.

3 IN-VEHICLE NETWORKS (IVN)

There are more than 42 protocols (proprietary or standard) and structural topologies (nominally called "busses") for in-vehicle communication and control networks and industrial applications in different categories. There are Emissions/Diagnostics, Mobile Media and "X-By-Wire" protocols, which are used for different applications within the automobile sector (*Automotive Buses*, 2005). Also by speed there are SAE's Class A (low speed applications, bit rate < 10 Kb/s), Class B (medium speed, between 10kb/s and 125 kb/s for general information transfer), Class C (high speed, bit rates higher than 125 Kb/s), and Class D protocols (for speeds > 1 Mb/s) -though there are no SAE implemented Class D protocols (Bell, 2002). Only those automotive protocols with standard potential are considered below.

3.1 Standard Automotive Protocols

There seems to be a growing consensus within the industry that the communications protocols that will prevail are amongst the following selected few:

LIN (Alford, 2003), (LIN, 2005), CAN and derivatives: L-CAN, CAN, TT-CAN (TTTech, 2004), FTT-CAN (Flexible TT-CAN), TTP/A or TTP/C (Kopetz, 1995), FlexRay (FlexRay, 2004) and MOST (Kibler, 2004).

3.2 Safety-Critical Protocols

An important distinction to match a protocol to the application is if the protocol is apt to implement a safety-critical fault tolerant application. There is a general opinion that time-triggered protocols are better suited than event-triggered protocols for safety-critical applications (Kopetz, 2003). CAN, LIN, and FlexRay are event triggered protocols, and TTP, TT-CAN, FTT-CAN, MOST and FlexRay are time-triggered protocols such as. TT-CAN and FlexRay carry identifiers, like event triggered protocols, while FlexRay and FTT-CAN can both handle time-triggered and event triggered transmission. However, the only protocols which are accepted as fault-tolerant for safety-critical applications are: TTA/TTP and SAFEBus™, (used in the avionics and automotive industries), SPIDER (non-commercial), and FlexRay (Rushby, 2001).

The first view in the requirements design space is the user perspective, considered below.

4 USER REQUIREMENTS

Imagine we arrive walking to a high-end car. An RF wireless signal will be used to inactivate the alarm system, and this event will trigger the opening of the locks wirelessly and remotely, with an RF signal, before a chivalrous virtual agent opens the car door automatically for you. Placing the key on the ignition, the person detector identifies the driver and adjusts the seat height, distance to pedals, and wheel tilt. Then, the window manager decides if it should open the roof window (only if it is not raining), and the light manager decides if the interior lights should be turned on or not at all, while activating the "back massage with seat-belt" feature. The CD/DVD player will set itself to the latest interrupted song position, or ask you verbally what type of song you want played from the iShuffle™ /iPod™ FireWire cable you just connected into the IDB 1394 network. A speech recognition system will transform your answer into a command to the Dolby surround music system, while the *IVN* is receiving my finger´s destination point on a GPS/Galileo Navigation Map, and trying to compute the best route to get to my destination. Meanwhile, I may plug my Bluetooth enabled PDA/Cell phone to download to a "navigating secretary" my day's client visit agenda, while it finds the best scheduling and routes to match the agenda, calculates approximate arrival time, and automatically calls my clients and schedules an arrival time. Then, I download the shopping list from my PDA and send it, with a push-of-a-button, to the nearest Bluetooth discovered supermarket, so that the groceries are sent to my house before I arrive home to cook at lunchtime.

This is but one imaginary use case of the myriads of one-of-a-kind scenarios we can think of, which require interaction of the IVN with external communication networks and which we cannot use directly as a specification, unless it represents a "generic user", defined by the strategic direction of the company, as the "market target". In order to approach a "generic, reconfigurable" use case, and translate it to a UML model, we may categorize the use scenario as:

Goal-Driven Use Cases: Defined by hierarchical successive refinement of the goals and sub-goals.

Context-driven Use cases: Sub-goals are reviewed in the light of differing environment or context scenarios such as Weather, Traffic Situation, Control Lever, Brake Position, Accelerator position, to refine use cases for the distinct context scenarios.

Reconfigurable (Both in Goal and in Context) Parameterized or flexible use cases, to form the "generic" strategically consistent use case to define the "target market segment" user requirements. These "more generic" IVN requirements can be inspired in service extension models such as the "UMTS 5Ms" model, explained below.

4.1 A User Trend Example: 5M's

User expectation trends in terms of service for multimedia wireless communications –voice, data, video- have been named by the 3G UMTS Forum as the "*UMTS" "5Ms* for Service Extension": Movement, Moment, Me, Money and Machine:

Movement: To escape a Fixed place, a memory, virtually and literally in a car, while keeping connected. A recurrent user requirement is to be always connected to the large variety of LANs, WANs, MANs, and global external networks to enable personal mobile communications, such as Bluetooth,WiFi (802.11), GSM/GPRS/EDGE or any of the 5 versions of the IMT-2000 standard for cellular voice, data and multimedia.

Moment: Comfort Function Control to improve the experience of present and Moment. Also, to expand the concept of time, from Discrete to Continuous / Past, present, future / Scenarios / Experiences into the Memory. Memory is enabled with emotion, and emotion with sense involvement. Appeal to the 5 senses (eyes, ears, taste, smell, touch) to create a better "moment" or "infotainment" experience. Eyes: Digital TV, in the shape of DVB-H, an open industry standard for the delivery of mobile broadcast digital TV, via satellite; Ears: DAB: Digital Audio Broadcast / Music download capability; Eyes/Ears/Touch: Entertainment Multimedia applications for collaborative and interactive games, video streaming. Taste/smell is still open to new "better moment" creation, and New Magic Worlds applications. ("Mobile Virtual" on the road Eating/Drinking/Smelling experiences?)

Me: The person and its expansion to a Community. Shared Access / Interactivity / Authentication / Shared Interests. Interactive Gaming or Collaboration. The car as a member of a community of services. Branding and Self-configurability, as expression of oneself, not only of "settings", but car "look" and functionality, based on electronic added-value The car as a personal extension of home or office, with Business Broadband Internet capability for Videoconferences and mobile Multi-site virtual meetings.

Money: Financial Services. Requires Wireless Security / Heterogeneous Networks / Broadband Anytime. Allows E-mobile commerce. Banking mobile applications, which also have to be made fault-tolerant and safe, a challenge with wireless connections implicit in the mobile car status. Money means also Cost to the User, in life-cycle terms (acquisition cost, operation, maintainability, insurance - prices should be lower for certified fault tolerant cars-, disposal/ recycling cost). Cost for the company is considered in the Industry perspective.

Machine: Empowering Gadgets & Devices. Added Processing Intelligence, with Power availability, and a "universal dock connection capability" to connect *PDAs,* Tablets, *iPods*, and charge Cell phones, will justify the trend towards a 14V/42V power network in future cars (Leen, 2002). Another machine trend is the automobile as an intelligent set of services, on a mechanical support "envelope". This would enable the design of Active Safety / Intelligent automobile systems such as Telematics, and *adaptive* electronic steering, braking or other power-train control applications - with augmented proactive safety and predicting capability to take over the driver in case of danger (falling asleep and approaching an obstacle too closely).

5 NATURE OF THE APPLICATION

In the context of Automotive Communications and Control Electronic Subsystems, the four characteristics that emerge as defining the "nature of the application" are: 1) the *distributed* nature of the network, 2) The *real time* application requirements for some of the subsystems, 3) The *safety-critical* requirements for X-by-wire applications, for example, and 4) The *Resource Constraints*, which is derived from the implementation of the application. We examine, briefly, the "application nature" below.

5.1 Distributed Networks

A distributed network (Kopetz, 1997), (Tanenbaum, 2002), (Coulouris, 2001) is usually recognized because there are *concurrent processes* running in parallel on various processors, there is a *distributed memory or shared state*, and *data is communicated* through an *interconnection medium* (copper, fibre or wireless link) that links the *multiple processors and the storage recipients*, be they volatile or non-volatile, or stable storage (a mixture of both).

Concurrency of processes over a distributed network implies that communication and access to the controllers has to be arbitrated. Concurrent can be either *programmed* and *without contention*, such as in TDMA, FTDMA, FDMA, CDMA access schemes, or random assigned schemes with resource contention and possible collisions, such as in CSMA/CD/CA/CR or DAMA (Demand Assigned Multiple Access).

Independently of its classification, a distributed network implementation should be "invisible" to the user, i.e., the system should be *transparent* in the way processes *communicate*, the way they are *scheduled* and *synchronized*, independently of what functionality the interconnected *ECUs* have. We expand on these three requirements below.

5.1.1 Transparency

The transparency requirement means that the user should not be able to distinguish between the performance of a uniprocessor central controller architecture, and a multiprocessor distributed architecture, except perhaps for increased efficiency. Various types of transparency that can occur are the following:

Access: Local and Remote Resources are accessed using identical operations

Location: Users cannot tell where HW and SW resources are located

Migration - Mobility: Resources should be able to move without having their "names" changed.
Replication: System replicates critical data, without the user noticing it, for increased performance and reliability.
Concurrency: Users- processes will not notice the entry of other users in the system, even if they share the same resources.
Failure: Failure transparency implies fault independence, fail-silence, fail-operational, and fail-safe modes, so that if one part fails, the whole system does not come to a halt.
Performance: Load variation should not lead to performance degradation.

5.1.2 Inter-Process Communication

The separation of concerns between the Functionality of Processes vs. their Communication (which also require Scheduling and Synchronization among them) is an important requirement for later reusability of the designs.

All four types of behavior: function execution in controllers, synchronization, scheduling and finally the communication itself, take time. That is, one should consider realistic delay assumptions for communication (sending messages across an interconnect network) due to signal propagation delays, processor "interpretation", execution of processes, synchronization and scheduling delays. This means that during model simulation of an intended application, realistic delay assumptions have to be included in an imported zero delay ASCET-SD (ETAS, 1998), model and re-simulated, as is done, for example, in the VCC –Virtual Component Co-design- tool (Demmeler, 2001).

5.1.3 Inter-Process Synchronization

There are two types of process synchronization: a) synchronous or periodic, also called Time-triggered and b) asynchronous or aperiodic also called Event-triggered, (where specific Event signals act as the triggers to change state).

Inter-process synchronization is obtained by a global clock for time-triggered protocols, and by an arbiter, a "bus guardian" or "central guardian" (using the FlexRay or TTP terminology) which controls the handshaking communication for an event-triggered protocol. In both cases, there is a structural entity, the clock generator, in the synchronous case, or the arbiter, in the asynchronous case, which implement the synchronization. For process synchronization, it is important to schedule the order and timing of access to the network, through Inter-process Scheduling.

5.2 Inter-Process Scheduling

Scheduling amongst processes refers to the way tasks or processes are prioritized to give a fair share of access to all the processes from *ECU* nodes to the shared distributed, interconnection network. Depending on the topology, there exist centralized (i.e. Daisy-chain) and distributed scheduling algorithms (i.e. Token passing methods).

Concurrency of processes over a distributed network implies that communication and access to the controllers has to be arbitrated. Concurrent access is made through the shared medium –copper, fibre, wireless- and can be either *programmed* and *without contention*, such as in TDMA (TTP), FTDMA (FlexRay), FDMA (Bluetooth), CDMA (WCDMA -3G cellular), or minislotting access methods (used by ARINC 629, and Byteflight), or *random* assigned schemes *with resource contention* and possible collisions (CSMA/CD/CA/CR or DAMA (Demand Assigned Multiple Access) -CAN.

These access schemes motivate a triggering classification for protocols, related to the synchronicity or *periodicity of events*: time-triggered or synchronous, or periodic protocols, vs. event-triggered, or asynchronous, or aperiodic protocols.

This classification is not the only one, as we can also classify protocols by their *push/pull* characteristics, *periodicity*, and *message broadcast mode* (Kopetz, 1997) or by their *message broadcast mode* (one to one, one to many, many to one, and many to many) (Kopetz, 1997). Client initiated transactions are called *push oriented* while server initiated transactions are called *pull oriented*. Whatever the category, they may be in Real-Time.

5.3 Real-Time Requirements

Real – time requirements are sometimes also part of the distributed applications nature of the information required. When this is the case, it is often related to Safety Critical applications (Kopetz, 1995), (Dilger, 1997), (Merceron, 2001). Here, we only list the requirements implicit in the Real time Nature of an Application (Kopetz, 1995), due to space constraints, stressing its importance: Timeliness of Response, Protectiveness, Real-time Scheduling, Real-time Communication, Clock Synchronization, Membership Services, Composability, Error-Detection, Robustness, Fault Independence /Tolerance, Faults and Failure Modes for Safety-critical applications in the Automotive Industry.

6 CBD: DEVELOPMENT PROCESS

A *CBD (Component Based Design Process)*, typical of the automotive industry, consists of (CBDP, 2005): *component architecting* (specifying to second-tier development firms in the semiconductor business and constructing their own design*)*, component *assembly* (parts provided by first-tier suppliers such as Bosch, Siemens and Magneti-Marelli) and component *provisioning* (often by third parties) to form subsystems with ICs from Motorola, Texas Instruments, Hitachi & ST Microelectronics.

7 NATURE OF THE INDUSTRY

The automotive industry has a competitive context made of (Porter, 1988): Suppliers, Substitute Products-Technologies, Competitors and Potential Entrants, Clients (considered in User Requirements), and the Company itself, which have to be analyzed to search for industry context imposed requirements.

Furthermore, the "Nature of the Industry" can be static or dynamic (trends and direction). The static perspective from a strategic point of view considered was developed by Michael Porter (Porter, 1988) to analyze the competitive environment of a company in a given industry. The dynamic model considers each of these views and their evolution in time, and should also be considered to produce strategically relevant, scalable and updateable automotive *IVN*s.

8 CONCLUSIONS

This paper has introduced a novel, holistic "automotive requirements meta-model" to analyze requirements for the design of a distributed, (sometimes real-time), (always) heterogeneous system, for (safety-critical) user functions and create complete, strategically consistent requirements, viewed from four different perspectives: User, Application, Development Process and Industry.

ACKNOWLEDGEMENTS

The authors would like to acknowledge support from CENTIA/DIP, & UDLA Electrical Engineering Dept.

REFERENCES

Alford, C., Paskvan, J., 2003. *"Local Interconnect Network: Hands-on LIN Training",* retrieved March 2005, from Volcano Automotive Group Website.

Automotive Buses, 2005. "Logic Design Information: Automotive Buses", retrieved Feb 4, 2005 from http://www.interfacebus.com/Design_Connector_Automotive. Bell, J., 2002. "*Network Protocols used in the automotive industry*", Doc. Ref SD/TR/PRO/01, July 24. 2002.

Byteflight, 2005. Available at http://www.byteflight.com/

CBDP, 2005. "*Chapter 30 - Component-Based Development*", SEPA 6/e, Downloadable Reference Library, available from http://www.rspa.com/reflib/CBSE.html, April 2005.

Coulouris, G., Dollimore, J., Kindberg, T., 2001. "Distributed Systems – Concepts and Design", Addison Wesley Publ. Comp., 3ed., 2001.

Demmeler, T., Giusto, P., 2001. "*A Universal Communication Model for an Automotive System Integration Platform*", IEEE Proc. 1530-1591/01, pp. 47-54, 2001.

Dilger, E., et al., 1997. "Towards an Architecture for Safety Related Fault Tolerant Systems in Vehicles", On-line document available at http://www.vmars.tuwien.ac.at/projects/xbywire/projects/new-esrel97.html

ETAS GmbH, 1998. "Whitepaper ASCET-SD, ETAS GmbH, 1998", mentioned (Demmeler, 2001) above.

FlexRay, 2004., "*FlexRay Communications System, Protocol Specification, Version 2.0*", June 2004, retrieved on February 1, 2005 from FlexRay site at http://www.flexray.com/specification_request.php.

Kibler, T., Zeeb, E., 2004. *"Optical Data Links for Automotive Applications",* IEEE Proceedings Electronic Components and Technology Conference, pp., 1360-1370, 2004.

Kopetz, H., 1995. "*A Comparison of CAN and TTP*", available from TTTech website: http://www.tttech.com/technology/articles.htm

Kopetz, H., 1997, "*Design Principles for Distributed Embedded Applications*", Kluwer Academic Publishers, 1997.

Kopetz, H., 1998, "*TTP – A New Approach to Solving the Interoperability Problem of Independently Developed ECUs"*, On-line Document Available from http://www.vmar.tuwien.ac.at/projects/xbywire/projects/new-ecu.html, on February 1st, 2005.

Kopetz, H., 2003. "*Fault Containment and Error Detection in the Time-Triggered Architecture*", Proc. of the Sixth International Symp. On Autonomous Decentralized Systems (ISADS´03).

LIN, 2005. Local Interconnect Network protocol website available at http://www.lin-subbus.org/.

Mayer, A., 2005, "*Innovation is accelerating in the Automotive Electronics*", Compiler, retrieved from http://www.synopsys.com/news/pubs/compiler/art1lead_bmw-1101.html

Merceron, A., 2001. "*Proving "no Cliques" in a Protocol (TTP/C)*", IEEE Proc. 1530-0900/01, pp. 134-139.

Ong, E., 2003, "From Anonymity to Ubiquity: A Study of Our Increasing Reliance on Fault-Tolerant Computing", MIT SERL, NASA Goddard OLD Presentation, Dec. 9, 2003.

Porter, M., 1988. *"Competitive Strategy",* Free Press Ed., 1988.

Rushby, J., 2001. "*Bus Architectures for Safety-Critical Embedded Systems*", Proceedings of EMSOFT 2001, 8-10, Oct. 2001, Lake Tahoe, CA. Springer-Verlag LNCS

Tanenbaum, A.S., Van Steen, M., 2002. "Distributed Systems", Prentice Hall International, 2002.

TTTech 2004, "CAN/TTCAN – Byteflight-FlexRay-TTP: Technical Comparison of protocol properties with a focus on safety-related applications", PPT presentation available at TTTech Website on http://www.tttech.com.