



Cost Efficient Dependable Electronic Systems

Cost Efficient and Dependable: CAN in Advanced Applications

Author Carl Bergenhem, Håkan Sivencrona

Document number 003

Date 28 June 2005

Availability Public
Status Final

Cost Efficient and Dependable: CAN in Advanced Applications

Carl Bergenhem

Dept. of Electronics and Software, SP Swedish
National Testing and Research Institute,
Borås, Sweden
carl.bergenhem@sp.se

Håkan Sivencrona

Mecel, Delphi Corporation, Automotive
Systems, Gothenburg, Sweden
hakan.sivencrona@mecel.se

Abstract

Today, CAN is the most common communication principle used in the automotive area; the main reason being that it is cost efficient. However, is it still possible to use CAN, with its limitations, in the large number of emerging safety-critical applications? Is it possible to achieve cost efficient systems without sacrificing dependability? Is it possible that increased dependability can be realized by enhanced capabilities such as new fault detection algorithms? Without further development, CAN must soon retire. The goal of this fast abstract is to present research ideas that may allow CAN to continue to be used and be applied for more advanced applications.

1 Introduction

Embedded systems, used for control of advanced applications, are continuously growing in complexity with lower dependability as a result.

Although CAN [1] is by far the most common communication paradigm used by the automotive industry today, it does not seem to be the optimal solution for the coming situation.

However it would be interesting to investigate whether new algorithms and capabilities, could cost efficiently increase the life cycle of CAN with required dependability even for more advanced applications.

This fast abstract intends to present interesting issues to be investigated further. First we briefly explain the rationale behind our initiative and present some related research which will serve as the input. Then we will present the directions for research that we propose and finally draw early conclusions.

2 An improved CAN

By enhancing CAN, new applications can be implemented either by adding software or hardware mechanisms. Fig. 1 shows that CAN is more cost efficient than time-triggered alternatives, for applications with low function complexity. Our goal is to show that this also holds for applications with medium functions complexity, provided that CAN is enhanced with further capabilities to be dependable enough. The “cost

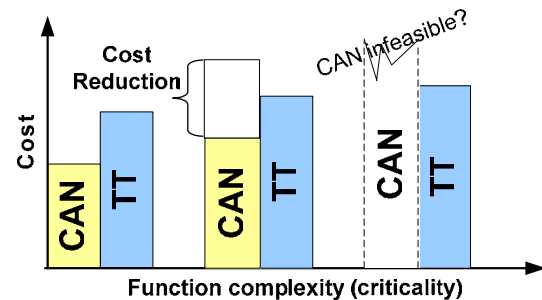


Fig 1. Cost vs. function complexity in the new vs. old platform. Please observe that these plots are estimates.

reduction”-term is the assumed cost cut by using an enhanced CAN in applications with medium function complexity (centre bars). If the introduction-cost for a new time-triggered platform is taken into account, the advantage for CAN would supposedly be greater. Without enhancement, CAN is not dependable enough, and too costly, to be used in advanced applications.

Because of the uncertain number of “high spec” vehicles that will be produced, the centre bars in Fig. 1, it is unsure how many that actually require the capabilities of a new platform. This implies surplus cost for “low spec.” vehicles, the left-hand bars, since manufacturers wish to use the same platform in all models. This means that the shift to a completely new platform should be taken in smaller steps: Evolution rather than revolution.

Despite advances made in time-triggered networks such as TTA (www.ttagroup.org) and Flexray (www.flexray-group.com), another key issue is that new technology must find acceptance and maturity in industry. Here the case is not purely technological but also aspects such as return on investment and “follow-the-leader” are involved.

We acknowledge that CAN does have an upper boundary on function complexity in the application, indicated by the right-hand bar in Fig. 1. The question that we pose is where this boundary is?

3 Related research

The DECOS, Dependable Embedded Components and Systems, (www.decos.at) and IMA, Integrated Modular Avionics, (see [2]) initiatives, address aspects of how large and complex integrated and distributed systems with multiple functions should be designed to meet high requirements on dependability. The IMA initiative uses

processor partitioning to improve the fault isolation of complex systems.

DECOS intends to develop the necessary technology to allow a smooth shift from the traditional federated to integrated architectures. This must eventually be done in order to reduce development, production and maintenance cost of future systems as well as to achieve required ultra dependability of embedded applications and systems. Earlier concepts, such as CAN, can co-exist within a DECOS network.

Our research initiative, CEDES, Cost Efficient Dependable Electronic Systems (www.cedes.se), addresses the requirement of dependability in electronic systems with the added constraint of cost efficiency. The concept of “lean redundancy” implies that a dependable application should take advantage of replication of components that already exist in the architecture or is inherent to the application.

4 Proposed research

We will study software-based mechanisms, which require minimal redundancy in hardware to achieve the required system safety. With the theme of lean redundancy, acceptable levels of dependability can be maintained by software and only minimal additional hardware. An example is nodes (ECUs) in a vehicle. The various nodes are not necessarily identical but have resources similar enough to provide coverage in presence of faults. A software mechanism that functions together with CAN is required to achieve the goal.

A typical system with inherent redundancy, that will be studied, is a brake-by-wire (BBW) system with nodes at each wheel. All nodes are wheel-nodes but at different positions. If one node fails, another cannot replace it directly but can compensate for the loss of its function and thus a graceful degradation may take place (i.e. safe braking). This requires that the nodes monitor each other and are notified about failure. When a failure is detected, the software in the distributed application (BBW system) adapts its function to the new situation. The application itself will, however, not be part of our research.

How can node monitoring help to solve the dual goal of cost efficiency and dependability using CAN? We will investigate if node monitoring, briefly described above, can be designed around CANELy [3], possibly updated with further capabilities for node monitoring. A goal is to show that CANELy can be used to take advantage of an inherent redundancy in a distributed architecture, such as the application example described above.

To answer the research questions, experimental verification of the monitoring function will be performed. We plan to implement a fictive automotive application using GAST-boards (www.chl.chalmers.se/gast/). These boards implement

several different communication concepts, time and event triggered, e.g. CAN, TT-CAN and TTP. The application may be a simple BBW system as described above. The most important part of the application will be the implementation of a node monitoring protocol, based on CANELy.

A important goal is to verify and validate the function and dependability of the node monitoring protocol in presence of arbitrary and byzantine faults will be done using fault injection, e.g. HIFI [4] and injecting faults into frames on the CAN-bus in real-time.

5 Discussion and Conclusion

The CEDES project encompasses the briefly described areas and has just been initiated. Therefore it is too early to draw conclusions. The research directions have been defined in several work packets that have the theme of lean redundancy. The main areas are: software, hardware, and formal methods. Parallel to this, suitable development processes are researched.

We foresee that protocols such as CANELy and the proposed monitoring function will have an important role of extending the usability of CAN in critical applications. Because of the criticality, it is vital that new features be verified and validated.

6 Acknowledgments

This research will be conducted within the project CEDES, which is funded by the Swedish industry and government joint research programme IVSS - Intelligent Vehicle Safety Systems.

7 References

- [1] International Standards Organisation. ISO 11898. Road vehicle – Interchange of digital information – Controller area network (CAN) for high-speed communication, 1993.
- [2] J. Rushby, “Partitioning in Avionics Architectures: Requirements, Mechanisms, and Assurance,” Draft technical report, Computer Science Laboratory, SRI International, Menlo Park, CA, Oct. 1998.
- [3] J. Rufino, P. Verissimo, G. Arroz, “Node Failure Detection and membership in CANELy”, Proc. of the 2003 International Conference on Dependable Systems and networks (DSN03), San Francisco, California, USA, Jun. 2003.
- [4] H. Sivencrona, P. Johannessen, J. Torin, “Protocol Membership Agreement in Distributed Communication System – A Question of Brittleness”, SAE World Congress, Cobo Center, Detroit, Michigan, USA, Mar. 2003.