Towards Understanding the Sensitivity of the Reliability Achievable by Simplex and Replicated Star Topologies in CAN

Manuel Barranco, Julián Proenza
Dpt. Matemàtiques i Informàtica. Universitat de les Illes Balears, Spain
manuel.barranco@uib.es, julian.proenza@uib.es

Abstract

Star-based field buses are gaining importance in the context of highly-dependable systems. However, although the error-containment and fault-tolerance capabilities of different stars have been evaluated, no one had appropriately quantified the system dependability benefits stars actually yield. Thus, in previous work, we quantitatively demonstrated, for the case of CAN, that a simplex and a replicated star called CANcentrate and ReCANcentrate can improve the system reliability when compared with a bus. However, we characterized all the dependability-related aspects of the system and the network to favor whenever possible the bus; except in one case, in which we studied the benefits of the simplex star over the bus depending on the error-containment capabilities of the nodes. Thus, to completely understand the full potential of stars, it is still necessary to assess how variations in each one of those aspects affect the reliability achievable with them when compared with the bus. This paper presents two of the set of analyses we are carrying out in this direction.

1 Introduction

In the context of highly-dependable critical systems, some field-bus protocols are shifting from bus to star topologies, given the dependability capabilities stars can provide [10], e.g. resilience to spatial-proximity and common-mode failures, error containment and fault tolerance. This is the case of TTP/C [2] and FlexRay [1] among others. Moreover, given the growing interest on improving the dependability of the Controller Area Network (CAN), e.g. [8], we have proposed a simplex and a replicated CAN-compliant star topologies respectively called CANcentrate and ReCANcentrate [4] (collectively referred to as (Re)CANcentrate).

The hub of CANcentrate couples every non-faulty node contribution in a fraction of the bit time, thereby being transparent to the nodes while providing error-containment. Specifically, the hub is able to detect and isolate, at the corresponding port, faults that compel any node or link to generate stuck-at-recessive, stuck-at-dominant or bit-flipping streams [4]. As concerns ReCANcentrate, it can be basically considered as a replicated CANcentrate star with two hubs (Figure 1) interconnected by means of at least two interlinks [4]. Both hubs couple with each other in a manner that forces them to broadcast the same value bit by bit, thereby creating a single logical broadcast domain. Each

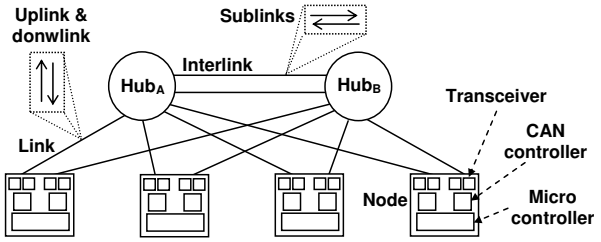

Figure 1. ReCANcentrate architecture

node connects to this domain by means of two independent CAN controllers, each of which attached to a different hub. These features make ReCANcentrate tolerant to faults affecting one of the hubs (no matter which), several interlinks, and one of the connections (which are constituted by cables, connectors, transceivers and one communication controller) of each node to the hubs.

All the work that has been done on star-based field-bus infrastructures such as (Re)CANcentrate relies on the commonly accepted idea that stars do actually improve dependability. Certainly, there is plenty of work on fault-injection tests that demonstrates the efficiency of the error-containment and fault-tolerance capabilities of stars, e.g. [2]. However, we identified in [6] that previous mathematical analyses of star and bus topologies do not adequately elucidate, in a quantitative manner, whether or not these capabilities compensate the reduction of dependability derived from the extra hardware complexity of stars. Thus, in order to fill this gap in general and for the case of CAN in particular, in previous work [6] [5] we modelled and quantified the reliability of equivalent systems relying on CAN and (Re)CANcentrate. Reliability was chosen because, together with safety, it is one of the dependability attributes of main concern in critical systems.

Reliability is defined as the probability with which a system continuously delivers its intended service throughout a given interval of time [12]. In the case of a distributed control system, the reliability depends not only on the probability with which nodes operate, but also on the probability with which they communicate among them. Thus, in order to include the contribution of the underlying communication infrastructure on the system reliability, we defined two metrics in [5] called NFTAR and FTAR$_k$ (previously referred to as the PNS in [6]). The first one corresponds to the reliability of what we call *non-fault-tolerant-accepting* (NFTA) systems, which are those that can only deliver its services as long as all their nodes are not faulty and can communicate with each other. The second one is the reli-

 doi:10.1109/ETFA.2011.6059166

ability of what we call *fault-tolerant-accepting* (FTA) systems, i.e. those that can correctly operate even if up to k of N nodes are faulty or disconnected from the rest of the system, because those failures are either tolerated or simply accepted. We are specially interested in FTAR_k for $k = 1$, i.e. in the reliability of systems that accept or tolerate up to 1 node failure or disconnection, as this value of k is the one that intuitively yields the least benefits for stars [3]. Note that these metrics differ from the well-known concepts of *all-terminal* and *k-terminal* reliability, which generally exclude the reliability of the nodes themselves [12]. Furthermore, the FTAR is a more general metric than the k-terminal reliability, as the FTAR does not distinguish which are the nodes that must communicate with each other for the system to be non-faulty.

Results demonstrated that when compared with CAN, CANcentrate improves the FTAR [6], whereas ReCANcentrate yields benefits in terms of both NFTAR and FTAR [5]. Moreover, our models include parameters to characterize several dependability-related aspects. We used these parameters to assess the sensitivity of the NFTAR and the FTAR with respect to the number of nodes [6] [5] and, in the case of CAN and CANcentrate, also with regard to the error-containment capabilities of nodes [6]. However, in order to completely understand the benefits of stars in field-buses such as CAN, it is still necessary to carry out sensitivity analyses with respect to other important parameters, e.g. the error-containment capacity of the hub and the reliability of the extra components that stars include when compared with a bus.

This paper shows the first analyses we are conducting in this direction, which assess the influence of the reliability of one the most important extra elements of stars: the hub. Our analyses reveal relevant issues to be taken into account when increasing the reliability of this element; and open room for further analyzing these two topologies with respect to additional dependability aspects.

2 Previous analyses

We built our models using the Stochastic Activity Network (SAN) formalism, which is an extension to stochastic Petri Nets [11]. The modeling strategy was throughly described in [6] [5] [3]. Each model was built as a hierarchical composition of SANs that represent fault occurrences at hardware components; that evaluate how errors propagate and how faults are isolated/tolerated; and then, that elucidate whether or not the system still delivers its service.

Each component is supposed to independently fail in a permanent manner, and its *Time To Failure* (TTF) distribution is considered to be exponential and Non-Defective, with mean $1/\lambda$, where λ is the failure rate expressed in number of failures per hour. These failure rates and many other assumptions our models rely on are parameterized. This allows performing sensitivity analyses with respect to several dependability aspects. All modeling assumptions and parameters are thoroughly explained in [6] [5] [3]. In any case, as a first step, we defined a case of reference, by assuming specific values for each of those parameters, for comparing the bus with the stars, in which it is guaranteed that results are not biased towards stars. Table 1 shows some of the values that characterize this case.

In [6] [5] we analyzed the results obtained when considering the case of reference. In particular, we focused on the achievable *mission time*, i.e. on the maximum amount of time during which the system exhibits a reliability equal or greater than a certain degree [9]. In this sense we consider, just as a reference, a reliability degree of 0.99999, which is the one required by the less demanding x-by-wire applications in cars during a mission time of 10 hours [9].

Results reveal that CANcentrate improves the mission time of FTA systems with $k = 1$ when compared with CAN, e.g. around the 22% and the 260% for 3 and 20 nodes respectively. However, results show that due to its extra hardware CANcentrate slightly reduces the mission time of NFTA systems. This is because the extra hardware of CANcentrate may also fail and isolating a hub port for containing errors is useless in an NFTA system, since it does not accept or tolerate the failure/disconnection of the node placed at that port. As concerns ReCANcentrate, its fault-tolerance mechanisms amply compensate its extra hardware. Although it does not significantly improve the mission time of NFTA systems from an absolute point of view, it does so from a relative perspective: around the 35% and the 100% when compared with CAN and CANcentrate respectively. Furthermore, its improvement of mission time is outstanding in absolute terms for FTA systems when compared with CAN, implying benefits of around 626% and 360% for 3 and 20 nodes respectively.

3 New sensitivity analyses

We start by studying the sensitivity of the NFTAR and the FTAR_1 with respect to the failure rate of the hub. This failure rate is a parameter of main concern because, in a simplex star, the hub is not only an additional element, and thus an additional source of potential failures, when compared with a bus, but it is also the star's single point of failure. Moreover, the redundancy included in a replicated star is mainly devoted to tolerate a hub failure and, thus, the advantages of a replicated star when compared with a single one should be less evident as the hub reliability increases.

We varied the order of magnitude of the failure rate specified in the case of reference for the part of the hub that actually constitutes the CANcentrate's single point of failure: the *Hub core* [6]. This part includes the components (basically a dedicated IC and an oscillator) that implement the hub's coupling and fault-treatment functionalities. Note from Table 1 that the Hub core's failure rate depends not only on the number of nodes it couples, but also on its own complexity and, thus, on the star we are considering (the ReCANcentrate's hub is more complex). In particular, we considered 3 and 15 nodes to cover a wide range of applications: 3 is the minimum number of nodes needed to tolerate the failure of one of them, whereas 15 is the average size of a typical in-vehicle CAN subnetwork [7].

Table 1. Some models' parameters values

Parameter	Default value	Meaning
ctrlFlipCov	0.95	Coverage with which the CAN controller diagnoses a bit-flipping fault
lnkFlipCov	0.95	Coverage with which the hub diagnoses a bit-flipping port
busAttchFR	$6.34588 \cdot 10^{-8}$, $4.63159 \cdot 10^{-8}$	Failure rate of a section of a CAN bus interconnecting 3 and 15 nodes respectively (the same bus length is considered for 3 and 15 nodes)
lnkAttchFR	$6.34588 \cdot 10^{-8}$	Failure rate of the uplink or the downlink of CANcentrate (star diameter is assumed equal to the bus length)
nodeIOFR / hubIOFR	$6.73258 \cdot 10^{-7}$	Failure rate of each node and hub transceiver
ctrlFR	$1.25537 \cdot 10^{-6}$	Failure rate of the node's CAN Controller
nodeCoreFR	$3.25312 \cdot 10^{-6}$	Failure rate of the node's microcontroller
hubCoreFR	$1.20843 \cdot 10^{-6}$, $1.27559 \cdot 10^{-6}$	Failure rate of the hub core of CANcentrate and ReCANcentrate for 3 nodes

3.1 NFTAR vs Hub core failure rate

Figure 2 shows the NFTAR_1 achievable by equivalent systems relying on CANcentrate and ReCANcentrate for different Hub core's failure rates (*HFRs*) when 3 and 15 nodes are considered. The figure also depicts as a reference the NFTAR achieved by equivalent CAN-based systems. For the sake of brevity, the legend only shows the order of magnitude of each HFR. Moreover, although we measured the NFTAR for a perfect hub that cannot fail, Figure 2 does not include the corresponding curves either for CANcentrate or for ReCANcentrate, as they overlap the curves obtained when HFR $= 10^{-8}$.

As concerns ReCANcentrate, the first conclusion that can be drawn from Figure 2 is that it is impossible to further improve the mission time of CAN by using this star if only the reliability of its hub is increased. In fact, results show that to decrease the hub failure rate with respect to the case of reference (10^{-6}) does not significantly improve the mission time of ReCANcentrate. Specifically, and independently of the number of nodes, the ReCANcentrate's mission time only improves by the 3% approximately with respect to the case of reference when the HFR is reduced to 10^{-8} (or when the hub simply cannot fail).

Nevertheless, results indicate that it is essential to use a hub with a high-enough reliability, as the NFTAR of a ReCANcentrate-based system is specially sensitive to a decrease in this reliability. For instance, if the HFR is one order of magnitude higher than in the case of reference, i.e. it increases from 10^{-6} to 10^{-5} failures/hour, then the ReCANcentrate mission time diminishes by around the 22%, with both 3 and 15 nodes, and becomes close to the one achieved by the CAN bus.

Finally, the sensitivity of the NFTAR of a CANcentrate-based system with respect to the HFR is similar to the sensitivity of a ReCANcentrate-based one. The only difference is that the CANcentrate's sensitivity slightly varies with the number of nodes. It is higher than the one of ReCANcentrate for 3 nodes, but lower for 15. In any case, it is impossible to improve the NFTAR of CAN by using CANcentrate as the star includes more hardware. Moreover, results indicate that investing in its hub reliability does not significantly improve the mission time with respect to the case of reference.

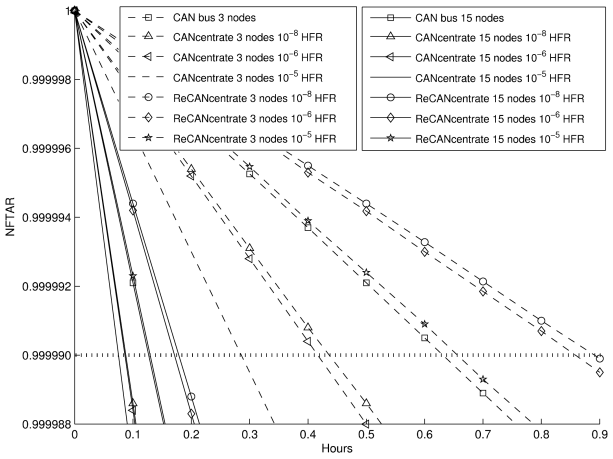

Figure 2. NFTAR vs hub core's failure rate

3.2 FTAR_1 vs Hub core failure rate

Figure 3 is analogous to Figure 2, but considering the FTAR_1. It demonstrates that the FTAR_1 is very sensitive to the HFR in both stars. For example, if we consider 15 nodes and that the HFR increases in one order of magnitude with respect to the reference case, i.e. from 10^{-6} to 10^{-5} failures/hour, then the mission time is drastically reduced from 4.1 to 0.5 hours (around the 88%) in CANcentrate and 7.1 to 1.2 (around the 83%) in ReCANcentrate.

Likewise, if the reliability of the Hub core is improved, then the mission time is hugely increased. This is specially noticeable when using CANcentrate with a small number of nodes. For instance, if for 3 nodes the HFR of the reference case is decreased in one and two orders of magnitude, i.e. from 10^{-6} to 10^{-7} and 10^{-8}, then the mission time is increased from 7.6 to 43 and 77 hours, which are improvements of the 466% and 913% approximately. Results are similar for 15 nodes, even though the improvement of mission time is lower. For example, the mission time of a CANcentrate-based system can be approximately improved by 212% and 287% if the HFR is decreased by one and two orders of magnitude with respect to the case of reference. This is because the contribution to the FTAR_1 of the reliability of the components that are not part of the Hub core grows with the number of nodes and, hence, the relevance of the Hub core reliability decreases.

But maybe the most surprising result is that CANcentrate can outperform ReCANcentrate when the HFR is around to 10^{-8}, e.g. CANcentrate and ReCANcentrate respectively achieve near 77 and 61 hours of mission time for 3 nodes. This result would encourage the use of a sim-

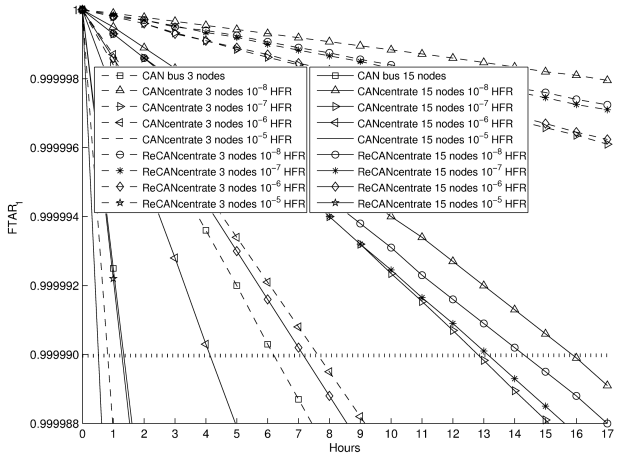

Figure 3. $\mathbf{FTAR}_1$ vs hub core's failure rate

plex star for FTA systems, since it is actually possible to achieve such low HFRs by using electronic components of the highest quality for its construction, e.g. components that are typical in military applications. Note that although it is not shown in Figure 3, the mission times achieved with HFRs of the order of 10^{-8} are very close to what would be theoretically reached with an HFR of 0.0 failures/hour.

4 Conclusions

In previous work, we modelleded the reliability of equivalent systems relying on CAN, CANcentrate and ReCANcentrate, in order to quantify the dependability benefits of star topologies for field-bus systems when permanent hardware faults may occur. We quantitatively demonstrated that a simplex star topology fairly improves the reliability of FTA systems, whereas a replicated one slightly improves the reliability of NFTA systems and boosts the reliability of FTA ones. However, these results are likely to be lower bounds to the reliability achievable with stars, as they were obtained taking into account a case of reference, in which all assumptions concerning any dependability-relevant aspect were made favoring the bus in the comparison. Thus, to completely quantify the potential dependability benefits of stars, we are currently analyzing the sensitivity of the reliability with respect to several of these aspects.

We present two of these analyses, which focus on the reliability of the hub. Results show that increasing the reliability of the hub is not enough in order to allow ReCANcentrate to boost the reliability of NFTA systems. Conversely, the hub reliability has an enormous impact on the reliability of FTA systems when using both CANcentrate and ReCANcentrate, so that the stars' benefits can be increased even further.

Surprisingly, results also show that with a highly-reliable hub, the simplex star can even outperform the replicated one. Although this would encourage the use of a simplex star for FTA systems, it is important to note that failure rates can only be calculated considering faults that result from malfunctioning of components, but not those provoked by external or fortuitous causes such as an impact. Thus, the benefits of ReCANcentrate's redundancy are not totally reflected in our classical calculation of its reliability. If an impact damages one of the ReCANcentrate hubs this will be tolerated.

We think that the results of this paper encourage further analyses with respect to other parameters, as it is necessary to identify which are all the key factors to be considered for taking full profit from the potential of stars.

Acknowledgements

This work was supported by the Spanish Science and Innovation Ministry with grant DPI2008-02195, FEDER funding, and M. Barranco was partially financed by the Portuguese Fundação para Ciência e a Tecnologia with grant SFRH/BPD/70317/2010 in the context of the POPH/FSE program.

References

[1] Flexray communications system-protocol specification, 2005.

[2] A. Ademaj, H. Sivencrona, G. Bauer, and J. Torin. Evaluation of fault handling of the time-triggered architecture with bus and star topology. In *Proceedings. 2003 International Conference on Dependable Systems and Networks*, pages 123–132, June 2003.

[3] M. Barranco. *Improving Error Containment and Reliability of Communication Subsystems Based on Controller Area Network (CAN) by Means of Adequate Star Topologies*. PhD thesis, Dep. Ciències Matemàtiques i Informàtica, Universitat de les Illes Balears (UIB), 2010.

[4] M. Barranco, J. Proenza, and L. Almeida. Boosting the robustness of Controller Area Networks: CANcentrate and ReCANcentrate. *Computer*, 42:66–73, May 2009.

[5] M. Barranco, J. Proenza, and L. Almeida. Reliability improvement achievable in CAN-based systems by means of the ReCANcentrate replicated star topology. In 8^{th} *IEEE International Workshop on Factory Communication Systems, Nancy, France*, 2010.

[6] M. Barranco, J. Proenza, and L. Almeida. Quantitative comparison of the error-containment capabilities of a bus and a star topology in CAN networks. *IEEE Transactions on Industrial Electronics*, 53(3):802–803, March 2011.

[7] C. Braun, L. Havet, and N. Navet. Netcarbench: a benchmark for techniques and tools used in the design of automotive communication systems. In *Prooceedings of the 7th IFAC International Conference on Fieldbuses and Networks in Industrial and Embedded Systems (FeT 2007)*, pages 321–328, Toulouse, France, November 2007.

[8] B. Gaujal and N. Navet. Fault confinement mechanisms on CAN: analysis and improvements. *IEEE Transactions on Vehicular Technology*, 54(3):1103–1113, 2005.

[9] J. Morris and P. Koopman. Representing design tradeoffs in safety-critical systems. In *Proceedings WADS, St. Louis, MO.*, pages 1–5, 2005.

[10] N. Navet, Y. Song, F. Simonot-Lion, and C. Wilwert. Trends in automotive communication systems. *Proceedings of the IEEE*, 93(6), 2005.

[11] W. Sanders. *Moebius User Manual, T. B. of Trustees, Ver. 1.6.0.*, 2004.

[12] M. Shooman. *Reliability of Computer Systems and Networks*. 605 Third Avenue, New York, USA, 2002.