System Level Reliability Issues and Their Enhancement in Drive-by-Wire (DBW) Systems

M. Abul Masrur

US Army RDECOM-TARDEC, RDTA-RS, MS-121, 6501 E. 11 Mile Road, Warren, MI 48397-5000, USA

Abstract: Drive-by-wire systems in automobiles and fly-by-wire systems in aircrafts have made these vehicles versatile with added features and benefits, along with ease of reconfiguration, in particular during graceful degradation. However, there are certain consequences of such by-wire systems in terms of overall system reliability. The issue has not been quantitatively discussed in the literature in a systematic manner, to the best of the knowledge of the author. The chapter discusses details of the drive-by-wire system architectures from a system viewpoint, analyzes the reliability with quantitative metric, and indicates methods of enhancing reliability by using both hardware and software redundancies.

Keywords: Drive by Wire, Fly by Wire, Multiplexed Systems, System Load Availability, Multi-Protocol Communication, Controller Area Network (CAN).

SYSTEM VIEWPOINT

Drive-by-wire (DBW) for automobiles (Isermann *et al.*, 2002) or its counterpart fly-by-wire (FBW) (Seidel, 2009), and in general X-by-Wire, and sometimes termed “multiplexed system” in a general sense, have significantly helped to achieve better size, weight, packaging, and overall performance in ground vehicles (including airborne and waterborne vehicles, i.e. aircrafts, ships etc.), allowed easier inclusion of higher number of components and subsystems within the vehicle in a modular fashion, allowed multiple platforms using common architecture, and contributed to overall flexibility in manufacture. Multiplex system “normally” involves computer type of network, where several signals can be combined (or “multiplexed”) and sent out through the same common media like copper wire, fiber optic cables etc. Although “by-wire” systems these days involve communication networks, in principle it need not be so. In other words, it is possible to use direct wirings to actuate loads separately. These topics have been discussed in other sections within this eBook. However, incorporation of multiplexing has also introduced certain risk factors as well, in terms of catastrophic failure conditions. Since DBW incorporates various components and subsystems, and since its successful functionality leads to the overall system performance, it is worthwhile to look at it from a holistic and system level viewpoint. The purpose of this section will be to discuss DBW from a total system level perspective to see what is involved to enhance its reliability and how component and subsystem level reliability can affect the overall system reliability. We will also try to quantify the overall system reliability with numerical example. With the above in view, it is necessary to study the overall architecture of the system first.

TYPES OF THINGS DEALT WITH IN DBW

As is well known, DBW (or equivalently FBW etc) is intended to “make something happen” or actuate something (a device or “load”) at a distance by communicating from remote, and in consequence, the source of power or energy can be at a different location than the actuation requesting agent or the load. Besides actuation of some component, multiplexing can also imply flow of signals in response to some request, e.g. speed of a vehicle, where a transducer signal due to the speed will be taken to the instrument cluster through some signal wire, and not through the actual transducer component, and thus it is not necessarily that only high power items are commanded through multiplex system. These are the main categories of DBW. FBW is no different. Obviously, then, multiplexing involves both hardware and software (software is involved in communication network and also actuation algorithm etc.) and both are equally important for its successful operation.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **01 SEP 2012**	2. REPORT TYPE **Journal Article**	3. DATES COVERED **01-08-2012 to 23-09-2012**

4. TITLE AND SUBTITLE **System Level Reliability Issues and Their Enhancement in Drive-by-Wire (DBW) Systems**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **M Masrur**	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army TARDEC,6501 East Eleven Mile Rd,Warren,Mi,48397-5000**	8. PERFORMING ORGANIZATION REPORT NUMBER **#20882**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) **U.S. Army TARDEC, 6501 East Eleven Mile Rd, Warren, Mi, 48397-5000**	10. SPONSOR/MONITOR'S ACRONYM(S) **TARDEC**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S) **#20882**

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Drive-by-wire systems in automobiles and fly-by-wire systems in aircrafts have made these vehicles versatile with added features and benefits, along with ease of reconfiguration, in particular during graceful degradation. However, there are certain consequences of such by-wire systems in terms of overall system reliability. The issue has not been quantitatively discussed in the literature in a systematic manner, to the best of the knowledge of the author. The chapter discusses details of the drive-by-wire system architectures from a system viewpoint, analyzes the reliability with quantitative metric, and indicates methods of enhancing reliability by using both hardware and software redundancies.

15. SUBJECT TERMS

Drive by Wire, Fly by Wire, Multiplexed Systems, System Load Availability, Multi-Protocol Communication, Controller Area Network (CAN).

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Public Release**	**10**	

ACTUATION PROCESS IN DBW

As we noted above, it may be our interest to actuate something at a distance through DBW. For example, we might need to steer the vehicle wheel, or move the aircraft flaps in the wing, or the rudder of a ship. The final actuation may be implemented by means of a hydraulic device, e.g. a hydraulic pump driving a hydraulic motor or perhaps a hydraulically driven piston etc., or it could be an electric motor to do the same. In the former case, the source of hydraulic energy could be far away from the requester and located more conveniently near the load, with all the hydraulic plumbing, pipes etc. packaged conveniently at a suitable location. In the latter case if the actuation is done electrically, and the battery or the electrical power source could be located at a convenient place and the actuation motor could be very next to the load. Of course, besides hydraulic or electric it is possible, like earlier days, to have direct mechanical linkage (through linkages, levers etc.) from the driver which will actuate something – though in a very cumbersome way. Similarly "non-power" items like speed or odometer signal etc. can be communicated from the source to the instrument cluster through direct link, or through hydraulic link, or direct electrical wirings.

ENERGY SOURCE AND ACTUATORS

It is obvious, therefore, from the above that we either need hydraulic, electric, or even direct mechanical linkage to actuate something or receive signals. Multiplexing (or DBW, FBW) has taken out that "directness" between two points through communication network.

ARCHITECTURE

A system level architecture of a multiplex system is shown below in Figure 1 (Masrur *et al.*, 2004). In this system, the red line indicates the power bus and the blue line indicates the communication signal line, which in the case of a CAN (controller area network) network can be a twisted pair copper wire. The benefits of the above are obvious. The power line can be simple with less connectors etc. The information from the driver does not need a high power cable to activate the power switch, only low power signal wire (thin in size) is sufficient. The rectangular boxes are what is known as ECU (electronic control unit) or nodes. Each node can cater several loads (the oval shaped ones). The information in the "blue" line can operate in a multiplexed manner, i.e. several ECU's can share the same wire using some protocol or communication "mannerism". For CAN protocol, there are priorities (Masrur, 1989) based on which a particular function will get hold of the bus. For safety critical devices there can be different protocols, e.g. TTP (time triggered protocol), Flexray, or sometimes there can be mixed protocols (Arora *et al.*, 2004) and it is possible to have separate and dedicated bus to deal with safety critical loads and to have some kind of gateway between multiple communication buses, somewhat like a computer network or internet gateways.

WHAT CAN HAPPEN DURING ECU FAILURE

Obviously, it can be seen from the architecture in Fig. (1) that if an ECU fails, it will take down with it several loads which won't operate any more. That is a very dangerous situation, especially if the loads are vital ones.

Before delving into this issue, it may be instructive to discuss briefly why an ECU will fail in the first place. Normally the ECU will have sockets to connect the signal bus and the power bus. This can be something comparable to the power and data cables which connect devices in a computer motherboard. The picture of an ECU and a circuit board are shown below. The circuit board in Fig. (2b) below is not for the item shown in Fig. (2a). These pictures are merely to give an idea of the thing. This could be the engine control unit, which can be very complicated. On the other hand there are simpler ones with simple functions.

Many times the failure in these devices are due to mechanical reasons like connector getting lose or damaged due to vibration, heat, corrosion, dirt etc., or the solder getting cracked due to thermal fatigue due to repeated heating and cooling. These could sometimes be to items outside of a microprocessor chip and in some cases could be internal problem with the large scale integrated circuits. In addition, there are elements like resistors, capacitors, inductors on the circuit board which could eventually fail after many hours of usage. Some of these causes of failure are preventable by taking good care during usage, but some items are beyond that and will eventually fail regardless.

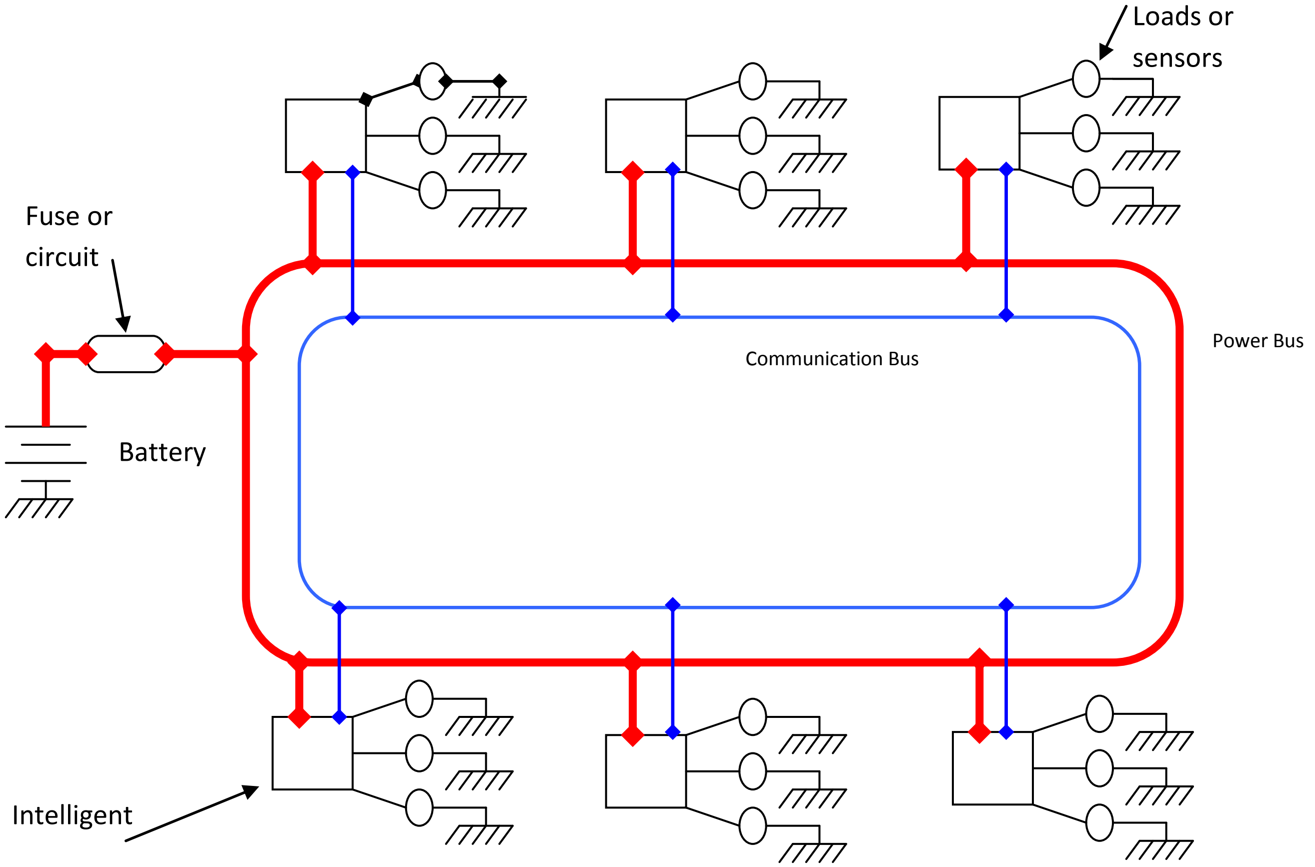

Figure 1. An automotive multiplex system architecture configuration with power and communication buses, loads, and intelligent nodes for processing communication protocol and load management.

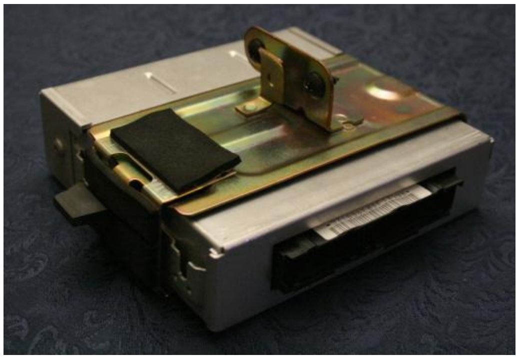

Fig. 2(a) ECU picture from outside

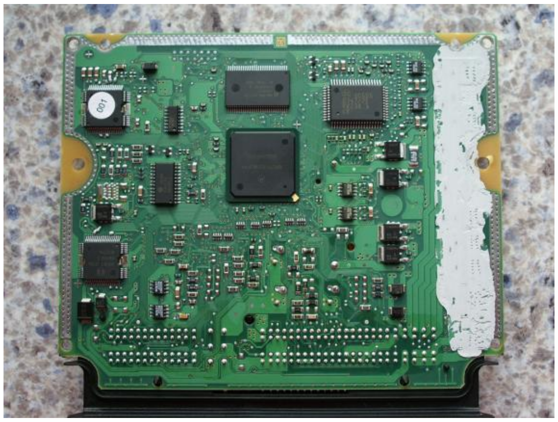

Fig. 2(b) Inside of an ECU

(a)http://upload.wikimedia.org/wikipedia/commons/6/66/2008-04-17_ECU.jpg (b)E-book_FT_DBW_ Anwar_r4. docxhttp:// upload.wikimedia.org/wikipedia/ commons/a/a6/ElectronicDieselControlEcuBottomside.jpg

WHAT OTHER FAILURES CAN HAPPEN

In addition to the ECU, other items like cables and connectors outside the ECU could fail as well for similar reasons as before.

All the above are hardware failures. Software failure can happen too, though due to different reasons. Most likely cause of a software failure will happen if the algorithm encounters a situation which was never anticipated before, and which was not considered during design of the algorithm. This can lead to generation of wrong messages or lead to something not activated when asked for, or something suddenly getting activated when not asked for. Both are obviously not very desirable. Or, sometimes one can get into an unending loop, which can be dangerous too.

Hardware failures can, in general, be corrected by replacing the faulty item, or sometimes a whole set of items surrounding the faulty item, together with the faulty item. However, software problem cannot be rectified so easily, but from a user perspective cured tentatively by shutting down the power and resetting the system etc. But sooner or later such an event will need to be referred to the manufacturer to come up with a revised version of the device/software, and is more complex in nature since it cannot be addressed by the dealership immediately.

QUANTITATIVE ANALYSIS OF THE CONSEQUENCE OF FAILURE

As noted earlier, obviously a failure in the ECU node can lead to all loads connected to it to fail. Some failure can be catastrophic or even fatal, like brake or steering system failure. Other failure like an entertainment system malfunction may not be important at all. Some items like window mechanism failure may have security issues etc. So, failure items are not all alike. Hence to analyze such a system a methodology has to be developed. Another thing to be noted here is that it is really not necessary to know microscopic details of all the failure mechanisms to study such systems. Most of the time it is good enough to know an overall (macroscopic) component or subsystem level reliability number which can be quantified by mean time between failure over a period of time or over a given mileage covered. The author discussed these in more detail in his other works (Masrur *et al.,* 1989; Masrur *et al.*, 2003; Masrur *et al.*, 2004; Masrur *et al.*, 2008).

QUANTITATIVE METRIC FOR SYSTEM LOAD AVAILABILITY

As previously noted, the ultimate purpose of the wiring harness (consisting of both the power and the communication buses) is to actuate certain loads, based on the information received from the driver of the vehicle and/or the various sensors, and to coordinate these in a certain desired manner. That is essentially what makes a "drive-by-wire" system. To study the overall system level reliability of such a system, we have to know about all the items from source to load. Hence we can define the following terms.

$\lambda_{i\,=}$ probability that the i-th load/sensor is up (or available) at a particular moment, -- which can range from 0 to 1.

C_i = criticality of the i-th load/sensor, -- a number which indicates how critical it is for this particular load to be up.

A range of 1 to 10 is chosen for convenience, where 1 means not at all critical, to 10 meaning absolutely critical.

H_i = number of times on an average the i-th load is invoked or its status updated, during a given span of time (hr, min, sec etc.), -- a number which will depend on the nature of the load. The duration can be chosen to be in units of hour, if it is deemed that H_i may be a small fraction and inconvenient to use.

Based on the above, we can define a figure of merit indicating how detrimental it is for a particular load/sensor (the i-th load/sensor) to be down, by introducing,

$$F_i = C_i\, H_i\, (1-\lambda_i)\, \{ \prod_{j = 1, \dots n,\ j \neq i}^{n} (\lambda_j) \} \qquad \text{…….. (1)}$$

where n is the total number of loads (including sensors) in the system. In equation (1), the term $(1-\lambda_i)$ indicates the probability of the i-th load being down. In this equation we make the assumption that the probability of more than one load being simultaneously down is of second order, and hence much smaller compared to the terms used in equation (1). Based on the above, a cumulative system level figure of demerit can now be defined as:

$$F_s = \sum_{i=1}^{n} F_i \qquad \text{…... (2)}$$

assuming that the total number of loads = n.

* The two sections immediately above and below are based on the author's paper referenced above.

ILLUSTRATION OF APPLICATION EXAMPLE

The most important item involved in evaluating the cumulative system figure of merit (or demerit) requires finding the value of λ_i. If we want to evaluate this for the example architecture shown in Figure 1, the following items are to be accounted for. This list is just a possible example of items that can lead to failure, and depending on the specific architecture it will vary. But the methodology described here will be valid regardless of the particular case being studied.

Hard Items:

1. Battery to battery-cable connector
2. Battery-cable to main-fuse connector
3. Main-fuse to power-bus connector
4. Power-bus cable
5. Power-bus cable to intelligent-node connector (each node consisting of both the power module and also the communication module).
6. Signal-bus (twisted pair etc.)
7. Signal-bus to node connector
8. Node-module
9. Node to load-fuse connector
10. Load-fuse to load connector
11. Load to ground connector
12. Electromechanical relay or solid-state switches connecting the load (can replace the fuse depending on the system).

Soft Items:

1. Network message overload and/or error at source end (at message initiating node) causing priority based queuing and leading to delay and/or error in transmission (Masrur, 1989).

2. Failure to win contention with other nodes leading to delay for the message to reach destination, and/or error in message transmission.

It should be noted that the probability of failure of hard items changes with time, starting from infant mortality to deterioration with usage and age. For the soft items, the probability of failure will depend on the message loading and interval used in the system, and is directly related to the quantity $\sum H_i$, for i = 1 to k (number of loads), which was defined earlier. In the above example the numerical values were arbitrarily chosen though based on some reasonable assumptions.

Let us assume for now that there are six nodes in the system with three loads connected to each node. This is the configuration shown in Figure 1. The reliability of each item is indicated by the symbol ξ.

For hard items 1 to 7 let us choose: $\xi_1 = 0.99999$ $\xi_2 = 0.99997$ $\xi_3 = .99997$ $\xi_4 = 0.99999$ $\xi_5 = 0.99998$ $\xi_6 = .99999$, $\xi_7 = 0.99999$

For node module itself let us choose $\xi_8 = 0.99995$

For node to fuse connectors let us choose $\xi_9 = 0.99996$ (same for other node to load connectors)

For fuse to load connectors let us choose $\xi_{10} = 0.99996$ (same for other nodes to their respective load connectors)

For load to ground connectors let us choose $\xi_{11} = 0.99996$ (same for other nodes to their respective ground connectors)

For the electromechanical (or solid-state) relays (can replace the fuse where applicable), let us choose $\xi_{12} = 0.99995$

For soft items 1 and 2, let us choose as follows: $\xi_{13} = \xi_{14} = 0.99998$

In the above we just traced the items for one single node. The same will apply to the other loads. For hard items, only the items from 1 to 4 will be common to all nodes, and the rest of the items will be separate for each nodes.

For the 18 loads let us assume the following quantities for C_i and H_i:
$C_1 = 10$ $H_1 = 20$ $C_2 = 10$ $H_2 = 3$ $C_3 = 7$ $H_3 = 10$ $C_4 = 8$ $H_4 = 12$ $C_5 = 1$ $H_5 = 20$ $C_6 = 4$ $H_6 = 20$ $C_7 = 10$ $H_7 = 100$ $C_8 = 3$ $H_8 = 8$ $C_9 = 6$ $H_9 = 14$ $C_{10} = 2$ $H_{10} = 10$ $C_{11} = 1$ $H_{11} = 1$ $C_{12} = 2$ $H_{12} = 20$ $C_{13} = 3$ $H_{13} = 150$ $C_{14} = 9$ $H_{14} = 60$ $C_{15} = 10$ $H_{15} = 2$ $C_{16} = 10$ $H_{16} = 8$
$C_{17} = 5$ $H_{17} = 5$ $C_{18} = 6$ $H_{18} = 40$

For the example case here, the probability that a particular (n-th) load is available is given by the product of all the reliability terms ξ_i for i = 1 to 14.

$$\lambda_n = \prod_{i=1}^{14} \xi_i \qquad \text{.......(3)}$$

In the particular example, if the values of ξ_i are inserted, we get $\lambda_n = 0.99962$, for all n=1 to 18, assuming same component reliabilities in each node. Hence we can easily see that whereas the individual component failure probabilities (ξ_i) were chosen to be between 1 to 5 per 100000, after combining all the components together, we get a failure rate of about 38 per 100000. Although this number is quite small, it might still contribute significantly toward the overall system availability or lack thereof.

In addition to the above, since in general multiple loads are connected to a particular node, there is a reliability issue which leads to the failure of a cluster of loads all together, should any one or more of the linkages leading to the node fail. This can pose a potentially dangerous situation during failure. Thus we also define a group load reliability (or availability) in the following manner. For the n-th node, the group reliability is given by:

$$\lambda_n = \prod_{i=1}^{8} \xi_i \qquad \text{.......(4)}$$

In the example above, this becomes = 0.99983, or 17 failures per 100000, which is about half the individual load failure rate.

It is therefore noticed that the group reliability of the loads connected to node 1 and indicated by equation (4), is somewhat higher than the individual load reliabilities given by equation (3). This is naturally expected, since there are more linkages preceding an individual load than for the group of loads connected to a particular node.

Using these quantities (based on equations (3) and (4)) for all the nodes, we can easily compute that for this 6-node, 18-load system, the figure of merit (actually demerit to be more exact) according to equation (1) will be as indicated in the following.

Figure of demerit for the system considering individual load failure probabilities is computed by excluding multiple failure probabilities, which is normally of second order, compared to single component failures. So, we compute the probability of failure of load # 1 in node # 1, and assume that all the other loads and nodes are up (available). This leads to, with all the loads taken into account, a cumulative figure of demerit due only to individual load failures to be:

$$F_s = \sum_{k=1}^{18} C_k H_k (1-\lambda_k) \left\{ \prod_{m=2}^{17} (\lambda_m) \right\} \prod_{j=1}^{6} (\lambda_j) \qquad \ldots\ldots(5)$$

where λ_k for k-th load is evaluated using equation (3), and λ_j is evaluated by equation (4). λ_m is evaluated equation (3), but slightly modified, so that the reliability of elements already included in λ_j are excluded here (in other words, only components 9 to 14 are now included during this evaluation, rather than 1 to 14, as in equation (3)). Inserting all the necessary values, we get from equation (5),

$$F_s = 0.7677 \qquad \ldots\ldots(6)$$

In equation (5), the value of j runs from 1 to 6, for the six separate clusters of loads. Since this system also has the possibility of group failure as indicated earlier, we have to account for that as well. This is computed by using equation (1), except that we now use equation (4) instead of equation (3) to compute the λ_j and this λ_j (for the j-th cluster) will correspond to each cluster of loads corresponding to each node, there being a total of six such clusters in the example case. During computation of the group failure, we assume that only one cluster can fail at a time. Thus the equation for computation of cumulative failure probability, assuming all the clusters can fail one at a time is given by:

$$F_s = \sum_{k=1}^{18} C_k H_k \left[(1-\lambda_j)\right]_{j=1} \prod_{j=2}^{6} (\lambda_j) \qquad \ldots\ldots(7)$$

Here, first we compute the probability of cluster # 1 being down and others up, but since the result is symmetric, we can extend it to others to compute the cumulative figure of demerit. Thus, in our example case this group failure figure of demerit will become = 0.3448. Hence adding this with equation (6) we get the next level of figure of demerit for the system to be = 1.1125. Finally there is the probability of a total system failure due to the hard linkages 1 to 6. Following the same line of thought, it leads to an additional figure of demerit = 0.2233. Hence if we add this number to the previous ones, the final cumulative system figure of demerit will be:

$$F_s = 1.3358 \qquad . \qquad \ldots\ldots(8)$$

which is a combination of items due to figure of demerit from individual load failures (0.7677), figure of demerit from group load failures (0.3448), and the figure of demerit from total system failure (0.2233). It can be immediately observed that the contribution to the total system figure of demerit comes mostly from the individual load failures, next from a group of loads failing together, and least from the total system failure. This is naturally expected. To best capture the phenomena of total system, group and individual failures, it is rational to add these numbers as has been done to get the equation (8), since all of these contribute towards the demerit of the overall system. This number can therefore be used as a metric for the purpose of evaluating the quality of a system, and the larger the number, the worse the system availability.

WHEN TRYING TO IMPROVE, IT IS IMPORTANT TO HAVE A HOLISTIC VIEWPOINT OF THE SYSTEM

In the previous example (though used assumed items involved in the by-wire system, and assumed numerical values for reliability numbers) it is clear that several things contribute to system failure. Obviously then, to improve the system reliability and robustness, all of those items have to be "improved". The followings could be done to achieve that goal.

Quality enhancement at component level - by increasing this we are basically increasing the reliability number ξ_i noted previously for various components. However, to increase these numbers like 0.99995, it becomes extremely costly as one tries to increase the value at higher decimal points. This means, in practical terms, that to increase the value of ξ_i from 0.999 to 0.9999 is relatively costlier than trying to increase the number from 0.99 to 0.999. So, at one point component quality enhancement may be impractical.

Introducing redundancy – a very important method to increase the overall system level reliability is to have additional components with parallel functionality. Even though the components themselves may have same reliability, the overall probability of failure is substantially reduced by redundancy. For example, if a component has $\xi_I = 0.99$, then by having two such items in parallel the overall reliability becomes {1- (1-0.99)(1-0.99)} = 1-(.01)(.01) = 0.9999, under the assumption that overall failure requires both of the components to fail simultaneously. To achieve such a degree of reliability enhancement by merely using one component and improving its quality would be very difficult. This is a case of system architecture modification. Redundancy is a very important mechanism, which is abundantly noticed in nature e.g. biological system like human brain.

Software reliability – software reliability can be compromised primarily due to human error during design by not being able to account for every foreseeable circumstances that an algorithm might be subjected to. This can, to some extent, be mitigated by introducing dual paths for an algorithm where the algorithms in these dual paths can be developed by different software groups. Through some voting scheme, if two or more software paths are in agreement, the software function may be considered correct.

The above methods involving hard and software redundancy are indicated through the block/flow diagram below between the system input and outputs as shown in Fig. (3).

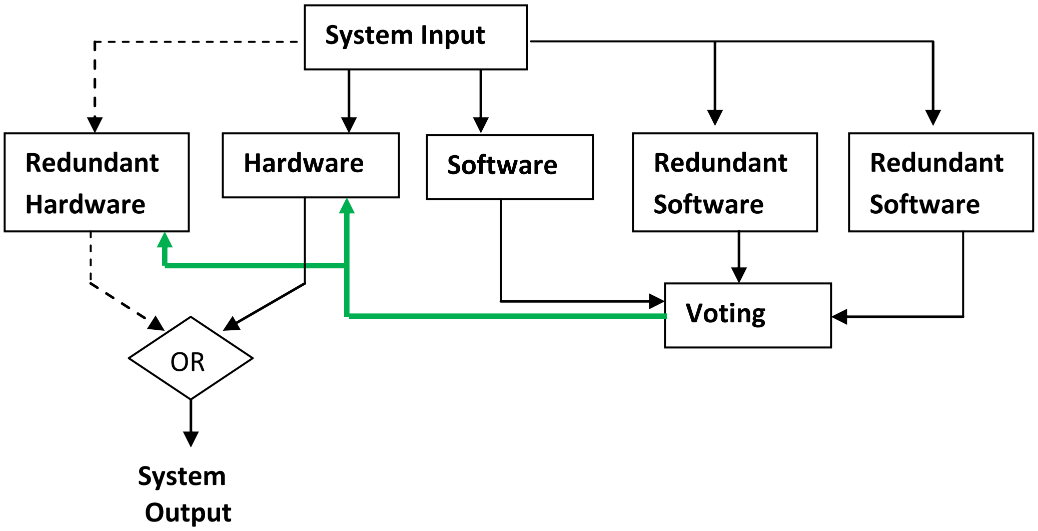

Figure 3. System level hardware and software redundancy.

Architectural reconfiguration for reliability enhancement – In a by-wire system, especially for safety critical items, it is extremely beneficial to have redundancy of the type indicated in the above diagram, which can have different variants. If a system encounters a fault, the above redundancy can make it “fail safe” or “fail silent”, to the extent of a single failure. In the system above, if there is a software failure in one of the 3 software blocks, it can still continue to function. After that there won’t be any way to know through voting scheme which software is correct. Since software does not pose space issue in terms packaging or physical cost, it is easier to introducing redundancy. For hardware it is difficult to do so. Hence in case of hardware one cannot normally afford to have more than one extra. Normally if a malfunction is detected through any diagnostic scheme, or if a future risk is identified through prognostics, it will become necessary to use the duplicate or redundant hardware and disconnect or isolate the faulty one.

Multi-system separate network architecture with gateways when beneficial – A by-wire system, depending on its situation can sometimes be partitioned into multiple ones with different network protocols to carry information. For example the unimportant or less safety critical loads can be controlled by a CAN network and the safety critical ones may be kept under a more deterministic network like a TTP (time triggered protocol). Depending on the needs, there can be some kind of gateway between the two networks to exchange information between the two. This is shown in the following diagram which is a revised version of the previous diagram, and indicates a partitioning of the loads into two different network buses, one catering more safety critical loads than the other.

Failure due to non-network reason - As is obvious, in our analysis of reliability above, we have taken into account the hardware components, software, and communication network into consideration. Through this process it has been emphasized that overall system reliability is dependent on the complete and successful working of everything in unison, and not just the communication network in a DBW. It is the intent of this section to drive this point.

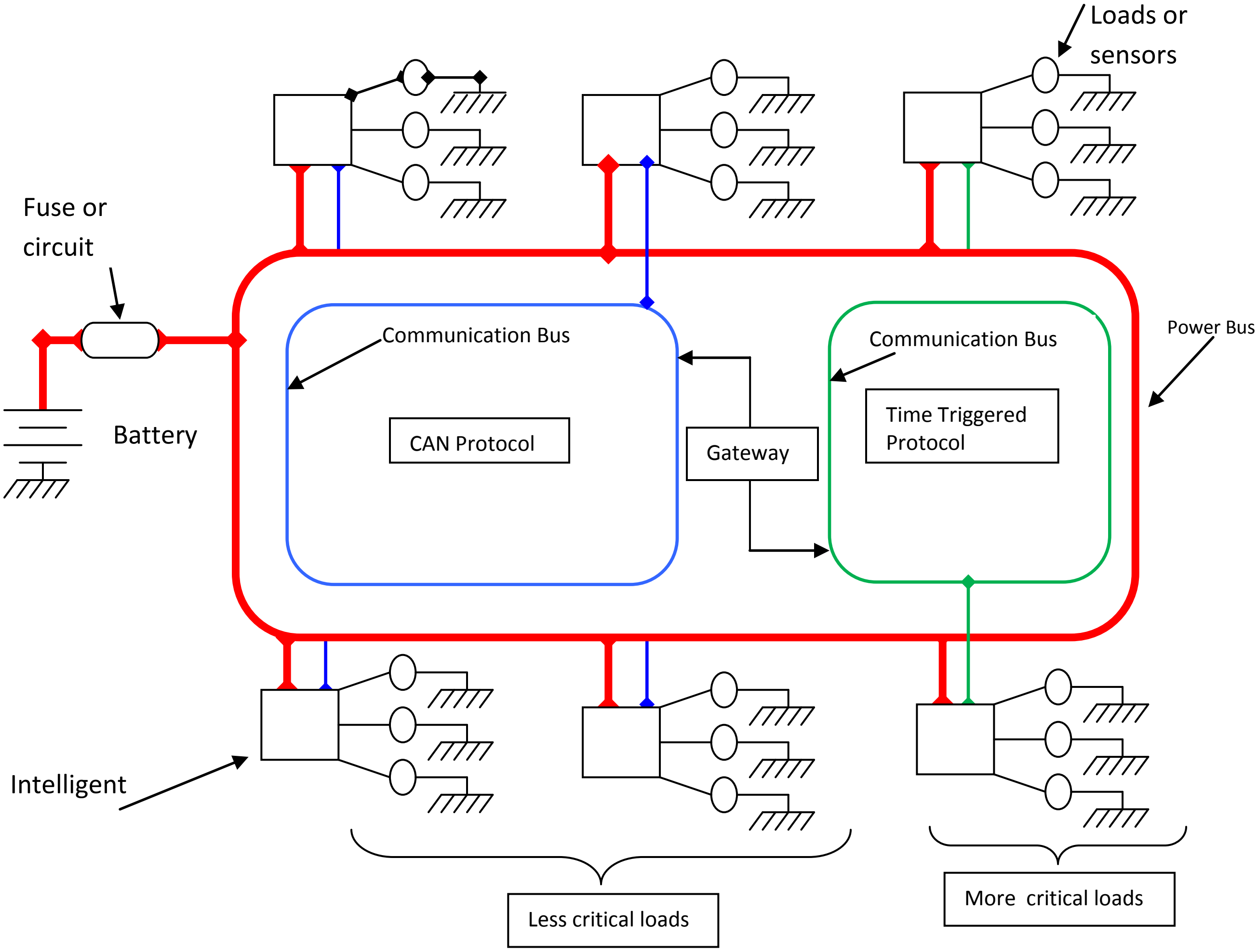

Figure 4. Multi-protocol communication with gateway.

CONCLUDING NOTES

The main aim of this section has been to take a complete system level perspective towards reliability of drive-by-wire systems. The intent was to create a generic framework applicable to study any DBW. The author has extended the above ideas to HEV's (hybrid electric vehicular systems) and provided a quantitative metric to compare between different HEV's against regular IC engine vehicles (Masrur, 2008). From the discussion in this section, it is seen that the overall system reliability (for DBW and also non-DBW) comes initially through the quality of components used, but at some point a limitation arrives in quality enhancement due to cost and other fundamental limitations. At that point it becomes important to use redundancy in terms of both hard and software. The treatment of analysis for both DBW and non-DBW can be done by using the general methodology discussed in this section. It should also be emphasized here that it is not possible to completely eliminate system failure. However by using good diagnostic and prognostic methods (which is not within the scope of this section) it is in many cases possible to know about the health of a system before a failure occurs, and take preemptive steps to avoid those failures, which is of great importance, particularly for safety critical systems.

REFERENCES

Arora, A., Ramteke, P., & Mahmud, S. (2004). Fault Tolerant Time Triggered Protocol For Drive-by-Wire Systems. Proceedings of the 4th Annual Intelligent Vehicles Systems Symposium of National Defense Industries Association (NDIA), National Automotive Center and Vetronics Technology, Traverse City, Michigan.

Isermann, R., Schwarz, R., & Stolzl, S. (2002, October). Fault-tolerant Drive-by-Wire Systems. IEEE Control Systems Magazine, 64-81.

Masrur, M.A. (1989). Digital simulation of an automotive multiplexing wiring system. *IEEE Trans. on Veh. Tech*., 38(3), 140-147.

Masrur, M.A. (2008). Penalty for Fuel Economy – System Level Perspectives on the Reliability of Hybrid Electric Vehicles During Normal and Graceful Degradation Operation, *IEEE Systems Journal*, 2(4), 476-483.

Masrur, M. A., Garg, V. K., Shen, J., & Richardson, P. (2003). Comparison of System Availability in an Electric Vehicle with Multiplexed and Non-Multiplexed Wiring Harness. IEEE Vehicular Tech. Conf. Proceedings.

Masrur, M.A., Shen, Z.J., & Richardson, P. (2004). Issues on Load Availability and Reliability in Vehicular Multiplexed and Non-Multiplexed Wiring Harness Systems. Society of Automotive Engineers (SAE) Transactions, Journal of Commercial Vehicles, 2003-01-1096, 31-39.

Seidel, F. (2009). X-by-Wire. Hauptseminar Transportation Systems, Chemintz Univ. of Tech., Feb, 1-9.

Wikimedia Page. Retrieved on 06th June, 2011, http://upload.wikimedia.org/wikipedia/commons/6/66/2008-04-17_ECU.jpg

Wikimedia Page. Retrieved on 06th June, 2011, E-book_FT_DBW_Anwar_r4.docxhttp:// upload.wikimedia.org/ wikipedia/ commons/a/a6/ ElectronicDieselControlEcuBottomside.jpg.