Debate about CAN fault

Fuyu Yang

Chongqing Institute of Instrumentation and Automation, Chongqing, China. Email: yfy812@163.com

Abstract: Papers [1], [2] published in this journal concerning the fault embedded in CAN protocol are answered by the inventor Bosch. It admits the existence of transmission and receiving delay caused by the fault confined mechanism. But it denies the bad side effect by not mentioning it and emphasizing the good effect of introducing this fault confining mechanism and calling it as feature but Bug. Present paper points the bad effect of quasi bus off and real bus off to the application. It is possible to cause a large scale recalling. Actually, the bad side and good side of introducing this fault confining mechanism are separable. Improving the protocol will not only is a necessary for current applications, but also will increase the competitive edge of CAN in the future applications.

Keyword: CAN； fault； safety； fault confining mechanism

The debate about CAN fault originates from two papers published in <micro controller and embedded system> (a Chinese journal) [1], [2]: “An undiscovered safety related fault in CAN” and “A bus off case of CAN error passive transmitter”. Before sending to journal these papers were sent to specialists inside country and abroad for their comments. No argument about the main point of papers was received except the supporting. The founding of fault is an important issue; it has affect on the interest of many participants, e.g. chip maker, developing tool provider, ECU supplier, OEM, high layer protocol supplier, high layer product supplier, and various service provider etc. to avoid the possibility that these participants intentionally underestimate the severity of the problem for their interest, it is thought that inform to the independent third party organization is necessary which represents the interest of third party and makes the judgment if the problem does exist and its danger. The third party includes driver, occupants, passengers, insurance company and highway regulation organization etc. hence not only the papers should be sent to the CAN industry related party, but also be noticed to the concerning safety related party. Then the problem could be treated properly. Based on this consideration the papers were sent to the hot line of U.S. Department of Transportation, National Highway Traffic Safety Administration for their attention. Later papers were passed to ISO. ISO TC/22/SC3 is in charge of standardization of communication in vehicle. Head of TC/22/SC3/WG1/TF1 is Mr. Zeltwanger , president of CiA. Convener of ISO TC/22/SC3/WG1 is from Bosch. CiA had responses and were answered. Finally a statement from Bosch was transferred from Mr. Zeltwanger through registered specialist of China in ISO. Naturally, the readers of <Micro controller and embedded system> have known the original two papers, they also should be noticed the opinion of Bosch and new progress. Here is my comment on the statement of Bosch. The full text of Bosch statement is also appended for reader’s reference.

The title of Bosch statement is "It's not a bug, it's a feature!" it says “In these articles there have been concerns regarding the CAN protocol's fault confinement regarding local errors seen by error-passive nodes. It is stated that an error-passive node, after having seen a local error (i.e. an error not seen by other nodes), may not be able to complete its passive error flag when the traffic load on the CAN bus is so high that there is virtually no idle time between consecutive frames. The consequence is that this node will not be able to receive or to transmit frames, until it can complete its passive error frame in an idle phase or until an active error frame is sent by another node. An error-passive transmitter could be caused by this condition to increment its error counter until it reaches bus-off state. “ then it says：“ This is the intended behavior of the CAN protocol!“at last part it says: “But both methods try to solve a problem that does not exist.”

The quotation is slightly different from the original papers. The bus idle time is uncontrollable, so the traffic loads. Even there are some bus idle times, the distribution of

bus idle time is also uncontrollable. That can not assure correct ending of passive error frame. Peak traffic load is formed by the nature of message arriving time. The arriving time of event triggered message is random variable. The arriving time of periodic message changes according its local timer. For example if there are two message which have 5ms initial phase and 200ppm oscillator difference, the phase will be diminished in 25 seconds. In some common multiple time all periodic message will have almost zero phase and form a peak traffic load that is assumed in CAN scheduling analysis for worst case delivering time. The slightly difference does not affect the meaning of Bosch statement. Based on above description, the word “feature” and “intended behavior” actually admit the existence of quasi or real bus off. Bosch has a direct behavior description in later part. At the same time Bosch does not admit that the consequence is harmful. It emphases the good effect of this behavior.

It says:”The purpose of the fault confinement mechanism is to prevent potentially faulty nodes from disturbing the communication of the remaining nodes.” It explains that the purpose can be reached by entering error passive state or bus off state of faulty node. Then it says: ” a receiver that reached error-passive because of its REC can switch back to error-active after receiving one single fault-free message (see fault confinement rule 8), giving it back the possibility to send at least one active error frame.” After talking about allowable bus load of 50%, it says: “A peak load is typically caused by disturbances on the CAN bus. In this case, communication is disrupted for some time and the pending transmissions accumulate. When the disturbance ends, all those pending messages will be sent, in the order of their identifiers, consecutively.” “If the disturbance was caused by a faulty node, and was ended by the faulty node entering error-passive state, it is the intended function of the fault confinement to *keep this node in the error-passive state at least until all messages that have been delayed by the disturbance have been transmitted,* i.e. until the peak load has ended.”

Here the claim of the peak load ends with the ending of disturbance is not fully correct as said before. The bus load limitation of 50% is also not a guarantee to prevent the occurrence of quasi or real bus off state which has been described in example in paper [1]. The good effect and bad side effect can be divided. When a node has entered into error passive state, it has no intervention to the communication of other nodes, because the passive error frame is a string of recessive bits. It is unnecessary to keep it out off the communication. From this paragraph it is clear that the current fault confinement mechanism will *keep this node in the error-passive state at least until all messages that have been delayed by the disturbance have been transmitted.* Hence it will stop the transmission of that error passive node no matter how high the priority of pending message is. This evidences the analysis in paper [2]. But it does not mentioned directly if the receiving is disabled.

Today the industry acknowledged that the introducing of error passive state is a positive compromise between reliability and availability. Bosch only emphasis the good side, but does not evaluate the consequence of losing communication service. If the losing of communication service is a bug should be decided by users based on the harm to the application. It will not be changed by how it be named.

Further research shows that there is a very serious failure scenario. The basic track is: there is heavy conductive disturbance (ISO7637 type 1）-CAN driver will have the bit error of writing”0”/reading”1” in case of decreasing CANH-CANL due to supply voltage drop –rule of CAN protocol stipulates the sending of error frame (node can repeatedly send error frame) –rule of CAN protocol stipulates that bit error in active error flag will cause TEC+8. This means that a long supply voltage drop will easily push the node in error passive state immediately. The error passive state is not a rare case. Then a further local error will push the node into quasi or real bus off case; make it loss the communication service. The simulation in paper [3] shows the consequence of losing CAN communication service that the plow out or spin in turning road is possible. The bug in CAN fault confinement design is a danger block in this possible failure chain.

The consequence of losing service destroys the basis of real time application- Timeliness. In many applications only a limited number of data losses could be allowed. These applications have considered the data fault tolerant. If such long losing communication should be tolerant, the traffic load should be increased further. When considering the limitation of bus load this is very hard to satisfy.

When safety standard IEC61508，EN50159 are applied in automotive industry, it is necessary to do fault and risk

analysis. Because a small fault may result an error in component, the component fault may result an error in sub-system, the sub-system fault may result an error in its upper-system… the fault tree must be clearly define, and its probability be assessed. After doing these analysis the original fault can be ascertained to be safety related or not. As to this fault in CAN fault confinement design, it is very typical one that could cause vehicle safety failure. In general communication system a local fault may cause one frame lost. If the application can tolerate this loss, the failure chain is end; no propagation further exists. The fault in CAN fault confinement design may cause about 100 frames lost. Besides, it makes all frames pending in this node unable to transmit. That means it can affect other system function. For example, based on the realization of message implementation in ECU, if motor speed signal is lost, it will affect gearbox control, ABS, ASR and air conditioner system. If the wheel speed signal is lost, it will affect electronic fuel injection system, ASR and exhaust recycling system. If gear ratio signal is lost, it will affect electronic fuel injection system, ASR and exhaust recycling. If the gateway in dashboard is the faulty node, the engine may stop working. These examples show that a local fault may turn a node to failure state; the node fault may cause other system function failure. Among the affected functions some are related with energy saving, or exhaust control, or operation stability, but some are related with braking or steering.

If CAN bus lost serviceability, it will lead to control system failure. Vehicle is a moving object; the failure of control system will cause the motion uncontrollable, and then leads to a safety problem. I don't know to what extent the car must be recall. But from news report, any fault that will endanger human life will be recalled. This makes great pressure to the related party. It is understandable that they take a cautious and a wait-and-see attitude in front of this bug. But, if the failure of loss service do exist that is admitted by Bosch implicitly, the consequence of recall is inevitable.

Bosch has not mentioned this bad consequence of losing serviceability in its statement. This means that they don't realize this bad side effect. As mentioned in paper [1], the origin of quasi bus off status is that the passive error frame has no enough time to finish its error delimiter. But the possible scenarios are far more than what described in Bosch CAN 2.O specification. If Bosch has known these scenarios, they would have been included in CAN 2.0 specification. Bosch has not warn the designer of the CAN design tool. Because any high priority message can not be serviced when the fault activated; and the error passive state is not rare case; scheduling design become less useful. Just like a leak bucket, when there is a hole in its bottom, the length of side board has no meaning. Bug destroys the completeness of theoretical basis of tool. The scheduling result is not guaranteed, so is the control function. At same time there is no report to show the delay effect in case of the fault activated like what described in this statement before. Hence the bad side effect of this fault and its scenarios are not thoroughly considered before. It is a bug.

Actually, the bad side effect-losing serviceability- can be remitted. In paper [1] two schemes are mentioned which are also mentioned in Bosch statement. There are other possible solutions. For example, define the dominant bit in passive error delimiter part as a request of overload frame instead of an error. This overload frame will coexist with other nodes error frame. This make the error passive node quickly synchronized with other node. This scheme has the drawback of waste communication band and artificially increase error counter of other nodes. The scheme in paper [1] is a better solution. While it retains the good effect of introducing error passive state, it avoids the bad side effect. The problem of losing serviceability is solved. The limitation of bus load due to this fault can be weakening. It is beneficial to most of us. No need to pray the bug not activated.

For massive CAN applications, especially those that have good environment and less critical requirement (even in vehicle some application are not safety related), the panic about CAN fault is unnecessary. What is needed is make an evaluation about the environment and the requirement of the application. Doing some test if necessary to strengthen the confidence.

The discussion about CAN fault does not mean the objection of CAN. Though CAN has some other problems or shortcomings, maybe serious problems, it is still a best protocol for vehicle control communication. The most outstanding feature is the function of auto-retransmission-on –error. In the recent years the debate about the relative merit on time triggered protocol and event triggered protocol prefers the time triggered protocol for safety critical

application. It is said that time triggered is more suitable for x-by-wire applications. But research [4] shows that because the ability of auto-retransmission-on–error of CAN, the probability of untimely delivery of CAN is several orders lower than TTCAN with duplication transmission. It is reasonable to presume that other time triggered protocol will loss in this kind of comparison except it is equipped with complicated high layer fault correction measure. But the bug in CAN fault confinement design will make this great cost/performance edge useless. Hence a further improvement in CAN has a great value. Whose party who does will satisfy the current urgent demanding, also will win in the future. This is the time of industry shuffling. The debate becomes clear because of Bosch statement- the inventor of CAN. The time to making your conclusion is synchronized between insides of county and abroad. As to me, it is a bug. To Chinese IC maker, ECU maker and OEM of vehicle, great attention must be paid to this issue, quick action must be taken. Any delay in decision will be punished, because this will lead to loss trustiness of consumer. There is report that CAN is used in avionic application [5]. Delay in action to modify CAN chip will also affect the plan of giant jet plane.

Reference：

1. 杨福宇，“CAN 总线系统中的一种安全隐患“，《单片机与嵌入式系统应用》，2009 年第 1 期，第 20-22 页。Fuyu Yang,”An undiscovered safety related fault in CAN”. English version can be provided on request to the author.
2. 杨福宇，“CAN 消极报错发送节点变为离线状态的故障“，《单片机与嵌入式系统应用》，待发。Fuyu Yang,”A bus off case of CAN error passive transmitter”, English version can be provided on request to the author.
3. F.Corno et al.” A MULTI-LEVEL APPROACH TO THE EPENDABILITY ANALYSIS OF CAN NETWORKS FOR AUTOMOTIVE APPLICATIONS” 17th Symposium on Integrated Circuits and Systems Design, 2004. SBCCI 2004. Volume, Issue, 7-11 Sept. 2004 Page(s): 71 – 75
4. Ian Broster, Alan Burns and Guillermo Rodr´ıguez-Navas, “Comparing Real-time Communication under Electromagnetic Interference”， Proceedings of 16th Euromicro Conference on Real-Time System 2004. ECRTS 2004 p.45-52
5. 刘亚飞，“控制器局域网协议(CAN)技术隐患分析”，《中国电子报》2009 年 2 月 5 日第 4 版

---

appendix：

Statement of Bosch

"It's not a bug, it's a feature!"

In the CAN licence specification there are described several examples similar to the examples mentioned in the articles from Fuyu Yang. In these articles there have been concerns regarding the CAN protocol's fault confinement regarding local errors seen by error-passive nodes. It is stated that an error-passive node, after having seen a local error (i.e. an error not seen by other nodes), may not be able to complete its passive error flag when the traffic load on the CAN bus is so high that there is virtually no idle time between consecutive frames. The consequence is that this node will not be able to receive or to transmit frames, until it can complete its passive error frame in an idle phase or until an active error frame is sent by another node. An error-passive transmitter could be caused by this condition to increment its error counter until it reaches bus-off state.

This is the intended behavior of the CAN protocol!

CAN's fault confinement mechanism is designed to distinguish between local errors and global errors. Global errors are assumed to be caused by external influence (e.g. electromagnetic interference), while for local errors it is assumed that the root cause may be located in the local node (e.g. aged components or bad contacts). The purpose of the fault confinement mechanism is to prevent potentially faulty nodes from disturbing the communication of the remaining nodes.

That is the reason for fault confinement rule 2: "When a RECEIVER detects a 'dominant' bit as the first bit after sending an ERROR FLAG the RECEIVE ERROR COUNT will be increased by 8." This causes REC to be additionally

increased if the cause for the error frame seems to have been local. So the potentially faulty nodes will reach error-passive or bus off state earlier than those nodes, which see mostly global errors. Without the ability to start active error frames, they are less likely to disturb other node's communication.

But a receiver that reached error-passive because of its REC can switch back to error-active after receiving one single fault-free message (see fault confinement rule 8), giving it back the possibility to send at least one active error frame.

CAN systems should be designed with an average bus-load of less than 50%. This leaves a reserve for peak loads and ensures that error-passive nodes having seen local errors will get enough idle time to re-integrate themselves into the CAN communication. A peak load is typically caused by disturbances on the CAN bus. In this case, communication is disrupted for some time and the pending transmissions accumulate. When the disturbance ends, all those pending messages will be sent, in the order of their identifiers, consecutively.

If the disturbance was caused by a faulty node, and was ended by the faulty node entering error-passive state, it is the intended function of the fault confinement to keep this node in the error-passive state at least until all messages that have been delayed by the disturbance have been transmitted, i.e. until the peak load has ended.

Two methods have been proposed how error-passive nodes can re-integrate themselves faster after local errors. The first method is to shorten the error delimiter of error-passive nodes by a constant value. This method would cause disruptions in case of global errors, when the error-active nodes would see an SOF (transmitted by the error-passive node) during their error delimiter or intermission. The second method is to shorten the error delimiter of error-passive nodes by a variable value, the variable to be calculated from the position and type of the assumed local error. This would lead to better results at the cost of high effort in the CAN protocol controller.

But both methods try to solve a problem that does not exist.

Florian Hartwich, Robert Bosch GmbH
Automotive Electronics, Engineering Integrated Circuit Systems (AE/EIY)