CAN的安全隐患

An Undiscovered Safety Related Fault in CAN

----消极报错节点不能正常收发

Real bus off state of error passive node

杨福宇 Fuyu Yang

Email:yfy812@163.com

成熟的CAN有问题的严重性

- 2006年一年CAN售出5亿片

  ”CAN in Automation celebrates first 15 years”, 15-year-cia.pdf

- 2007年中国生产880万辆车
- 对安全，环保，节能的影响

引用的标准

- ISO/TC 22/SC3. International standard: ISO -11898-1, 2003,"Road Vehicles-Controller Area Network (CAN) –part1: Data link layer and physical signaling"
- ISO/TC 22/SC3. International standard: ISO 16845, 2004 "Road Vehicles-Controller Area Network (CAN)-Conformance test plan"
- Robert Bosch GmbH. CAN Specification Version 2.0, September 1991

问题的根源在标准（一）

- ” In order to terminate an ERROR FRAME correctly, an ’error passive’ node may need the bus to be ’bus idle’ for at least 3 bit times (if there is a local error at an ’error passive’ receiver). Therefore the bus should not be loaded to 100%.” ---Bosch CAN 2.0A 3.1.3
- 即使负载率小，也无法保证3bit总线空闲

问题的根源在标准（二）

- “A message, which is pending for transmission during the transmission of another message, is started in the first bit following INTERMISSION.”
- 最坏的情况是所有的消息都挂起在那里等待发送

问题的根源在标准（三）

- 消极报错帧分界符的长度是8位隐位
- 消极报错帧分界符内的显位是格式错，它要引起新的消极报错帧
- ISO 16845 :7.5.6 Form error in passive error delimiter (receiver)
- ISO 16845 :8.5.13 Form error in passive error delimiter (transmitter)

7.5.6内容（8.5.13相同）

- 7.5.6.1 Purpose and limits of test case

…测试设备将报错分界符的8个隐位之一用显位代替 …The LT replace one of the eight recessive bits of the error delimiter by a dominant bit. …

- 7.5.6.2 Test case organization

…在接收报错分界符时测试设备按7.5.6.1款制造一个格式错，然后等（6+7）位再送一个显位破坏报错分界符的最后一位，被测设备在测试设备送的最后一个显位后开始一个过载帧…During the reception of the error delimiter, the LT creates a form error according to 7.5.6.1.

After creating the form error, the LT waits for (6+7) bit time before sending a dominant bit, corrupting the last bit of the error delimiter.

The IUT shall generate an overload frame starting at the position following the last dominant bit sent by LT.

可能造成此类故障的情况超过Bosch预计

- 消极报错接收节点的本地故障引起（Bosch提到）
- 消极报错发送节点的本地故障引起
- 偶尔主动报错节点的本地故障引起
- 避免故障要求的空闲时间要更多(10 bit 而不是3 bit)

出错情况举例

- 消极报错接收节点因本地故障（如干扰）有误判时

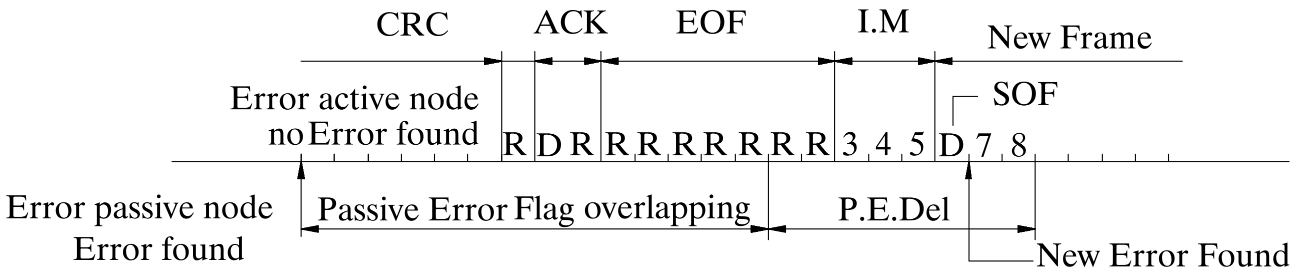


Figure 1 Local fault in error passive receicer

出错情况举例

消极报错接收节点有一次漏判时

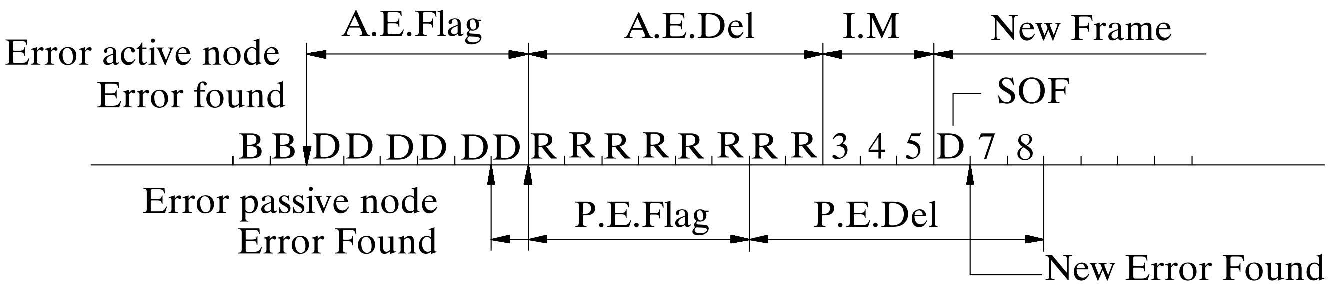


Figure 2 Global bit stuffing error with local fault in error passive receicer

出错情况举例

- 消极报错接收节点误判发生在EOF域，至少10bit总线空闲才能使它与其它节点同步

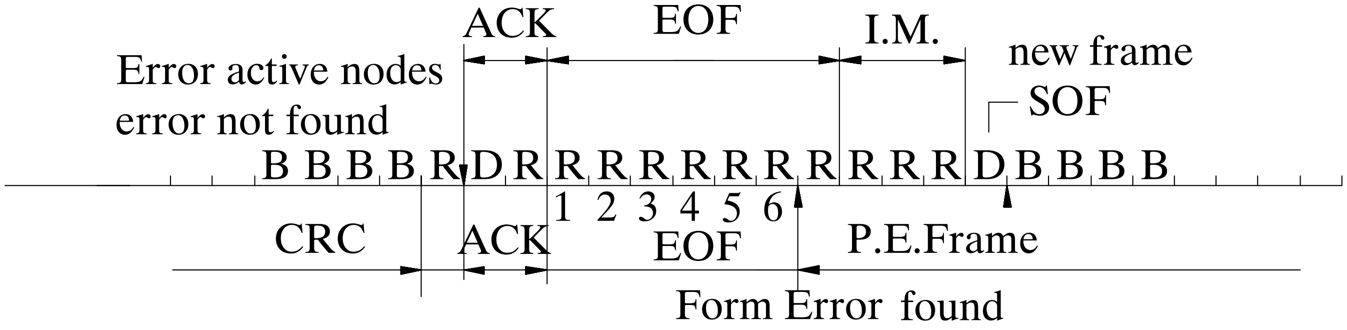


Figure 3 Local fault in error passive receiver only

出错情况举例

- 消极报错发送节点误判ACK位

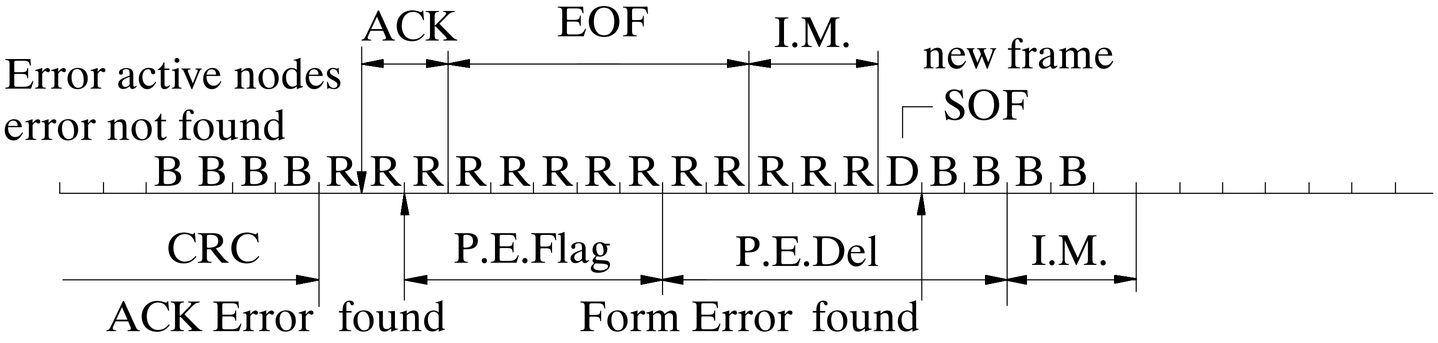


Figure 4 Local fault of error passive transmitter only

出错情况举例

- 消极报错发送节点在CRC分界符处误判

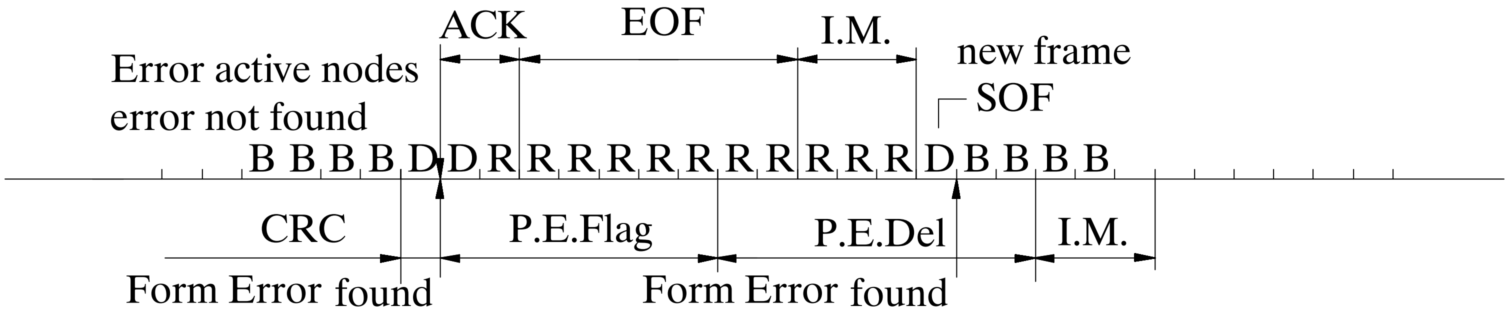


Figure 5 Local fault of error passive transmitter only

出错情况举例

- 消极报错发送节点在ACK分界符有误判

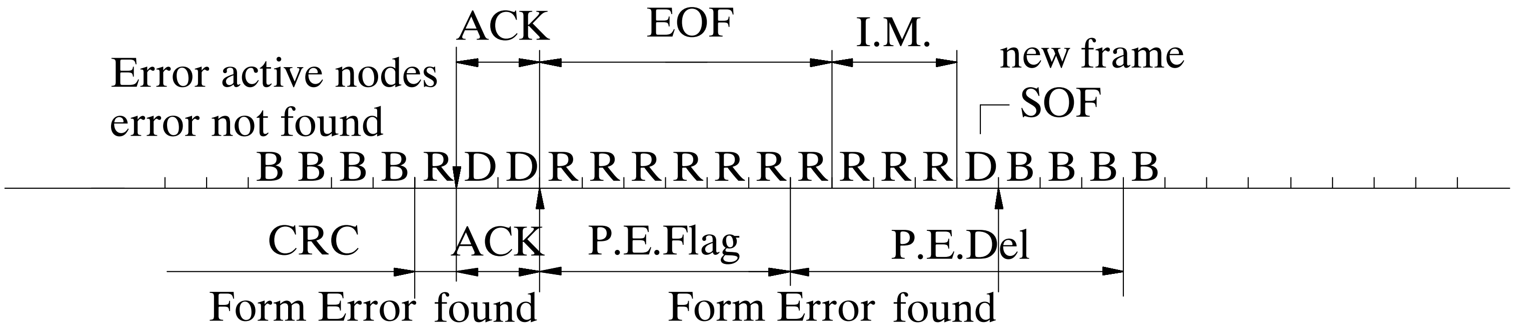


Figure 6 Local fault of error passive transmitter only

出错情况举例

- 当系统小，只留下一个主动报错节点时，它的误判引起消极报错节点不同步

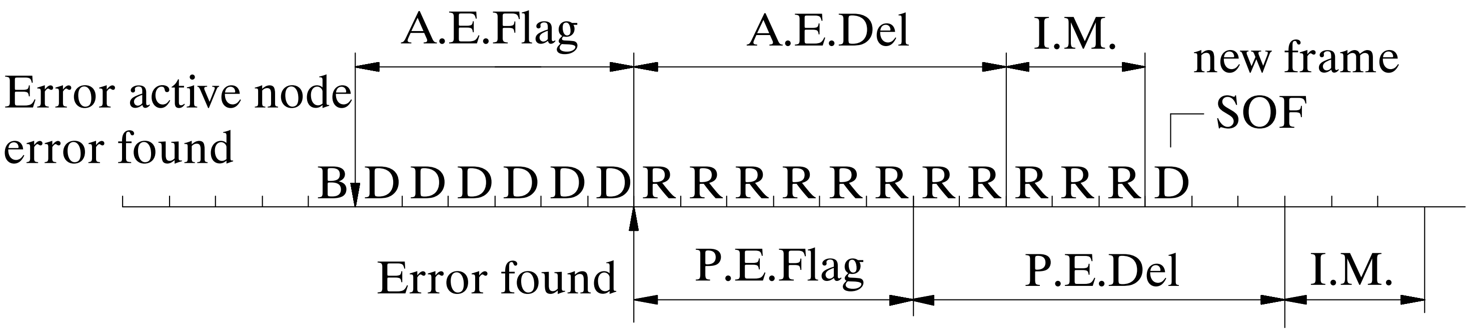


Figure 7 local fault in error active node causes failure in error passive node.

总的出错情况

- 出错后消极报错节点与其它节点同步的情况有很多
- 出错情况造成消极报错节点不同步的例子还有很多

消极报错节点不同步后续情形（一）

□ 新帧中有全局错，节点在主动报错帧结束时同步

□ 连续出错的概率小，意味着此种情况概率小

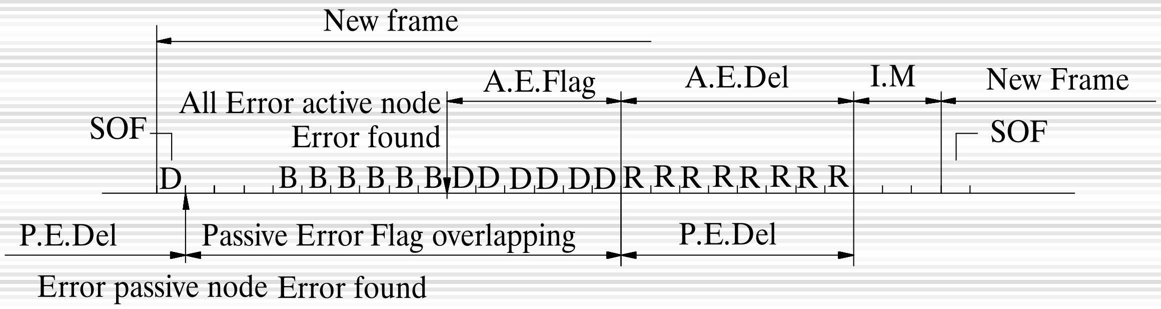


Fig.8a) Error passive node is synchronized at an active error frame

消极报错节点不同步后续情形（二）

- 新帧结束后空闲时间足够长后同步
- 这是事件触发协议无法保证的

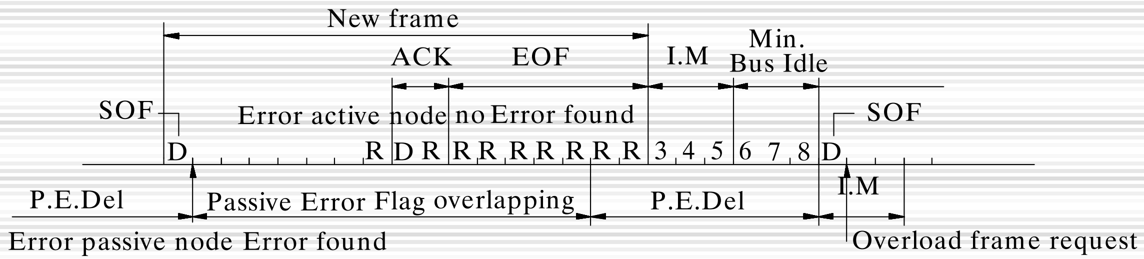


Fig. 8b) Error passive node is synchronized at bus idle time

消极报错节点不同步后续情形（三）

- 新帧正常结束后又有新帧
- 只要挂起帧未送完，消极报错节点就一直错

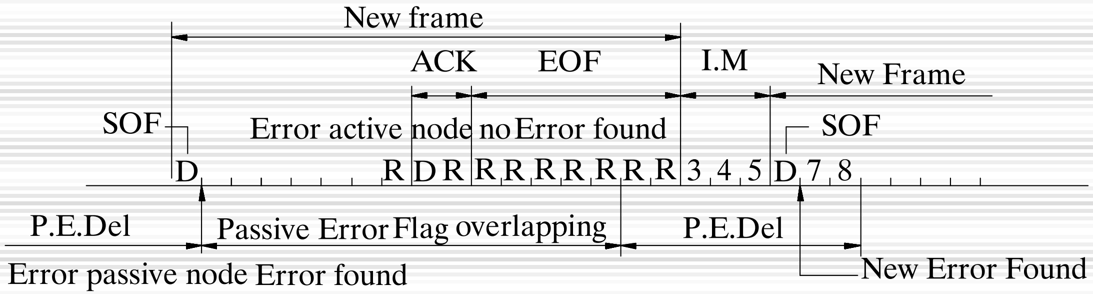

New frame
ACK
EOF
I.M
New Frame
SOF
Error active node no Error found
SOF
D
R D R R R R R R R R 3 4 5 D 7 8
P.E.Del
Passive Error Flag overlapping
P.E.Del
Error passive node Error found
New Error Found

Fig. 8c) Error passive node has new error at SOF of new frame

消极报错节点失去同步的后果

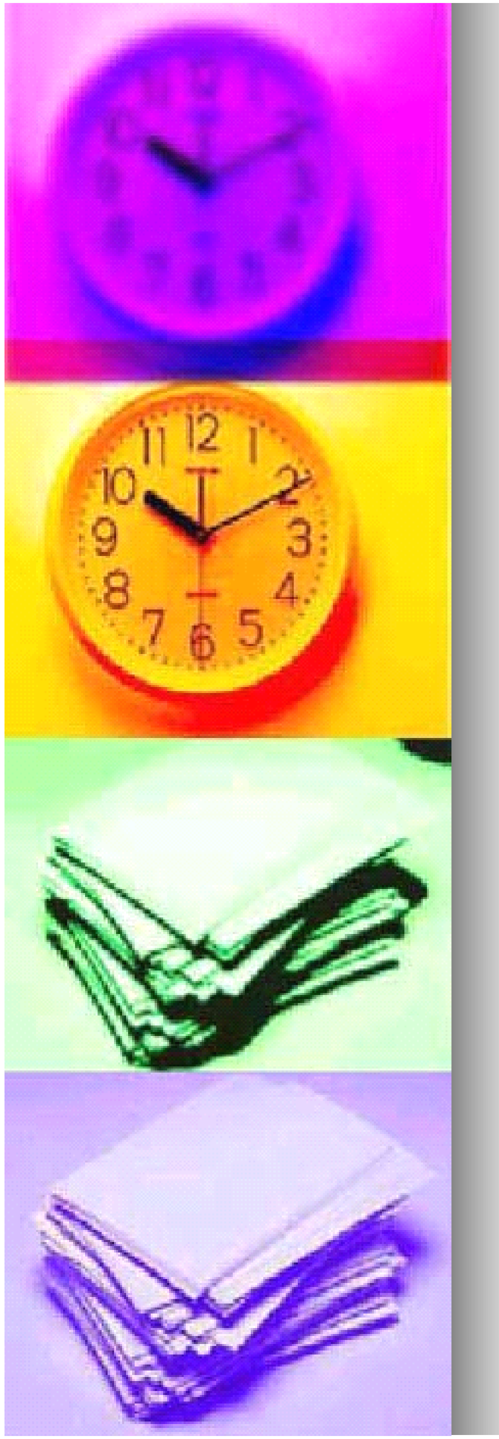
- 消极报错节点在后续帧正常时一直错，它不能收也不能发，处于事实上的离线状态
- 离线的时间为最长最坏响应时间
- 以Tindell计算SAEbenchmark结果为例:250kbps,负载率47.1%时最长最坏响应时间为14ms,若该节点为收发制动压力帧（周期5ms）的节点，相当于丢了3帧
- K. W. Tindell and A. Burns. “Guaranteed Message Latencies for Distributed Safety-Critical Hard Real-Time Control Networks”. Technical Report YCS229, Dept. of Computer Science, University of York, June 1994. YCS-94-229.pdf

消极报错节点失去同步的后果

- 目前的CAN调度理论没有考虑消极报错节点失去同步而离线这种工况
- 即使有一些总线空闲时间，目前的理论也没有考虑因消极报错节点失去同步时引入过载帧的工况
- 调度工具软件的分析结果可信力下降
- 安全性？99.9...%

必须解决消极报错节点出错后的同步问题

- 一种根据消极报错节点出错情况确定消极报错帧分界符长度或状态自动机复位信号的方法已设计好，以保证出错后的同步
- 专利申请中
- ISO16845相应条文应修正
- CAN通信控制器相应功能应改正



谢谢关注！