Items that must be fixed (currently broken) –-2 Errata soon and updated in -3.

* Section 3
  + 3.1.1.3.3 “The sample point shall not be at less than 75% of the bit timing and only one sample point shall be used.” Maximum sample point needs to be specified, such as at 85%? Additionally this requirement is restated a few times… requirements should not be restated. CAN\_FD sample point and CAN 2.0 should be identical (no difference)
* Section 4
  + 4.7 needs to expand to explicitly state not only shall nodes be in recessive state on power up/down but not emit dominant disturbances at all. Ever. – aka transceivers never touch bus until fully initialized. *-3 changes the location of this statement but still needs to be stronger.*
  + 4.7 Does Bus Off Disconnect transceiver? Not at the CAN controller level… maybe this means CAN-off at the processor level by activating the Transceiver disable line?
* Section 5
  + Statement that the ARINC identifier format shall be used? Otherwise it is implied optional
  + Section 5.3 needs to mandate Big Endian with a shall somewhere
  + 5.3.3.1 “To facilitate interchangeability the pre-assigned FIDs in Table 5-3 should be adhered to.” Needs to be shall.
  + 5.3.3 limits units to SI only – this needs to be changed to optional and the unit can be specified in the A825 profile. Chart also needs typo corrections. There is no reason to standardize this as all data is really opaque unless the receiver knows what it means (through the A825 profile). The definition here gets down into the deeper BFE levels and should be left to things like A812.
    - Would like to see this moved in section 7.
  + 5.4.2 NB\_RST needs to specify number of BusOffs. Because as stated an LRU reset counts. This needs to address the possible use of Auto bus\_on as there will not be a reset request.
  + 5.5 should say with the exception of PHSM as it is peer-to-peer but not using the node service interface
  + The current peer-to-peer format does not allow for uniquely addressing a client node. While this may not be a problem for some implementations it will prevent some architectures from using peer-to-peer. Example: smoke detectors needing to communicate with another LRU on the same bus of which there are two of the same unit. Now there are no longer unique IDs. Possible proposal: Client ID instead of the Server FID.
  + 5.7.4 CRC (MIC here…) should not include CAN ID – ID may not travel with the data through a gateway. This means that every user of the data must have knowledge of the associated CAN ID in order to accurately decode the CRC and accept the High Integrity Message. Any benefit for the inclusion of the Message Id in the CRC is nullified by the CAN Frame CRC. If this change is made step 4 of 5.7.4 would no longer be needed (could be deleted)
  + 5.7.4 CRC Polynomial, equation, and test result are incorrect. Needs to be 0x90D9 := x^16+x^15+x^12+x^7+x^6+x^4+x^3+x^0 with check value 0x4084
    - Change initial CRC value to 0xFFFF
    - Change final XOR value to 0xFFFF
    - Change test string of characters to "123456789" (current write-up has incorrect leading "0" value compared to code and the 32-bit CRC test value elsewhere in the standard)
    - May want to clarify that the leading 3 bits of the test string are NOT set to zero since the highest order bits of "0" are '001', which could possibly be confusing in light of item 4 about the message ID bits being set to zero.
    - May want to clarify that the CRC is computed Most Significant Bit first to reduce ambiguity (be careful about abbreviation MSB because that also means "Most Significant Byte")
    - Could we define a CAN Message (ID, Payload and SNo) as a test instead of a test string?
* Section 7
  + No Shalls or musts in section 7 (there are 2)

Items that Boeing would like to see changed

* Inclusion of a requirements matrix at the end of the document with the shalls and maybe shoulds? These should be uniquely numbered to facilitate tracability.
* Section 3
  + 3.1.1.1 As there are two shalls for capacitance, should the method used to measure it be defined? The second Iso-11898-2 reference in 3.1.1.2.1 should be moved to the electromagnetic protection section.
  + Figure 3-10 (in draft -3) needs to say shall use linear topology (not star) and then reference the picture. It can’t say “shall be like this picture”
* Section 4
  + 4.6.3.2 in supplement -3 should mention this is processor managed and not using Autobus on.
  + 4.7 Sleep Mode commentary “currently not used in aircraft environment” should be removed.
  + 4.6.3.1 “The TEC and REC counter values shall be monitored by the node. If the limits that are mentioned under 4.6.3 Error Containment and Bus Off Management have been reached, the node shall either change to “error passive” or “bus off”.” This is in ISO 11898, no? the controller sets Error Passive and Bus Off. no need for shall as we already said several times to be iso compliant. If this is the processer and not the controller, the “shall monitor” should be referenced to PHSM later on.
  + 4.6.3.1 “For network monitoring purpose, the values of TEC and REC should be transmitted regularly on the network.” This should just say shall be transmitted as a part of the PHSM
* Section 5
  + What is the point of having a PVT bit? What does this provide beyond using an opaque data type?
  + 5.2.2 and 5.5 Peer-to-Peer needs to reconsider the PVT bit definition; PVT can be Start of Frame or distinguish data messages from control messages. If a server were to experience an intermittent interrupt it is possible that it would recover in the middle of a transfer and not know where in the transfer process it was, it could interpret the next block as the first in the series.
  + 5.3.2 should be moved to design guidelines or a profiles appendix.
  + 5.3.3.1 Says FID list shall be used with A825 profiles… should change to “FID list shall be used for A825 communication.”
  + FID List should not be split onto the two pages like it currently is. All page 1 FIDS should out prioritize page 2 list
* Requirement that failed node shall fail silent? No disturbances or bringing down the bus? (Section 4 – CAN Controller State management)

Questions

* Section 3
  + 3.2.3.2 “A node shall continue to communicate in normal mode with ground-offset up to or equal to ± 2 Vdc.” Where does this come from?
  + 3.2 “The lines to the transceiver (wires and / or traces on the PCB) must be equal, parallel and as short as possible.” How can this be verified when there is no metric on short? Should be changed to “should be”
* Terminating Resistor: Why @ 1.5 m beyond last node? Empirical data indicates @ node is best. Is this really the right requirement?
* Would like to see guidance on the impacts of splices to the electrical signal and the communication.
  + Is this different by bus speed?
  + What is the impact by the # of splices?
* Would like to see added commentary in Redundancy Management section 7.7 regarding the use of high integrity protocol and sequence numbers. Would there be a reason to NOT employ this for redundancy?
* Additional bus fault scenarios:
  + CAN\_L short to shield
  + CAN node segments with mid bus cross wire
* Architecture Specific Point: Babbling idiot requirement does not take into account system design; meaning that it a failure of a control unit that communicates with lower critical units on a bus is no different than any other failure for that unit (assumes control unit has greater priority on the bus). Requirement is good for lower priority units but not applicable for the higher priority controlling unit