**National Hydrologic Warning Council, ALERT2 Technical Working Group**

**Subject: OEM Compliance to ALERT2 Standard**

**By Robert Thompson (NHWC ALERT2 TWG International Representative)**

**Introduction**

The credibility of a standard is determined by its users and the broader competing industries that have a vested interest for it to succeed or even fail. Original equipment manufacturers (OEM) implement to a standard and in doing so should also ensure it is not only compliant but fully interoperable with other like OEM equipment. Importantly doing so ensures that not only does the device meet the required standard or standards, but it also validates the business decision to what drew the implementer to take this strategic path and purchasing decision in the first place.

Unfortunately building to a standard does not always given assurance that different OEM devices will be interoperable. The reason being is that to do so would require all functionality and behaviour to be the same, to do this a standard would need to include and disclose detail to a level that caters for every operating scenario. This is why interoperability is just as important to follow as the defined standard or set of standards.

Over the years in previous TWG meetings interoperability was an important topic of discussion with initial thoughts as to how this would occur. One option canvassed was to use the original ALERT2 decoder prototype as the reference framework for OEM's to test against. From my understanding this is no longer viable as the standard has moved past the original prototype. There was also discussion as to whether a fee could be paid to a third party to test and validate to the standard/s certifying devices all behave (function) in the same way against the standard.

**Discussion**

**Standard and Interoperability Certification**

1. I raise this topic with the TWG again as I am concerned that we do not have an agreed policy as to what OEM's must demonstrate, if any, to meet the ALERT2 standard and also whether tested and validated interoperability between OEM's is a requirement to allow an OEM to use and distribute devices using the term "Meets ALERT2 standard Version X.X with extensions A, B, C".
2. Currently compliance to the standard and to what level is a risk borne by the entity procuring the equipment. To mitigate or accept the risk an entity procuring devices would need to either:
   1. Undertake a formal expression of interest to market for supply under a detailed specification with terms and conditions. Bidding OEMs or suppliers that put equipment forward must met standard X.X and demonstrate interoperability with other specifically listed OEM devices. They may also wish to nominate future version compliance as a requirement.
   2. Trust OEM devices to be fully standard/s compliant and interoperable with any anomalies being fixed by the OEM. However where is the non-compliance? Company A, B or C? Who will pick up the costs to rectify the network fault? This may include remote sites that are only accessible by costly charter helicopter trips?
   3. Entity to accept all risk and costs to rectify non-compliance, non-interoperability, and implementation ambiguities due to the standard not having enough clarity.
3. The Australian Government would normally take the approach outlined in 2(a) and I think USA Federal Government would also follow similar processes. As part of procuring with Government strict terms and conditions with expressed liabilities must be entered into. This process is often time consuming for smaller OEMs and suppliers who are often not prepared to go through such lengthy and costly processes. This is why being able to state the equipment meets a proven standard and validated as being interoperable could reduce the formal process. As a procurement risk assessment would then demonstrate lower likelihood of non-compliance during operations and maintenance demonstrating lower total cost of ownership.
4. If we were to look at another ICT industry like Internet Protocol networking equipment what approach would OEMs follow? Standards in this space are from the Internet Engineering Task Force IETF with working technical documents called RFCs, Request for Comments. So how does an OEM meet compliance and is their equipment certified? Well it depends? There are standards consortiums or assigned certification partners that large companies contribute funding and/or resources to such testing groups. This allows vendors to submit and undergo certification and interoperability testing. They can then label their equipment as meeting X or is certified X. There are also independent labs that provide testing on a fee basis, these can be commercial or government owned.
5. So what about ALERT2? Standard Compliance, Certified as Interoperable or both? The ALERT2 OEM community is small in comparison to other network and communications hardware OEMs. On that basis I would suggest that funding and appointing a Certification Partner or independent authority is not viable, unless the technology footprint grows at a rapid rate. So is self-regulation the answer and will it be accepted by large enterprise and government procurement governance processes? How do these entities manage this risk and at the same time be accountable for public or shareholder expenditure?

**Non-Compliance and Openness**

1. Why am I raising this topic and why is it a big deal? It is because we probably have all experienced a situation when a device had a defect (hardware or software bug) or didn't behave as documented. The ramifications to resolve could be small, just requiring a software patch that had no other undesired outcomes and low cost as it was a locally accessible device. At the other end of the spectrum the equipment needed to be swapped out or modified at a remote site which was costly and affected operations. The worst case would be a swap out with another manufacturer device being purchased leading to operating procedure changes and even possible retrofitting of plugs, housings, etc.
2. Compliance and Interoperability are sought after attributes as we know it will ease management and associated costs. It should be pointed out that we are focused ALERT2 standard compliance and interoperability and not physical interoperability such as connectors, etc. Therefore any non-compliance in a device that causes a field visit or worse, replacement of the device are the ones that cannot be easily tolerated as it will usually require a report to Senior Management explaining why the device didn't meet the design parameters that you outlined in your business case or tender document. Not a happy place to be in as everyone wears some egg on the face, worst case people can lose jobs.
3. At the moment from my understanding (I have been away for a while so current position could have changed) I feel there are two key areas that need tightening up.
   1. Versioning and an associated compliance matrix. The ALERT2 standard needs to have a numbered version which supports through a documented matrix what parts of each specification are mandatory and must be implemented to meet the quoted version. This matrix would if required clearly state what needs to be done to meet the standard and what is required to meet interoperability if relevant. There needs to be clear disclosure as to what is part of the core standard. Functional enhancements should be separately specified as long as they are independent to affecting the core standard at that version release. For example, if encryption is introduced as a functional enhancement at the application layer and it does not affect anything in the core standard it can be labelled on the device with the associated ALERT2 version as a specified enhancement module (?). However if the encryption implementation requires a small change like a identifier bit in the header or requires integration into one of the other layers then that would require a new ALERT2 version to be created together with the associated functionality matrix showing core (mandatory) and optional parts of the standard to be implemented for this version compliance.
   2. The other area that I feel is very significant and puts at risk the credibility of the ALERT2 standard is TDM slot overrun. The ALERT2 protocol was pitched to most of us that it would have guaranteed delivery if we move away from ALOHA and over to GPS sync'ed TDM. However this is predicated on devices observing and only transmitting within their defined slot allocation, i.e. frames cannot be longer and transmit past their allocated slot window. Currently I understand the practice is reliant on network design to manage sites not clobbering one another. Well unfortunately with all good intentions over time design parameters are pushed, original intent is lost through intellectual property being lost when staff go or neighbours start adding sites which push large frames that run into your slot due to lack of understanding when implemented, poor design or a "I am ok Jack, not my problem". For these reasons I feel this is a critical area for standard compliance in order to keep a key promise.

**Recommendations**

1. The committee support the formal introduction of versioning of the standard with clear documentation accompanying the version that defines specification detail that is mandatory to implement for compliance. Deprecated, optional, developmental and experimental functions, parameters, etc. for that version must also be listed in the documentation and support matrix. There should never be undocumented changes creep into a release version including experimental ones. THE TWG is the Change Advisory Board and as such must approve changes and notifications to all stakeholders. A list of supported enhancements that can be independently implemented from the core standard (app layer encryption) and their associated ALERT 2 core version should also be listed. This recommendation is a critical requirement to allow meaningful discussion around interoperability and standards compliance between hardware and software developers. It will also allow users to request specific versions of ALERT2 devices knowing exactly what they are getting as it is clearly documented in the version feature matrix.
2. Providing some assurance to purchasers and users of ALERT2 as to standards compliance and interoperability at this stage needs to be industry lead and funded. My recommendation is that OEMs make it their responsibility to undergo interoperability and compliance testing of their equipment. This could be through lending or purchasing another OEM device and undertake their own testing or OEMs enter into buddy arrangements. The OEM would test the buddy OEM device against theirs using an agreed test plan, the buddy in turn tests the other OEM .device against theirs. This way they are not testing their own device. If no industry compliance or interoperability testing program is devised it will push the risk back onto the user procuring the equipment. We had this exact scenario happen in Australia and the result was that one company become the dominant supplier with a company folding due to non-interoperability. The Australian ALERT community was then reluctant to purchase from anyone else as interoperability was always there to be proven.
3. If a mandatory feature in an ALERT2 version is not fully implemented as specified in the standard, or only partially it must be clearly disclosed by the OEM and subsequent resellers through a cross reference showing compliance to that version matrix. i.e. TDM slot overrun.
4. TDM slot enforcement to be agreed as 'required to meet the standard'. To assist two new information bits are suggested. This will ensure network integrity but also assist in base network management health reporting.
   1. One bit is (set) and required to indicate that a frame was larger than the allowed slot size and rest of the message is dropped. Or if a second info bit is supported it is processed as per the second TDM Slot indicator bit (described next).
   2. The second bit could have three options, (1) whole frame dropped; (2) frame truncated and rest of data outside of frame dropped; (3) frame truncated and remained data will be sent in next available slot. Yes there are three options for a two option bit implementation. This is where discussion will determine picking two or implementing all three requiring two a bit status flag (described next).
   3. An alternative would be to have a two bit TDM slot info flag,
      1. 00: Frame within slot size, sent as normal.
      2. 01: Overrun - whole frame dropped
      3. 10: Overrun - frame truncated and excess dropped.
      4. 11: Overrun - frame truncated and excess processed into buffer for future frame processing and transmission (may be at lower priority to real-time data as device was naughty).
   4. Please note that I decided not to specify how and where this bit information should be applied. I felt that providing the functional requirement is best and the equipment implementers are in a better position to suggest how, especially considering the number of other protocol enhancements being suggested. The brute force approach would be to drop whole frame or truncate the frame to the slot size to enforce the standard and have no information bits. The down side is that you would not get this valuable information making it harder to determine a slot overrun is happening. Data loss analysis would be more difficult.

**END OF DOCUMENT**