ATNP WG 2 WP/241

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL (ATNP)
WORKING GROUP 1

5-14 February, 1996

"End-through-End" Data Integrity and the ATN

Presented by Ron Jones
(Prepared by W. Scales)

Summary

This paper examines certain aspects of "end-through-end" data integrity in the ATN environment. The term "end-through-end" is used to denote the complete information path, including non-OSI extensions of the ATN. The FAA has documented "end-through-end" data integrity requirements as part of an Operational Requirements Document (ORD). Relative to these requirements, the ATN is expected to provide excellent end-to-end data integrity, even when all of the physical paths making up the network operate in a severely degraded mode. The terrestrial extensions of the ATN in the US are also expected to provide excellent data integrity. Although non-OSI extensions on the aircraft are still being defined, it is entirely within the state of the art to provide excellent integrity for these extensions.

References

1. "Operational Requirements for the Aeronautical Data Link System," FAA Data Link Operational Requirements Team, 3 January 1995.

2. J. Fletcher, "An Arithmetic Checksum for Serial Transmission," IEEE Transactions on Communications, January 1982.

3 . T. Fujiwara, et al., "On the Undetected Error Probability for Shortened Hamming Codes," IEEE Transactions on Communications, June 1985.

1.0 Scope

Data integrity is only one aspect of system safety. This paper is limited in scope, in that it does not consider the following effects:

lost messages,
duplicate messages,
out-of-sequence messages,
the frequency of connection reset or release operations,
software errors, or,
deliberate attempts to corrupt data.

The paper does not constitute a safety study; it is only intended to illustrate, through a series of examples, the feasibility of meeting the data integrity requirements for air/ground data link in the expected ATN environment.

2.0 Overview of Significant Results

The FAA ORD (Reference 1) for aeronautical data link defines data integrity as the probability of undetected error. For addressable data link functions, the required integrity value is 10^{-6} or 10^{-7}, depending on the flight domain (oceanic, en route, terminal, airport), time frame (near term, long term) and the service category (e.g., pilot/controller communications). Based on the use of the TP4 checksum, in conjunction with link layer Cyclic Redundancy Checks (CRCs) of length 16 or greater, the end-to-end ATN data integrity is expected to be better than the most demanding FAA requirement by more than an order of magnitude, even if all of the physical layers in the end-to-end path operate continuously in a severely degraded mode. The terrestrial non-OSI extensions of the ATN in the US will degrade the overall integrity by some small amount, but probably by not more than a factor of about two. Non-OSI extensions of the ATN on the aircraft currently represent the greatest area of uncertainty. However, the avionics industry has experience with high-integrity onboard systems, and it is clearly feasible to provide high levels of onboard data transfer integrity at reasonable cost.

Appendix A treats two cases in which links operate at normal, rather than severely degraded, physical bit error rates. The results of these analyses suggest that the actual data integrity provided by link layer and transport layer mechanisms is many orders of magnitude better than the "nominal worst case".

Safety analyses usually address the probability of one or more undesirable (potentially unsafe) events per flight hour. An initial attempt was made to scope the probability of undetected message hour per flight hour, based on the RTCA SC-165 oceanic traffic model. This exercise yielded less than 4×10^{-7} corrupted messages per flight hour, under a general set of assumptions. This figure compares very favorably with current safety guidelines for air traffic control communication errors, and is certainly far below the rate of human error with ATC voice communications. There is no corresponding standardized

traffic model for domestic airspace, so the corresponding domestic calculation was not made.

3.0 Simplified Error Model

The primary error model used here is a well-known model in which all of the bits within each frame are scrambled by the physical layer (i.e., bit error probability = 0.5). Nevertheless, it is assumed that modulators do not lose synchronization, frame synchronization is maintained, and the network somehow manages to get all of the packets to their intended destinations. Thus, the entire data integrity burden falls on the data integrity checks within the data link and transport layers. This is obviously much worse than any real situation, but it greatly facilitates calculation, and if this "nominal worst case" model yields acceptable results, intensive analysis and simulation can usually be averted. The model is also relatively immune to questions about what happens if one or more links are degraded, since all of the physical layers in the end-to-end path are assumed to be severely degraded.

4.0 ATN End-to-End Data Integrity

We first examine the ATN end-to-end integrity. The integrity through the total path, including non-OSI extensions (i.e., for distribution of application data beyond the ATN end system), will then be examined.

The primary end-to-end data integrity mechanism in the ATN is the Fletcher checksum (TP4 checksum -- see Reference 2). This checksum is known to have the following characteristics:

- Detects all but ~ 1 in 65,000 of all possible error patterns
- Detects all single bit errors
- Detects all double bit errors PROVIDED there are fewer than 2040 bits (255 octets) between the corrupted bits.

Clearly, the TP4 checksum, considered in isolation, cannot assure an undetected error probability of 10^{-6} or 10^{-7}. However, the transport service (using the TP4 checksum) will provide an undetected error probability of e.g., 10^{-6} if no more than one in 16 of the TPDUs delivered to it are corrupted or 10^{-7} if no more than one in 160 TPDUs are corrupted. (This conclusion assumes that the transport protocol does not segment TSDUs.) Note that these are stated as sufficient conditions, not necessary conditions.

The simplified error model will be applied in three examples. In each example, a controller-pilot message is transferred across the ATN. The three examples relate to the use of Mode S Data Link, VHF Data Link, and Aeronautical Mobile Satellite Service (AMSS) as the air/ground subnetwork. The results of these examples are as follows:

Air/Ground Subnetwork	Probability of Undetected Error (Transport Service Data Unit)
Mode S	$< 10^{-9}$
VDL	$< 1.2 \times 10^{-9}$
AMSS	$< 2 \times 10^{-9}$

Note that these results are expressed as nominal upper bounds. The differences between the upper bounds do not necessarily reflect the degree of differences between the subnetworks in normal operating conditions. Note also that the results are strongly influenced by the integrity limitations of the terrestrial and airborne links.

4.1 Example 1: CPDLC via Mode S

This example is illustrated in Figure 1. A CPDLC message is transferred from the ground ATN end system to the airborne ATN end system. It can be seen that there are only four links in the ATN end-to-end path. (This assumes that the Mode S ADLP is co-hosted with either the Mode S transponder or the Communications Management Unit.)

In these examples, a CPDLC (application) message containing 6 octets will be considered. The transport layer adds 9 octets to this message; the Internetwork Protocol adds an additional 60 octets, so the uncompressed packet handled by the ground-ground subnetworks is 75 octets. In general, packets of this length can be handled in a single frame, e.g., by X.25 or LAN protocols. For transmission over the air/ground subnetwork, the network header is compressed to 6 octets, so there are 6 + 9 + 6 = 21 octets of subnetwork user data. An additional 3 octets of subnetwork overhead brings the total link user data field to 24 octets. This can be transmitted in four Standard Length Messages (of 7 octets each), which are link layer frames.

In summary, there are two ground-ground links, each using a 16-bit CRC, and one avionics link, also using a 16-bit CRC. The message is handled in a single frame on all three links. The message is handled in four frames on the air/ground link, but this link is protected with a 24-bit CRC.

As with any well-designed data integrity check, an r-bit CRC will detect all but one in 2^r of all possible error sequences. The probability that one or more of the CRCs will fail to detect an error during the message transfer is therefore bounded by:

$$1-(1-2^{-16})^3(1-2^{-24})^4 \sim 5 \times 10^{-5}.$$

Note that the contribution of Mode S data link to this result is approximately 4×2^{-24} or 2×10^{-7}, which is a negligible component of the total.

Since the CRCs are structurally unrelated to the TP4 checksum, the error patterns that cause a CRC to fail (i.e., modulo-2 multiples of the CRC generator polynomial) appear to the TP4 checksum as more-or-less pseudo-random sequences. Therefore, only one of these sequences in 2^{16} will cause a corrupted TSDU to be delivered to the transport service user. The probability of such an event is bounded by:

$$(5 \times 10^{-5}) \times 2^{-16} \sim 10^{-9}$$

4.1.1 Caveats for the CPDLC via Mode S Example

It can be shown that pure digital noise in each frame does not generally produce the worst-case undetected (frame) error rate. (The potential impact of this counter-intuitive effect will be examined later.) For this reason, it is more appropriate to refer to a "nominal worst case" than to a strict mathematical bound.

This example deals with the Mode S uplink. In some cases, the Mode S downlink uses forward error correction (FEC) based on the CRC after error detection. For this reason, the "pure noise" model used on the other links does not yield meaningful results for the Mode S downlink. There is a finite probability that the (forward) corrected frame will be "incorrectly corrected", e.g., by confusing an uncorrectable error sequence with a correctable error sequence. The impact of this effect is still under review, but preliminary information available to date suggests that, in an operational environment, the integrity degradation due to the downlink FEC may be a second-order effect.

Finally, the ground topology shown in the example is represented as a typical case rather than a worst case.

4.2 Example 2: CPDLC via VHF Data Link

This example is illustrated in Figure 2. As in Example 1, A CPDLC message is transferred from the ground ATN end system to the airborne ATN end system. It can be seen that there are now five links in the ATN end-to-end path. The packet length calculations for VDL are generally the same as for Mode S data link, except that VDL adds four octets of subnetwork overhead, resulting in 25 octets of link user data. This can be accommodated in a single VDL frame.

VDL applies a 16-bit CRC to each frame. Using the methodology described above, the probability that one or more of the five CRCs in the end-to-end path will fail to detect an error is nominally bounded by:

$$1-(1-2^{-16})^{5} \sim 8 \times 10^{-5}$$

The probability that such an error will occur, then go undetected by the TP4 checksum, is nominally bounded by

$$(8 \times 10^{-5}) \times 2^{-16} \sim 1.2 \times 10^{-9}$$

4.3 Example 3: CPDLC via Satcom

The third example uses AMSS as the data link (Figure 3). The example is structurally identical to the VDL example, except that the message would be segmented into four AMSS frames (P-channel signal units), each with a 16-bit CRC. Thus the total number of CRCs in the end-to-end path (including segmentation effects) is eight. The probability that one or more of these CRCs will fail to detect an error is nominally bounded by:

$$1-(1-2^{-16})^{8} \sim 1.3 \times 10^{-4}$$

Applying the further protection of the TP4 checksum yields

$$(1.3 \times 10^{-4}) \times 2^{-16} \sim 2 \times 10^{-9}$$

4.4 Caveats for the AMSS and VDL Examples

The topology in these examples is represent as a typical topology, not a worst-case topology. As noted in the Mode S example, pure noise in each frame is not always the worst case. The impact of this limitation will now be examined.

4.5 Limitations of the Error Model

Table 1 shows, for the CRC used in CCITT X.25, VDL, AMSS, and many other links, the actual undetected error probability for random errors throughout the frame, and for the Bit Error Rate (BER) that produces the worst-case frame error probability for each of several frame lengths. (See Reference 3.)

Table 1: Actual Worst Case Error Probabilities for CCITT-16 ($1 + x^5 + x^{12} + x^{16}$)

Frame Length (Bits) -- Including Checkbits	Worst Case Bit Error Rate	Undetected Error Probability
32	0.13	1.0×10^{-4}
40	0.105	7.8×10^{-5}
50	0.0885	5.1×10^{-5}
64	0.0703	3.2×10^{-5}
128	0.0455	1.7×10^{-5}
32, 767		$1.5 \times 10^{-5} \sim 2^{-16}$

It can be seen that the undetected error probabilities significantly greater than 2^{-16} can occur only for very short frames. Of the frame structures that are known to be planned in support of the ATN, the shortest is AMSS, which uses 96-bit frames. Table 1 suggests that the "worst case" nature of the model should be re-examined if the results are within a factor of two of the requirement. This will prove not to be the case for the examples given here.

4.6 Errors Introduced by Intermediate and End Systems

Errors induced by intermediate systems above the link layer are obviously not subject to link layer CRCs. The same can be said of errors induced by end systems within the network layer. Since the scope of this paper excludes software errors, the system-induced errors of concern here might be described as "glitches" produced, e.g., by power transients, memory errors, or lightning effects.

As noted earlier, the TP4 checksum will detect all single bit errors and all double bit errors where the distance between the two bits is 1039 bits or less. The TP4 checksum will also detect all but one in about $2^{16} \sim 65{,}000$ of all possible error patterns, independent of the origin of the errors. To extend the Mode S data link example, if each intermediate system and each end system (acting below the transport layer) randomly corrupts one packet in 80,000, then the probability of one or more undetected errors in a TSDU is $< [1-(1-1/80{,}000)^5][2^{-16}] \sim 10^{-9}$. In practice, it seems feasible that COTS hardware of reasonable quality, suitably protected from power transients, can produce errors in fewer than one in 80,000 packets. (If an average packet is 100 octets long, the corresponding bit error rate for one bit error per 80,000 packets would be $\sim 1.6 \times 10^{-8}$. Although this would be a very low bit error rate for an unprotected data transmission path, it seems very high for the internal functioning of a computer system.)

4.7 Errors Induced by ATN End Systems above the Transport Layer

In typical implementations, errors induced in end systems (e.g., by power transients) may impact any ES software function. To the extent that such errors directly impact the application (or layers between the application and the transport layer), the only practical remedies are (1) to provide very reliable end systems or (2) to provide data integrity check(s) as part of the application. Format checks by the application may detect some such errors, but typically will not reduce the undetected error probability by as much as an order of magnitude. In an air traffic control environment, highly reliable end systems with protection against power transients are the norm.

5.0 Non-OSI extensions of the ATN (Domestic ATC)

The total "end-through-end" integrity includes non-ATN extensions on the ground and in the aircraft to support the distribution of application data beyond the ATN end systems. In the U.S., it is planned that some ATN applications will reside in the Data Link Application Processor (DLAP, i.e., the ATN end system) The DLAP serves as a gateway that will communicate with the ATC automation system using the Internet Protocol Suite (IPS). (See Figure 4.)

Arrangements for hosting the ATN end system protocols in the aircraft are still under development by industry, but some options involve hosting the ATN ES protocols in the

Communications Management Unit (CMU), while the "real" application resides in an external avionics unit, e.g., a Flight Management System (FMS).

6.0 Sample End-through-End Error Budget

Let

W = Probability of undetected error in an ATN TSDU

X = Probability of undetected error in a message induced by ATN end systems outside the TP4 checksum.

Y = Probability of undetected error induced by link(s) forming the non-OSI extensions of the ATN.

Y1 = Component of Y attributable to terrestrial extensions of the ATN
Y2 = Component of Y attributable to airborne extensions of the ATN

Z = Probability of undetected error induced by non-ATN end systems

Then the overall probability of undetected error, "end-through-end" is:

$1-[(1-W)(1-X)(1-Y1)(1-Y2)(1-Z)]$

$\sim W + X + Y1 + Y2 + Z$ (for very small values of W, X, Y, and Z)

It is possible to use this framework to illustrate how order-of-magnitude figures can be applied to an end-through-end data integrity budget.

In the previous examples, the end-to-end integrity was in all cases $< 2 \times 10^{-9}$ for errors induced in the physical layers between network nodes. An argument was also given to suggest that 10^{-9} is a conservative value for the probability that an error induced in an intermediate system or end system (below the transport layer) will go undetected. So a reasonable end-to-end bound for data integrity within the ATN segment might be 3×10^{-9} for the CPDLC messages used in the examples, provided that the intermediate system and end system hardware is of reasonable quality and is reasonably protected from transients. This value is used for "W" in the sample end-through-end budget.

Local area networks (part of the non-ATN extensions) planned for FAA Air Route Traffic Control Centers (ARTCCs) will be protected by 32-bit CRCs. For four such CRCs (two frames on each of two links), the nominal maximum probability of undetected error is on the order of $2^{-32} \sim 10^{-9}$. This value is used for "Y1" in the sample end-through-end budget.

The total end-through-end integrity in this example is therefore on the order of 4×10^{-9} or less, not including the impacts of "X" (undetected errors in ATN end systems above TP4), "Y2" (undetected errors induced by non-ATN links on the aircraft), and "Z" (undetected errors induced by non-ATN end systems on the aircraft); all of which are difficult to quantify at this point.

7.0 Integrity "Per Flight Hour"

Aviation safety analyses often deal with the probability of undesirable events "per flight hour". Although the FAA has stated no formal requirements for the ATN in this context, it is interesting to examine the results of the previous examples on a "per flight hour" basis.

Heuristically, the probability of one or more undetected errors per flight hour should be equal to the probability of an undetected error multiplied by the number of data transfer events per hour. This simple equation has been verified for constant message rates (e.g., periodic reporting) and for Poisson message generation processes.

In order to compute the number of frames (CRCs) per flight hour, a traffic model is needed. In the case of oceanic operations, the RTCA SC-165 oceanic traffic model is available. Applying this model to the overall end-through-end integrity results in a nominal bound of no more than about 4×10^{-7} undetected ATS message errors per flight hour. It appears that a value of 10^{-5} per flight hour would be sufficient for ATS communications.

This exercise was not repeated for domestic ATC communication because there is currently no standardized traffic model for that environment.

8.0 Open Issues

This paper deals with the feasibility of achieving the FAA's end-through-end data integrity requirements. The actual achievement of those requirements will require positive implementation steps, e.g., requiring the use of the TP4 checksum for all ATS communications. It is usually easier to identify sufficient conditions to meet a set of requirements than to identify necessary condition. Within the scope of this paper, a sufficient set of conditions would appear to be:

- use of the TP4 checksum for ATS communications,
- use of 16-bit data integrity checks (CRCs or the equivalent, but not checksums) on links supporting the ATN, unless those links can be isolated from ATS communications,
- the use a 32-bit CRC (or a 16-bit link layer CRC combined with a 16-bit checksum at the transport or application layer) for non-OSI extensions of the ATN (providing ATS communications), and.

- use of hardware (intermediate and end systems) of reasonable quality, with appropriate measures of protection against transients due to power and lightning effects.

It seems likely that other sets of sufficient conditions could be easily identified.

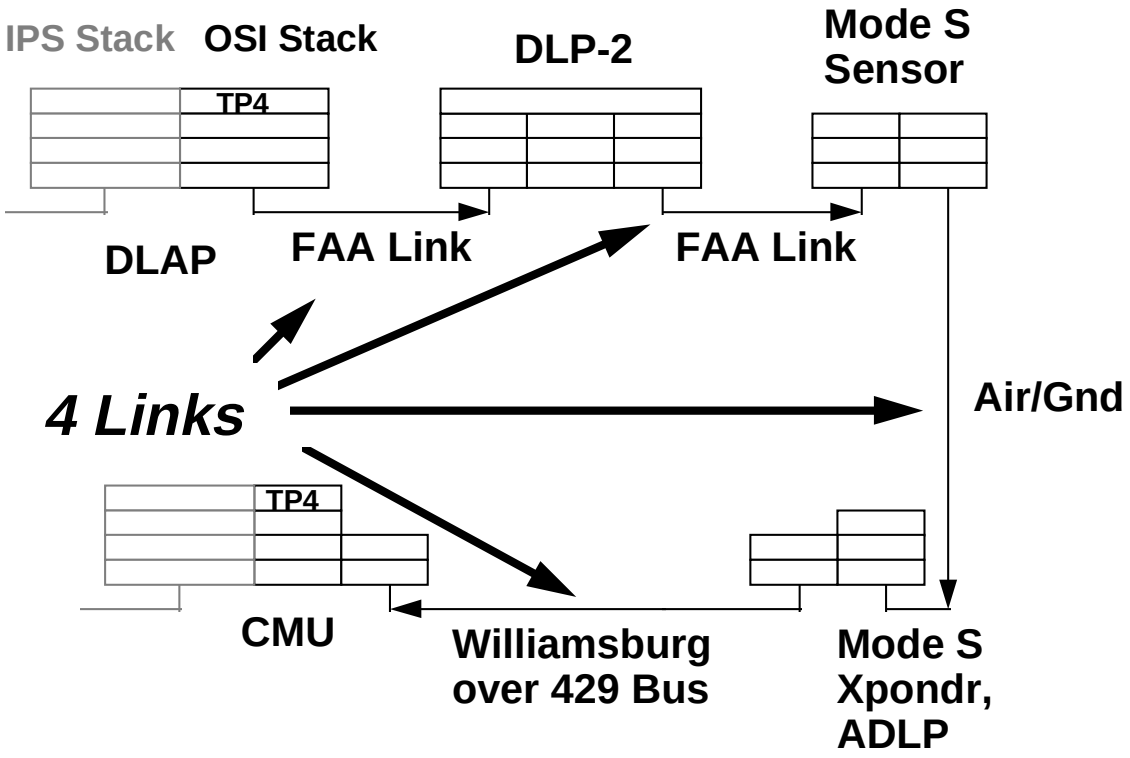

Figure 1: Mode S Data Link Example

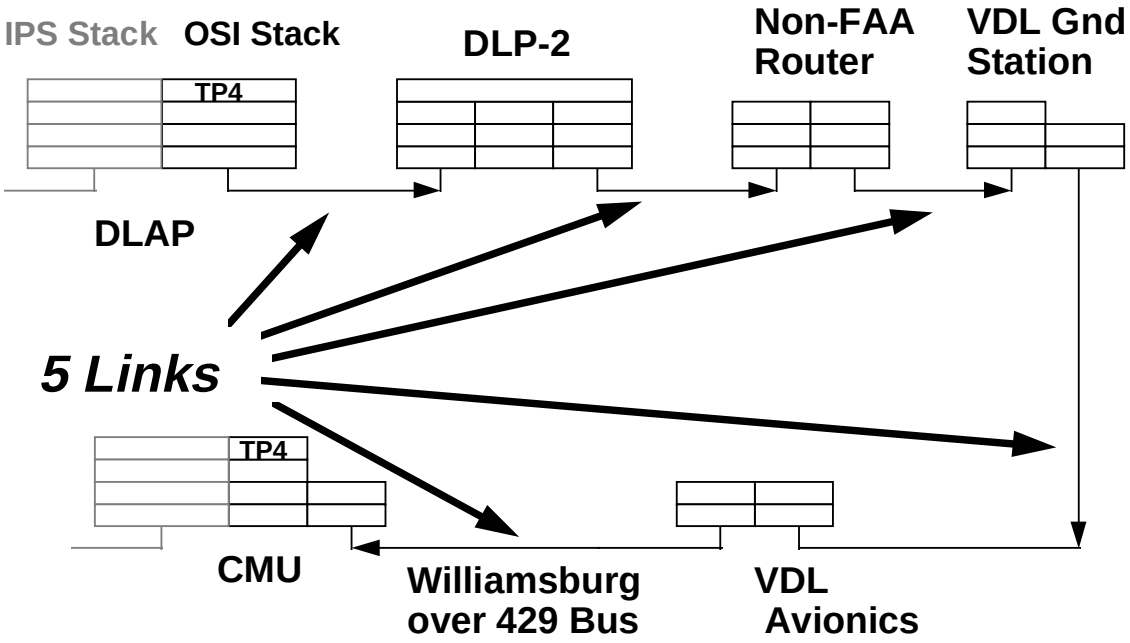

Figure 2: VHF Data Link Example

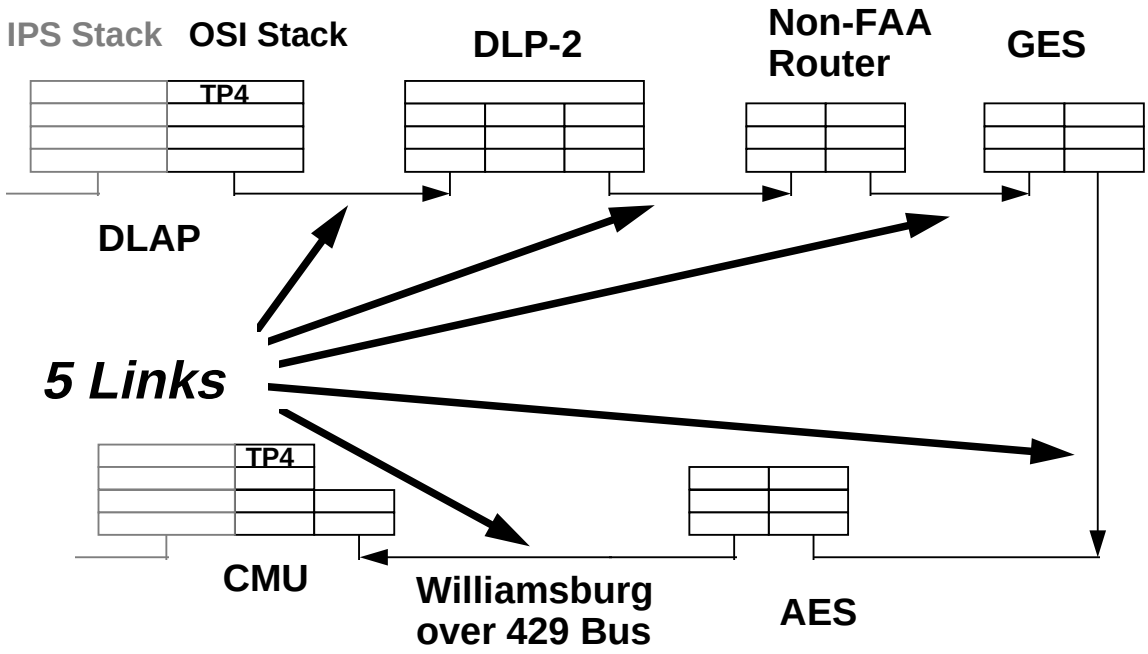

Figure 3: AMSS Example

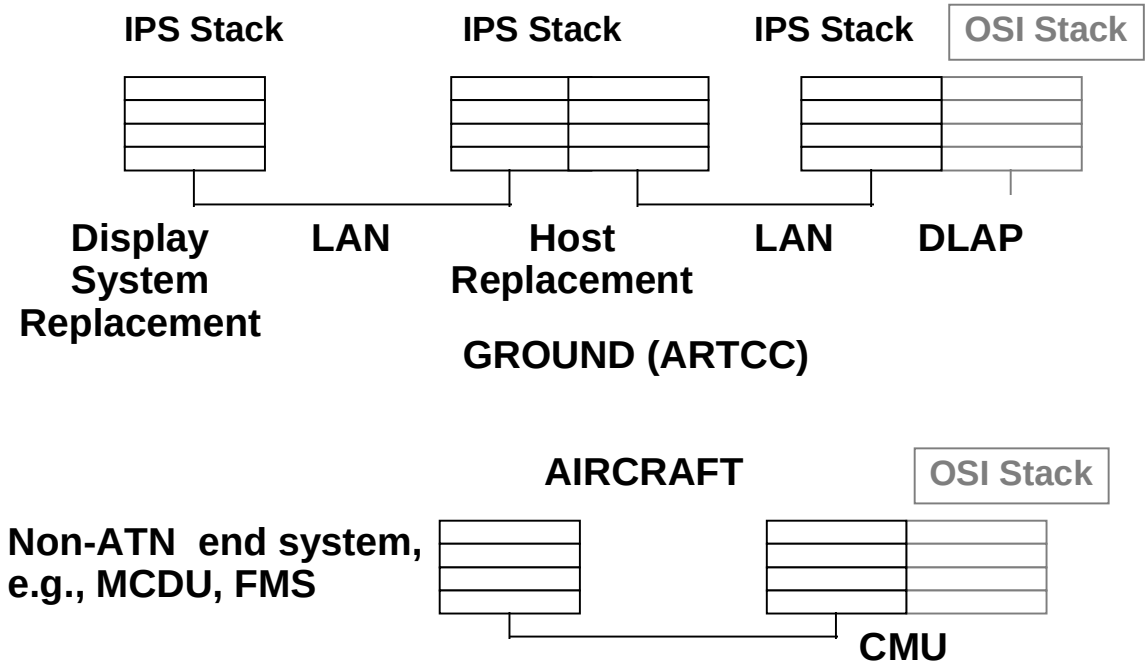

Figure 4: Non-OSI Extensions of the ATN (U.S. Domestic)

Appendix A: CRC Performance under Normal Bit Error Rates

References

A.1 Miller, et al, "On the Error Statistics of Viterbi Decoding and the Performance of Concatenated Codes," JPL Publication 81-9, September 1, 1981.

A2. Inmarsat Aeronautical System Definition Manual (SDM), Module 1.

A1. AMSS

The AMSS physical layer uses forward error correction (FEC) based on rate 1/2, constraint length 7 convolutional coding and Viterbi decoding. The advertised bit error rate from the physical layer is 10^{-5}. However, the errors are not random, independent errors. The Viterbi decoder produces error bursts of random length and random content, separated by error-free intervals of random length. A burst error model for this type of FEC was published in Reference A1. The model assumes a non-fading channel, which is only approximated by AMSS (through the use of interleaving between the channel and the FEC). The model can be summarized as follows:

$P[\text{burst length} = m] = a(1-a)^{m-1} \quad (0 < m)$

where "a" is the reciprocal of the mean burst length

$P[\text{error-free run length} = n] = q(1-q)^{n-K+1} \quad (K-1 < n)$

where "K" is the constraint length of the code and
"q" is 1/(Mean error free run length - K + 2)

For a BER of 10^{-5}, and K=7, the appropriate parameters are

Mean burst length ~ 4.4 bits; a ~ 0.2273
Mean error-free run length ~ 2.6×10^5 bits; q ~ 3.85×10^{-6}

The AMSS link layer (i.e., frame) CRC will detect all error bursts of length 16 or less. The fraction of bursts that are of length 16 or less is

$$\sum_{i=1}^{16} a(1-a)^{i-1}, \text{ or } 0.98385$$

Therefore, the fraction of bursts of length greater than 16 is 1 - 0.98385 = 0.01615. The mean run length between bursts of length greater than 16 is therefore

$(2.6 \times 10^5)/0.01615 \sim 1.6 \times 10^7$ bits

Since the average burst length is small relative to a frame length, the probability that one of these bursts will intersect a particular 96-bit frame is roughly

$$96/(1.6 \times 10^{7}) \sim 6 \times 10^{-6}$$

The CRC can be expected to detect all but about one in 2^{16} of all possible error patterns. For practical purposes, the number of possible error patterns in a frame is so large that this is equivalent to saying that the CRC can be expected to detect all but one in 2^{16} of all bursts of length greater than 16. Therefore, the probability of undetected error in a 96-bit frame, at a BER of 10^{-5}, should be on the order of

$$(6 \times 10^{-6}) \times 2^{-16} \sim 9 \times 10^{-11}$$

This result is in excellent agreement with the figure advertised by Inmarsat in Reference A2, i.e., 10^{-10}.

Taking into account the impact of the TP4 checksum, the probability of undetected error in a TSDU, attributed to the transmission of a single AMSS frame, should be on the order of

$$(9 \times 10^{-11}) \times 2^{-16} \sim 1.4 \times 10^{-15}.$$

For a message that traverses AMSS as four frames (as in Example 3 of the main body of this paper, but at a physical BER of 10^{-5}), the resulting TSDU undetected error probability due to AMSS should be about

$$4 \times 1.4 \times 10^{-15} \sim 5.6 \times 10^{-15} .$$

This value is so low that it is probably overshadowed by other mechanisms, e.g., fading events that overcome the AMSS interleaving scheme (thus producing abnormally long error bursts), software errors, and “glitches” in end systems.

A2. X.25 over M-ary Modems

This example examines an X.25 (or equivalent) terrestrial link operating over a modem that uses M-ary modulation, where M = 4 or 8 However, the only relevant feature of X.25 that contributes to the quantitative results is the use of a 16-bit CRC by the link layer frames. Therefore, the results are generally applicable to any terrestrial link using a 16-bit CRC and operating over an M-ary modem.

M-ary modems segment the data stream into groups of k bits, where $k = \log_2 M$ (M= 4 or 8) and transmitted as a symbol. Errors generally occur in bursts of up to k bits (k=2 or 3).

Symbol Error Probability as a Function of Bit Error Probability

For 4-ary modems, there are two bits per symbol. If the transmitted symbol is 00, the possible symbol errors are 01, 10, and 11. In practice, these errors are not equally likely, but for simplification, the mean number of bit errors per symbol error can be taken to be approximately 4/3 or 1.333. So the symbol error probability is the bit error probability divided by 1.333.

Similarly, for 8-ary modems, there are three bits per symbol. The possible symbol errors are 001, 010, 100, 011, 101, 110, and 111. The average number of bit errors per symbol error is approximately 12/7 = 1.714. The symbol error probability is the bit error probability divided by this factor.

Probability of More Than One Symbol Error in a Frame

A 16-bit CRC will detect all single error bursts of length 16 or less. Therefore, all single symbol errors from a 4-ary or 8-ary modem will be detected by the CRC. The probability of more than one symbol error within a frame is

1 - P[no errors in frame] - P[one symbol error in frame]

In a non-fading environment, where impulse noise is not dominant, it may be reasonable to characterize symbol errors as random occurrences. In this case, the above expression expands to

$$1 - (1-P_s)^n - (n-1)P_s(1-P_s)^{n-1} ,$$

where "n" is the number of symbols in a frame, and P_s is the symbol error probability.

Approximation of the Undetected Error Probability

For a nominal bit error probability of 10^{-5}, the corresponding values of P_s for 4-ary and 8-ary modems are approximately 7.5×10^{-6} and 5.8×10^{-6}, respectively. Table A.1 shows the corresponding probabilities of more than one symbol error per frame, for a frame of 100 octets.

Table A.1: Probabilities for M-ary Modulation

Modulation	BER	Symbol Error Prob.	P[more than 1 symbol error per frame]
4-ary	10^{-5}	7.5×10^{-6}	10^{-5}
8-ary	10^{-5}	5.8×10^{-6}	7×10^{-6}

With the usual simplification that the CRC will detect all but one in 2^{16} of all possible error combinations, and that the multiple bursts from the demodulation simulate a pseudo-random selection of possible error combinations, the probability of undetected error in a frame becomes $\sim 1.5 \times 10^{-10}$ for 4-ary modulation and $\sim 8.8 \times 10^{-11}$ for 8-ary modulation.

Taking into account the impact of the TP4 checksum, the probability of undetected error in a TSDU, attributed to the transmission of a single frame, should be on the order of

$(1.5 \times 10^{-10}) \times 2^{-16} \sim 2.3 \times 10^{-15}$ (4-ary modulation)

$(8.8 \times 10^{-11}) \times 2^{-16} \sim 1.3 \times 10^{-15}$ (8-ary modulation)

These two figures are so close as to be indistinguishable for practical purposes. They are both so low that they are probably overshadowed by other mechanisms, e.g., software errors and "glitches" in end systems.