Introduction to DO-326A/ED-202A – Aviation Cyber-Security "Set"

FOR ENGINEERS AND MANAGERS

Foreword:

The Worst Nemesis – Aviation Cyber Threats… or DO-326/ED202?

A passenger walks into a commercial-flight airplane with a laptop, hacks its network, making it fly even higher… funny? Well, unfortunately, this is not the beginning of a joke – but rather of a potential nightmare.

The bad news? This (almost as described above) allegedly happened in 2015… The good news? The person was a "white-hat-hacker" – one of the "good guys", who only strive to prove their point about the need to strengthen cyber-defense, so the airplane was actually "safe".

That hacker got banned from almost any future flight, but RTCA & EUROCAE didn't even require this stimulus, as by then – they were already frantically developing a solution for almost a decade. This solution, the first complete and workable DO-326/ED-202 "set" of documents was finally published in June 2018 – but even earlier than that, the FAA and EASA made the set's earlier versions as mandatory as practical at any given point in time. Following its mid-2018 publication, this DO-326/ED-202 "set" is already widely regarded as an "Acceptable Means of Compliance" (AMC), i.e.: a de-facto mandatory standard.

How did we get "here" from "there"? Good question:

The "digital aircraft" is already as commonplace as the aircraft itself – as natural as aircraft wings or engines, to the extent that modern aircraft could be regarded as winged & powered computers.

The turn of the millennium saw the rise of the next aviation digital phenomenon – the "connected aircraft": in which everything is connected to… well… everything else… This trend is anything but novel – digital radio-systems, GPS, ACARS, ADS-B: all these, and more, have been integral components of passenger aircraft for decades. Consequently, today's new aircraft contain thousands of processors performing both independent and intricately related operations: where old aircraft had hundreds of processors in a "closed" system, today's aircraft architectures and connectivity necessitate more openness. However – the rapid

AFUZION

AUTHOR:
AHARON DAVID

- **BsAe, MBA Info-Tech & Tech Management**
- ***Member of both WG-72 (EUROCAE) & SC-216 (RTCA): "Aeronautical Systems Security"***
- ***Former Commander of IAF's Avionics & Control Software Centre (ACSC).***
- ***Adviser for the CAAI on UAS avionics safety and Aviation Cyber Security***
- ***Member of RTCA SC-216 and EUROCAE WG-72***
- ***AFuzion-InfoSec's Chief WHO (White Hat Officer)***

Technical Reviewer

Mr. Vance Hilderman, CEO AFuzion Inc.

connectivity trend, accelerated by the dramatic surge in commercial hardware and software performance, together with factors that were not previously accounted for, have made "connectivity" both a benefit-multiplier AND a menace. As a direct consequence, the DO-326/ED-202 "sets" of regulatory documents were jointly developed by the aviation industry, synchronized by RTCA (U.S.) and EUROCAE (Europe) – in order to retain the indispensable benefits of connectivity without exposing civilian aviation in general, and airworthiness in particular – to unmitigated cyber-threats that might eventually compromise safety. This "set" is already mandated for several aspects of airworthiness certification, and rapidly gaining more ground – making it an absolute necessity to get acquainted with as soon as possible for anyone in or around the business of airworthiness.

The DO-326/ED-202 "set" encompasses multiple documents containing many hundreds of pages. Therefore aa deep understanding of this ecosystem's nature, mandates and potential trade-offs is required. Before approaching this Cyber-Security ecosystem", it is necessary to first become acquainted with the ecosystem's terminology and processes.

There are some major questions that need to be dealt with prior to engaging in any DO-326/ED-202 project:

- ✓ What is Cyber-Threat / Cyber-Security?
- ✓ How does it relate to Aviation/Aircraft?
- ✓ What guidance/standard for Cyber-Security exist today?
- ✓ To What Extent Are The Existing Standards Applicable to Aviation/Aircraft?
- ✓ What is "DO-326/ED-202", and why couldn't just "ARP-4754/DO-178" be applied?
- ✓ What is the "DO-326/ED-202 set"?
- ✓ To what extent is the "DO-326/ED-202 set" mandatory?
- ✓ What are the "326/202 set" "guidance/recommendations "(and what they are not…)?
- ✓ What does it take to meet the "326/202 set" "guidance/recommendations"?
- ✓ How can the "326/202 set" "guidance/recommendations" be efficiently met?

Honest answers to these questions are found below.

What is Cyber-Threat/Cyber-Security?

The U.S. Department of Homeland Security, in its 2010 Privacy Impact Assessment, defines "Cyber threat(s)" as "… any identified effort directed toward access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or a federal system, without lawful authority…"

Unfortunately, everyone living in the 21st century is acquainted with this "digital menace": computer viruses, worms, Trojan-horses and other forms of malware, have been plaguing computers since the first lab-virus. Just a quick historic perspective of this evolving digital-menace:

Phase I – "Prehistory" (pre-www):

- ✓ [1971] "Creeper": 1st computer virus, developed by Robert H. Thomas at BBN Technologies;
- ✓ [1982] "Elk Cloner": 1st malware to use an attack vector, originally built to combat piracy on Apple II systems;
- ✓ [1988] Morris worm: bombarded computers with traffic, could infect multiple times, brought down ~6,000 systems – Morris becomes 1st person tried & convicted under the 1986 U.S. Computer Fraud and Abuse Act;
- ✓ [1991] "Michaelangelo", a strain of the "Stoned" virus: "wakes up" every year on March 6th (the artist's birthday), to wipe 1st 100 sectors of local hard drives & floppy disks.

Phase II – "Early History" (www-age):

- ✓ [2000] "Love Letter" worm: an email with the subject line "ILOVEYOU" and an attached "LOVE-LETTER-FOR-YOU" txt-file, infects ~50 million computers in 10 days, causing damage estimated at a few billions of USD;
- ✓ [2007] "ZeuS" Trojan: a "package" containing a variety of "popular" malware programs designed for cyber thieves. The FBI arrests more than 100 hackers for bank fraud in Eastern Europe after stealing $70M using "ZeuS".

Phase III – "Going Pro":

- ✓ [2009] "Operation Aurora": massive Cyber Attacks – attempts to break into- and tamper with- source code repositories from security and defense contractor companies. Affected companies include (for instance): Google, Symantec and many more;
- ✓ [2010] "Stuxnet" virus & Cyber Attacks: 1st to efficiently spy-on and tamper-with industrial-level systems.

Phase IV – "Global Menace":

- ✓ [2013] "CryptoLocker" ransomware: cyberattack spread through email phishing scam, propagated using the ZeuS Trojan. Once downloaded, ransomware payload encrypted hard drive files, "releasing" them only after ransom had been paid;
- ✓ [2016-2017] Specific attacks targeting aviation: typically aimed at airports and/or airlines, notable victims – Vietnam and Ukraine;

- ✓ [2017] “WannaCry” ransomware attack: Worldwide-synchronized attack, estimated ~$4B damage, including infrastructure, among them Civil Aviation “actors”, such as Boeing, LATAM Airlines Group and others.

This concise history, from naïve, "experimental" malware, to professional, well-funded global cyber-crime today, puts at risk every aspect of modern life, from private computers to entire countries' strategic infrastructure.

So, are we all going to die? Of course we are, but probably of old age, not of cyber-crime. The reason? Cyber-Security. But what is Cyber-Security?

Cyber-Security evolved very much like cyber-threats: in a gradual manner – responsive at first, growing more professional and collaborative as threats became professional and global.

At the private, home level, the first to appear were simple protective security measures: "anti-virus", "anti-spyware", then – in general "anti-malware", intended to detect and eradicate any "viruses", "worms", "Trojans", and in general – any malware. A bit later, preventive measures made their debut – popularly known as "firewalls", intended to control entry-points and block any attacks in a preemptive manner. Another type of counter-measure, although not "security-specific" was resilience and recovery, i.e. tools that enabled at least partial/degraded operation even under attack, and tools that backed-up the system and could restore it if corrupted. These types of security measures in modern, sophisticated forms are the core of most technical security-tools even today.

However, what may be sufficient for private home-usage would hardly suffice for large organizations or facilities, so "technical security measures" became, with time, only one element among many in a more holistic approach of Cyber-Security. This approach, despite many variations among different cases, comprises the same basic principles: corporate strategy, clear roles and responsibilities, explicit codes and standards, a top-down security architecture – and eventually, yes – a variety of security measures: technical, organizational and others.

How Does Cyber-Security Relate to Aviation/Aircraft?

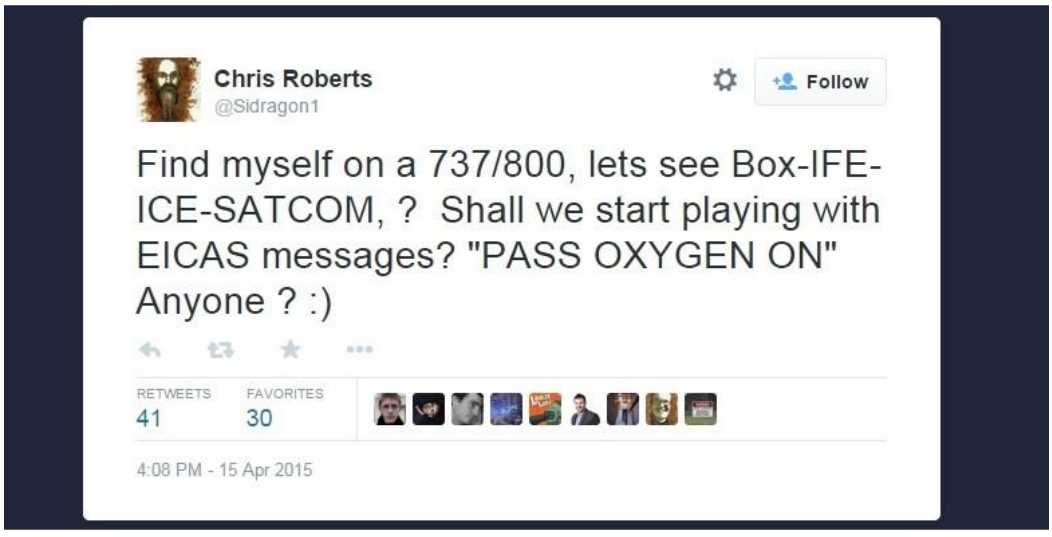
As long as early, amateurish, cyber-threats could be shrugged off by the Information-Technology (IT) industry as "merely annoying, but not posing any real challenge to safety", complacency was the norm. Gradually, attackers grew bolder, malware morphed from static "beasts" to sophisticated; adjusting mechanisms with the ability to wreak havoc, and the accumulated damage grew exponentially, as previously described here. However, this trend, which sent the IT-systems community on a rapid course to devise the methods and means of establishing proper Cyber-Security, had been matched by a much slower such trend among the traditional heavy industry community, including the aviation industry, until as late as the early 21st Century. But why so?

Two main considerations led to the relative longer-lasting complacency of the traditional heavy industries towards the emerging cyber-threats: 1) the different nature of IT-systems and industrial

information systems, 2) the perceived notion that such complex attacks on industrial infrastructure can only be carried out by state-level "actors", regarded as reasonably responsible (even rogue regimes), thus, creating a "natural deterrent" for such disastrous undertakings. These two considerations were eventually proven overstated:

Industrial Information systems are indeed different from conventional IT systems; unlike IT, they arrive in a few common "flavors", such as OT (Operational Technology), ICAS (Industrial Control & Automation Systems), SCADA (Supervisory Control and Data Acquisition), CPS (Cyber Physical Systems) and more. Typical CPS's used to be of proprietary technology and even physically isolated from "standard" ITs (such isolation used to be referred to as "air gap"), both attributes making it virtually impossible for "mainstream" hackers to crack. However, at about the turn of the millennium, COTS hardware and software made their way slowly but surely into this solid segment, and the "connected aircraft" all but eliminated the "air gap". As information technology and network technology exponentially evolved and their cost exponentially declined – the perceived notion of the "state-level" effort "barrier" that ensured restrain, suddenly disappeared: during the first decade of the 21st every determined hacker could acquire (or even develop) attack tools that came "too close for comfort" for the aviation world. Even the state-decency assumption for huge attack schemes suddenly did not seem so safe, as world order destabilized and terror-organizations, criminal-organizations and even some governments drifted to the "dark side".

As a result of the above two considerations, the second decade of the 21st century saw cyber-attacks on airports – mainly in Vietnam and Ukraine, and on civil aviation infrastructure (Boeing, LATAM and more) but the most dramatic event to demonstrate the fragility of the presumed safety was, as implied at the beginning of this paper, this:



Fortunately, Mr. Roberts is a "white-hat hacker", so no immediate damage – but the warning signs were loud and clear and comprised the "tipping point" catalyst for the changes leading to today's new Cyber-Security guidelines.

What Guidance/Standard for Cyber-Security Exist Today?

Guidance and later, standards, directing organizations about the proper handling of Cyber-Security made their debut as early as the 1970s, a period when the perceived threat was still minor. After a few decades of development, literally hundreds of various types of Cyber-Security standards, guidance and best practices exist, however, three major "families" of civilian standards plus one military "family" can be pointed out as most popular:

1) Common Criteria (CC) / Common Methodology (CM), a.k.a. ISO/IEC 15408 – originally, a fusion of 3 sources: the U.S. TCSEC a.k.a. DoD 5200.28 Std. with origins in the 1970s; the Canadian CTCPEC from 1993; the European ITSEC from the 1990s and adopted in some other countries. CC/CM is a generic set of documents that mainly standardizes the terminology and methods used for Cyber-Security, providing systems/organizations assurance for their Cyber-Security claims. This set of documents does not suggest any specific (or even general) methods or solutions.

2) ISO/IEC 27000-series (a.k.a. "ISO27K") set – this "Information Security Management System (ISMS) Family of Standards" is a systematic, inclusive set of many dozens of specific standards, intended at covering every aspect of Cyber-Security and widely accepted as a de-facto mandatory standard around the world. Its most notable documents are 27000 – Overview and vocabulary, 27001 – Requirements, 27002 – Code of practice, 27005 – Risk Management: to mention but a few. ISO27K originates from the 1990's UK standard BS7799, based on an information security policy manual developed by the Royal Dutch/Shell Group in the late 1980s and early 1990s.

3) NIST SP-800 Series – since the 1990s, the U.S. National Institute of Standards and Technology (NIST) publishes its SP-800 series of "…information of interest to the computer security community ..." which "…comprises guidelines, recommendations, technical specifications, and annual reports of NIST's cybersecurity activities...", which has become an indispensable source of knowledge and served as the baseline of most other Cyber-Security standards, including the other prominent "families". The series' documents are widely used as de-facto standards, especially for aspects that are not (yet) well covered by other standards. In addition to the SP-800 series, NIST published some major policy documents that are also highly used worldwide, such as the NIST "Cybersecurity Framework", FIPS-200: "Minimum Security Requirements for Federal Information and Information Systems" that made the SP-800s de-facto standards, and some others.

4) DoD 8500 Series – a set of directives and instructions for the U.S. Department of Defense, aimed at "Mission Assurance", specifically – "Information Assurance", in which "Cyber-Security" is a tool for ensuring the performance of military missions.

All these, and many more, are used as standards and/or best-practices for various Cyber-Security purposes worldwide.

To What Extent Are The Existing Standards Applicable to Aviation/Aircraft?

While any of the major Cyber-Security standard "families" could (and do) serve as useful references for any aviation Cyber-Security standards, there were quite a few issues in which all of these standard-families came short when aviation safety was at stake, back in 2005, when aviation Cyber-Security standardization started in earnest.

All such issues related to the nature of the major "assets" that needed to be secured by such Cyber-Security standards: the passengers on-board commercial airplanes, and accordingly, aircraft and their essential systems:

1) IT .vs. OT: Almost all aircraft systems, and many aviation control and ground-support systems, are Cyber Physical Systems (CPS) / Operational Technology (OT), as opposed to pure IT-systems. This single distinction almost precludes the usage of any major Cyber-Security standard-families previously described.

> OT/CPS Cyber-Security, as previously described, had been late to get on-board, however, in 2002, the International Society for Automation (ISA) and American National Standards Institute (ANSI) launched the ANSI/ISA-99 standards committee, that started working on the "Industrial Automation and Control Systems Security" set of standards. Their baseline was the NIST SP-800-82 "Guide to Industrial Control Systems (ICS) Security", the only existing viable OT Cyber-Security standard at that time. ANSI/ISA-99 went through a few name changes, and currently this set of standards is known as ISA/IEC-62443.
>
> Great solution? Hardly… and for two main reasons: aviation is indeed based on OT/CPS – but also includes generic IT, and a wealth of additional considerations that cannot possibly be dealt with in a generic "one size fits all" type standard set; and, the even stronger setback – by the time the world of aviation was ready for Cyber-Security standard-setting, around 2005, ANSI/ISA-99 was not yet ready… in fact – even as late as 2019, only 8 of the 13 planned documents of the set were published.

2) Military .vs. Civilian: Military-type standards, such as the DoD 8500-set were not adequate due to the same reason that precluded military safety standards from being adopted by civil aviation: the focus of military standards would normally be on mission accomplishment, thus – of a functional nature, while civilian standards would focus on public safety with reasonable slack for performance. Indeed – even the title of DoD 8500 is "Mission Assurance", so this was never really an option.

3) Other sectors: Quite a few specific Cyber-Security standards for specific sectors were developed based on generic Cyber-Security standards, and some of these sectors are even reasonably close to aviation to be seriously considered as baselines to be developed into aviation requirements, however – in 2005 no such selection existed. The closest such "relative" is SAE's J3061 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems", published in 2016, and which is currently (2019) under a joint ISO & SAE revision process into a new standard: "ISO/SAE 21434 Road Vehicles – Cybersecurity Engineering".

4) Existing aviation standards: In 2005, there were virtually no "existing aviation Cyber-Security standards", at least no general-purpose and specifically – no development-phase standards. ICAO had its "Annex 17" security guide, but cyber-threats were added to it only in 2011, in two top-level paragraphs. Airlines to America (ATA), now Airlines for America (A4A) issued its "Spec 42: Aviation Industry Standards for Digital Information Security comprising about 400 pages of technical encryption guidance for aviation", but only in 2008.

ARINC did a bit better, and in 2005 issued its "Specification 664 Part 5: Aircraft Data Network", which was (and still is) a resourceful document for aircraft secure networking specifics. In the same year, ARINC published Technical Report 811, "Commercial Aircraft Information Security Concepts of Operation and Process Framework", that was indeed focused on Airlines and Operations rather than development, but included the fateful recommendation:

"… Encourage the harmonization of existing aeronautical assurance practices (e.g., RTCA DO-160D and DO-178B) with security assurance practices/standards (e.g., NIST FIPS-140 and Common Criteria).

Note: The need is to bring these two domains together to provide airlines and regulators with a common ground in assessing aircraft information security solutions (e.g., evaluating COTS security solutions)…"

What Is "DO-326/ED-202", And Why Couldn't Just "ARP-4754/DO-178" Be Applied?

As previously implied, when the European and American aviation industry via coordination with EASA and FAA, embarked on their standard-setting process circa 2005, no existing Cyber-Security standard at the time could provide a "ready-made" solution. So, in 2006 EUROCAE formed Working Group 72 (WG-72) and in 2007 RTCA formed Special Committee 216 (SC-216), both named "Aeronautical Systems Security", and the process that yielded DO-326/ED-202 and their companion ecosystem documents, began.

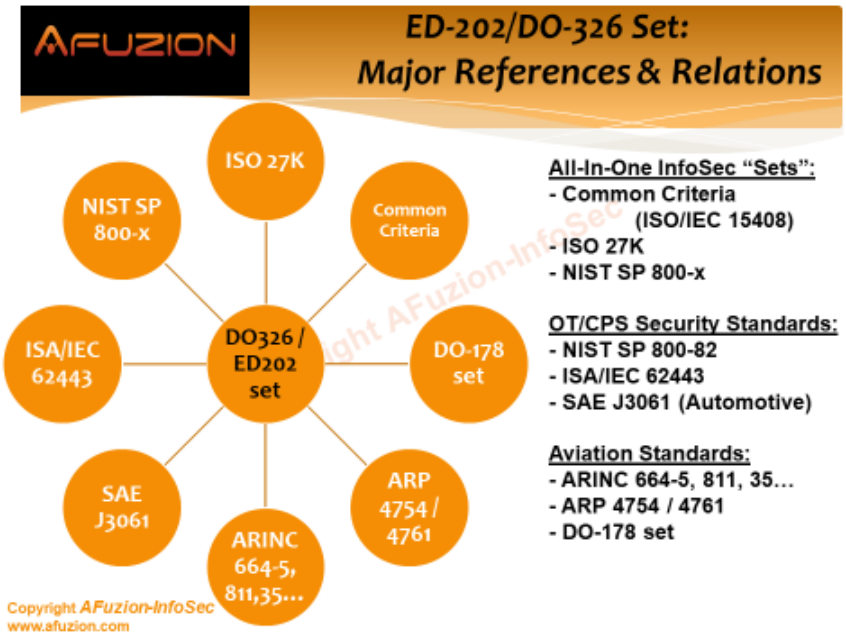
The first resulting documents, ED-202 in Europe and DO-326 in the U.S., both named "Airworthiness Security Process Specification", were published in 2010. The original DO326/ED-202 documents were intended to serve as an "all in one" guidance for the Information-Security of the development phase of aircraft from inception to certification and deployment. The original document language clearly stated that they are "…the first of a series of documents on Aeronautical Systems Security that together will address information security for the overall Aeronautical Information System Security (AISS) of airborne systems with related ground systems and environment…", but this phase was yet to come.

DO-326/ED-202 were heavily based on the then-already-published ISO/IEC 27005 of the ISO27K family, and on the de-facto industry standard SAE ARP 4754, "Certification Considerations for Highly-Integrated or Complex Aircraft Systems", and created a useful continuum with those in a relatively seamless manner.

However, anyone who ever had even a brief acquaintance with ARP4754 and/or RTCA's DO-178, "Software Considerations in Airborne Systems and Equipment Certification", should be rightly wondering why was this effort required in its entirety: why couldn't Information-Security simply made part of ARP4754 and/or DO-178, especially in light of both going through major revisions at the time?

The simple, practical, reason is stated in a DO-326/ED-202 companion document, published a few years later: "… Airworthiness security is its own discipline, needing unique expertise, and requires its own analysis techniques and assurance considerations…", in the sense that it is distinct from safety, and from other security considerations. Another consideration was – that Information Security was not necessarily all about software – as it involves quite a few other aspects of aviation. Therefore – ARP 4754 and DO-178 had to be coordinated with, but they also had to be kept "clean" of Cyber-Security issues.

The final deterrent from integrating Information Security into ARP 4754 and/or DO-178, was the fact that their "source of legitimacy", FAA/EASA AC/AMC 25.1309 "System Design and Analysis", explicitly excludes this option, by the mere definition of the term "event" covered by the document: "Event: An occurrence which has its origin distinct from the airplane, such as atmospheric conditions (e.g. gusts, temperature variations, icing and lightning strikes), runway conditions, conditions of communication, navigation, and surveillance services, bird-strike, cabin and baggage fires … The term is not intended to cover sabotage…". Realizing that any change to FAA/EASA formal documents may delay the process for a decade or so, and reacting to the need to close the Information-Security regulatory gap immediately – both WG-72 and SC-216 were encouraged to develop separate documents, that would be tightly coordinated with ARP 4754 and DO-178, and so they did.



What Is The "DO-326/ED-202 Set"?

As previously implied, the original DO-326/ED-202 documents were originally meant to become the first of a series for Aeronautical Information System Security, and indeed, in the years following the 2010 initial publication, WG-72/SC-216 proceeded with the development of this "series".

Although WG-72 were (and still are) tightly coordinated and many members share both committees, there are yet some variations between the two, mainly on the basic philosophy: whereas SC-216 (U.S.) pursues a straight forward, quick-results approach and focuses almost solely on aircraft information-security ("…document guidance for security of aircraft systems…"), WG-72 (Europe) adopted a more holistic approach, encompassing more aspects of aviation information security ("WG-72 will adopt a holistic approach, addressing security-related topics throughout the entire lifecycle of products…"). The holistic approach of WG-72 was easily recognizable right from the start, by allocating the entire ED-20x range of document numbers for the evolving series, while SC-216 simply used the sequential running-numbers of the entire DO series.

The first steps following the publication of DO-326 & ED-202 were still tightly coordinated:

1) "Clean" DO-326/ED-202 to make it a "core" document that would only cover the "WHAT" of the certification process. The revised version, DO-326A/ED-202A, was published in 2014.
2) Publish a new document, DO-355/ED-204, "Information Security Guidance for Continuing Airworthiness", to cover the post-production, in-service phase: also in 2014. The new DO-355/ED-204 incorporated DO-326/ED-202 "spin-off" parts.
3) Publish a new companion document that addresses the "HOW" of the certification process. The new pair, DO-356/ED-203, "Airworthiness Security Methods and Considerations", intended to be a "security DO-178" to DO-326s "security ARP4754".

However, at this third stage, the different nature of WG-72 and SC-216 started to take its toll, as the resulting DO-356 (published in 2014) and ED-203 (published in 2015) took different approaches, and were not technically identical like the other members of the "series". Additionally, WG-72, applying its holistic approach, published in 2015 a document of its own, without an SC-216 equivalent: ED-201, "Aeronautical Information System Security (AISS) Framework Guidance", intended as a strategic, top-level document to provide a "big picture", aided by two background reports: ER-013, "Aeronautical Information System Security Glossary" in 2015, and ER-17, "International Aeronautical Information Security Activity Mapping Summary" in 2018.

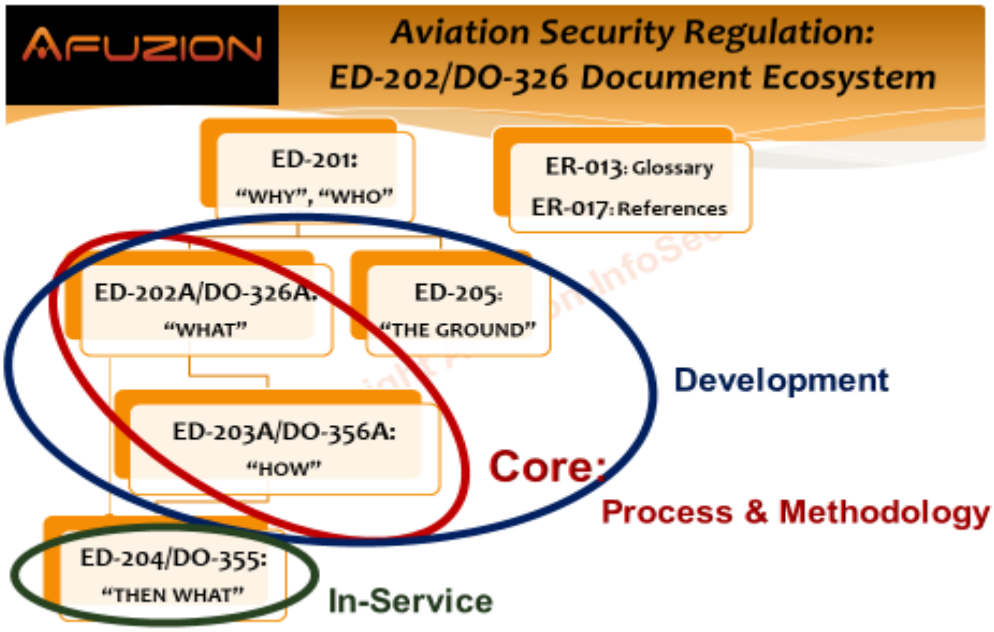
At this stage, an FAA rulemaking committee, coordinating with EASA, ANAC (Brazil) and TCCA (Canada) intervened, and among a variety of other issues approached, brought EUROCAE and RTCA committees together again, resulting in a revised DO-356 and ED-203, that were published in 2018 as DO-356A/ED-203A, unifying their technical content. However, ED-201 was not matched by a DO equivalent, as it was not deemed a "working document" but an "orientation document".

Meanwhile, WG-72 went on to produce another document of its own, ED-205, "Process Standard for Security Certification/Declaration of Air Traffic Management/Air Navigation Services (ATM/ANS)

Ground Systems", again – without an SC-216 equivalent, as the FAA manages most of its air-traffic ground-components internally, while EASA is a coalition of a few dozen civilian aviation authorities.

Thus, as of early 2019, the DO-326/ED-202 set comprises:

1) The "core" guidance and considerations, DO-326A/ED-202A and DO-356A/ED-203A;
2) The "in-service" guidance, DO-355/ED-204, based on the "core" guidance;
3) The "top-level" documents, ED-201, ER-013, ER-017, serving as "philosophy guidelines";
4) The ground systems standard, ED-205, intended for mainly European usage, scheduled to be published in 2019.



To What Extent Is The "DO-326/ED-202 Set" Mandatory?

As most other RTCA and EUROCAE documents, the DO-326/ED-202 set is considered a de-facto aviation industry standard, as official mandates keep coming in. While “guidelines” in title, the lack of any meaningful “alternatives” mean these “guidelines” are treated as “standards” which need to be considered and their intent shown to be followed.

The previously mentioned FAA rulemaking committee, FAA Aviation Rulemaking Advisory Committee (ARAC) Aircraft System Information Security / Protection (ASISP) Working Group (WG), that during 2015-2016 examined the entire information security regulation, considerably accelerated the process of establishing formal, mandatory, regulation, and the very clear recommendation on this was for the FAA to "…consider RTCA standards DO-326, DO-356 and DO-355 and EUROCAE standards ED-201, ED-202, ED-203, ED-204 as acceptable guidance materials to comply with the security rule 25.13xx for large transport aircraft for new Type type-certifications or new significant major changes or when the applicant elects to use them on a voluntary basis…", which in regulatory parlance translated to "FAA: make it mandatory, now". As EASA (Europe), ANAC (Brazil) and TCCA (Canada) actively cooperated with the FAA ARAC ASISP WG, the clear meaning of this is – the DO-326/ED-202 set is becoming mandatory, and very soon, all over the world. This recommendation is well harmonized with EASA's task force RMT.0648, developing the "Certification Specifications for product design" and task force RMT.0720, developing the "Rules for risk management within organizations and service providers" – both "horizontal" guidance, designating the DO-326/ED-202 set, scheduled to be published in 2020.

Other critical ARAC ASISP WG recommendations were to retroactively carryout a "Table-top Review" of **existing** Airborne CNS/ATM TSOs and standards, and establish guidance for the Use of Commercial Off the Shelf (COTS) and **Previously Certified** Products.

As the ARAC ASISP WG also recommended that the DO-326/ED-202 set should be adapted to all categories of aircraft, engines and propellers, together with very explicit language for new rules and regulations, the very clear answer is: everyone in the aviation business should be ready for the DO-326/ED-202 to be completely mandatory within no more than a decade, possibly – much sooner.

Some aspects of the DO-326/ED-202 set that are already mandatory:

- ✓ FAA Policy Statement PS-AIR-21.16-02 Rev. 2, "Establishment of Special Conditions for Aircraft Systems Information Security Protection" from 2017, states that the FAA "…will issue special conditions for initial type certificate (TC), supplemental type certificate (STC), amended TC, or amended STC applications for aircraft systems connecting to non-trusted services (e.g., non-governmental) and networks…", for all aircraft categories: part 25 Transport, part 23 Commuter Category, part 27 Multi Engine Normal Category Rotorcraft and part 29 Transport Category Rotorcraft. As the said revision 2 is the product of the ARAC ASISP WG, and as the DO-326/ED-202 set was recommended as AMC, the meaning of this policy is that de-facto, the DO-326/ED-202 set is now the norm for this type of certification, for all aircraft categories.

- ✓ FAA Advisory Circular AC 119-1, “Airworthiness & Operational Authorization of Aircraft Network Security Program (ANSP)”, from 2015, uses the "in-service" part of the set: DO-355, which relies on DO-326 & DO-356.
- ✓ FAA Advisory Circular AC 20-140C, “Guidelines for Design Approval of Aircraft Data Link Communication Systems Supporting Air Traffic Services (ATS)”, from 2015, uses the "core" and the "in-service" full set: DO-326, DO-356 & DO-355.

Note that more mandates are coming, so ignore the DO-326/ED-202 set at your peril…

What Are The "DO-326/ED-202 Set" "Guidance/Recommendations"?

(…and What They Are Not…)

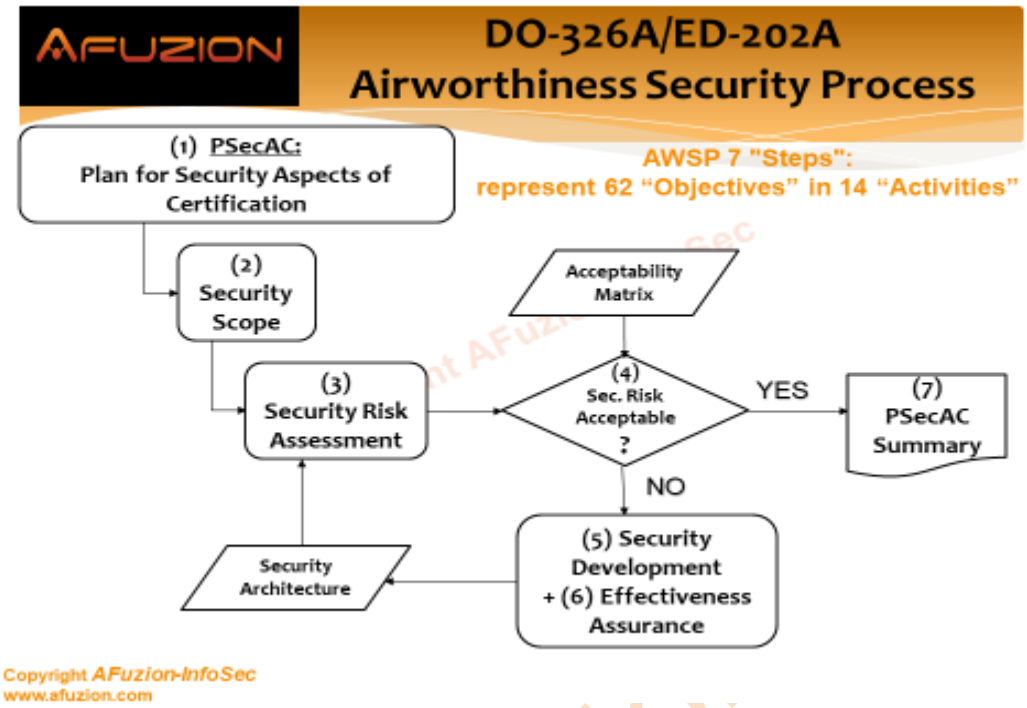
The DO-326/ED-202 set's guidance and recommendations are dispersed across all the documents comprising the set, but for airworthiness purposes, it can be regarded as a 2-part set: (1) DO-326/ED-202 & DO-356/DO-203, the "core" addressing the development phase, (2) DO-355/ED-204, the "continued airworthiness" addressing the "in-service" phase. In order to properly comply with the set – it would be best regarded by applicants as … a set – one unified body of text, for development, service or both – rather than an eclectic collection of documents…

Neither part nor any specific document of the set dictates any specific security measures, techniques or methods to be deployed – so by no means should the DO-326/ED-202 set regarded as a "cook book", but rather, as their titles imply, guidance, ranging from top-level strategy to detailed tactics, which would, in many cases, necessitate applying further information security standards: some are even explicitly recommended by the set, e.g. ISO 27K.

As for the guidance/recommendations that are included in the set, these can be roughly described as:

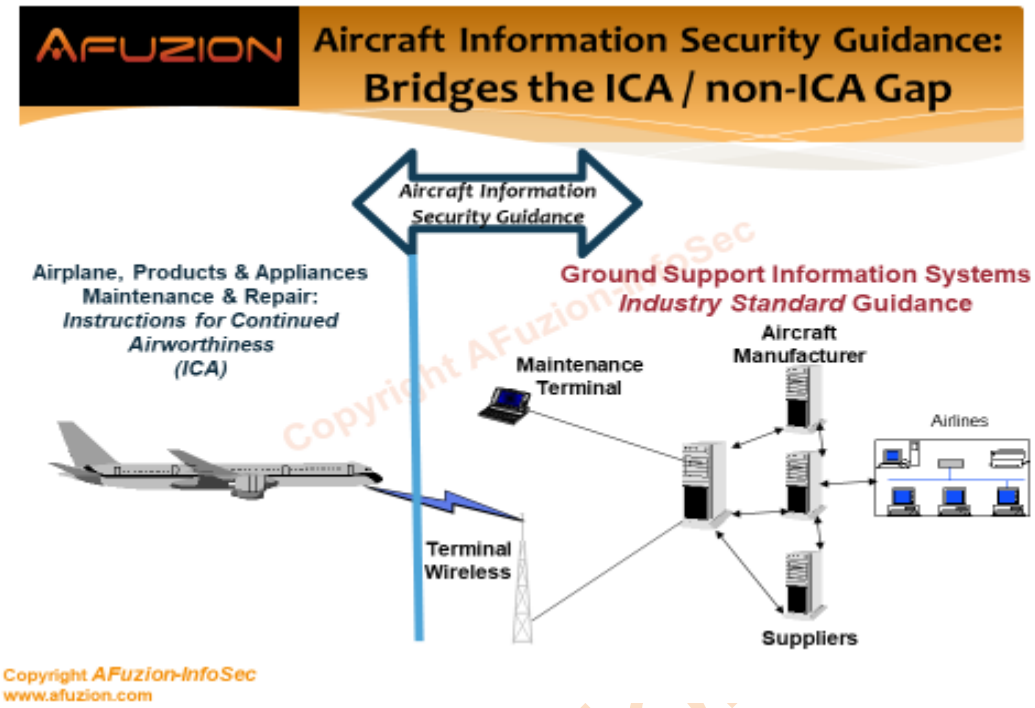
1) The "Airworthiness Security Process" (AWSP), mostly detailed in DO-326A/ED-202A, that outlines the major steps, activities and objectives of security certification for airworthiness:

a) AWSP comprises 7 steps: Plan for Security Aspects of Certification, Security Scope Definition, Security Risk Assessment, Risk Acceptability Determination, Security Development, Security Effectiveness Assurance and Communication of evidences.
b) These 7 steps are detailed into 14 activities: Plan for Security Aspects of Certification (PSecAC), Plan for Security Aspects of Certification Summary (PSecAC Summary), Aircraft Security Scope Definition (ASSD), Preliminary Aircraft Security Risk Assessment (PASRA), Aircraft Security Risk Assessment (ASRA), System Security Scope Definition (SSSD), Preliminary System Security Risk Assessment (PSSRA), System Security Risk Assessment (SSRA), Aircraft Security Architecture and Measures (ASAM), Aircraft Security Operator Guidance (ASOG), Aircraft Security Verification (ASV), System Security Architecture and Measures (SSAM), System Security Integrator Guidance (SSIG), System Security Verification (SSV).
c) These 14 activities include 62 objectives (combined) to be met.
d) Detailed "Acceptable Means of Compliance" (AMC) – provided mostly in DO-356A/ED-203A.



2) "Guidance for Continuing Airworthiness", mostly provided by DO-355/ED-204, but supported by the "core" documents of the set as well. This Guidance is provided for the following eleven aspects: Airborne Software handling, Aircraft Components handling, Aircraft Network Access Points, Ground Support Equipment (GSE), Ground Support Information Systems (GSIS), Digital Certificates, Aircraft Information Security Incident Management, Operator Aircraft Information Security Program, Operator Organization Risk Assessment, Operator Personnel Roles & Responsibilities, and Operator Personnel Training.

Combined, the AWSP and Guidance for Continuing Airworthiness form one integrated entity that comprises a complete set of information-security AMC for achieving and maintaining airworthiness for the entire aircraft life cycle.



What Does It Take To Meet The "326/202 Set" "Guidance/Recommendations"?

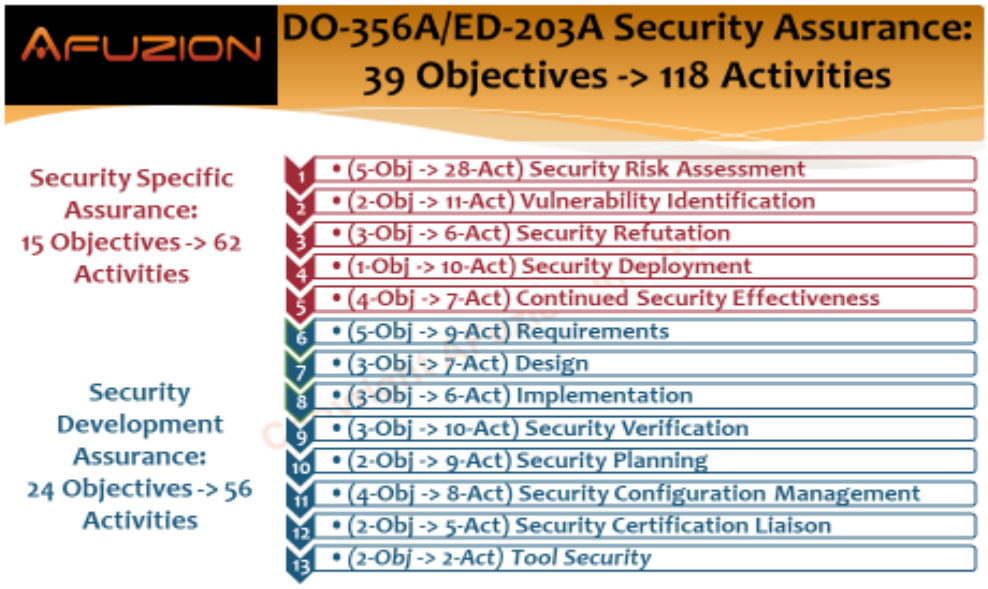
While DO-326A/ED-202A specifies the top-level formal requirements of the information-security airworthiness process, DO-355/ED-204 specifies in more detail what it takes to retain airworthiness, but here, too – the emphasis is on due process and following a variety of other, more elaborate information security generic standards, with clear roles for the Design Approval Holder (DAH) – typically the developer of the equipment, and the operator of the equipment.

As for the airworthiness certification process itself, it is mostly DO-356A/ED-203A that comes to the rescue. This 370 page long document details the specifics of the security aspects of the 3 key sub-processes of avionics certification: Planning (including Security Scope), Development, and Integral Process (including Risk Assessment and Security Effectiveness Assurance). Note that these three key sub-processes are thematic to many of the DO-XXX documents including DO-178, DO-254, DO-278, etc.

For the information security aspects, a more useful grouping of sub-processes would be: (1) Security Scope & Risk Assessment, (2) Security Development, (3) Security Effectiveness Assurance, while planning would refer to the top-level-certification.

These 3 sub-processes are further detailed in DO-356A/ED-203A (and partly in DO-326A/ED-202A):

(1) Security Scope & Risk Assessment:
   a. Security Scope Definition
   b. Threat Conditions Identification & Evaluation
   c. Threat Scenario Characterization
   d. Level of Threat Evaluation
(2) Security Development:
   a. Aircraft Security Architecture & Measures development
   b. System Security Architecture & Measures development, which can be further broken down to the Sub-System level, Item level, etc.
   c. System Security Integrator Guidance development
   d. Aircraft Security Operator Guidance development
(3) Security Effectiveness Assurance – 118 Activities, in 39 Objectives, included in 13 Sections, of 2 types:
   a. Security Specific Assurance – comprising 62 Activities, in 15 Objectives, included in 5 Sections
   b. Security Development Assurance – comprising 56 Activities, in 24 Objectives, included in 8 Sections



A crucial aspect of information security is ”Time”: it is not merely a one-way safety-type process that has a clear end-point and then retreats to just monitoring – but a continued struggle against any potential attacks and attackers, that keep evolving even if nothing else happens concerning the said system. Thus, any modification, addition, removal or even altered function should be re-processed according to the DO-326/ED-202 set in order to assess what time has wrought. Furthermore, even the mere passage of time, without any modification of the system or its functions can bring changes in the hostility of the cyber-environment, so keeping up with the DO-326/ED-202 set would require periodic risk analysis in order to assess whether the system is still as secure as originally intended. Both the DO-326/ED-202 & DO-356/DO-203 "core" development phase documents and the DO-355/ED-204 "continued airworthiness" phase document need to be followed on this aspect.

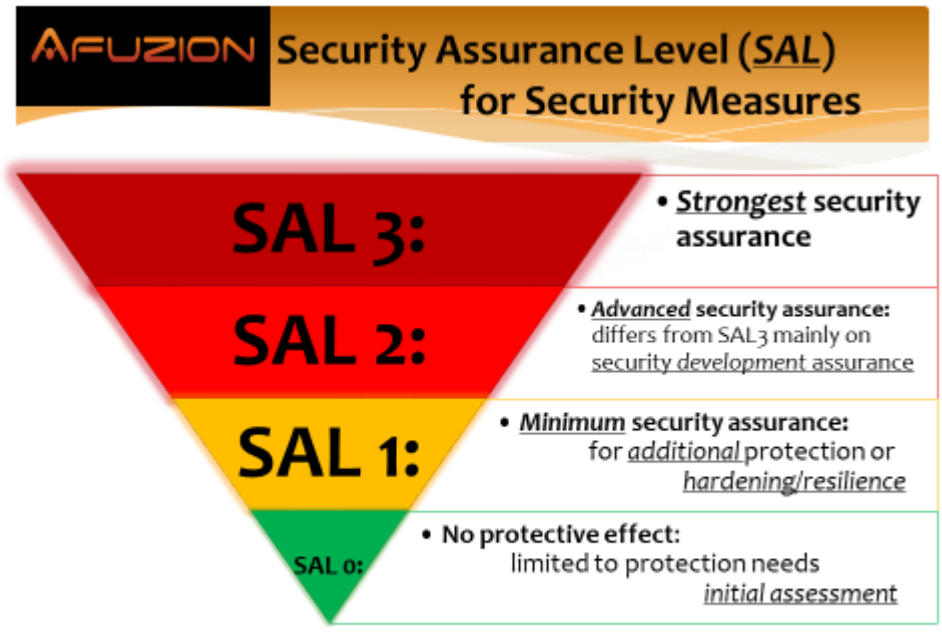
How Can The "DO-326/ED-202 Set" "Guidance/Recommendations" Be Efficiently Met?

Detailing the information security processes, even to the finest item does not ensure success, of course. Moreover – it definitely does not even start to deal with efficiency, in fact – DO-326A/ED-202A clearly states: "… the notion of efficiency, defined as the relationship between obtained results and resources engaged, is not considered in this standard." – no less…

So, what should an applicant do to keep the time and cost of this process reasonable?

For Security Effectiveness Assurance, DO-356A/ED-203A specifies two methods to contain the required effort:

1) Up to ~25% of assurance-activities are not "security specific", so they can be satisfied by providing evidence that the applicant has been applying "regular" safety development assurance practices, such as ED-79A/ARP4754A, DO-178C/ED-12C, DO-254/ED-80 etc.
2) The security measures requirements vary According to the Risk Level of the system, which mandates different levels of assurance. The levels of assurance assigned to the proper security measures are SAL: Security Assurance Level, similar in mentality to the FDAL/IDAL of the parallel safety assurance process. SAL 3 is the highest level of assurance, SAL 0 means – no assurance; just prove this is actually SAL 0. As a result, properly performing the Risk Analysis and designating appropriate assurance levels would mean that assurance efforts would be more relaxed for systems/items that are not rated SAL 3.



For the risk assessment and security development, there are various techniques, and even DO-356A/ED-203A provides, for instance, four different options for risk assessment that could be acceptable. The general approach of the DO-326/ED-202 set is – "there could be more than one acceptable means of compliance (AMC)", so the applicant should carefully define the proper AMC for the specifics of their case. Even more so – the DO-326/ED-202 set recognizes that Airworthiness Information Security is “Work-In-Progress”, so that emerging measures, techniques, standards, even methodologies can be brought into play to streamline the process.

A final consideration that can considerably affect the efficiency of the Airworthiness Security Process is its integration level with the parallel Airworthiness Safety Process. One aspect of this similarity is – the two processes are very similar, so inputs can be taken in and lessons can be learnt from the safety process, so efforts are reduced. The other aspect that has to be considered is – the extent to which the processes are combined. The DO-326/ED-202 set's take on it is "it depends": there are advantages to closely coupled safety and security, e.g.: avoiding the repetition of tasks and lowering the integration effort, BUT, there are also prices to such a close coupling, e.g.: whereas safety requires as few changes as practical after configuration change, security may require very frequent changes to accommodate changing threats, so the safety and security aspects may contradict each other if integrated into the same item.

Summary & Conclusion: Paranoids Live Longer

A passenger walks into a commercial-flight airplane with a laptop, hacks its network, making it fly even higher: extremely unlikely when using the DO-326/ED-202 set. The major takeaways following this brief introductory review:

(1) Aviation Cyber-Security…
   a) …is a discipline of its own – it needs unique expertise, and requires its own analysis techniques and assurance considerations;
   b) …involves many stakeholders, internal and external to applicant's organization, with whom All-Way Trustworthiness should be established – not "Assumed"…;
   c) …is a "never ending story", as cyber threats keep evolving with time – so Airworthiness Security needs to be implemented, as an ongoing process throughout the entire lifetime of all certified aircraft and other equipment.

(2) The DO-326/ED-202 set…
   a) …is already a usable set of documents, regarded as the Acceptable Means of Compliance (AMC) for Aviation Cyber-Security in the U.S. and Europe, and rapidly becoming so in the rest of the world;
   b) …should be approached as a whole, rather than "document-by-document";
   c) …draws from a variety of solid references in the areas of Cyber-Security and Aviation-Safety to create an entire "eco-system", to the extent that certain DO-326/ED-202 set methods and solutions are derived directly from these references – thus, providing multiple specific options, that need to be applied as a function of the specific organization, project and system;
   d) …is still an evolving "Work In Progress", so care should be taken to not "set in stone" any specific solutions.

(3) The Airworthiness Security Process (AWSP)…
   a) …is the core process of the DO-326/ED-202 set, from which all the set's documents draw;
   b) …includes 7 steps, 14 activities, 62 objectives – so cannot be treated as an "afterthought" of airworthiness certification;
   c) ...heavily relies on integral processes, namely "Security Effectiveness Assurance", including 118 objectives in 39 activities – applied as a function of a few variables, mainly the "Security Assurance Level" that determines the required security defense level of the element under consideration;
   d) …is similar in nature to the Airworthiness Safety Process, as both use hazard/risk assessments, severity of failure/threat, mitigation requirements and similar assurance techniques – and this similarity provides rich opportunities for mutual benefits for the two processes, including the usage of up to ~25% of Safety Assurance evidence as Security Development Assurance evidence…
   e) …however, the most cost-effective level of integration between the Security and Safety Airworthiness Processes depends on a variety of specific variables – organizational, equipment type etc. – so it should be best determined on a case-by-case basis.

As these points amount to 12 major takeaways, it is necessary to add one more takeaway, to get to exactly 13, so it would be appropriate to conclude with a sound advice from Mr. Pedro Bustamante, Technology VP, Malwarebytes, that may arguably be the most important takeaway:

"If you're not paranoid, you're not going to survive."

For DO-178C & DO-254 details, procure the book "Avionics Certification: A Complete Guide To DO-178 & DO-254", from major bookstores such as Amazon.com. (The author of this whitepaper is the primary author of that book.)

For customized training in ARP4754A, DO-178C, DO-254, DO-326A etc., AFuzion's trainers have provided more such training than all other trainers in the world, combined.

Contact us to find out why: info@afuzion.com

For related Training information, see: http://afuzion.com/training/
For related Gap Analysis information & video, see: http://afuzion.com/gap-analysis/

What is AFuzion? Fun One-Minute Video: https://www.youtube.com/watch?v=RMzLRzcahJE

AFuzion's Worldwide Onsite Engineering Footprint - *When Safety Is Critical ™:*

…and for Aviation Cyber-Security - *When Safety Needs To Be Secure™:*

