Secure deterministic L2/L3 Ethernet Networking for Integrated Architectures

Bernd Hirschler, Mirko Jakovljevic
TTTech, Austria

Abstract

Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems. This paper investigates the context and use of key security technologies, processes, challenges and use cases for the design of advanced integrated architectures with security, safety, and real-time performance considerations. In such architectures, deterministic Ethernet standards are used as a baseline for system integration in closed embedded systems or open mixed criticality systems.

Security-informed safety development processes for integrated architectures are required to prevent catastrophic failures caused by environmental and cyber threats, due to expanding number of security threats in complex and increasingly open systems. State-of-art safety/security processes for integrated systems in cross-industry environments are considered and similarities examined, for different types of integrated architectures.

In integrated systems and IMA which share common resources, multi-level secure systems and composable modular architectures such as MILS based on separation kernels and ARINC653 API are gaining importance for design of safe and secure distributed applications with real-time performance requirements. Network security is a core component of the overall cyber-security and defense-in-depth capability for distributed architectures. Protection mechanism for information, interface and system integrity, communication availability, and data confidentiality are required for design of safe and secure integrated embedded infrastructure. In deterministic Ethernet networks with Time-Triggered Ethernet (SAE AS6802) and ARINC664 services, the network partitioning, dataflow isolation, configuration protection, per-flow traffic policing, link and end-to-end encryptions or authentication, and internal network device partitioned architecture can actively support security measures for mixed-criticality applications. This can be useful for design of open networked systems which can also accept previously unknown soft-time and/or bursty traffic, while hosting highly critical functions with temporal boundaries.

After an overview of security issues in networks within integrated architectures, this paper continues with discussion of MACsec and IPsec mechanisms, packet firewalls, secure shells and Denial-Of-Service (DoS) protection mechanisms for secure and deterministic L2/L3 networking.

Introduction

While safety protects the environment and humans from the system and catastrophic events, security protects the system from environmental and cyber-threats. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems. Different vital assets, integrated transportation systems, onboard electronics, or avionics can be harmed by rogue cyber activities, and can create hazards to safety, financial stability, and reputation to OEMs, 1st Tiers, or transportation in general. Organizational risk objectives, the changing threat environment and business/mission requirements determine the level of cybersecurity risk management, to ensure sustainable operation of systems and society.
The design and integration of systems which are resilient, and have a convincing safety case always need to take into account security threats and protection mechanisms, to avoid threats which have the potential to work around safety properties and create catastrophic system failures. This paper addresses system integration capabilities and considerations relevant to integrated system and network security.

Integrated Systems and Security

Advanced integrated systems for transportation applications are critical for the wellbeing of modern society. Aircraft, railway and automotive systems are converging toward similar integrated and technology capabilities – and the number of threats is growing. These systems and their respective embedded platforms become more open to accommodate different functions and provide optimized performance, such as IMA (Integrate Modular Avionics) tied to cabin functions or air traffic management, industrial Internet-Of-Things (IIoT), railway controls systems and TCMS or emerging automotive CAR2X architectures [16]. The embedded resources and assets are shared among different functions and components, but under certain conditions only or frequently also accessible to the external world. In advanced integrated real-time architectures which can host different critical and non-critical functions, the safety and security capabilities may impose additional performance limitations, such as the limitations on communication paths and additional processing latencies – to the point where only careful trade-offs and criteria selection can help to design sustainable and affordable system architectures.

Integrated systems represent a set of embedded resources which can be adaptively used for hosting mixed criticality functions – hard RT, real-time and soft-time, with different functional, safety and performance requirements.

High-bandwidth Ethernet networks enable integration and sensor fusion from different data sources in closed and open environments. Ethernet networks can integrate safety-critical systems, hosting critical and non-critical functions with hard real-time (HRT), real-time (RT) and soft-time performance, using a plethora of computing models (client/server, publisher/subscriber, TTA [1], L-TTA[2], …). Due to its capabilities, it is possible to design flat reconfigurable architectures which do not rely on several separated networks and gateways. Therefore, the network consists of network devices which can access any other device, sensor and actuator in the system, if configured and permitted. Obviously, this seemingly creates a new vector of cyber-attacks, which can be prevented with a selective set of design patterns, design and integration methodologies, and security considerations in every lifecycle step. It is an imperative to have a set of capabilities which can support security and prevent threats in deterministic networks which serve as a backbone of advanced integrated architectures, IMA and embedded platforms. But before we continue with network security topics, it makes sense to assess key aspects of security and standards in embedded systems and describe the context relevant for the design of advanced integrated architectures.

Network Security in Integrated System Context

Primary objective for security in transportation systems is to protect the safety of the transportation systems and humans, and minimize threats which could lead to catastrophic consequences.
Network security is a subset of cybersecurity, and protects any data that is being sent through devices in your network to ensure that the information is not altered, intercepted or made unavailable. Networks have always played the significant role in cyber security, which is concerned with protection of cyber space and critical digital systems or embedded platforms from cyber-attacks.
Information security is focused on information and information systems, and protection of unauthorized access, use, disclosure, or modification of data. As the majority of relevant information is stored in digital systems, the security features of modern networking protocols provide a multitude of services, e.g., prevent unauthorized access, or modification of information, or prevention of network DoS (Denial-of-Service) attacks. The relationship is presented in Figure 1.

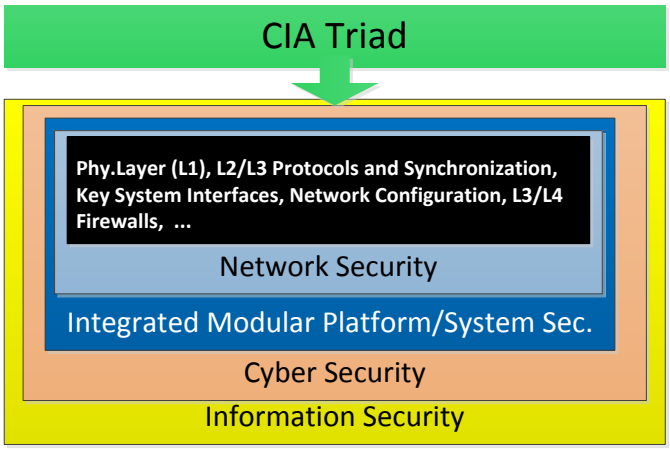

Figure 1: Relation of CIA Triad and Network/Cyber/Information Security

The security features and capabilities of networking protocols and interfaces also provide trust in the information that is sent or received. This trust is based on the services that support a security triad: Confidentiality, integrity and availability. Ensuring these properties is a crucial part in designing secure organizations, systems and networks.
System integration and networking are concerned with the flow of information, system interfaces (interaction points), and system functions exchanging data.

In domain of embedded systems hosting critical controls or safety-critical functions, the priorities are somewhat different, with availability, integrity and confidentiality in different priority order (see Figure 2). With increasing levels of integration both IT and embedded systems views should be integrated and become mutually complementary.

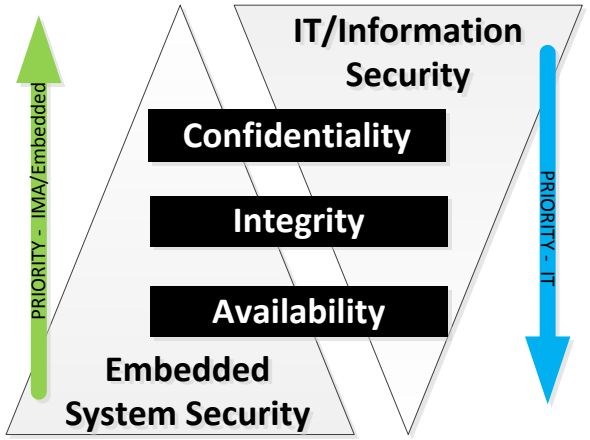

Figure 2: CIA Triad and Different Security Priorities for Embedded Systems and IT

Confidentiality

For most of the applications in today's civil airborne vehicles confidentiality is not being a primary target or even desired. There are several use cases where this property is up for discussion. The two diametrical cases are:
1. Real-time data is transmitted and the relevance of this data is soon obsoleted. This data can include frequent value changes of control loops or clock synchronization. In this case confidentiality does not increase the viability of the data. Furthermore, one can argue that this data can be regarded as common good and every device that needs this information should have access to it.
2. Configuration data that holds information about algorithms or tables about the schedule of the traffic in the network can be regarded as very valuable for an attacker. In this case, the data has to be protected. But this only applies to seldom maintenance use-cases in a special network device operation mode, e.g., update of configurations. Typically, the usual traffic for running the network in standard operational mode does not require this kind of protection.

Integrity

In the safety domain, the integrity of data is of high interest to support critical services. It ensures the data is accurate and trustworthy.
In this case, the integrity not only ensures that the data (or interfaces or systems providing data) is not modified unintentionally but also, that intentional modification of data can be spotted immediately. This kind of property is already used in the safety domain to ensure the validity of the data for unintentional modifications and memory faults.
The addition of the security enhancement can easily be facilitated by the change of the algorithm that is used. An example for an algorithm used for protecting information integrity is SHA256. The cryptographic algorithms used for such cases are designed to provide a large hamming distance which is also a feature needed in the safety domain. These algorithms can also be used to ensure the authenticity of the data with cryptographic proof that the data is sent by a specific sender or group and cannot have been sent from an unauthorized user. The algorithms used in such cases are called Hash Message Authentication Codes, e.g., HMAC-SHA-256 which are used with TLS and IPsec.
Furthermore the authentication and nonrepudiation are essential for keeping the communication, system, and application integrity intact [3].

Nonrepudiation

Authentication is important to keep the configuration of protocols, devices and applications, but nonrepudiation ensures that all communication participants, devices, and components are really who they claim to be. Supply chain for electronic devices and software shall support nonrepudiation and counterfeiting. In addition to authentication, logging mechanisms shall be used to track down past modifications and their origin, to enforce accountability. SSL/TTL provide authenticity, but not the nonrepudiation. Digital signatures and hardware security modules designed for strong authentication can support nonrepudiation.

Availability

The availability is at the heart of safe and secure implementations, especially in integrated systems which have a limited set of safe states. Specifically, for the security context it has to be ensured that the critical information is available whenever needed to critical functions. The availability of networked systems focused on Denial of Service (DoS) attacks, e.g., flooding with ARP requests, tampering with the physical layer or key system interface operation.
From a safety perspective, additional components necessary to provide this security service have to be taken into account when calculating safe system availability numbers.
The availability in safety-critical systems is supported by network design, using system architecting methodology and models of computation and communication (MoCC) which prevent specific classes of cyber-attacks, and by minimizing the number of attack vectors.

Security Frameworks and Standards for Integrated Transportation Systems

Cyber-security risks are handled in the scope of the broader system engineering process, based on the preliminary security architecture. Then the results and considerations are provided to the safety process. Safety-critical systems require safety as a prerequisite for doing business, and security threats may impact safety. Therefore, both security and safety considerations shall be addressed in parallel with system engineering and design processes – so called security-informed safety.

Security-Informed Safety

As the authors of [4] rationalize, the safety is concerned with protecting the environment from the system and security is concerned with protecting the system from the environment. This necessarily leads to a differentiated key objectives and assumptions. It is widely recognized that the integration of security with safety assurance and system engineering processes, and the implementation in transportation, aircraft and road vehicles industry should operate as one entity to be fully effective. As a hot research topic, European SESAMO project [5] has handled the joint reasoning about safety and security properties in integrated systems for cross-industry applications, and discussed their conflicts and synergies. Aerospace industry already combines safety and security considerations [6], and automotive industry is on the way to integrated those considerations with different assumptions and perspectives. Railway industry currently works on fully integrated rolling stock TCMS systems with Shift2Rail activities [7].

Aerospace Standard and Security in Integrated Systems

Aerospace industry uses a tailored security standards designed for specific considerations in aircraft design, in addition to robust safety and system engineering assurance for aircraft system design. As discussed, the underlying considerations, methodology and terminology are different for safety and security experts, and they have different perspective on system threats, fault hypotheses and risks.
Aerospace industry relies on different standards in ground, airline and air traffic management operation. Aircraft OEM use a specific set of standards which is aligned with existing safety and system engineering practices, and focuses on on-board integrated aircraft systems and avionics design – specifically for companies which apply for type certification in new aircraft design, or system modifications in aircraft which have been already designed using similar practices. Airworthiness Security Processes also take into account interfaces with other external systems which may influence safe and secure operation of on-board systems.

The following set of standards is used in aircraft systems design:

- DO-326A/ED-202A “Airworthiness Security Process Specification”
- DO-356/ED-204 [8] “Airworthiness Security Methods and Considerations”
- DO-355/ED-203 “Information Security Guidance for Continuing Airworthiness”

and partially corresponds in its structure with aircraft safety standards:

- SAE ARP 4754B “Aircraft and System Development Process”
- SAE ARP 4761 “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment”
- SAE ARP 5150/5151 “Safety Assessment of Aircraft in Commercial Service”

Aerospace standards for safety and security define a design process framework and safety/security activities (i.e. SAE ARP 4754B and RTCA DO-326A), and propose methods for analysis of safety and

security issues (i.e. SAE ARP 4761 and RTCA DO-356), but also other alternative methods can be deployed, assuming sufficient alignments with certification authorities have been conducted.
The approach adopted in the aerospace standard RTCA DO-326A explicitly concludes that safety and security processes may be handled independently, with well-defined interfaces. It is more about the divide-and-conquer approaches to control process, engineering culture and design complexity, and not about real intent to separate those activities, as they are in reality inseparable.
As safety is a primary driver in commercial aviation, to keep the complexity and design space considerations at acceptable levels, safety design assurance processes interact with security processes at specified project points. This allows security teams to provide feedback to issues relevant for safety and airworthiness from the security perspective.
The design process includes system engineering processes and safety assurance design processes at system and components level, are selectively interwoven with security processes and considerations. Typically, some higher level organizational authority is implemented within the company to oversee both activities and enable the appropriate level of integration.
In addition, DO-326A explicitly allows a blended safety/security process assuming a suitable evidence on security and safety can be provided.
Those standards and guidance may also be useful for non-commercial aerospace applications which integrate more complex systems and require "security-informed safety".
Commercial aerospace standards do not specify exactly how the airworthiness objectives are met, Networking devices and protocols, or network capabilities are not directly discussed in those standards. Therefore, the security practice from other domains can be utilized. But DO-326A requires the identification of services and protocols running over hardware and data (information) interfaces, and physical paths for information sharing with the security perimeter. The scope of DO-326A requires to capture requirements and assumptions involving elements outside the aircraft, and differentiates between integrated and federated architecture types. Integrated architectures enable access to all or the majority of resources, and require an aircraft (vehicle)-system level analysis. Aircraft network and system security depends on risks introduced by the modification, which may or may not ensure that previous security measures and requirements are taken into account. When accompanied with safety analyses, the effort for change impact analyses and updates can be considerable in the case of an integrated architecture which can host critical and non-critical functions. Therefore, networked systems hosting functions of different criticality (or novelty) will be split into separate zones/domains with "firewalls" and careful control of all traffic and information exchange among them. Necessarily this leads to a domain-based architecture with separate aircraft control, airline and passenger connectivity [9]

According to DO-356, the characteristics of sound security architecture are:

- Non-bypass: Security measures cannot be by-passed.
- Protection: Security measures cannot be manipulated.
- Independence: The security measures do not unintentionally depend on each other.
- Detection and Restoration: The architecture provides means for detecting threat conditions, with means to restore correct configuration of the architecture.

DO-356 recognizes the need for defense in depth layered security architectures, with avoidance of common vulnerabilities which can emerge when several less capable security mechanisms are combined.

All those aspects listed above are essential for design of advanced integrated architectures. They are compliant with MILS architecture objectives, explained later in this text.

Specifically, DO-356 references ITU-T X.1205/X.805 on "Architecture Design and Network Security Domains" using their classification of failure and threat conditions:

- **Loss of function or function continuity** caused by permanent or intermittent unavailability of interfaces or information required for the system operation.
- **Malfunction** (incorrect operation) caused by the integrity breach of required system data and interfaces.
- **Loss of confidentiality** (exposure of information) caused by the confidentiality breach of information, or interfaces.
- **Unintended function** (e.g. malware) caused by the information provided by the unintended function, or/and by the system or interfaces associated with unintended function that are the source of information.
- **Misuse** caused by the integrity breach of information or interfaces or systems, invoked by an unauthorized entity.
- **Tampered information** caused by the integrity breach of information, or/and of the system or interfaces that are the source of information.
- **Counterfeiting** (tampering with persistent/configuration data) caused by the integrity breach of persistent information. For network devices, this may lead to modified network operation, policing, non-perfroming packet firewalls, and network failure.
- **Spoofed Information** (apparently correct information from/for wrong source/destination) caused by the integrity breach in the systems or interfaces providing spoofed information.

Furthermore, common criteria EAL levels are allowed in software and hardware item development, and if they are used generically, and in addition to the separately implemented safety processes with corresponding DAL levels, then for the most critical systems (i.e. DAL A/B), the CC EAL5 semiformal security design and verification shall be used. To avoid false assumptions, the system-level verification shall be performed to show that the deployed methods correspond with the intended use and environment of the function within complex systems.

Assurance Level	EAL
E	CC EAL 1
D	CC EAL 3
C	CC EAL 4
B	CC EAL 5
A	CC EAL 5

Figure 3: Safety and Common Core EAL Levels in DO-356

Railway Standards and Security for Integrated systems

IT security in the Railway domain will be handled in a new standardization project called *Railway Applications - Communication, signalling and processing systems – IT security requirements for electronic systems for signalling* is under preparation in SC9XA of CENELEC. This standard will focus on security risks in safety-related applications and intentional cyber-security attacks. The standard will profile IEC 62443 series, which deals with the cybersecurity in industrial systems. The approach adopted in IEC 62443 will be integrated into the established approaches of EN 50129. As such, the segmentation of the system into security zones and conduits connecting the zones, with separate

security risks is required. Unfortunately, threats from Security Risk Assessment cannot be compared to systemic errors and safety risks, and therefore it is hard to assess in probabilistic terms – therefore the "likelihood" of security risks and threats is assessed. It is expected that potential security threats for safe communications EN 50159 will be incorporated in this standard.

In addition, other standards such as ISO/IEC 15408 has developed criteria for evaluation of IT security in SW/HW products. DIN VDE V 0831 standards relate to railway signalling IT security and common core criteria assessment.

ISA/IEC 62443

The ISA/IEC 62443 [12]is a series of standards addressing the cyber security for Industrial Automation and Control Systems (IACS). This standard was originally created as ANSI/ISA-99 by the International Society for Automation (ISA) and published as standard by American National Standard Institute (ANSI). Standard series was submitted to IEC for review and consequently approved as the IEC standards. The ISA is responsible for the further development of the standard.

The standard introduces the concept of the zone model reflecting the segmentation of the system into zones which are connected by conduits. The segmentation addresses the case where there are parts of the system with different security requirements, or with the same security requirements but communicating through an untrusted channel. Another key concept defined is *Security Level* (SL1-4).

ISA/IEC 62443 can be applied to the system and the Common Criteria to some of its components. For instance, network devices can be evaluated according to ISO/IEC 15408 (Common Criteria - CC) [10] making use of existing Protection Profiles (PP). A PP can address a complete device of a given type or its part (e.g. Firewall, VPN Gateway, Web server, operating system).

DIN VDE V 0831-104

The draft standard DIN VDE V 0831-104 [11] named "IT Security Guideline based on IEC 62443" tailors IEC 62443 [12] for railway signalling systems, and applies to electrical, electronic and programmable electronic safety-related systems. To enable the easy integration of IT security aspects to EN 50129 [13] this DIN standard defines IT security tasks and assigns them to the phases of the safety life cycle. The EN 50159 [14] as well as DIN VDE 0831-102 [15], which deal with safety-related communication, are also the parts of this integration framework.

ISO/IEC 15408 – Common Criteria

The "Common Criteria for Information Technology Security Evaluation", standardized as ISO/IEC 15408 [10], is a framework in which computer system users can specify their security functional and assurance requirements through the use of Protection Profiles (PPs). Developers can then implement and/or make claims about the security attributes of their products, and evaluators can evaluate the products to determine if they actually meet the claims. In other words, the CC provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use. The CC defines 7 assurance levels (EAL – Evaluation Assurance Level), whereas for the levels above EAL 4 secure-by-design techniques with enhanced formality are required (semi-formally or formally designed/verified/tested components).

DIN VDE V 0831-102

The draft standard DIN VDE V 0831-102 "Protection profile for technical functions in railway signalling" tailors ISO/IEC 15408 (Common Criteria - CC) for the domain of railway signalling. As it addresses the transmission of safety-related data, this standard complements EN 50159 as well as EN 50129 with the aspects of integrity, authenticity and confidentiality.

Automotive Standards and Security for Integrated systems

Until recently the automotive industry has relied on common standards and industry expertise, and the automotive systems are designed as closed low-cost systems. Beyond simple access control and protection of confidential information, integrated system security enables further integration and new functions for public transportation, especially in future applications which will rely on CAR2X [16] communication.

The McAfee paper [17] on automotive security identifies key objectives for network security as message and device authentication, and access controls with security alerts (data confidentiality, availability, integrity, counterfeit component detection, man-in-the middle attacks), enforcement of the predictably holistic behavior in all networked systems (data integrity/availability, networked system availability and integrity), which is aligned with cross-industry best practices.

With increasing integration of functions and the integration of cars with transportation controls systems or Internet, the security risks and threats rapidly change. In addition, after-market purchases of car functionality options can lead to innovative business models, and modifications of core software and car functions. Therefore, a significant security capability is required for future automotive and public transportation infrastructure. Furthermore, the safety of key mobility functions, such as braking, navigation and accelerating cannot be safe without tight security measures and seamless detection of all unintended system parameter modifications. Currently the SAE J3061 [18] has been in progress since early 2016, and it will collect the best practices applicable for automotive industry lifecycle including the definition of security objective and goals, analytics, methodology and process implementation. It will specifically identify approaches how to define security processes in addition to safety practices for automotive industry as defined in ISO26262. In those aspects it also relies on experiences from DO-326A and DO-356, and other standards and work. As example, EVITA[19] focuses on secure on-board automotive networks, with a focus on protecting components from compromise due to tampering or other faults. SESAMO [5] targets integrated layered safety/security, while Swedish HEAVENS project [20] focuses on security vulnerabilities in software-intensive automotive systems with methodologies for software security testing. To simplify design of integrated networked systems and embedded platforms the automotive industry has worked on EVITA (European project) and SHE [21] standards (German HIS initiative) to simplify hardware acceleration for security mechanisms implemented in SoC, while meeting different security objectives and cost targets.

EVITA provides the following set of key security capabilities in embedded systems:

- Integrity of hardware security modules and components with tamper prevention/detection
- Integrity and authenticity of on-board software and data: Unauthorized alteration must be infeasible / detectable.
- Integrity and authenticity of on-board communication: Unauthorized modification must be detectable by the receiver.
- Confidentiality of in-vehicular communication and data
- Unauthorized disclosure of confidential data must be infeasible.
- Proof of platform integrity and authenticity to other entities: Remote attestation of integrity and authenticity of the platform configuration
- Access Control to in-vehicle data and resources: Enable availability and well-defined access to all data and resources.

The majority of those issues is already considered from the safety and mission-criticality perspective in closed systems, in an environment with low probability of external cyber-threats. Deterministic Ethernet networks used in critical infrastructure applications are typically designed to prevent and isolate system faults and malicious behavior, but require additional security hardening to protect against intended internal and external cyber-attacks conducted by capable attackers, with a good insight in the internals system operation.

Security domains and Multiple Independent levels of Security (MILS) in Integrated System

Introduction

Zonal security and separation of different zones by trustworthy security monitors, firewalls or "diodes" is a traditional approach to separate and control interactions among different security domains. This is a simple approach which leads to hierarchical or domain computing, which require multiple computing resources for different security levels, or separate security zones.

This approach can be relatively simple, but for systems which are both secure and safe, security gateways or physically separated infrastructure will be required. From the physical SWaP- or component cost-reduction perspective, for some applications this approach cannot be sustained, if different security levels (e.g. example MLS, multiple level security) require multiplication of computing and networking resources. Therefore, it makes sense to deploy security approaches which at high-level share some similarities to IMA (Integrated Modular Avionics) architecture patterns, sharing common computing and networking resources. MILS is a high-assurance security-critical architecture which. decomposes MLS (multi-level security) systems into separately evaluable components. MILS relies on the separation/isolation and control of critical and security relevant dataflows and processes, required for MLS (Multi-Level Security) operation on one networked system. It provides separation mechanisms that support both untrusted and trustworthy components, thus ensuring that the total security solution is non-bypassable, evaluable, always invoked, and tamperproof (NEAT) – which is also to large extent the objective of high-integrity avionics architectures. Without MILS approach, each function with specified MLS security level (top secret, secret, confidential, unclassified) would run on a separate computer using the Bell La Padula Mandatory Access Model "*no read up* and *no write down"* with unidirectional communication and avoidance of covert backchannels.

The objective of MILS is to decrease the time and cost of developing, evaluating, certifying, and accrediting multi-level secure (MLS) systems throughout the system life cycle. It is recognized that integrated safety and security system architectures use similar means for separation, partitioning and fault isolation, and MILS enables the security evaluation and certification of a complex system to be modularized.

However, it does not mean that the same monolithic RTOS within ARINC653 API can be simply used for safety-critical and multi-level secure applications. Depending on implementation, MILS approach also imposes additional costs in the form of higher complexity on modification verification and validation, with mutual interdependencies in safety, security and real-time performance of integrated applications. It cannot be easily abstracted from the HW platform (multicore SoC) capabilities and internal architecture considerations.

Today multi-level security can be also hosted in containers and virtual machines on Linux, assuming the secure unidirectional inter-process communication mechanisms without backchannels are implemented [23], but its realtime performance and safety design assurance are questionable.

In practice, MILS implementations have been different in comparison to ARINC653-based RTOS, as MILS requires a small software core for security evaluation, and may for example run drivers in the user space. Additional Separation Kernel Protection Profile (SKPP) [24] requirements shall be taken into account for its design. Safety-critical applications until today can use multicores only under certain conditions and with advanced MPSoC architectures with provable non-interference. MILS architecture may experience similar challenges in multicore and distributed embedded platform environments due to issues with application isolation, SoC resource sharing and core separation. The concept of Multi-Level Secure IMA has been described [25], which is primarily designed as a MILS platform with a secure hypervisor, and uses ARINC653 ports for communication with high assurance partitions with guards, but there are no publicly documented large-scale attested system deployments which support IMA and integrated system security. Another MILS-capable hypervisor may be applied to automotive or IoT applications [26]. Obviously, Multi-Level Secure IMA is a work in progress which provides improved capability to isolate information flows secure and safe applications, suppress covert channels, enable safe partitioning of common resources and enable modular certification to a higher extent for both security and safety in the future. Taking into account all of above it can be concluded that secure hypervisors are better suited as a starting point for integrated modular safe and secure architectures, than the legacy monolithic RTOS with ARINC653 API.

Deterministic Networking and MILS

From the networking perspective, the Partitioning Communication Systems (PCS) or Secure Inter-Process Communication (SIPC) supports separation kernel communication policies in a distributed system concerning information flow policy enforcement, data isolation and determinism, end-point authentication, periodic processing/transmission, message encryption, traffic padding, and fault isolation.

MILS security policies alone do not prevent covert channels, nor analyze packet content, and cannot enforce security policies designed for higher layers (L4 and above), but it supports design of distributed

MILS systems with partitions and information flows completely abstracted from the topology and partition location. The unidirectional communication approach used in avionics Ethernet networks is compliant with non-blocking L-TTA and TTA computation and communication models used in IMA architectures with ARINC653 port-based inter-process communication (IPC). Partitioned communication or special security relevant components (data guards, filters, downgraders) with limited code size may be implemented on a separate partition, and isolated within a partition in the scope of high-assurance environment and separated from all other applications [27]. As example, in D-MILS project (Distributed MILS), the approach has been examined how to define controlled information flows, taking advantage of the inherent robustness and fault-tolerance mechanisms built-in TTEthernet which can mitigate a large class of security attacks, such as Denial of Service (DoS) attacks or performance attacks. While standard MILS solutions protect the information exchange inside a D-MILS node based on a separation kernel and access policies, deterministic Ethenret capabilities for synchronous Ethernet communication can be hardened to support the secure exchange between two D-MILS nodes [28]. In addition, it is possible to define synchronous strictly deterministic communication with fixed latency, to suppress covert channels among distributed computers.

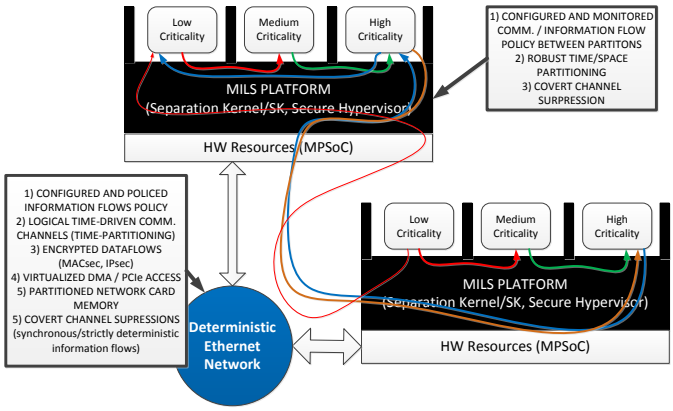

Figure 4: Distributed MILS approach with network rules and policing contributing to information flow control and covert channel prevention

Potential Performance or System Architecting Limitations with MILS

The definition of integrated security/safety policies and architectures in integrated systems have limitations. The work from [22] shows that for some use cases integrated safety and security architectures might make perfect sense. However the challenges in the seamless integration of safety and security aspects for real-time systems will emerge if the required safety and security methods are particularly sophisticated.

MILS may limit the execution performance or impose additional information flow constraints for the execution of real-time functions [29]. With several critical applications hosted in a partitioning RTOS on a single core, the partition execution order can take approximately 10-100ms to complete, which can create excessive latency for real-time systems communicating via a dedicated secure and networking partitions.

For MPSoC (Multi-Processor System-on-Chip) implementations, the partitioned communication system imposes less constraints as it can be hosted on a dedicated computing core. Therefore, all other cores can send data to the dedicated network interface-handling core, equipped with security, fault detection, isolation and recovery capabilities. This may raise other issues tied to safety certification, which requires full evidence of the MPSoC memory architecture and core interference to maintain realtime performance and prevent resource starvation or deadlocks.

As an example, a system contains several hundreds of safety-relevant and secure dataflows (logical communication channels) may drain computing power, if encryption is deployed, or secure control application might be split into secure functions in separate partitions (or cores) to stay analyzable, but also require much faster access to network resources. At some point engineers will need to prioritize on performance and security, if safety aspects are non-negotiable, or design a different, less integrated architecture.

Aircraft Domains and Security Zones

In line with security and safety constraints described in ARINC664-P5, aircraft domains are defined as separate domains with different criticality [2630]. Aircraft systems are divided into four main domains: Aircraft Control Domain (ACD), Airline Information Services Domain (AISD), Passenger Information and Entertainment Services Domain (PIESD) and Passenger Owned Devices Domain (PODD). The last two are using consumer technologies and can be seen as independent functions, as long as they do not exchange data or share domain gateways with other domains.

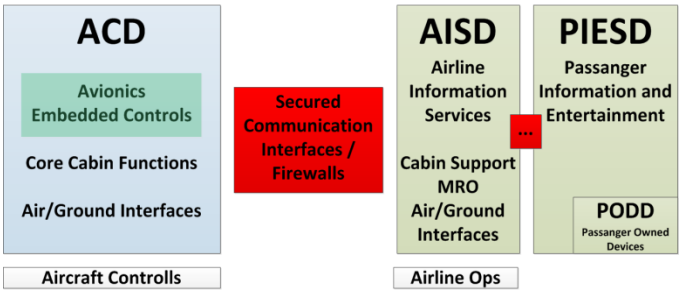

Figure 5: Target applications in aircraft control domain (ACD)

While the PIESD and PODD represent a technologically fast-changing networked system category, which integrates wireless devices or wired media servers, and can be more frequently upgraded or exchanged, we focus on ACD (and portions of AISD) domain with aircraft embedded controls, avionics and core cabin systems which rely on wired networks. AISD does not contain critical applications or functions for direct aircraft controls. ACD relies on strong policing and planning of network traffic profile, so that any unintended traffic is simply discarded. Any unintended and not planned network scenario which may lead to system failure is prevented. All key mechanisms to support traffic policing, rate limiting and compliance monitoring reside at Layer 2, below TCP/UDP/IP layer. ACD uses either ARINC664 networks with Layer 2 or very profiled UDP/IP application, or non-IP networks for the data exchange among functions and subsystems. In contrast, TCP/IP is used for AISD and PIESD domains in more open networking environment relying on commercial Ethernet networking. Depending on the Ethernet network's switching device implementation, higher layers can also be monitored and policed. Historically, ACD involved many different

networks, while with new IMA architectures their number is gradually reducing to deterministic Ethernet (AFDX).

Fortunately, the domains can be physically isolated and spatially separated in aircraft systems, which have quite static configuration.

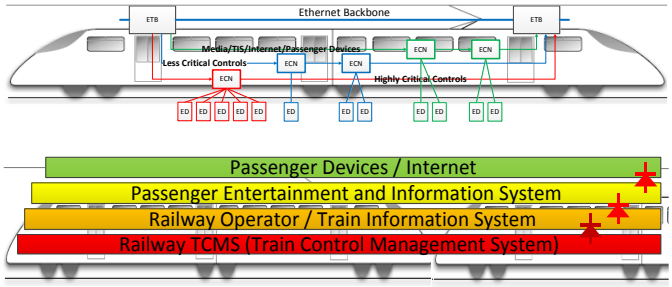

Figure 6: Security domain in railway architectures

Railway Domains and Security Zones

In opposite, railway domains do not provide equivalent separation opportunities if a common Ethernet network is used for system integration. In integrated railway systems the domains are spread over the whole set of train consists which may use common infrastructure in the future. Obviously, specific security zones and domains may share common embedded infrastructure on a train level.

As there is a common ETB (Ethernet Train Backbone), all domains with different security constraints can potentially share common ETB resources. The information flow between domains (TCMS, Operator Network/Train Information System, Passenger Devices), shall be carefully controlled and secured. Either information/dataflow diodes shall be enforced at network layers, or a complete MILS-type architecture shall be implemented. In comparison to aerospace systems, this use case is harder to optimize, as domains are not located in specific place, but interwoven, along the set of vehicles (train cars).

Automotive Domains and Security Zones

Automotive vehicle architectures are currently moving from CAN-based toward multi-domain Ethernet based architectures without central gateway. This architecture supports zonal security approaches. The next step after 2025 [31] would be a fully integrated flat architecture – the structure of domains and their communication points may be similar to a blend of railway and aerospace security zones, with some applications with security levels spread among several domains, and others contained in their own domain.

DETERMINISTIC ETHERNET BACKBONE: SYSTEM INTEGRATION FOR DISTRIBUTED PLATFORMS AND IMA

Deterministic Ethernet Networking

In commercial avionics and ACD domain, ARINC664-P7 [32] (Avionics Full Duplex Ethernet or AFDX) QoS enhancement has been added to standard Ethernet switches to enable redundant rate-constrained communication with defined maximum latency. AFDX networks are used in commercial programs such as Airbus A380 and Boeing 787 as a backbone network for integrated avionics / IMA, and in military avionics (Airbus A400M) and rotorcraft cockpits for display integration. With a known network traffic profile, virtual link prioritization, defined switch buffer dimensioning and decent network calculus and configuration tools, very deterministic operation with respect to maximum latency can be ensured for all end-to-end virtual links (VLs) in AFDX networks. VLs enable point-to-point communication among different functions in the switched network system. Configured VLs have guaranteed bandwidth use and periodicity with defined maximum latency. ARINC664-P7 standard describes traffic policing and shaping required to ensure planned AFDX network performance.

Under assumptions of correct partitioning, airworthy internal network device architecture and bounded packet processing latency, the network design can use existing best practices for avionics network design associated with the ARINC 664 standard. The only difference is that synchronous networks rely on time-division and scheduling of the communication, while AFDX relies on statistical bandwidth partitioning and shaper configuration. All technologies for the design of critical systems can support partitioned virtual links (VLs) or data streams with defined temporal behavior.

From the perspective of the ARINC 664 network designer and integrator, additional synchronous communications in SAE AS6802 [33] and IEEE TSN [34] messages can be seen as AFDX messages with fixed latency and jitter. While SAE AS6802 and ARINC664 can operate in one avionics network, additional mechanism would be required to support that in IEEE TSN traffic. Therefore, it makes sense to use it in different domains, separately or selectively use IEEE TSN for network subdomains with less critical functions. This opens new opportunities for system-level time partitioning for critical application, or more deterministic integration of less critical applications such as media streaming, at different price point [35].

Integrated Architectures with Deterministic Ethernet Networks

Network and system integration attacks focus on network traffic analysis, intercept, rerouting, modification of data inputs and outputs of a control systems, denial of service (or message removal) to critical applications or the network configuration and message modification [36]. In hard RT applications, small modification of timing or synchronization function can create faults and errors, with hard to diagnose root-causes. While the threats to critical dataflows (rerouting, message modification, availability/DoS) in operation can be handled by L2/L3 communication protocol mechanisms, the configuration and design of network devices or network design process requires a holistic network and device design, installation and maintenance security management.

Typically, for deterministic Ethernet networking platforms used in advanced integrated systems, the dataflow control is permanently enforced at the network level, by safety-critical networking devices which are designed to protect themselves from faults, and fulfill required availability and integrity properties of the network. The system is designed to host unicast/multicast critical dataflows with specified bandwidth use and temporal behavior.

The operation of ingress ports is similar to L2/L3 security firewalls and filters out any non-compliant traffic and dataflows, based on network device and port configuration. The non-compliance of ingress dataflows is policed based on temporal behavior (jitter,

latency, periodicity), bandwidth use per period, frame format, dataflow identifier, MAC and/or IP destination and source addresses.

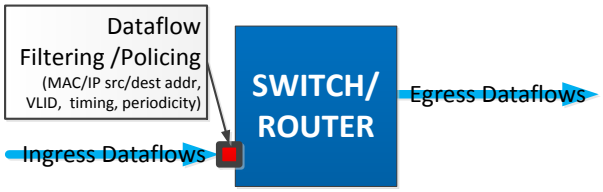

Figure 7: Dataflow filtering and policing for real-time systems

A minimum level of unintended data sharing and bandwidth isolation breaches between nodes is provided by using plain safety mechanisms (e.g. CRC calculation with implicit sender source address) which prevents that the information sent to the wrong device is transmitted to the software layer and applications. This mechanism is essentially designed only to protect shared bandwidth from switches and end devices sending data to wrong destinations by omission (bit flips, wrong configuration). It is also possible that the end system which is not aware of full system configuration for all switches on the path, will not be able to transfer this information to specific destinations.

Avionics systems do not support dynamic port opening and closure, and do provide TFTP services, only if the system network is in "Quiet" mode, grounded and ready for maintenance. Point-to-point services which operate via UDP/IP such as SNMP and TFTP, should be equipped with strong authentication, digital signatures and secure and safe logging of operations to support nonrepudiation. Additional health monitoring capabilities at application level can help to identify any incompliant behavior.

Man-in-the-middle attacks with injection of malicious traffic are viable if the physical security and maintenance fails, or if the attacker succeeds in accessing ACD network in flight, and the traffic profile and network configuration at specific access point is known in advance. This is not practicable as the physical access in aircraft is not viable without damaging cabin interior or avionics bay.

MAC address spoofing, VLAN trunking, or DHCP server attacks are not viable, as those services either do not exist in ACD domain or are not relevant due to modified network operation and static configuration.

Denial-Of-Service (DoS) Prevention

Availability and integrity are probably the most admired parts of CIA triad in integrated controls. Ethernet-based integrated systems provide mechanisms for different system faults which could use more resources than planned by the system architect. The network bandwidth partitioning, L2/L3 dataflow policing and shaping are clearly the mechanisms which support high system/interface integrity and availability.

With deterministic Ethernet policing at L2 MAC layer, the attacker would need to have a the knowledge of all configurations for every switch between its access point and the attacked endsystem. Furthermore, L3 IP/IPsec filtering can further complicate the process of sending malicious packets to target endsystems.

For instance it is not possible to overflow the network from several endsystems with gigabits of data, and expect that other critical information flows and their timing will be influenced. It is not only about the protocol or capability implementation, but also about the internal device architecture and implementation methodology, as all dataflows end up sharing common resources on the network device. The switching device (e.g. Deterministic TTEthernet (SAE AS6802) with ARINC664 services) has all knowledge of all dataflow behavior so it can permanently monitor and drop any non-compliant packets.

Such safety and fault isolation mechanisms can be also an obstacle for cyber attackers trying to stop the network information flows, via application, middleware or network device configuration tampering. To stop the network operation, in-depth knowledge of network and system configuration and tools to change configuration on every/many network device (and vehicle, if every vehicle used different digital signatures) are required. Furthermore it is necessary to get all configurations aligned and right to inject unintended traffic or modify the system operation. In other cases it is necessary to break communication paths, by uploading wrong configurations and working around recovery mechanisms, which ensure that the last working configuration cannot be simply removed from the network device.

Ethernet Network Protocol Security

Ethernet is a set of protocols for LAN and is standardized in IEEE 802.3. It has become a standard for home networks. It also provides the base for ARINC 664 part 7 (also known as AFDX) for the domain of aeroplane networks. Over the decades, the speed of Ethernet has been increased gradually, starting with 10MBit/s in late 1980s and currently providing speeds up to 100GBit/s, with first deployments of 400Gbit/s networks in datacenter applications. The speeds above 10Gbit/s are necessary for Internet and datacenter related connections and future advanced integrated architectures, but they are currently not used for safety related networks in automotive, railway,or aerospace systems. All transportation industry roadmaps for the next 10 years consider the use of 0.1 – 10Gbit/s, due to specific embedded system environmental (EMI, temperature range) and robustness constraints. It can be expected that automotive industry will dictate the development roadmaps for the next generation embedded Ethernet networks due to autonomous driving requirements.

Physical Layer Issues

Typically, security focuses on higher level OSI layers, as it is considered that very little harm can be caused at physical layer. Physical layer is an active and intelligent component on its own and represents a complex analog/digital device, which is typically a proprietary design and contains a lot of domain-specific know-how. As an example, one of the function of the physical layer is to send data by using coded and scrambled symbols which prevent long series of zeros or ones, and allow physical Ethernet link synchronization. By scrambling, any significant DC component can be removed from the signal statistically, but it does not prevent the worst case where the scrambler polynomial is defeated and creates a long sequence of ones, which saturates AC-coupling capacitors, thus leading to link and data errors.
Depending on the scrambler, numerous sequences can be defined which can lead to datalink errors. This problem existed in early 100MBit/s systems. For integrated systems which rely on a specific computing model and periodic non-blocking communication scheme, it is harder to deploy such weaknesses broadly, as the traffic is

selectively policed at every switch, so that an endsystem cannot be reached by such a series of packets. For the policing switches this assumption may not work, as a malicious node could intentionally defeat one or several ports in the system by using such “killer” packets. Fortunately, those early issues have been resolved by additional DC restoration circuits.
Which other type of challenges exist in 1GbE, 10GbE and 100GbE systems, remains to be seen, as there is very little literature and public research on those topics. Ethernet physical layers could represent a significant, but underestimated threat vector with potential further weakness which can be exploited by capable SL3/4 (SL=security levels from IEC 62443) level attackers. Such physical layer attacks may become fatal for critical infrastructure and result in a denial of network service (or its parts), and impede system availability and safety.

Media Access Control Security

Secure communication on Layer 2 comes in different varieties, depending on wired or wireless communication approach. Its functionality depends on specific implementation details and interfaces provided to other layers. Therefore, many implementations exist and are not compatible to each other. For the purpose of this paper we focus our attention on an implementation for wired networks. An extension providing layer 2 security for Ethernet is called MACsec.

MACsec

The MACsec [37] secures the communication between endpoints and, each packet on the wire is encrypted using symmetric key cryptography so that communication cannot be monitored or altered on the Ethernet physical link.
The communication is protected between trusted components of the network infrastructure. The protocol offers several features to maintain a secure network, e.g., correct network connectivity or isolation of denial of service attacks. Services offered by MACsec for devices located within the security parameter:

- Connectionless data integrity
- Authentication of data
- Confidentiality of payload
- Replay protection
- Bounded receive delay

MACsec does not feature support for non-repudiation or protection against traffic analysis, as its scope is limited to Ethernet link and port-to-port communication.
The use of MACsec does not introduce additional frame loss on a specific segment, but it increases the size of the frame (and bandwidth use) itself. This increased size can have an influence on the facilitated MAC and therefore due to higher bandwidth use, and higher number of bits per frame, also on the frame loss. Depending on the replay protection parameters, frame loss can occur if reordering of packets happens, e.g., while making use of a provider bridged network between customer networks. MACsec itself preserves the order of frames that are received or sent by this layer. When the order of packets is not changed, each protected frame remains independent of a predecessor and the loss of predecessor does not influence the current frame.
The increased packet size directly influences the introduction of an additional delay which must be considered in time-sensitive networks. Furthermore, some cipher suites need some buffering to meet their processing requirements, which further extends the packet switching delays. If necessary the lifetime of the frame can be increased by MACsec to be able to provide this security services. Within a single network multiple instances of MACsec can be used. But, each instance has to be uniquely identified by an unencrypted field in the frame structure. Currently one mandatory cipher is specified GCM-AES-128.

MACsec Frame Structure

The difference between an Ethernet frame without security and with added MACsec security, see Figure 8a and Figure 8b. The existing structure of the Ethernet frame is expanded by: A SecTAG, the encrypted data field, and a cryptographic hash also called an Integrity Check Value (ICV) to ensure the integrity of the frame. These three modifications together are called the MAC Service Data Unit (MSDU) and have to be present on every secured packet. The size of the secured packet is expanded by:

- 16 Byte for the SecTag and
- 16 Byte for the ICV.

The coloured parts of Figure 8b highlight the security extension.

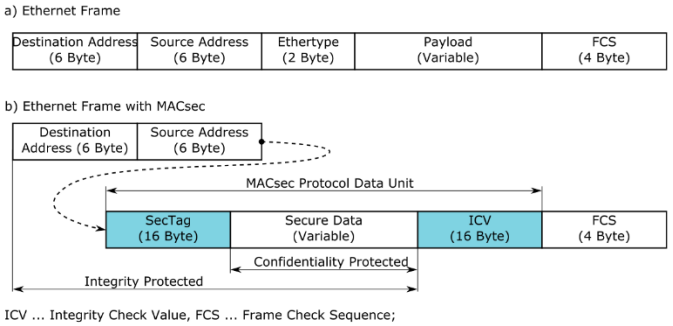

Figure 8: Ethernet Frame with MACsec.

The details needed to manage the secured connections are contained in the SecTAG, see Figure 9. It starts with the MACsec Ethertype (0x88E5), that allows for mixed setups of secured and non-secured systems. It is followed by the Tag Control Information (TCI). This field has multiple functions such as: version number of MACsec, determine the use of integrity and/or confidentiality etc. The Association Number (AN) field is used to identify up to four different Security Associations (SA). Special treatment for frames with short length is provided via the Short Length (SL) field. When the payload of the original payload is less than the value is inserted, otherwise this field is set to zero. The Packet Number (PN) has two functions:

1. It is used as a Initialization Vector (IV) for the cryptographic calculations
2. It is used as a replay protection mechanism. The last field is the Secure Channel Identifier (SCI), which can be used to identify a specific MACsec entity.

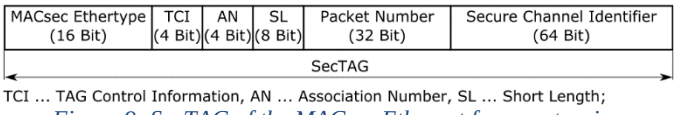

Figure 9: SecTAG of the MACsec Ethernet frame extension

Internet Protocol Security

The native Internet Protocol security (IPsec) was developed for IPv6 and was also back ported to IPv4 [38](RFC 4301, 2005 updated by

RFC 6040, 2010). IPsec supports communication integrity and confidentiality, and supports secure transfer of data and synchronization [39] information with some performance boundaries [40], relevant for secure cyber-physical systems.
This standard consists of a collection of protocols to secure IP traffic (RFC 2460, 1998 updated by RFC 5095 and RFC 5722 and RFC 5871). The extensive specification includes protocols for key exchange, e.g., IKEv2 for IPv6, IKE and ISAKMP for IPv4, or KINK (RFC 5996, 2010 updated by RFC 5998).
In the future it can be expected that alternative keyless security infrastructure [41] based on blockchain may be provided, which will minimize risks of using secrets to sign components, configuration or assets, and simplifies their tagging and modification tracking.
This is useful for avoiding insider attacks, non-repudiation and network configuration tampering. For IPsec this can have a positive impact on integrity and confidentiality, but further research is currently conducted on formal verification of this approach [42].

IPsec Modes

IPsec in transport mode uses the standard IP packet and does not add any additional header, see Figure10a or 10b. The biggest difference between transport mode and tunnel mode is that the latter adds a new IP header in front of the already existing IP header, see Figure 10c or 10d. Newly added IP headers are coloured in green. The original IP packet is treated as payload. This applies also to existing extension headers that are part of the original IP packet.

Authentication Header

The Authentication Header (AH) (RFC 4302, 2005) offers the following security services: Authentication of an IP packet and replay protection. To determine the authenticity of the packet Authentication Data (AD) (sometimes also referred to as Integrity Check Value (ICV)) is used which is included in the AH header itself.

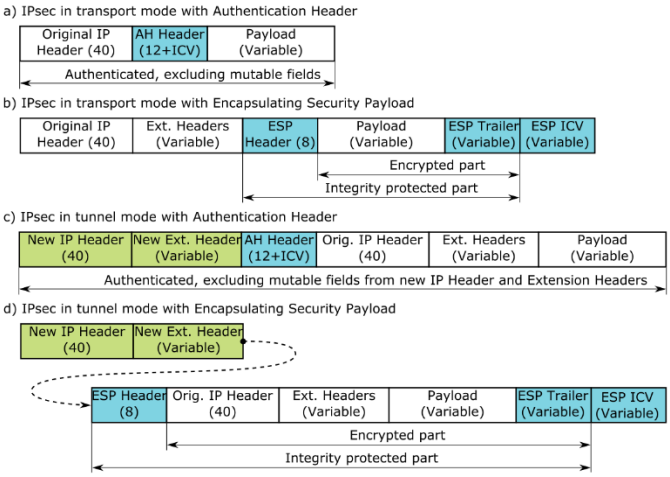

Figure 10: Examples for IPsec services and modes; additional IP headers (green) and IPsec header/trailer (blue) are colour coded. The size of the parts are given in Byte in parentheses.

The value of this field is obtained through the calculation of a cryptographic one-way hash function, called a Hash-based Message Authentication Code (HMAC). This hash starts with the first bit of the IP header and ends at the last bit of the payload, represented in Figure 10a for AH in transport mode and c for AH in tunnel mode.

Encapsulating Security Payload

The second IPsec service, Encapsulating Security Payload (ESP) (RFC 4303, 2005), offers the following security services: Authentication of payload and encryption of payload. The design of ESP allows to use symmetric encryption algorithms and supports both block ciphers and stream ciphers according to (RFC 4835, 2007). The services offered by ESP take a similar approach as AH does. The big differences are the fragments that are added to the packet. Parts of ESP in an IP packet are located at the beginning and others at the end of the original packet. The original payload data is enclosed in a new ESP header and trailer. Packet structures containing ESP are shown in Figure 10**Error! Reference source not found.**b and 10d. Also in this case, the header and the trailer of IPsec are coloured blue to be able to distinguish these parts from a generic IP packet.

Secure Shell

The protocol is a composition of several protocol standards to allow remote logins and services over an unsecured network connection (rfc4251, rfc4252, rfc4253, rfc4254 in [38]). It supports Confidentiality, Integrity, and Authentication. The protocol is divided into three separate function blocks: Transport Layer Protocol, User Authentication Protocol and Connection Protocol.
The Transport Layer Protocol works on the application layer and usually makes use of TCP/IP connections. It is the foundation for the other network services offered by SSH, such as the User Authentication Protocol and the Connection Protocol. The header structure of the Transport Layer Protocol is depicted in Table 1.

Table 1: Structure of a Transport Layer Protocol message

Type	Size in Byte
Packet Length	32
Padding Length	8
Payload	Variable
Padding	Variable
Message Authentication Cod (MAC)	Variable

The packet length of the Transport Layer Protocol message is the length of: Padding Length + Payload + Padding. The block ciphers used need clear text input with a length similar to the block size of the used algorithm. To adapt the size of the existing payload, padding is applied. The length of this padding is inserted between the Packet Length field and the payload itself. To save data rate the payload can be compressed.

The encryption of the packet applies to all fields of the packet excluding the MAC. Examples of supported encryption algorithms are: Blowfish in CBC mode, Twofish or AES in CBC mode. Therefore, the sum of all fields (again excluding the MAC) have to be a multiple of the block size of the used block cipher algorithm.

The message is concluded by the MAC and the length depends on the negotiated authentication algorithm. Supported HMACs would be HMAC-SHA-256 with a length of 32 Byte. HMACs based on MD5 or SHA-1 should not be used anymore, due to flawed collision resistance. It is possible to truncate the length of HMAC-SHA-256 to fit bandwidth limited environments. Beware that such truncation is always a tradeoff between security and bandwidth efficiency.

Security Infrastructure for Advanced Integrated Systems

To illustrate the different approaches provided by the implementations see Figure X. There are three examples given:

1. MACsec
2. IPsec
3. SSH

Each of these solutions are based on different layers of the ISO/OSI layer model.
MACsec operates on the data link layer (L2). Therefore, it operates on a hop-by-hop basis. At each hop the frame is touched and prepared for the next hop. This approach makes it necessary to trust each component in the network. Because, it could be manipulated at each hop where the frame is cryptographically modified. Trust is established only on a hop basis.
IPsec is used one layer higher on the network layer and operates on a packet level. The packet is prepared at the host, e.g., fully transparent for applications running on the host. Only at the end when the packet has arrived at its destination it is decrypted. In this approach only the end points have to trust each other. No other component in between can alter the packet. Trust is established at end-to-end network interface card (L3).
As a last example, the Secure Shell operates on the upper layer up to the application layer. In this case it is possible to have specific implementations per application. Therefore, trust can be established directly between two or more applications providing application-to-application information. This is particularly important for TFTP and SNMP services which are relevant for network management and system configuration.

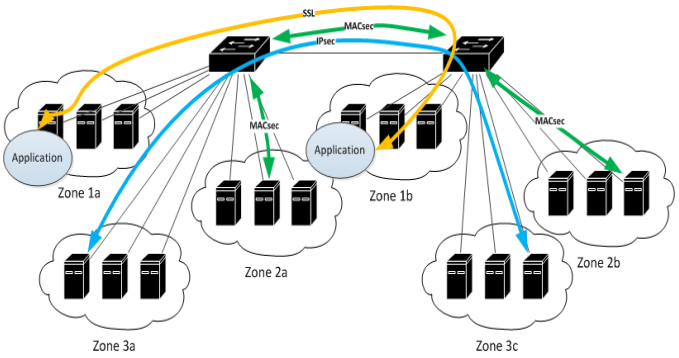

Figure 11: IPsec, MACsec and secure shell perimeter

Summary/Conclusions

Networking infrastructure becomes more important as the system complexity and controlled information exchange increases. Future deterministic Ethernet networks and advanced integrated architectures in aerospace, automotive or railway domain will need to satisfy different safety and security criteria.

Different integrated system applications work with similar security standards and methods, and the convergence in cross-industry standards for security-informed safety can be observed.

The cornerstone of Ethernet network security for advanced integrated architectures lies on MACsec, IPsec and secure shell capability, as well as secure configuration and network management via TFT and SNMP. Both MACsec and IPsec are very well established protocols in the IT landscape and are viable candidates for aircraft networks. In general IPsec is useful for general use and enables end-to-end network security to ensure the confidentiality of specific data, while MACsec as a complementary protocol is suitable for specific use-cases only, to ensure the trustworthiness of specific devices in the network, with integrity and availability.

Secure network management and digital signatures are essential for real-time systems, and rely also on the management of organizational and physical security. New blockchain-based decentralized authentication, tracking and tagging of network configurations and assets can potentially contribute to seamless resolution of non-repudiation, integrity, configuration tampering, and insider threats in real-time.

Safety mechanisms for bandwidth policing and bandwidth partitioning at L2/L3, contribute to the isolation and information flow determinism used for inter-process communication in MILS architectures and multi-level security (MLS) systems. MILS is relevant for design of secure gateways between aircraft (or vehicle) domains, and for design of multi-secure level IMA systems.

References

1. Hermann Kopetz, Günther Bauer. „The time-triggered architecture.“ *Proceedings of the IEEE (Volume: 91, Issue: 1, Jan 2003).* IEEE, 2003. 112-126.
2. A. Benveniste, A. Bouillard and P. Caspi. „A unifying view of Loosely Time-Triggered Architectures.“ EMSOFT '10 Proceedings of the tenth ACM international conference on Embedded Software. Arizona, USA: ACM, 2010FAA AR-08-31 “Networked Local Area Networks in Aircraft: Safety, Security, and Certification Issues, and Initial Acceptance Criteria”, Report, (https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/media/AR-08-31.pdf, DOT/FAA/AR-08/31)
3. Eric Fleischman, Randall E. Smith, and Nick Multari, FAA Report, DOT/FAA/AR-08/31, “Networked Local Area Networks in Aircraft: Safety, Security, and Certification Issues, and Initial Acceptance Criteria (Phases 1 and 2)”, Nov 2008
4. Robin Bloomfield, Robert Stroud. Security-Informed Safety ”If it’s not secure, it’s not safe”. Marc-Olivier Killijian. Safecomp 2013, Sep 2013, Toulouse, France. pp.NC, 2013.
5. SESAMO project, http://sesamo-project.eu/
6. RTCA DO-326A Airworthiness Security Methods And Considerations, RTCA Standards, 2010 https://www.rtca.org/search/site/do-326a
7. Shift2Rail, shift2rail.org
8. RTCA DO-356A Airworthiness Security Methods And Considerations, RTCA Standards, 2014 https://www.rtca.org/search/site/do-356
9. “Descriptions of Aircraft Domains”, AERONAUTICAL COMMUNICATIONS PANEL (ACP), 6th MAY WEBMEETING OF THE WORKING GROUP S (SURFACE)”, International Civil Aviation Organization, WORKING PAPER, ACP-WG S Web Meeting-5 / WP-02, 2/05/14
10. ISO. „ISO/IEC 15408-1. Information technology - security techniques - evaluation criteria for it security - part 1: Introduction and general model.“

11. DIN. „DIN VDE V 0831-104. Electric signaling systems for railways - part 104: It security guideline based on IEC 62443, draft. October, 2015.“ 2015.
12. IEC. „IEC TS 62443-1-1:2009. Industrial communication networks - network and system security - part 1-1: Terminology, concepts and models.“ 2009.
13. EN 50129
14. EN 50159
15. DIN. „DIN VDE V 0831-102. Electric signaling systems for railways - part 102: Protection profile for technical functions in railway signaling, draft. December, 2013.“ 2013
16. Uwe Puetzschler, “LTE and Car2x:Connected cars on the way to 5G”, Mobile Broadband SIG, 6 April 2016, Cambridge
17. McAfee, Automotive Security, Best Practices, https://www.mcafee.com/it/resources/white-papers/wp-automotive-security.pdf]
18. SAE J3061 ” Cybersecurity Guidebook for Cyber-Physical Vehicle Systems”, http://standards.sae.org/wip/j3061/
19. EVITA Eu Project, https://www.evita-project.org/
20. HEAVENS, https://www.sp.se/en/index/research/dependable_systems/heavens/Sidor/default.aspx
21. John Day, “Protecting Automotive ECUs”, https://blogs.mentor.com/johnday/blog/tag/secure-hardware-extension-she/
22. Kateryna Netkachova, Kevin Müller, Michael Paulitsch, Robin Bloomfield ,“Security-informed safety case approach to Analysing MILS Systems”, International Workshop on MILS:Architecture and Assurance for Secure System, 20 January 2015, Amsterdam
23. Spencer Shimko, Joshua Brindle, “Securing Inter-process Communications in SELinux”, SELinux Symposium, http://selinuxsymposium.org/2007/papers/11-SecureIPC.pdf.
24. Separation Kernel Protection Profile (SKPP)
25. P. Parkinson, “Applying MILS to multicore avionics systems”, 2nd International Workshop on MILS: Architecture and Assurance for Secure Systems, HiPEAC 2016, Prague, Czech Republic
26. Mark Pitchford. Applying MILS principles to design connected embedded devices supporting the cloud, multi-tenancy and App Stores. 8th European Congress on Embedded Real Time Software and Systems (ERTS 2016), Jan 2016, TOULOUSE, France. Proceedings of the 8th European Congress on Embedded Real Time Software and Systems (ERTS 2016)].
27. Wind River, “Vxworks Mils Platform 3.0”, https://www.windriver.com/products/platforms/vxworks-mils/MILS-3_PN.pdf
28. EU D-MILS Project, Distributed MILS, Proj.No. 318772, Report, D1.3 Requirements for distributed MILS technology, Aug 2013
29. D. Adam, S. Tverdyshev, C. Rolfes, T. Sandmann, “Two Architecture Approaches for MILS Systems in Mobility Domains (Automotive, Railway, Avionics)”, MILS Workshop 2015, Amsterdam, The Netherlands, Jan 2015
30. ARINC Inc., ARINC664-P5: AIRCRAFT DATA NETWORKS – “NETWORK INTERNCONNECTION DEVICES” PART 5,2003
31. Automotive domain architectures …
32. ARINC Inc., ARINC664-P7: AIRCRAFT DATA NETWORK - PART 7: “AVIONICS FULL-DUPLEX SWITCHED ETHERNET NETWORK”, 2009
33. SAS-2D, "Time-Triggered Ethernet (SAE AS6802)," SAE, Warrendale, 2011
34. IEEE TSN Working Group, http://www.ieee802.org/1/pages/tsn.html
35. M. Jakovljevic, J. Gatard, “Heterogenous All-Ethernet Networking for Aircraft Systems”, Proceedings of Aircraft System Technologies AST Feb 2017, Hamburg
36. Steiner W, “Candidate security solutions for TTEthernet”, Digital Avionics Systems Conference (DASC), 2013 IEEE/AIAA 32nd, Sept 2013, Syracuse, NY
37. 802.1AE - Media Access Control (MAC) Security, http://www.ieee802.org/1/pages/802.1ae.html
38. IETF RFC, https://www.ietf.org/rfc.html
39. Treytl, A.; Hirschler, B.; Sauter, T.; (2010) Secure tunneling of high-precision clock synchronization protocols and other time-stamped data. In: IEEE, IEE World Conference on Factory Communication Systems (WFCS): S. 1-8, IEEE.
40. Hirschler, B.; Sauter, T. (2016) Performance impact of IPsec in resource-limited smart grid communication. In: IEEE, IEEE World Conference on Factory Communication Systems (WFCS): S. 1-8, IEEE.
41. Guardtime, “Use of a globally distributed blockchain to secure SDN”, Company Brochure, 2016 https://www.ciosummits.com/Guardtime_KSI_Use_of_a_globally_distributed_blockchain_to_secure_SDN_whitepaper_1602.pdf
42. Tim Greene, “New protocol from Guardtime hopes to unseat RSA for authentication, digital signatures”, Network World, May 20, 2015

Contact Information

Email contact details: for Bernd Hilscher bernd.hilscher@tttech.com, and for Mirko Jakovljevic mirko.jakovljevic@tttech.com

Acknowledgments

This project has received funding from the Shift2Rail Joint Undertaking under grant agreement No 730830. This Joint Undertaking receives support from the European Union’s Horizon 2020 research and innovation programme and Austria, Spain, Germany, Czech Republic, Italy, France.

Definitions/Abbreviations

none	None

Appendix