Elektrobit

EB TechPaper *i*

# Combining the strengths of Elektrobit's SecOC with Argus IDPS

elektrobit.com

After conducting several discussions in AUTOSAR and with customers regarding aspects of the Secure Onboard Communication (SecOC)[1] specification, Argus and Elektrobit propose a joint deployment of Elektrobit's SecOC and Argus Intrusion Detection and Prevention (IDPS) to overcome security challenges that were raised during the discussions.

While extensively detailing the techniques to secure a message, some security aspects remain out of the scope of the AUTOSAR specification, namely key management and freshness. In addition, the specification does not necessarily apply to all in-vehicle communications and when applied correctly, might be subject to the limitation of the CAN message size. Each of these aspects pose security challenges.

This paper outlines these challenges and proposes a joint approach of the Elektrobit SecOC mechanism and Argus IDPS to leverage the advantages of both technologies and greatly enhance the security of in-vehicle communications.

## How does SecOC profit from additional security?

### Specification gaps in SecOC scope

While specifying many aspects of SecOC in detail, AUTOSAR intentionally excluded aspects like key management or freshness value management from standardization. These aspects must be defined by each OEM individually, which involves addressing all the unique security aspects of each individual solution. Elektrobit offers solutions in plain AUTOSAR and in OEM variants. Nevertheless, for customers that are new to this subject, the challenges are quite demanding.

In a nutshell SecOC uses a symmetric, MAC based approach to make an explicit statement about the authenticity and integrity of transferred messages. Therefore, one or more corresponding symmetric keys are needed by all ECUs configured according to the SecOC specification.

To mitigate the risk of replay attacks, a freshness value is integrated in the scheme. The AUTOSAR standard refers to counter or time-based freshness values as typical options but, due to different OEM solutions, the topics are otherwise intentionally excluded from standardization.

This leaves two fundamental security-critical aspects to be defined by OEMs when implementing a SecOC scheme: Freshness value management and key management. Some typical challenges that need to be addressed are discussed below.

#### Freshness value management

Time management is a special form of counter management. To setup a SecOC scheme based on time values, you need a synchronized and secure time base in all ECUs participating in the SecOC group. The challenge is to ensure a secure time synchronization without relying on mechanisms of SecOC.

If an initial time value is transferred with a similar SecOC mechanism that is based on symmetric cryptography, all ECUs involved have access to the key used to authenticate timestamp messages. Any ECU could potentially impersonate the sender of a timestamp message and send spoofed timestamp messages to other ECUs. Therefore, a compromised ECU may attempt to do any of the following:

- Move time backwards (even slightly) to extend the message acceptance window.
- Alter time substantially in one network segment to take it out of sync with other network segments.

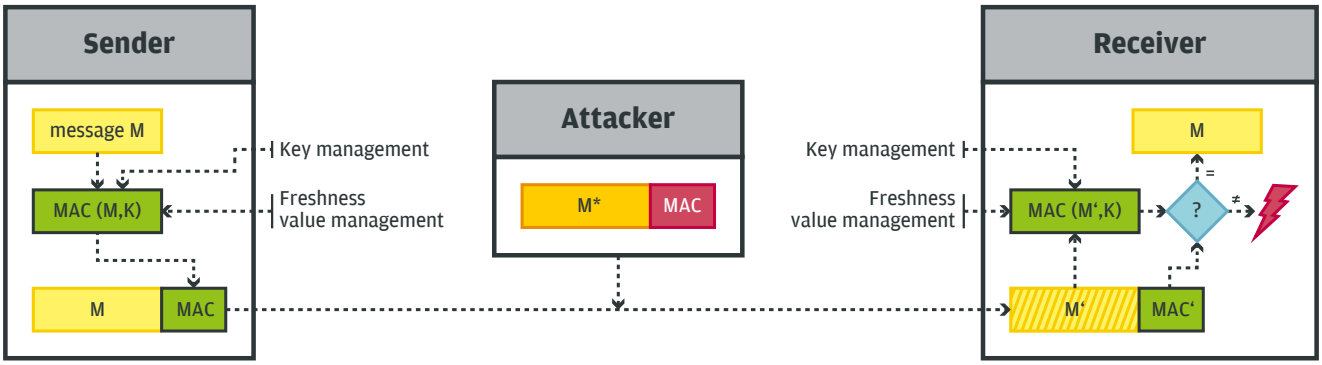


**Figure 1: Detection mechanism of Secure onbaord communication**

- Effectively disable the freshness mechanism by moving it to its maximum value. Typically, since a rollover of the value is not supported to prevent replay attacks, once the freshness reaches its maximum value, it will remain there indefinitely. Once the freshness value is fixed, replay attacks cannot be prevented.

## Key management

There are many strategies, to distribute and manage symmetric keys in relevant ECUs. Many less complicated strategies involve complicated logistics that can be difficult to maintain.

Typically, in order to handle symmetric keys in different ECUs, key exchange mechanisms based on additional asymmetric algorithms are used. These mechanisms allow for key exchanges between ECUs in the vehicle and might be triggered once, frequently or upon request (e.g., when out of sync).

Implementations of such key exchange mechanisms are frequently expensive in terms of computational power which may lead to certain speed optimizations that jeopardize security goals:

- An attacker may be able to listen in on the process of ECU replacement and extract the new key from the in-vehicle traffic (i.e., even if it is encrypted by another “known” key).
- An attacker may force a key exchange to take place. This can cause denial of service or may allow the attacker to listen in on the key material.

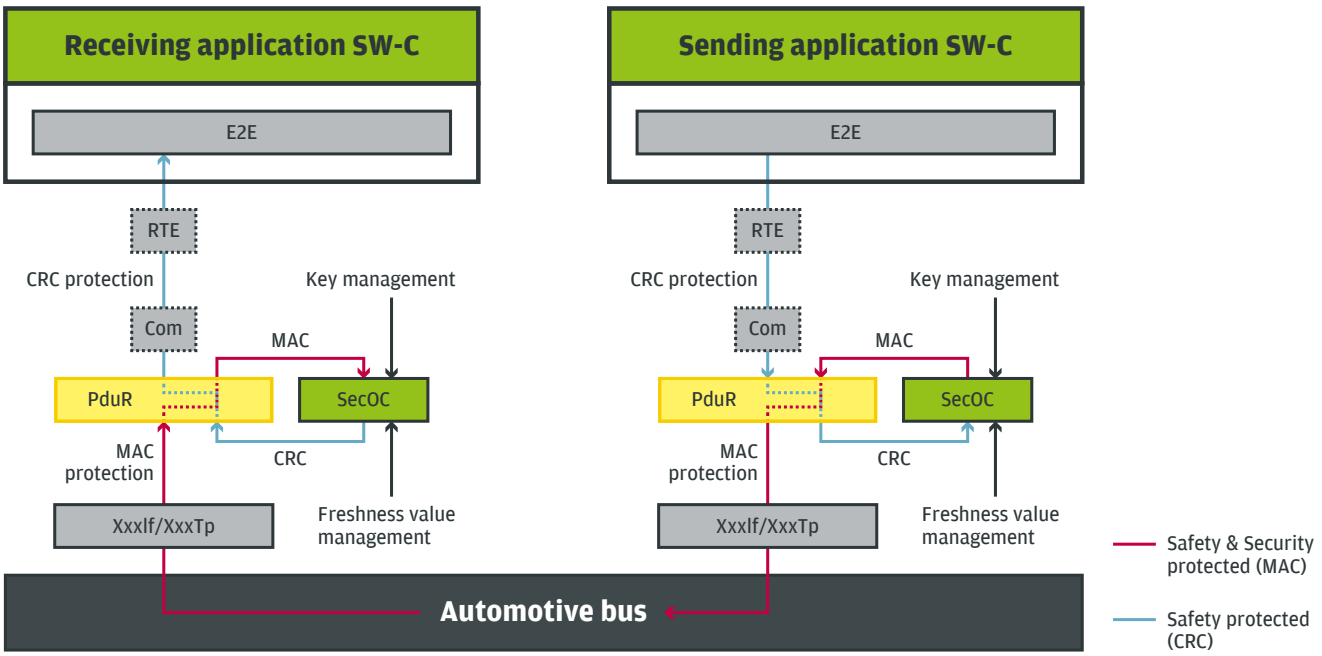


**Figure 2: Integration of Secure onboard communication in AUTOSAR architecture**

### Application of SecOC

The Elektrobit SecOC implementation is a mechanism that can give an explicit statement about integrity and authenticity of messages. However, each message that is to be protected by SecOC must be pre-selected and configured accordingly. For messages without a SecOC configuration, no statement regarding authenticity or integrity can be given.

### MAC truncation

When implementing SecOC over CAN networks (as opposed to implementation over a CAN-FD network), there are only 8 bytes of data available per message (as opposed to 64 bytes in CAN-FD). To perform message authentication, those 8 bytes must include the MAC and the message data.

As a result of this stringent limitation, short MACs have to be used (e.g., a 2-4 byte MAC makes the scheme vulnerable to brute force attacks – for 2 byte MACs, an in-vehicle brute force attack would be successful in a matter of hours[2], for 4 byte MAC - a brute force attack would take about 10 days. In this context, brute force attacks could lead to the successful injection of one valid, but malicious, message on the bus if those messages are valid for such time slots.

Some examples of the potential effects of such a single valid, but malicious, message may be:

- Malicious single messages may manipulate the freshness / timestamp value. This builds upon the analysis presented above but it does not require the attacker to know the SecOC key in order to pull off the attack.
- Malicious single messages may cause cyber physical damage to the vehicle. For example:
  - The message may simulate a pre-crash message which tightens the seat belts and cuts off the fuel pump.
  - The message may be able to unlock the doors or depressurize the anti-lock braking system (i.e., bleeding the brakes) in order to disable the brakes.

Attempting to execute this attack at scale on hundreds or thousands of vehicles across a large fleet can significantly reduce the time an attacker needs to successfully guess one valid message.

## How SecOC may be enhanced by Argus IDPS

Compared to SecOC, Argus IDPS can provide a different kind of statement regarding the security of the system. Monitoring all messages on the bus, Argus IDPS does not require explicit configuration of single messages and can detect anomalies in the traffic based on comparing each message to a predefined behavioral model of expected in-vehicle traffic behavior.

Part of the behavioral model of an Argus IDPS may include, among other things, properties of protocols, the logic of message sequences and bus traffic in general. This may include timing and content properties of messages as well as expected consistency of messages and plausibility tests regarding different messages in the vehicle. For example, an Argus IDPS may analyze diagnostic traffic in order to validate it and make sure it is consistent with the current state of the vehicle or it may detect deviations from a predefined cycle time of a periodic message.

These qualities can be used to enhance the security of SecOC schemes and the adjacent protocols necessary.

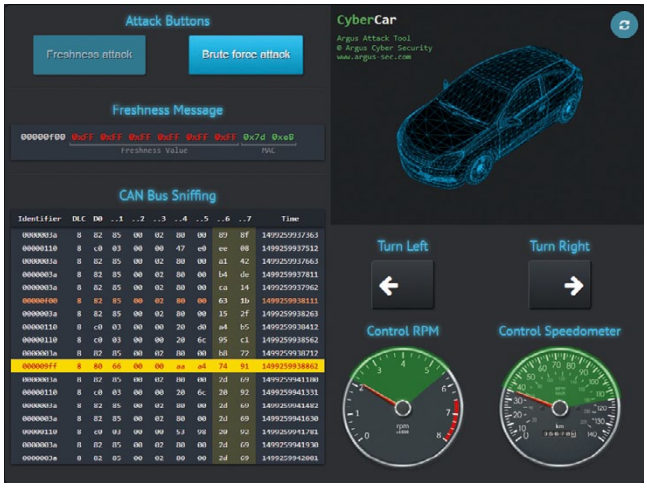


**Figure 3: Argus and Elektrobit demonstration of the combined solution presented at Escar US 2017**

### Detection of Attacks

The example attacks on the SecOC scheme mentioned above typically require the attacker to inject messages onto the bus or modify the traffic in such a way which is not in accordance with how the in-vehicle traffic is expected to behave in normal circumstances.

Therefore, Argus IDPS, which is deployed at a central location in the vehicle (e.g., on the gateway, depending on the vehicle architecture), may detect such attempts to manipulate the SecOC based on different message timing and content models as well as consistency and other plausibility tests.

The behavioral model of Argus IDPS may include properties of the freshness value and key management protocols. Therefore, Argus IDPS may be configured to detect replay attacks, attempts to manipulate the freshness values, manipulations of the key management and brute force attacks. This enables the Argus IDPS to detect attacks on relevant protocols and messages necessary for the proper functioning of a SecOC scheme.

Since all messages transmitted over the in-vehicle network are monitored by Argus IDPS, it can detect attacks on messages that are not covered by the SecOC scheme as well as attacks aimed at the SecOC scheme itself.

## Cyber security across the fleet

Security logs from both Argus IDPS and the Elektrobit SecOC mechanism, as well as other security mechanisms in the vehicle, may be collected and sent to a central aggregation and analysis hub.

This information can then be used to better understand the cyber security health status of the fleet and assist in the cyber security incident management process.

The information is accessible to the customer (e.g., OEM and/or Tier 1s) through a web-based dashboard that enables the examination of different measurements and indicators regarding the cyber health of the vehicles in the fleet: rReal-time and historical information about cyber-attacks, updating the security policy of the fleet over the air (OTA), a heat map of attacks, and more.

Additional technical information such as forensic data can also be analyzed by cybersecurity experts and vehicle engineers. Another integral part of the dashboard is the ability to view the configuration of the security layers and modify/update it through OTA fleet updates.


**Figure 4: The cyber health of the fleet is presented on a web-based dashboard**

## Proposal of a joint setup of Elektrobit SecOC and Argus IDPS

Working together, the Elektrobit SecOC implementation and Argus IDPS are able to provide comprehensive coverage of all network communications:

- Validate the authenticity and integrity of messages with Elektrobit SecOC. Secure relevant protocols and messages necessary for a proper SecOC scheme with Argus IDPS.
- Enhance the security of all messages with Argus IDPS (regardless of whether they are configured in accordance with SecOC or not).
- Understand and respond to attacks in real time with over the air security updates through the monitoring and analysis of vehicle data generated by Argus IDPS and Elektrobit SecOC and other sources.

## Conclusions

In this paper, we discuss the advantages of both SecOC and Argus IDPS as well as highlight some of the risk-prone aspects, and the related security challenges, posed by the current state of standardization in AUTOSAR.

To overcome these challenges, Argus and Elektrobit propose a combined solution of the Elektrobit SecOC mechanism and Argus IDPS to leverage the security benefits of each technology. This combined solution can greatly enhance the overall level of security of in-vehicle communications.

## Footnotes

1 See AUTOSAR „Specification of Module Secure Onboard Communication“

2 See M. Dworkin: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, U.S. Department of Commerce, Information Technology Laboratory (ITL), National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, NIST Special Publication 800-38B, 2005, Appendix A


**Author:**
**Yaron Galula**
ARGUS

Yaron Galula is co-founder and CTO of Argus. Yaron is a cyber security expert who served as Captain and a project manager in the Israeli IDF intelligence unit 8200 where he took part in two Israel Defense Prize winning projects and was awarded the Chief of Military Intelligence award twice. Yaron was previously an algorithms team leader at ConvertMedia and a VFX artist at Mr. X Inc. Yaron holds a B.Sc. in computer engineering, Cum Laude, from the Technion.



**Author:**
**Martin Böhner**
Elektrobit Automotive GmbH

Martin Böhner is the responsible Program Manager for Security Solutions. Since joining EB in 2005, Martin has served at different sites and in different roles at EB in the field of Automotive Security, e.g. as Engineer, Senior Consultant and as Project Manager. Today he is responsible for leading programs and conducting research in the area of applied Automotive Security.

## Notes




## About Elektrobit (EB)

EB is an industry leading supplier of automotive software and has a proven record in embedded and connected software development for over two decades. As a dedicated partner to the automotive industry, EB provides technologies and flexible software platforms, tools, and services to help automotive manufacturers and their suppliers to deliver the best products and services in order to meet the needs of drivers.

Elektrobit Automotive GmbH
Am Wolfsmantel 46
91058 Erlangen, Germany
Phone: +49 9131 7701 0
Fax: +49 9131 7701 6333
**sales@elektrobit.com**
**www.elektrobit.com**