www.dspace.com

# Validating TLS-Protected Ethernet Communication

Ralf Grosse Börger, Björn Müller, Tobias Schaeffer
dSPACE GmbH

Heinfried Cznottka, Dr. Michael Jahnich
achelos GmbH

achelos

YOUR PARTNER IN SIMULATION AND VALIDATION

dSPACE

Since the middle of 2022, vehicle manufacturers have to prove that their vehicles comply with the cybersecurity stipulations of UNECE 155 when registering a new vehicle type. So there is little time to effectively validate the integrity and authenticity of communication between ECUs and between the vehicle and back-end systems.

Since Ethernet typically uses transport layer security (TLS) for protocol security, test systems must be developed for TLS implementation that not only secure functional aspects, but also test for cybersecurity vulnerabilities. This white paper describes such a technical solution. Created in cooperation between dSPACE and achelos, it can be used extensively for the quality assurance of TLS-protected Ethernet communication in vehicles.

## Cybersecurity and the UNECE 155

For years, advanced driver assistance systems (ADAS) and autonomous driving (AD) have been among the key drivers of the automotive industry. They are milestones on the road to accident-free traffic and autonomous vehicles and are part of a comprehensive EU strategy that paves the way for cooperative, connected, and automated mobility, called CCAM. Direct vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication – commonly referred to as V2X – is a critical building block and will further transform the vehicle into a mobile IT data center with many embedded control units (ECU), sensors, monitoring systems, infotainment systems, and wireless communication modules.

However, the required communication interfaces also significantly increase the target for potential hackers or cybercriminals. Cyberattacks on connectivity are becoming scalable and can lead to major negative impacts for automobile manufacturers and their suppliers. UNECE Working Group 29 has therefore proposed a regulation on cybersecurity (Regulation 155) and a regulation on software update management (Regulation 156), which came into force at the beginning of 2021, bringing about a paradigm shift in the automotive industry in all participating member states. This EU regulation requires vehicle manufacturers to establish a cybersecurity management system (CSMS) for each new vehicle type. It also requires extensive testing and the mitigation of identified risks.

**UNECE Working Group 29 Guideline 155 is mandatory for all new vehicle type approvals from July 2022 and for all new vehicle approvals from July 2024. It therefore must be stated that, in addition to functional security, cybersecurity must also be ensured. While the process model for functional safety was defined in ISO 26262, the process model for cybersecurity is described in the new ISO 21434; the validation of security requirements is one component of this standard.**

A major focus of UNECE 155 is cybersecurity testing. The regulation states that „the Approval Authority or Technical Service shall refuse to grant the type approval with regard to cyber security where the vehicle manufacturer (...) did not perform, prior to the approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented. Without proper and sufficient testing, a vehicle manufacturer will not receive type approval with respect to cybersecurity. Therefore, the regulation requires that measures for testing the cybersecurity of a vehicle type be established and that cybersecurity tests be conducted with adequate test coverage. As cybersecurity testing aims to model and demonstrate resilience against malicious attacks, testing and quality control also face new challenges. UNECE 155 further specifies which vulnerabilities and threats that must at least be considered when implementing CSMS, see Annex 5. For example, OEMs must mitigate the threats with measures that are also specified, albeit in very general terms, in UNECE 155. Annex 5 serves as an example: Table A1 Vulnerability/Threat. Point 4.3.2, Regulation 155 lists threats to vehicles in terms of their communication channels. For example, messages received from the vehicle (e.g., X2V or diagnostic messages)

or messages transmitted within the vehicle may contain harmful content. For example, CAN messages can affect vehicle safety. Communication channels can therefore be used for the unauthorized manipulation, deletion, or other modification of vehicle data. Communication channels also allow data or code to be fed into the vehicle. Based on these potential vulnerabilities, Regulation 155 defines abstract mitigation measures for threats related to these vehicle communication channels. See Table B1 for details. The vehicle must verify the authenticity and integrity of the messages it receives. Confidential data transmitted to or from the vehicle must be protected from spying.

## IP-Based Communication

More than 10 years have passed since Ethernet was first introduced in vehicles for a dedicated function. Since then, Ethernet has become the central control unit networking technology worldwide. Its usage spans all domains and applications, ranging from infotainment, connectivity, and powertrain, to ADAS and AD applications. A current ECU architecture without Ethernet as a vehicle backbone is no longer possible.

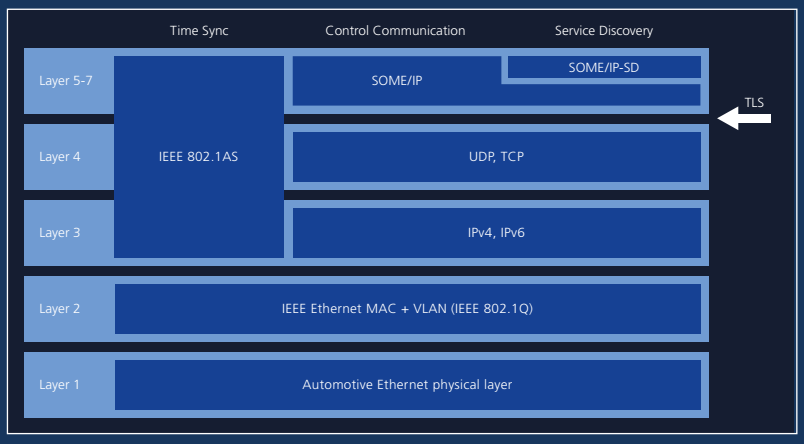
What all applications have in common is that they involve high-bandwidth data transmissions. However, data on ADAS/AD applications of vehicle longitudinal or lateral dynamics are particularly critical to safety. Since these are applications up to SIL level 4, functional safety must be ensured in accordance with ISO 26262. Typical tests include, among others, the modification of the input data of an application, for example, with the help of restbus simulations in the context of HIL simulations. In addition to tests with correct data (regarding the content as well as the time of sending), invalid data is also sent. Typical errors that are simulated during this are masking errors or repetition errors, which have to be detected with the help of additional data according to end-to-end protection profiles standardized in AUTOSAR. Therefore, these tests are used to ensure data integrity.

### What is TLS?

TLS is the abbreviation for Transport Layer Security. This is a standard consisting of several protocols with which data can be transmitted in encrypted form. The goal of TLS is to ensure the authenticity of the communication partners as well as the integrity and confidentiality of the data traffic.

As the successor to the well-known SSL (Secure Sockets Layer) standard, TLS is widely used in Internet communication via HTTPS (Hypertext Transfer Protocol Secure) between a browser and a web server.

In the ISO/OSI layer model, TLS is located in the session layer. As an intermediate layer, it is located between the transport protocols UDP/TCP and the application layer. In automotive applications, the use is thus transparent to the SOME/IP protocol located in the application layer above. Although version 1.3 has been described in RFC 8446 for some time, version 1.2 is currently still the most frequently used version in automotive and Internet communications. TLS was also introduced for the Classic and Adaptive Platforms of AUTOSAR version 4.4 in November 2018. The standard determined that TLS ≥ 1.2 versions should be used. For Adaptive AUTOSAR, dTLS support has now also been standardized.



In addition to the unintentional falsified transmission of input data, however, it is also possible to deliberately change or manipulate the data. In this case, cybersecurity measures are required to ensure the authenticity and integrity of the data. Authenticity is understood as the trustworthy exchange of data between sender and receiver. Integrity refers to the verification that the transmitted data is complete and unchanged.

A wide range of procedures and methods are used to ensure data integrity in automotive applications. The best-known procedures are:

- Secure onboard communication (SecOC)
- Transport Layer Security (TLS)
- Internet Protocol Security (IPsec)
- Media Access Control Security (MACsec)

Of the aforementioned procedures, SecOC is the most established in ECU communication, as it was already standardized in 2015 with AUTOSAR version 4.2.1. SecOC protection takes place in the application layer of the ISO/OSI layer model. Here, additional encrypted authentication information is transmitted in addition to the unencrypted user data. The MACsec method is the lowest-layer measure (layer 2) in accordance with IEEE standard 802.1AE. Here, encryption takes place between two interconnected network components. Technically, encryption is usually carried out via the transceivers that are connected to each other. IPsec and TLS are located between the hardware-related MACsec and the application-related SecOC protection. While IPsec is on layer 3, TLS is an intermediate layer between the transport protocols UDP/TCP and the application layer.
Universally applicable protocols and mechanisms are required since communication with the back end in addition to pure communication between control units is becoming increasingly important. The TLS process is a good choice here, as it has been used successfully for many years for security-critical internet applications.
These security protocols implement the authenticity, integrity, and confidentiality for IP-based communications as required by UNECE 155 and can be considered state-of-the-art.

### Testing the TLS-Interface

When server and client systems communicate with each other, it is essential today that these connections are protected. It must be possible to prove at any time who was or is connected to whom, and that

### What is IKE/IPsec?

IPsec stands for IP Security and refers to a family of protocols for cryptographically protecting communication over potentially insecure IP networks such as the Internet. The aim of IPsec is to authenticate the communication partners and to ensure the integrity and confidentiality of the IP packets, the payload.
IP packets are protected using the Encapsulating Security Payload (ESP), which is defined in RFC 4303. IPsec uses the Internet Key Exchange Protocol IKE (IKEv2 according to RFC 7296) to automatically agree on and manage the cryptographic keys used in the protocol. On the Internet, IPsec is used by VPN gateways to facilitate secure tunnels to central servers.
In the ISO/OSI layer model, IPsec is located in IP layer 3.

In 2019, AUTOSAR version 4.5 defined IPsec for both the Classic and Adaptive Platforms. Automotive IPsec complies with the requirements set out in AUTOSAR FO R19-11 „Requirements on IPsec Protocol“, which in turn are based on the current IETF standards RFC 4301 to 4303 and RFC 7296.

IPsec is defined for vehicle technology in AUTOSAR FO R20-11: Use of IPsec protocol.

the transmitted data was encrypted so that third parties cannot read or change it. These network connections use cryptographic technologies. The implementation and the correct use of existing libraries are a big challenge with this. achelos offers a powerful tool to detect these gaps and errors and thereby establish secure network connections.
When testing the TLS implementation, the following aspects must be considered:

- **Compliance with the standard:**
  The compliance of the functional behavior with the RFC standards as well as the functional requirements of the automotive application, e.g., according to AUTOSAR, must be ensured so that vehicle components can communicate with each other.
- **Configuration:**
  The available variety of configuration options is so extensive that loopholes for attackers can arise both during integration and during subsequent configuration of the vehicle component. The configuration check should ensure that the implemented configuration is secure in terms of the requirements, e.g., AUTOSAR or BSI checklists (BSI = German Federal Office for Information Security). This includes the protocol version (no SSL 3.0, no TLS 1.0, etc.), the cipher suite used (no EXPORT cipher suites, no weak encryption algorithms, etc.), the cryptographic parameters (RSA key length ≥ 2,048 bits), and protocol extensions (TLS compression, heartbeat, etc.).
- **Known vulnerabilities**:
  The vehicle component under test should be examined for known vulnerabilities. These include the BEAST, Bleichenbacher, CCS, CRIME, DROWN, FREAK, POODLE, ROBOT attacks, among others. This list is dynamic and will be continuously expanded as attacks are the subject of both research and the hacker community.
- **Tests for correct implementation:**
  A robust protocol implementation should also be checked, e.g., in case of message sequence manipulation. The implementation must check the inserted padding for correctness (e.g., by inserting invalid padding values). It should also be tested that the implementation under test is a constant-time implementation, e.g., that it is able to fend off the lucky-thirteen attacks.

The subject of the test is the establishment of the TLS connection up to mutual authentication, the reaction to incorrect behavior, and the termination of the connection. The following scenarios are considered in these test sequences:

- Missing or incorrect communication parts
- Missing or incorrect configuration settings
- Faulty key material
- Defective certificates
- Unsuitable cipher suites
- Faulty response to manipulations
- Untypical error messages
- Unexpected protocol changes

Attack scenarios that attack during existing TLS connections and side-channel attacks are not currently considered.
In the future, however, it will also be possible to check side channels that result, for example, from timing differences, error messages, and TCP statuses.

## Technical Implementation

In a hardware-in-the-loop (HIL) system, the real ECU (device under test – DUT) is always connected as directly as possible to a SCALEXIO HIL simulator.
If you want to connect another test system for TLS tests to the real ECU in addition to the HIL system, the easiest way to do this is via another Ethernet interface of the SCALEXIO simulator.

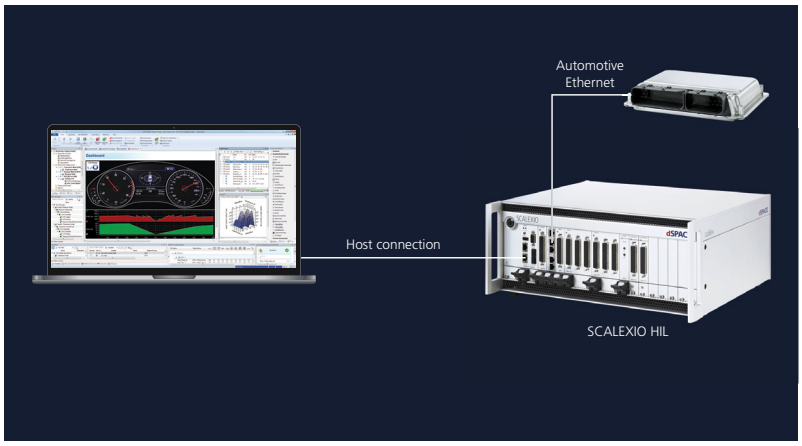
For this purpose, the control unit is connected to an automotive Ethernet port of the SCALEXIO system as usual (e.g., 1000BASE-T1).

## Full TCP Pass-Through

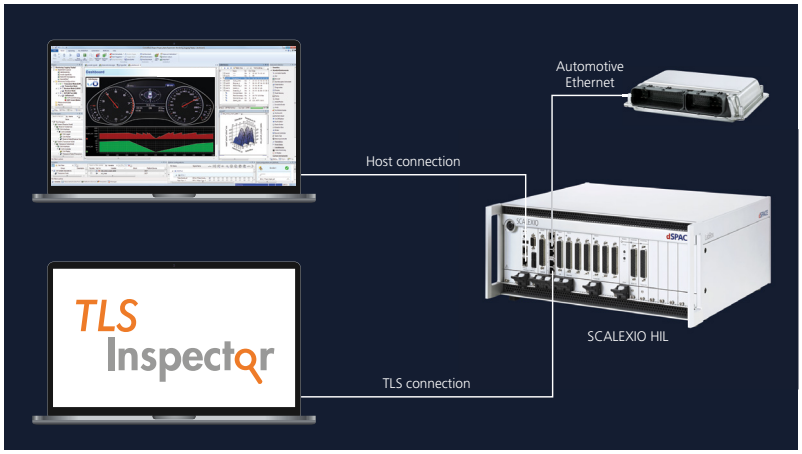
The achelos TLS Inspector test system is then connected to a second Ethernet port (standard Gigabit Ethernet), with traffic passing through as follows:

- A software component on the HIL only routes TCP connections to predefined TCP ports between the two Ethernet interfaces.
- This enables TCP or TLS connection establishment and data communication between the control device and the TLS Inspector.
- The exact same IP and MAC address is used for each pass-through. For the TLS Inspector and the control unit, the connection appears like a direct connection.
- This mechanism can be extended in such a way that the restbus simulation of the SCALEXIO system first establishes the prerequisites needed for the rest of the process (announcement of a TCP-based service via SOME-IP service discovery) and then the TLS-specific test sequences are started by the achelos test system.

This lets users test various test scenarios for setting up and terminating the TLS connection. These scenarios correspond to the aspects described in the chapter Testing the TLS Interface.




Standard dSPACE HIL setup without TLS Inspector




Integration of the TLS inspector

The parameters required for such TLS scenarios (IP address, TCP port, TLS version, cipher suites, etc.) can come from the restbus simulation of the SCALEXIO system. Certificates are usually not compiled permanently into the real-time model but are at least available as separate files on the real-time system. Since the parameters necessary for TLS communication are available on the real-time system, they could be used for (semi-)automatic configuration of the TLS Inspector. This reduces the configuration effort for the user.

In a further expansion stage, the available parameters can be used to carry out a complete configuration of the TLS Inspector.

This preconfiguration is especially useful when IP addresses and port numbers are determined dynamically (at simulation run time). This may occur in the context of the SOME/IP service discovery protocol, for example.

In practice, the problem often arises that the TLS client must be „motivated“ to establish a TLS connection to the server. The restbus simulation can flexibly and automatically establish the necessary preconditions and trigger the connection setup by the control unit.

However, since the TLS Inspector is neither real-time-capable nor does it offer the option of restbus simulation, no realistic user data can be sent or received via the TLS connection that has just been established during full TCP pass-through.

## Passing the TLS Handshake

In order to also support TLS connections with user data from the restbus simulation, as a next step, we are planning to make it possible to execute the TLS connection setup (TLS handshake) from the TLS Inspector and to forward the connection to the dSPACE HIL simulator and continue there with the user data from the restbus simulation.

In the connection setup phase, the same procedure is used as for full TCP forwarding. However, once the TLS handshake is complete, the parameters of the TLS connection (negotiated TLS version, cipher type, key, etc.) are passed to the HIL system.

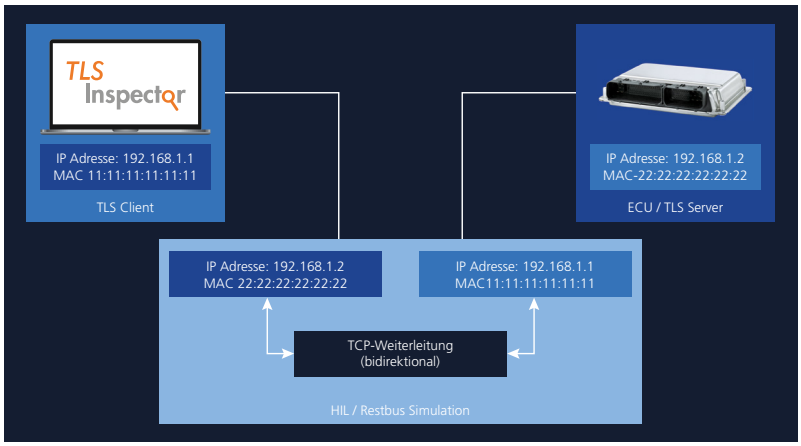
The HIL simulator can thus continue the TLS connection transparently so that the regular application data can be sent and received over the established TLS connection. A closer integration between the SCALEXIO system and the TLS Inspector allows the parameters from the communication matrix (IP addresses/port numbers, TLS parameters like the allowed cipher suites) to be passed dynamically to the TLS Inspector.

This also makes new test scenarios conceivable, in which errors are injected into the TLS handshake and their effects on further real-time communication are tested.

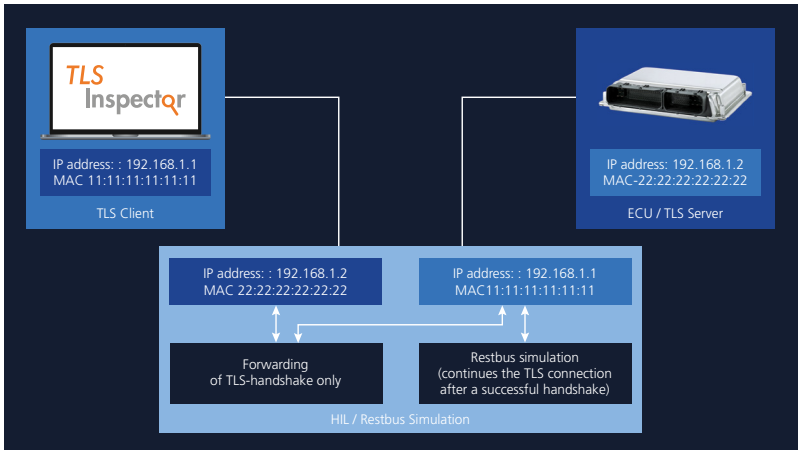
## Summary

With automotive Ethernet, IP-based communication is already in use as a high-bandwidth option for data transmission between central control units in the vehicle, especially in the ADAS/AD application environment. Due to the UNECE 155 requirement for cryptographic protection of such communication channels, security protocols such as TLS are used as a standard in newer vehicles. These cybersecurity measures are ultimately part of a vehicle type approval test. But how do you check that the TLS connections you have set up are securely implemented and configured to provide sufficient protection against hacker attacks? In this white paper, dSPACE and achelos show how ECUs with TLS-based Ethernet interfaces can be tested for known vulnerabilities, cryptographically weak configurations, and standards compliance by using the TLS Inspector test tool in conjunction with dSPACE restbus simulation.

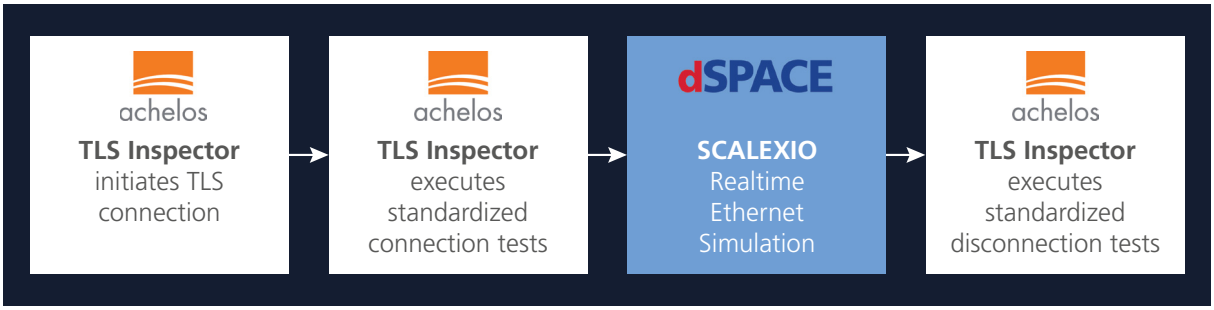
In a cooperative venture, the two companies have already built a prototype of an operational test system, which the experts from both companies are happy to present to customers and interested parties in more detail. >>


Network topology with IP/MAC addresses, forwarding of all TCP traffic




Network topology with IP/MAC addresses, forwarding of TLS handshake only




Test process: Parts that are not real-time-critical in white. Real-time-critical parts in blue.

**Heinfried Cznottka**
achelos GmbH
*heinfried.cznottka@achelos.de*

**Dr. Michael Jahnich**
achelos GmbH
*michael.jahnich@achelos.de*

**Ralf Grosse Börger**
dSPACE GmbH
*RGrosseBoerger@dspace.de*

**Björn Müller**
dSPACE GmbH
*BjMueller@dspace.de*

**Tobias Schaeffer**
dSPACE GmbH
*TSchaeffer@dspace.de*

We look forward to further discussing the specific requirements of cybersecurity testing with you and learning about your unique needs.

## About achelos

achelos GmbH is a manufacturer-independent software development and consulting firm based in Paderborn, Germany. Founded in 2008, the technology expert offers cross-sector solutions for security-critical application fields with core competencies in embedded development and subscription management. The company develops and operates highly specialised products, solutions and services for the international market. achelos boasts comprehensive expertise in development, Testing as a Service (TaaS) and certification. Alongside ISO 9001 and ISO 27001 certification, the achelos development site in Paderborn is also certified to Common Criteria. achelos Hungary Kft. has been operational since June 2022 as an additional development site in Budapest.

For more information visit *www.achelos.de*.

## About dSPACE

dSPACE is a leading provider of simulation and validation solutions worldwide for developing connected, autonomous, and electrically powered vehicles. The company's range of end-to-end solutions are used particularly by automotive manufacturers and their suppliers to test the software and hardware components in their new vehicles long before a new model is allowed on the road. Not only is dSPACE a sought-after partner in vehicle development, engineers also rely on our know-how at dSPACE when it comes to aerospace and industrial automation. Our portfolio ranges from end-to-end solutions for simulation and validation to engineering and consulting services as well as training and support. With more than 2,000 employees worldwide, dSPACE is headquartered in Paderborn, Germany, has three project centers in Germany, and serves customers through regional dSPACE companies in the USA, the UK, France, Japan, China, Croatia, and South Korea.

For more information visit *www.dspace.com*.

www.dspace.com

© Copyright 2022 by dSPACE GmbH.

All rights reserved. Written permission is required for reproduction of all or parts of this publication. The source must be stated in any such reproduction. dSPACE is continually improving its products and reserves the right to alter the specifications of the products at any time without notice. "ConfigurationDesk", "ControlDesk", "dSPACE", "MicroAutoBox", "MicroLabBox", "ProMINT", "SCALEXIO", "SYNECT", "SystemDesk", "TargetLink", and "VEOS" are trademarks or registered trademarks of dSPACE GmbH in the United States of America or in other countries or both. Other brand names or product names are trademarks or registered trademarks of their respective companies or organizations.

**Germany**
dSPACE GmbH
Rathenaustrasse 26
33102 Paderborn
Tel : +49 5251 1638-0
Fax: +49 5251 16198-0
info@dspace.de

**United Kingdom**
dSPACE Ltd.
Unit B7 · Beech House
Melbourn Science Park
Melbourn
Hertfordshire · SG8 6HB
Tel : +44 1763 269 020
Fax: +44 1763 269 021
info@dspace.co.uk

**France**
dSPACE SARL
7 Parc Burospac
Route de Gisy
91573 Bièvres Cedex
Tel : +33 169 355 060
Fax: +33 169 355 061
info@dspace.fr

**Croatia**
dSPACE Engineering d.o.o.
Ulica grada Vukovara 284
10000 Zagreb
Tel.: +385 1 4400 700
Fax: +385 1 4400 701
info@dspace.hr

**China**
dSPACE Mechatronic Control
Technology (Shanghai) Co., Ltd.
Unit 01-02,06-09, 19F/L
Middle Xizang Rd. 168
The Headquarters Building
200001 Shanghai
Tel.: +86 21 6391 7666
Fax: +86 21 6391 7445
infochina@dspace.com

**Japan**
dSPACE Japan K.K.
10F Gotenyama Trust Tower
4-7-35 Kitashinagawa
Shinagawa-ku
Tokyo 140-0001
Tel : +81 3 5798 5460
Fax: +81 3 5798 5464
info@dspace.jp

**USA and Canada**
dSPACE Inc.
50131 Pontiac Trail
Wixom · MI 48393-2020
Tel.: +1 248 295 4700
Fax: +1 248 295 2950
info@dspaceinc.com

**Korea**
dSPACE Korea Co. Ltd.
16th floor, Dongwon Building
60 Mabang-ro
Seocho-gu
06775 Seoul, Republic
of Korea
Tel.: +82 2 570 9100
info@dspace.kr

07/2022