KERNKONZEPT

L4RE OPERATING SYSTEM FRAMEWORK & L4RE HYPERVISOR FAMILY

The secure operating system for Germany

Kernkonzept GmbH

CONTENT

1. KERNKONZEPT

From open-source project to professional operating system specialist and solution provider

Since 1997, the L4Re system has been central to our development. Starting at Technische Universität Dresden as an open-source project with a clear focus on real-time applications, the operating system has developed considerably since then.

Between 2005 and 2010, our focus shifted towards IT security, for which we gained increasing attention in the business world.

In 2012, Kernkonzept GmbH was founded as a service provider for customized operating system solutions based on L4Re. Since then, Kernkonzept has been the official maintainer of L4Re and has developed many individual L4Re solutions that meet highest security requirements for customers from a wide variety of industries.

L4Re Secure Separation Kernel VS developed by Kernkonzept has been approved by BSI for processing data up to German GEHEIM and NATO SECRET. L4Re Secure Separation Kernel CC was certified according to Common Criteria (CC) EAL4+ in 2025.

Today, Kernkonzept GmbH is a renowned expert for secure operating system solutions in Germany. The owner-managed company has its headquarters in Dresden.

Our vision

Our goal is to make L4Re permanently available and accessible as an independent and secure open-source operating system technology in Europe. With our comprehensive expertise in operating system research, we are continuously improving L4Re – together with major partners from the fields of hardware, platform architecture, semiconductor manufacturing and tools, and in close cooperation with our customers.

To achieve this goal, we are prepared to try new organizational methods and innovative approaches.

Our mission

Kernkonzept provides a sovereign and secure open-source operating system for Germany and Europe. We are convinced that independent and trustworthy IT infrastructure plays a key role for our digital future.

- **More than 25 years of experience with L4Re**
- **Researchers and maintainers in the company**
- **Owner-managed Ltd. in Germany**
- **Independent, secure & sovereign operating system for Germany and Europe**

The founders of Kernkonzept: (from left) A. Warg, Dr. M. Hohmuth, Dr. A. Lackorzynski

2. L4Re OPERATING SYSTEM FRAMEWORK – SECURITY BY DESIGN

Future-oriented, modular, secure

In a digital world where the protection of critical infrastructures, sensitive data, and networked devices takes center stage, the **L4Re Operating System Framework** (often just called L4Re) is the ideal choice for organizations and companies asking for highest security standards.

Based on our in-house-developed microkernel technology, L4Re pursues the principle of least authority (POLA), allowing customers to design a minimal trusted computing base (TCB) for their product.

This significantly reduces the attack surface of a system and ensures that all components are strictly isolated from each other both spatially and temporally.

L4Re is more than just an operating system: it is a modular platform specifically designed to run safety-critical applications in an efficient and secure way alongside standard software on hardware. This is achieved through the integrated virtualization functions, which allow running different environments simultaneously and complete isolated.

This makes L4Re the perfect choice for use in areas that require maximum security and reliability.

Use-cases

- Secure government laptops and network technology
- Security gateways for the automotive industry
- Secure real-time server solutions and IT applications

The framework consists of the L4Re Microkernel, which securely executes both native applications (Micro-Apps) and virtual machines.

The Micro-Apps that were specially designed for safety-critical scenarios use the **L4Re runtime environment** and offer a trusted computing base (TCB) that is even further reduced than virtual machines. This makes L4Re the ideal solution for safety and security applications.

Why L4Re?

- **Security by design:** The microkernel is the only component that runs in privileged mode on the hardware. All applications and virtual machines are executed strictly isolated in user space. This raises security to a new level. In addition, object capabilities allow the implementation of a mandatory access control.
- **Capability-based security concept:** The L4Re Microkernel utilizes a mature system for access control

+ **Principle of Least Authority (POLA)**
+ **Minimal trusted computing base reduces attack surface**
+ **Modular platform for safety-critical applications**
+ **Integrated virtualization functions**
+ **L4Re Microkernel executes Micro-Apps and VMs**
+ **Security on a new level**
+ **Capability-based access control**

based on object capabilities. It assigns rights to all object references, while also protecting them. The L4Re system thus forms a seamless roles-and-rights system which clearly labels all objects and resources in the kernel and in the user space with capabilities. In addition, object capabilities provide a secure method of access control (mandatory access control, MAC). This is how the L4Re Microkernel offers the most advanced possibilities to realize security architectures with an L4 microkernel.

- **Flexibility and modularity:** L4Re is scalable and adjusts to specific requirements – from small embedded systems to big, complex infrastructures.
- **Tested technology:** L4Re builds on 25 years of research and development and has been used more than 10 years in many accredited and certified products. In 2025, L4Re Secure Separation Kernel CC got the **CC EAL4+ certification**.

Security by design starts with OS choice

Security in modern IT and IoT systems is not just a question of individual protection mechanisms but a holistic challenge, which must already be considered when choosing the operating system.

The operating system, together with the hardware platform, is the foundation of every system architecture. The choice of operation system determines how well security concepts such as isolation, access control, and minimizing of attack surfaces can be realized.

A microkernel-based operating system like L4Re provides a software architecture that was developed for security-critical situations from the start. Its modularity and the strict separation of applications enable L4Re to create an environment with minimized vulnerabilities.

Due to this consistent alignment with security, known as **security by design**, security aspects are not retrospective “add-ons”, but built deeply into the architecture of the system. This maximizes robustness and also keeps the system flexible to react quickly and effectively to future threats.

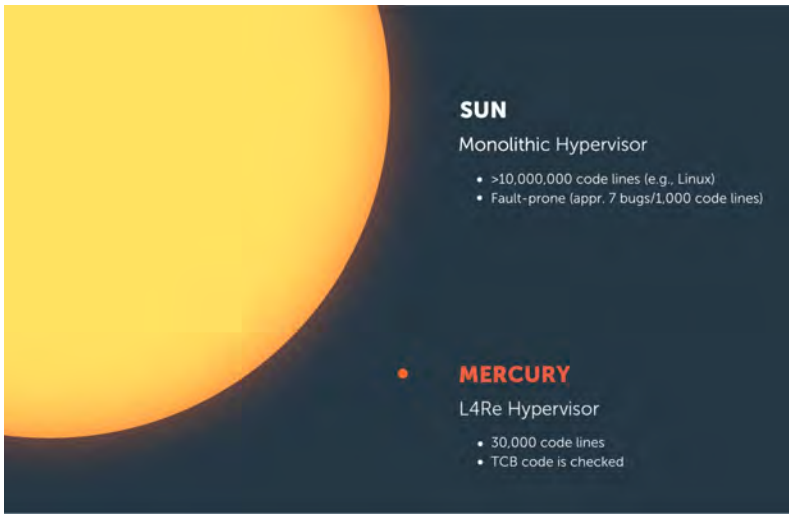
The focus on establishing security from the start also enables zero trust solutions.

The minimal trusted computing base

The best way to understand how advantageous a microkernel-based operating system or hypervisor works is by comparing it with a monolithic system like Linux or Windows.

When safety is paramount, it is important to minimize the number of elements of a system that you have to trust. This results in a minimal attack surface.

+ **L4 microkernel with mandatory access control (MAC)**
+ **Based on 25 years of research, used more than 10 years**
+ **Certified CC EAL4+ in 2025**
+ **Best suited for security architectures**
+ **Security as a holistic challenge**
+ **Only most basic elements in kernel space**
+ **Zero trust**



Trusted computing base: monolithic hypervisor vs. L4Re Hypervisor

Monolithic hypervisor

A **monolithic hypervisor** contains all the essential functions of the operating system – such as drivers, memory management, process management, network control, and security functions – directly in the kernel. This expands the code base and makes it more complex, harder to maintain and support, and enlarges the attack surface. Examples for monolithic hypervisors are VMware ESXi, Xen, and Microsoft Hyper-V.

Microkernel-based hypervisor

A **microkernel-based hypervisor** implements only the basic mechanisms in the kernel space. All other services (like drivers, file systems, and networks) are run as separate processes in userland.

Thus, the modular system architecture enhances security through increased resilience and a significantly smaller, application-specific TCB.

Microkernel-based systems have a reduced attack surface and are better suited for security-critical and real-time systems (such as in the automotive and aerospace industries).

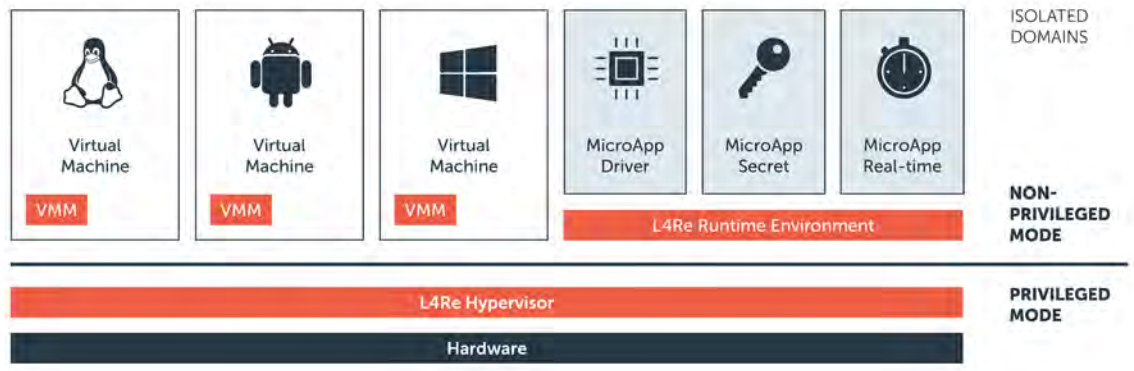
They are easier audited, accredited, and certified because of the small microkernel, which is easy to examine. An example for such a hypervisor is the L4Re Hypervisor.

The **microkernel-based approach** is therefore specifically well suited for security-critical applications that mainly require isolation and modularity. Separating services and the minimal kernel significantly reduces attack surface, which enables high security and makes certification easier.

In contrast, the **monolithic approach** is better for general virtualization tasks where performance and tight integration are more important than security. The centralized management of all functions in the kernel enables effective communication, however, at the expense of a greater attack surface and greater complexity, which makes evaluation extremely costly.

+ **Very well suited for IT security and security-critical applications**

+ **Only most basic elements in kernel space**



L4Re Operating System and Hypervisor Framework

3. L4Re SECURE SEPARATION KERNEL VS – CERTIFIED SECURITY

In January 2024, Kernkonzept GmbH achieved an important milestone: The Federal Office for Security in Information Technology (Bundesamt für Sicherheit in der Informationstechnik, BSI) granted L4Re Secure Separation Kernel VS the approval for processing classified information (VS) up to classification level GEHEIM.

In 2025, this was followed by classification level NATO SECRET and the Common Criteria EAL4+ certification.

L4Re is now the first operating system of its kind in Germany achieving this high security level, laying another foundation for the digital sovereignty of Germany and Europe.

The approval and the certification confirm the exceptional reliability, security, and quality of the L4Re technology, which is already running in many security-critical IT products.The L4Re Operating System and Hypervisor platform is used for the secure separation of sensitive information and networks, as well as the isolation of critical security functions.

Unique technology for maximum security requirements

As the first separation kernel that is approved for German GEHEIM/NATO SECRET, L4Re means immense advantages for manufacturers of security-critical IT products.

The strict isolation mechanisms of L4Re Secure Separation Kernel VS allow a reliable separation of security domains or classification levels within a computer system. This is essential in environments where information with different security levels is processed simultaneously.

The BSI approval enables manufacturers of security-critical IT products to directly employ the already German GEHEIM approved separation kernel, which accelerates and simplifies the certification process considerably.

+ **Approved up to German GEHEIM/NATO SECRET**
+ **Certified Common Criteria (CC) EAL4+**
+ **Extended to the arm platform**

The previous need for extensively evaluating your own operating system solutions becomes obsolete. This not only results in a significant reduction in costs but also ensures clearly defined quality and security.

Developing security by design

L4Re Secure Separation Kernel VS was developed following the strictest security principles. With a trusted computing base of only 30,000 lines of code and a capability-based mandatory access control (MAC), L4Re is tailored perfectly for zero trust architectures.

Starting in October 2021, L4Re Separation Kernel has been checked in an intense approval process. This was done in close cooperation with independent test centers accredited by the BSI, such as *atsec information security GmbH* and *SRC Security Research & Consulting GmbH*. This evaluation considered the technical implementation as well as organizational processes that are crucial for secure development and product care.

Change of paradigm for manufacturers

The approval of Kernkonzept's L4Re Secure Separation Kernel VS up to levels German GEHEIM and NATO SECRET gives new opportunities to manufacturers of security-critical IT products.

Responsibility for the approval process of the so-called secure execution platform is now with us, which not only means more efficiency for our customers, but also the considerably simplified implementation of security-critical IT products.

+ **Improved time to market**
+ **Less risk in approval process**
+ **Reduced time and cost**

4. NEW DEVELOPMENT APPROACH FOR IT SECURITY PRODUCTS THAT NEED APPROVAL

The compositional approach with L4Re Secure Separation Kernel VS

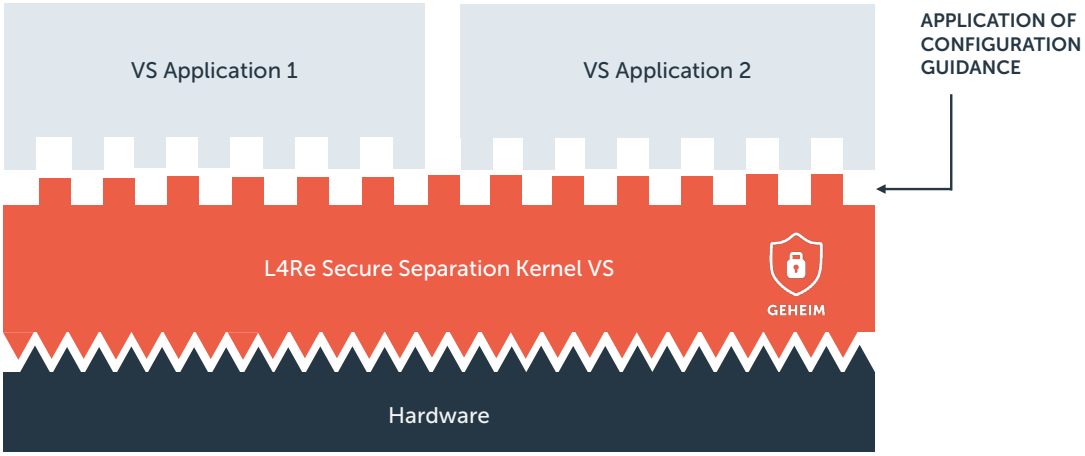
There is a growing need for IT security products that can be approved quickly and securely. Today, the approval or certification of IT security products for manufacturers, consumers and examining agencies is an increasingly complex process.

For the first time, L4Re Secure Separation Kernel VS enables all involved parties to orchestrate the configuration of products quickly and efficiently, by following the configuration guidance (the certification document available with the approved L4Re).

The approved operating system platform eliminates the need for additionally having the platform approved, as it replaces the specific hardware requirements. This significantly speeds up the approval process, because manufacturers only need to bring their own application through the approval process after having shown its correct implementation.

Our approach also allows the combination and integration of different security-critical IT products on a secure platform. Furthermore, companies benefit from a faster time to market and better utilization of resources, as duplication and additional work are avoided.

+ **Secure platform with operating system and hardware**
+ **Less expenses**
+ **Shortened time to market**



Compositional approach with the L4Re Secure Separation Kernel VS

5. SECURITY & SAFETY CRITICAL IT PRODUCTS WITH L4Re FOR PROTECTION UP TO CC/GEHEIM/NATO SECRET

Diverse product types with the L4Re Operating System Framework

L4Re technology provides the foundation for a diverse range of highly secure IT solutions. Our technology enables the development and integration of systems that meet the highest security requirements.

These products range from specialized applications for security-critical infrastructure up to innovative cloud and virtualization products.

In the following paragraphs, we will present a selection of product types that are based on our established operating system and are already successfully used in several areas.

5.1 CROSS-DOMAIN INTERFACES (RED/BLACK)

A cross-domain interface enables the secure exchange of data between networks with different security levels. Red describes networks exchanging data that is labeled as classified, black means networks for data without a security level or with a lower classification.

In general, cross-domain interfaces are employed to prevent unwanted data outflow and possible attacks by providing a strictly monitored, secure, and high-performance pathway for data exchange in one or two directions.

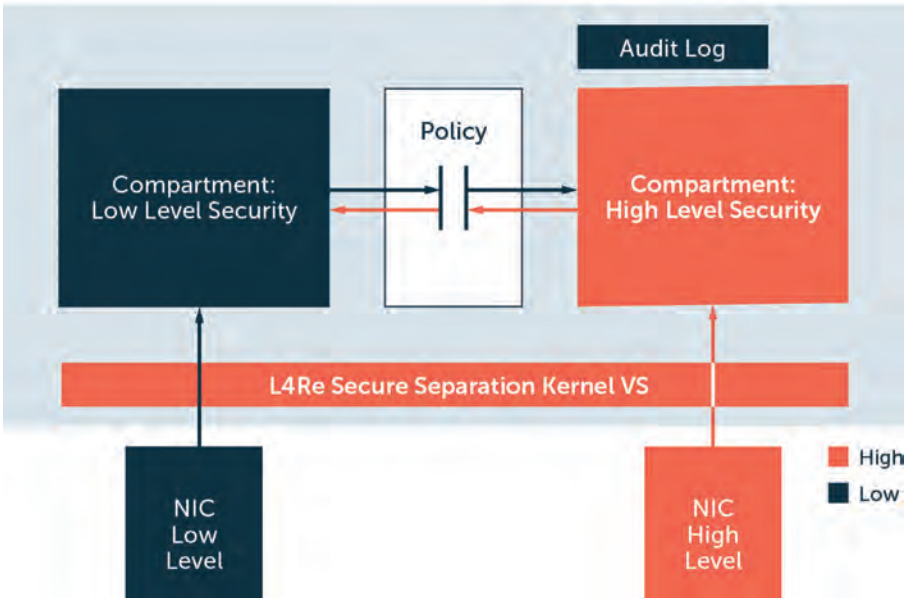
+ **Secure data transfer**
+ **Unidirectional and bidirectional data flow secured**

In a growing number of areas, red/black interfaces are not anymore realized by physical separation but rather by software, which saves space and energy. Hypervisor solutions such as the L4Re Microkernel play a prominent role here.

unauthorized data leaks from a higher classified to a less protected network. The gateway monitors the data streams and creates an audit log that records all events.

In the past, this security architecture was implemented by physically separating the systems. This hardware-based solution required considerable resources: equipment, space, and energy costs.

+ **Cryptographic labels**
+ **Unequivocal marking according to classification level**



Functionality of an Information Exchange Gateway (IEG)

Information Exchange Gateways (IEGs)

As cross-domain solutions (CDS), gateways are indispensable in modern IT security. Especially when connecting IT networks of different security domains (so-called red/black networks), IEGs enable the exchange of data between such networks and replace less efficient solutions, such as swivel chair interfaces.

Gateways have various important functions: They decide if and which data are allowed to be transferred from one network to another. They articularly check whether the data transfer complies with the defined security rules.

A central aspect of this security mechanism is the prevention of

The L4Re Microkernel achieves this separation efficiently on a single device by means of so-called compartments (sealed-off areas), which are strictly isolated. This separation refers to either data communication, memory, or other system-relevant resources. The data in the different compartments remain strictly separated and can only be accessed via controlled interfaces.

L4Re runs in the SDoT Gateway from infodas (with approval for German GEHEIM/EU SECRET/NATO SECRET and certification according to CC EAL4+ and NITES) and in the Airbus Security Exchange Gateway (SEG) with GEHEIM approval.

These products utilize the advantages of L4Re Secure Separation Kernel VS for secure and efficient cross-domain solutions. They offer a powerful solution for secure data transmission between networks of different security levels, without unwanted data outflow or leaks.

Data diode

Data diodes work similarly to gateways. The main difference lies in the direction of data flow. While a gateway allows data exchange in both directions under strict security rules, the data flow in a data diode is unidirectional: from a lower classified network to a higher classified high-security network. This is comparable to a physical diode that conducts electric current in one direction only.

A data diode is a small program specially developed to transfer data from a lower classified network to a secure network. In preventing any backflow of data, it avoids data leaks and effectively protects the high-security network. At the same time, a data diode can process large data volumes at high throughput.

A typical area of application for data diodes is the military. There, reconnaissance data obtained by drones or satellites can be transferred in large quantities quickly and securely into a high-security network.

With a transmission speed of up to 10 Gbit per second, data diodes exceed the performance of gateways and are ideal when a lot of data must be processed in a short amount of time.

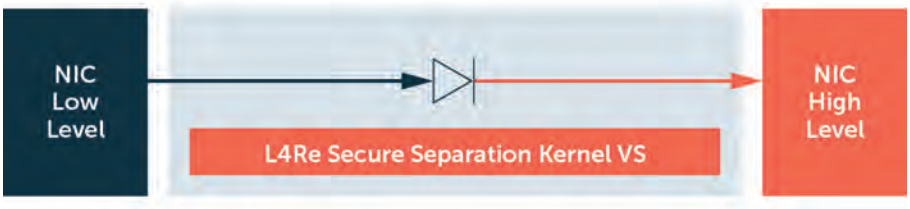
The data diode is another case where the L4Re Microkernel guarantees strict network separation via compartments. This architecture ensures that data flows only in the specified direction, and it protects the high-security network from unauthorized access. For this reason, data diodes are approved for use in security-critical environments, such as handling secret information.

An example for such products is the SDoT diode from infodas, which is approved for use up to secrecy levels GEHEIM, EU SECRET, and NATO SECRET, and certified for CC EAL4+. Another example is the vs-diode from genua with approval up to GEHEIM/EU SECRET/NATO SECRET.

Labelling

Labelling creates cryptographic labels for data which are transmitted via a gateway between networks of different security levels. This is necessary for unstructured data such as PDF documents or images. For those data, no automatic filter rules can be created, which is why these unforgeable labels are needed.

The labelling service works exclusively in the high-security (red) network. The data are labelled and classified by assigning a



Functional Principle of a Data Diode

+ **Cryptographic labels for networks with different security levels**

+ **Labelling based on the L4Re Microkernel ensures strictly isolated compartments**

+ **L4Re ensures strict separation of internal domains in secure endpoint appliances**

cryptographically secured label that uniquely identifies the respective file and marks its classification level. This ensures that data with different security levels are handled correctly.

This is another case where the L4Re Microkernel is the optimal technological foundation. As an approved separation platform, L4Re ensures that different parts of the labeling service are run in strictly isolated compartments.

These compartments make it possible to run different products or services on the same platform, without compromising security. Within the labelling, different components – for example for cryptography or logging – can work securely and separately.

A labelling product based on the L4Re Microkernel is the SDoT Labeling Service from infodas. It enables automatic or manual data classification via XML security labels and fulfills the requirements of NATO STANAG 4774/8.

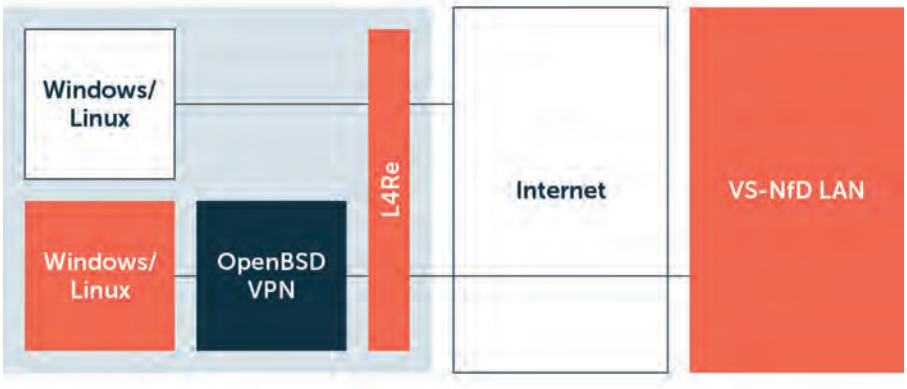
Secure Endpoint

For many companies and public authorities, reliable IT security is a top priority regarding the employees' mobile work. When sensitive data is being processed on their own laptop and transferred to other end devices via the internet, under no circumstances should third parties be able to read, manipulate or steal this data. It is even more important to prevent other users from accessing laptops which store confidential information via the LAN.

Secure endpoint appliances are specifically developed for scenarios like this. L4Re has been used in several of these appliances for years and ensures the perfectly reliable protection of sensitive data.

For this, the strict separation of the internal domains in a laptop is crucial. Unsecured applications such as e-mail programs or internet browsers are open to attacks.

+ **Processing of sensitive data on own device**
+ **Integrated VPN solution "made in Germany"**
+ **Strict separation of areas via compartments**



Secure domain separation with L4Re in genua's vs-top

An attacker or malware that, for example, compromises the browser, must not be able to penetrate any further, neither into the work domain dealing with sensitive data nor via VPN into the network.

vs-top

In the security laptop vs-top that was developed by genua in 2014, two separate working environments are set up for the reliable separation of confidential data: While one has the usual Windows or Linux applications (browser, e-mail program, word processing program, etc.), the other is reserved for processing sensitive data.

From this environment, users access the internal network via encrypted connections, which are provided by an integrated VPN solution (Virtual Private Network) “made in Germany”, using mobile network, WLAN, or ethernet. Strict separation is guaranteed by L4Re.

L4Re creates so-called compartments on the security laptop: In these strictly isolated areas, the browser, mail, and office applications are locked away. Other compartments are work domains for sensitive data or security systems, such as VPN gateway and firewall. Each area is controlled by its own operating system running virtualized by L4Re, so that there are no dependencies.

This strict separation prevents attacks or data loss during the transition between different working environments or to the security systems. L4Re thus offers a level of security that is otherwise only achievable by using separate hardware devices.

Version 1.6 of the vs-top received approval for processing classified data (VS-NfD and EU/NATO RESTRICTED) from BSI in 2020.

+ **Hypervisor as centerpiece of the cloud**
+ **VM for separation of resources**
+ **More flexibility, more efficient hardware utilization, additional security level**

genua‘s vs top 1.6 with L4Re, approved for VS-NfD and EU/NATO RESTRICTED in 2020

5.2 SECURE AND FLEXIBLE CLOUD SOLUTIONS FOR GERMANY

Modular architecture and GEHEIM/NATO SECRET approved hypervisor

A common cloud infrastructure consists of several key components. This includes the computing resources (servers) that host applications and services, as well as storage solutions that securely store large amounts of data.

Additionally, there are network resources that enable fast and secure communication between the various cloud elements.

Above all that, there is the virtualization layer which efficiently manages resources and gives users the flexibility to adapt their systems dynamically. Finally, a security and management layer protects and controls the entire cloud environment.

The virtualization layer, which is realized by a hypervisor, is the core of modern cloud infrastructures. A hypervisor is a software that enables running several virtual machines (VMs) on a single physical server at the same time. In doing so, it separates the physical resources – such as processors, memory, and network – and allocates them to the various virtual machines.

Each VM may run independently and manage its own operating system and its own applications. This separation of resources creates flexibility, improves the efficiency of hardware utilization and offers an additional level of security, as the VMs operate in isolation from each other. This makes the hypervisor the centerpiece of the cloud.

In cloud environments that process highly sensitive data, the use of a microkernel-based hypervisor is particularly recommended as it offers significantly more security and reliability compared to conventional hypervisors.

Today, cloud environments are exclusively using hypervisors that are monolithic. A large part of the functionality – including the management of drivers, network, and memory – within these hypervisors

+ **Microkernel-based hypervisor offers more security and reliability**
+ **Massive benefits for clouds with highly sensitive data**
+ **Modular architecture for more trustworthiness**
+ **Microkernel architecture for minimal attack surface**
+ **Strict isolation for multi-tenant environments**
+ **Hypervisor accredited up to GEHEIM/NATO SECRET**

runs in kernel mode. An error or a security vulnerability in one of these components can thus jeopardize the entire cloud infrastructure. A successful attack on one component could potentially allow control over all virtual machines in the cloud.

In contrast, a microkernel-based hypervisor like the L4Re Hypervisor or L4Re Secure Separation Kernel VS (approved for German GEHEIM/NATO SECRET) is designed to drastically reduce the attack surface. With a microkernel, only functionality where the kernel mode is absolutely necessary (e. g., resource management and the isolation of the virtual machines) is actually executed in kernel mode.

All other functionality, such as drivers or additional management processes, is operated in separate, isolated user processes. This separation means that even in the event of a successful attack on one of these components, the rest of the system remains secure, as access to critical parts of the infrastructure is strictly limited.

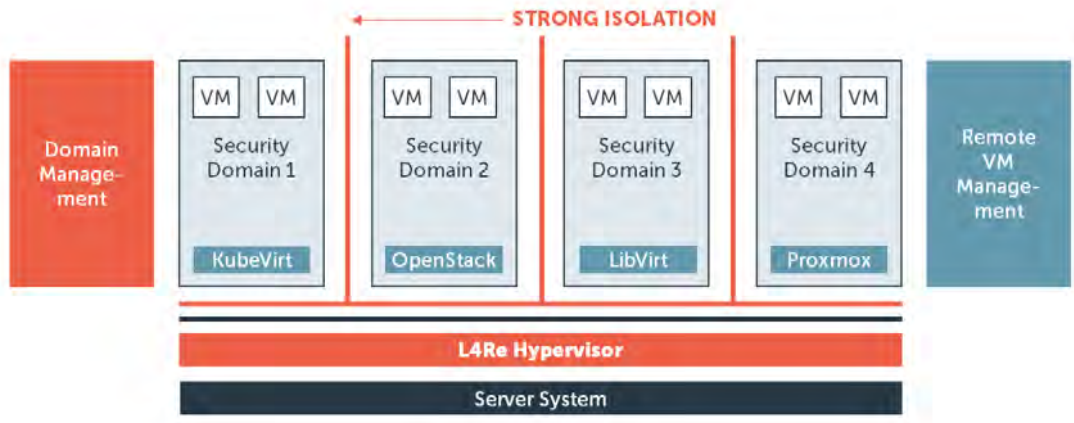
For clouds that store highly sensitive data (e. g., medical information, financial data, or government classified documents), the microkernel approach therefore has enormous advantages. It minimizes the risk of vulnerabilities, enables tighter control of data flows, and makes it easier to implement security guidelines on the highest levels. This architecture creates higher trustworthiness, which is particularly important for companies that must meet regulatory requirements such as ISO 27001 or CC EAL4+.

To summarize, a microkernel-based hypervisor is essential for security -critical clouds to ensure the highest level of data security and system integrity.

The L4Re Hypervisor/L4Re Secure Separation Kernel VS offers an ideal solution for building a high security cloud. There are several reasons why it should be preferred to other hypervisors and security solutions:

- **Minimal attack surface:** L4Re Secure Separation Kernel VS is based on a microkernel architecture which has been deliberately reduced to the essentials. L4Re executes only those functionalities in kernel mode that absolutely require it (such as resource management and isolation of virtual machines). This minimizes the potential attack surface, which in turn drastically increases security.

+ **Flexible via compositional approach**
+ **Several security domains on the same hardware**
+ **Optimal match between hardware and software**
+ **Common Criteria EAL4+**
+ **Combination with KubeVirt, LibVirt, OpenStack, Proxmox**



Several security domains or compartments with strong isolation

- **Strict isolation and multi-tenancy:** In a cloud environment in which different customers or applications run in parallel, strictly isolating the individual virtual machines and possible security domains is essential. L4Re Secure Separation Kernel VS ensures that all the VMs and their resources are clearly separated from each other, which prevents vulnerabilities in one VM from jeopardizing the entire cloud stack. This is particularly important in multi-tenant environments where data from different customers or departments must be securely separated.
- **Provable security via certificates:** L4Re is already approved for use up to secrecy levels GEHEIM and NATO SECRET and certified as CC EAL4+, as well as ASIL B in a customer product. Especially in highly regulated areas such as the public sector, defense industry, or public health, the availability of certificates like these is an important deciding factor for meeting compliance requirements.
- **Flexibility via compositional approach:** L4Re Secure Separation Kernel VS enables building cloud environments in a modular and controlled way. With the composition approach, companies can flexibly customize their cloud infrastructure by combining different applications and security requirements. This not only facilitates the development process but also makes it easier to obtain approvals and certifications for specific applications.
- **Availability of hardware requirements for secure integrations:** It is a special feature of L4Re Secure Separation Kernel VS that you can start tailoring the cloud infrastructure according to the requirements of the approval already in the stage of hardware selection. Legitimate interest provided, L4Re Secure Separation Kernel VS offers guidance for hardware requirements, so that the selected hardware meets highest security standards. Because of this optimal coordination between hardware and software, security benefits can be fully leveraged.
- **Future-proof and tested security:** With the CC EAL4+ certificate, L4Re sets a new industry standard. For companies that want future-proof cloud solutions not only for today but also for future security requirements, L4Re Secure Separation Kernel VS is the ideal solution. It offers certified security, more convenience through simple integration, and predictability in operation.
- **Flexibility through integration with leading virtualization and management solutions**: The open-source L4Re Hypervisor offers outstanding flexibility, as it can be easily integrated into existing virtualization and management ecosystems. Companies and institutions can therefore use L4Re in combination with established management applications such as KubeVirt, LibVirt, OpenStack or Proxmox. With this seamless integration you can manage cloud resources and virtual machines efficiently and centrally without having to compromise on the highly secure basis of L4Re. Companies therefore stay flexible and can customize their cloud infrastructure according to individual needs and requirements.
- **Adaptability for government institutions and authorities through open source:** As open-source technology, the L4Re Hypervisor opens a range of options for state institutions and authorities to customize their cloud environments to specific requirements.

+ **Open source, for state institutions and agencies**

+ **Sovereignty for sensitive cloud environments**

+ **Simple audits for stronger trust in cloud infrastructure**

With open-source code, they have full control over the technology and can ensure that no hidden components or unwanted functions are implemented. This transparency guarantees maximum security and also allows integrating the L4Re Hypervisor flexibly and long-term into national security architectures to build sovereign IT infrastructures.

- **Sovereignty and backdoor avoidance in sensitive cloud environments:** In highly sensitive cloud environments, it is crucial that the technology is sovereign and does not contain any backdoors that could be misused by third parties. L4Re offers full control over the code and is free from proprietary elements that could potentially be compromised by third parties. This makes L4Re the ideal choice for security-critical applications where trustworthiness and independence have top priority. The open-source approach makes it easy to do security checks and audits, which further increases trust in the cloud infrastructure.

In a world where data security becomes increasingly important, L4Re Secure Separation Kernel VS provides the reliability, flexibility and approved security that organizations need to protect their cloud infrastructures and meet compliance requirements.

5.3 THE WAY TO MULTI-SECURITY DOMAIN UP TO GEHEIM/NATO SECRET AND MULTI-TENANT CLOUD FOR AGENCIES AND DEFENSE

National Secure Cloud (NSC): Highly secure cloud infrastructure for public authorities and military organizations

NATIONAL SECURE CLOUD

+ **Strong partners: IABG, infodas, Utimaco, Xelera, mspaces, inxire, and Kernkonzept**

Authorities and military organizations require cloud solutions that meet the highest requirements of confidentiality, data protection, and digital sovereignty. In view of increasing cyber threats, the National Secure Cloud (NSC) offers a solution for the strict requirements of the classified information directive (“Verschlusssachen-Anweisung”, VSA) up to secrecy level GEHEIM.

The NSC is developed in a collaboration with the partners IABG, infodas, Utimaco, Xelera, mspaces, inxire, and Kernkonzept to make VS-IT technologies securely and efficiently usable. It enables the simultaneous processing of data of different security levels on a single piece of hardware, reducing costs and rendering physical separations obsolete.

The modular and multi-domain-capable architecture of the NSC allows the dynamic instantiation of security domains and ensures strict isolation and security with L4Re Secure Separation Kernel VS, which is approved by BSI for GEHEIM and NATO SECRET.

By applying open-source technologies, the NSC provides transparency and reduces dependency from international providers. At the same time, it remains user-friendly, scalable, and easy to integrate into existing infrastructures. Individual needs can be

implemented flexibly, and the open ecosystem approach allows integrating solutions from other providers.

The NSC offers the ideal platform for a secure cloud infrastructure in Germany that meets the needs of public authorities as well as the German Armed Forces (Bundeswehr).

Multi Domain Combat Cloud Demonstrator: High-security cloud for the Future Combat Air System (FCAS)

Europe's Future Combat Air System (FCAS) is a networked system of manned and unmanned platforms – including fighter jets, drones and satellites – that are coordinated via a Combat Cloud. This cloud infrastructure enables the integration and cross-linking of all elements for the secure exchange of data in real time.

The main contractor for this European initiative is Airbus Defence and Space, which, among other things, provides command and control elements for NATO.

As part of the FCAS initiative, several software and hardware demonstrators have already been developed, including AI-supported mission planning, certifiable cloud kernels, and unmanned aircraft launchers.

The L4Re Hypervisor serves as a high-security hypervisor that enables protected data connectivity between airborne platforms. This application has been demonstrated in successful flight tests on an A400M aircraft in 2021 and 2022.

The Secure Combat Cloud Demonstrator shows that the L4Re Hypervisor can be integrated as a secure operating system in an airborne cloud environment to coordinate highly sensitive data and missions in real time. After the launch of the FCAS demonstrator phase 1B, further progress is expected in the coming years, which will add to the functionalities of the FCAS components.

+ **L4Re as high-security hypervisor in FCAS demonstrator**

+ **Secure operating system in airborne cloud environment**

5.4 VARIOUS APPLICATIONS FOR L4Re IN SAFETY-CRITICAL AREAS

In addition to the automotive industry, the L4Re Hypervisor family is increasingly being considered for applications in areas such as industrial automation and aviation safety. The ability to securely isolate workloads of varying criticality and run them in parallel makes L4Re the ideal choice for applications that require maximum security and stability.

Its robust architecture and the strict separation of workloads enable the L4Re Hypervisor to be used in highly critical areas where the protection of the overall system is top priority. This is not only relevant for automotive safety solutions; it is also important for industrial control systems or networked devices in the smart home area.

In 2024, the L4Re Hypervisor received the safety certificate ISO 26262 ASIL B in Elektrobit's EB corbos Hypervisor.

+ **L4Re Hypervisor family ideal for maximum security and stability**
+ **Strict separation of workloads**
+ **L4Re Hypervisor received ISO 26262/ASIL B in 2024**
+ **L4Re Hypervisor and L4Re Micro Hypervisor provide a scalable, flexible, modular and secure automotive software architecture**

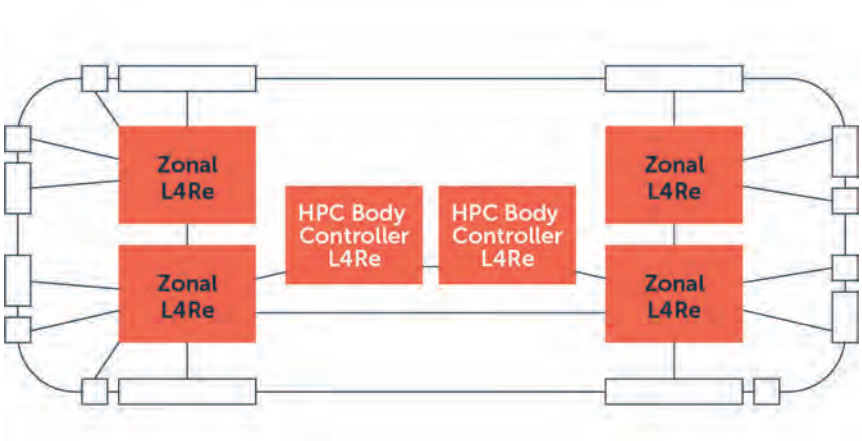
L4Re Hypervisor family: The flexible solution for secure and future-oriented automotive architectures

The automotive industry is at a turning point. While vehicles are increasingly software-controlled and linked, new requirements and safety standards pose major challenges for manufacturers. The growth of software applications that are integrated into larger control units requires a modular and secure software architecture. Kernkonzept's L4Re Hypervisor and L4Re Micro Hypervisor offer a flexible and scalable foundation to support the transition to a modern and robust vehicle architecture and to secure it.

3 key trends in the automotive industry

The requirements of vehicle architectures are changing rapidly and can be characterized by three trends:

- **Control unit consolidation:** In the future, a small number of high-performance controllers will replace the large number of traditional



Zonal E/E architecture in cars

control units. This new architecture reduces the number and complexity of the control units, resulting in considerable cost savings and leaner electronics, while at the same time allowing for more computing power in the vehicle.
However, this consolidation entails the challenge that functions previously operated on separate hardware now must be integrated and executed on the same HPC. The L4Re Hypervisor creates clear isolation and partitioning between the functions and makes it possible to run safety-critical applications on the same piece of hardware that executes comfort or infotainment functions.

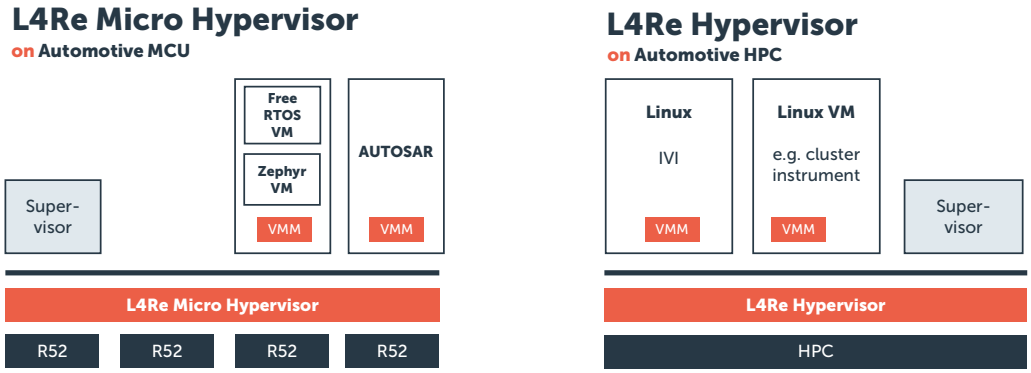
- **Connectivity:** Connected vehicles require a connectivity control unit to ensure a secure demarcation between internal and external network traffic. The L4Re Hypervisor provides the necessary separation and protection to securely isolate safety-critical vehicle functions against incoming connections from external networks. This protection mechanism is essential to prevent potential attacks on the on-board system from gaining access to security-relevant controls via the vehicle network.
- **Mixed criticality:** Safety-critical and non-safety-critical functions are increasingly operated on the same hardware, which necessitates strict separation and prioritization. The L4Re Hypervisor ensures that security-critical applications have priority and are not affected by other, less critical applications. With this approach, safety functions in the car can run continuously and uninterrupted.

L4Re Hypervisor and L4Re Micro Hypervisor for automotive

The traditional separation through static hardware configurations reaches its limits when implementing these trends. The L4Re Hypervisor family offers a software-based solution for hardware-supported virtualization that fully meets the requirements of isolation and flexibility.

A hypervisor creates a layer between the hardware and the running applications. This allows several virtual machines (VMs) on the same automotive HPC as well as on the same automotive MCU, while not influencing their individual task areas. The hypervisors of the L4Re Hypervisor family can even run VMs and L4Re applications at the same time, meeting different requirements.

+ **L4Re Hypervisor creates clear isolation and partitioning between control units on the same HPC**
+ **Run safety-critical applications on the same hardware**
+ **L4Re Hypervisor separates safety-critical vehicle functions and protects them from external networks**
+ **Priority of security-critical applications is ensured**
+ **L4Re Hypervisor family offers software-based solution for hardware-supported virtualization**



L4Re Hypervisor and L4Re Micro Hypervisor

Isolation and parallel system processing

The L4Re Hypervisor family has the outstanding ability to process different applications at the same time. Functions can be run securely and efficiently side by side, even on different criticality levels. This ability is of enormous advantage for the automotive industry, as safety-critical functions such as brakes and drive controls can be run without impairment together with infotainment or comfort applications. A classic example is the separation of in-vehicle infotainment applications and the dashboard display, whose underlying applications are executed on the same hardware.

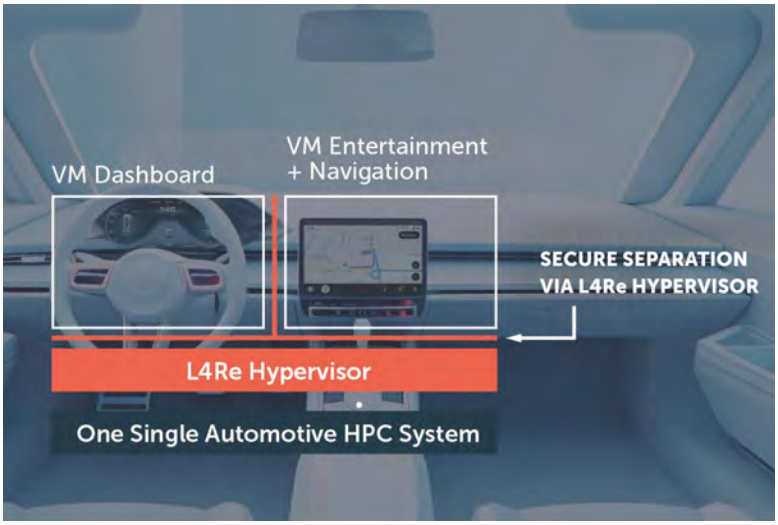
L4Re as reference hypervisor for NXP S32 Z/E

A reference hypervisor is an officially recommended or standardized solution used by chip manufacturers such as NXP for their processor architectures.

This means that L4Re is rated by hardware manufacturers as a suitable virtualization solution that works optimally with their processors. NXP tests and optimizes L4Re on its platforms and documents it as a reliable and compatible hypervisor solution.

Benefits for manufacturers:

- **Faster and more efficient product development:** For companies that rely on NXP processors, the L4Re Hypervisor is particularly efficient, as it is already optimized for the hardware. This shortens development time and minimizes potential compatibility problems.
- **Secure virtualization:** L4Re makes it possible to securely isolate software components from each other. This is increasingly important particularly in safety-critical areas such as the automotive industry (e. g., through ASIL compliance) or in the development of embedded systems.



Separation of dashboard and infotainment application through L4Re on a HPC

- **Compatibility with extensive ecosystem:** Companies that rely on L4Re can use a wide range of tools and development environments that are compatible with the NXP processors, which further increases efficiency in development.

L4Re as reference hypervisor for NXP GreenVIP

The L4Re Micro Hypervisor is the reference hypervisor on NXP's S32Z and S32E real-time processors. It was introduced in 2023 as reference hypervisor for the NXP Semiconductor families S32Z and S32E. These 16 nm real-time processors are equipped with 8 Arm R52 cores and run with up to 1 GHz.

By supporting the L4Re Micro Hypervisor, these multi-core systems can run multiple workloads or VMs in parallel and allow the secure integration of vehicle-wide functions. The L4Re Micro Hypervisor is included in the S32Z/E Vehicle Integration Platform (GreenVIP).

NXP and Kernkonzept are thus offering the first ever open-source hypervisor for Cortex-R52 processors.

L4Re as enabler of the digital twin

As a hypervisor solution on digital Arm processor designs, L4Re can enable customers to fully exploit the concept of the digital twin. This means that OEMs can create a precise virtual image of their system in preproduction. With L4Re, manufacturers can drive software and hardware development in parallel – long before the actual hardware is available.

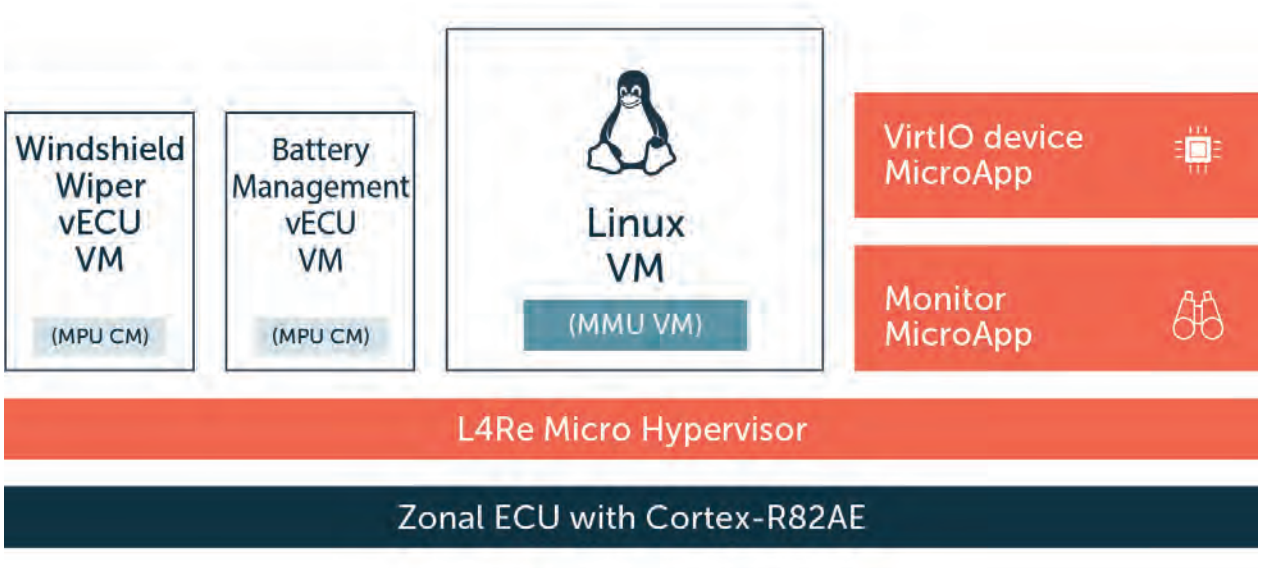
L4Re Hypervisor solutions can be used for the new Arm Virtual Platform IPs since 2024. Manufacturers can implement these solutions on high-performance Arm CPU designs as well as on low-power versions or other processor architectures. Consistent abstraction levels between hardware and software allow for a hardware-independent, flexible, and scalable system and software development from a single source. Thanks to the L4Re Hypervisor family supporting the new processor designs, development can start designing the software immediately after the IP release on the Arm Virtual Platform.

+ **L4Re tools and development environments are compatible with NXP processors**

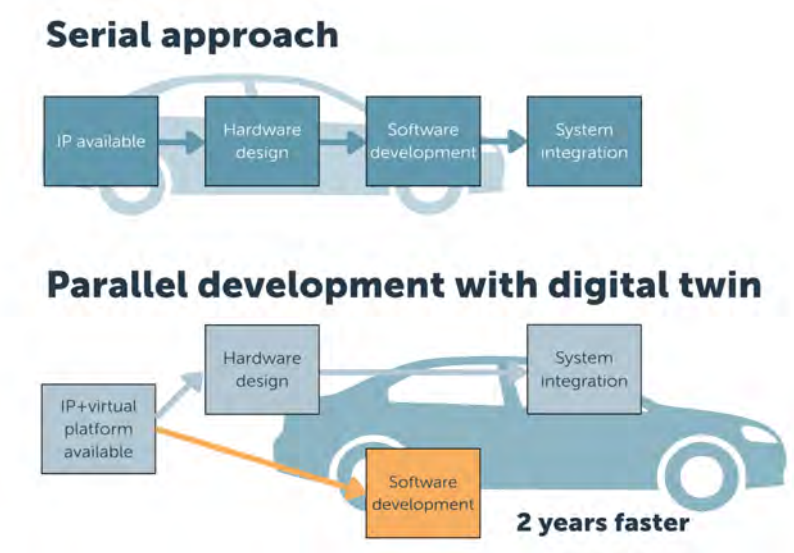
+ **L4Re Micro Hypervisor as reference hypervisor for NXP S32Z and S32E since 2023**

+ **L4Re first ever open-source hypervisor for Cortex-R52 processors**

+ **Since 2024, L4Re can be used for Arm Virtual Platform**



Example of a zonal ECU with L4Re Micro Hypervisor on Arm Cortex-R82AE



Comparison of product cycles with and without digital twin

Parallelization of software and hardware development

This means that software can be developed independently and in parallel with the hardware. OEMs and tier 1 can start working on virtual processors even before the physical hardware is ready. Manufacturers save valuable time, increase efficiency, and reduce risks that could arise from delays in hardware and software development.

Software tests and validation can be carried out much earlier in the development process, which reduces expensive and time-consuming error corrections in later phases and shortens overall development time. Software components can be developed, tested and integrated independently of the hardware, resulting in higher quality and faster time to market.

SOAFEE – The future of automotive architectures

Kernkonzept is actively involved in the design of SOAFEE (Scalable Open Architecture for Embedded Edge). The L4Re Hypervisor family is part of this new trend-setting safety architecture. The integration with the SOAFEE reference platform EWAOL shows how the L4Re Hypervisor supports the consolidation of Arm Cortex-A and Cortex-R CPUs and creates a flexible foundation for a variety of automotive applications.

This flexible architecture allows OEMs to develop a wide range of applications – from standard functions to safety-critical applications – and to bring them to market cost-effectively. The L4Re Hypervisor family promotes the efficient use of hardware and also offers the scalability required to keep pace with the rapid development of the automotive world.

Safety solutions with the L4Re Hypervisor family

Kernkonzept's L4Re Hypervisor family offers a comprehensive, flexible, and secure platform that fully meets today's requirements of the automotive industry. By utilizing its unique architecture and comprehensive separation mechanisms, OEMs and suppliers can effectively implement the complex requirements of software-defined vehicles and ensure a high level of security and performance.

+ **Software design can start immediately after IP release on Arm Virtual Platform**
+ **Higher quality, faster time to market**
+ **L4Re integration with SOAFEE reference platform EWAOL**

Credits: Adobe Stock p. 6/9/14/18/19; Arm (John Kourentis) p. 23

Kernkonzept GmbH
0351/41883232
contact@kernkonzept.com
Buchenstraße 16b
01097 Dresden