PHYTEC

Always the right level of
security for your product.

Embedded Security

Security is a continuous process that accompanies your project from development to the end of life in all of its changing phases. The starting point for this is our many years of experience in module development and in the most diverse security requirements of our customer projects.

Take advantage of our expertise to reach your goal faster and more cost-effectively. See security as an opportunity to stand out from the competition.

Smarter. Faster. Easier.

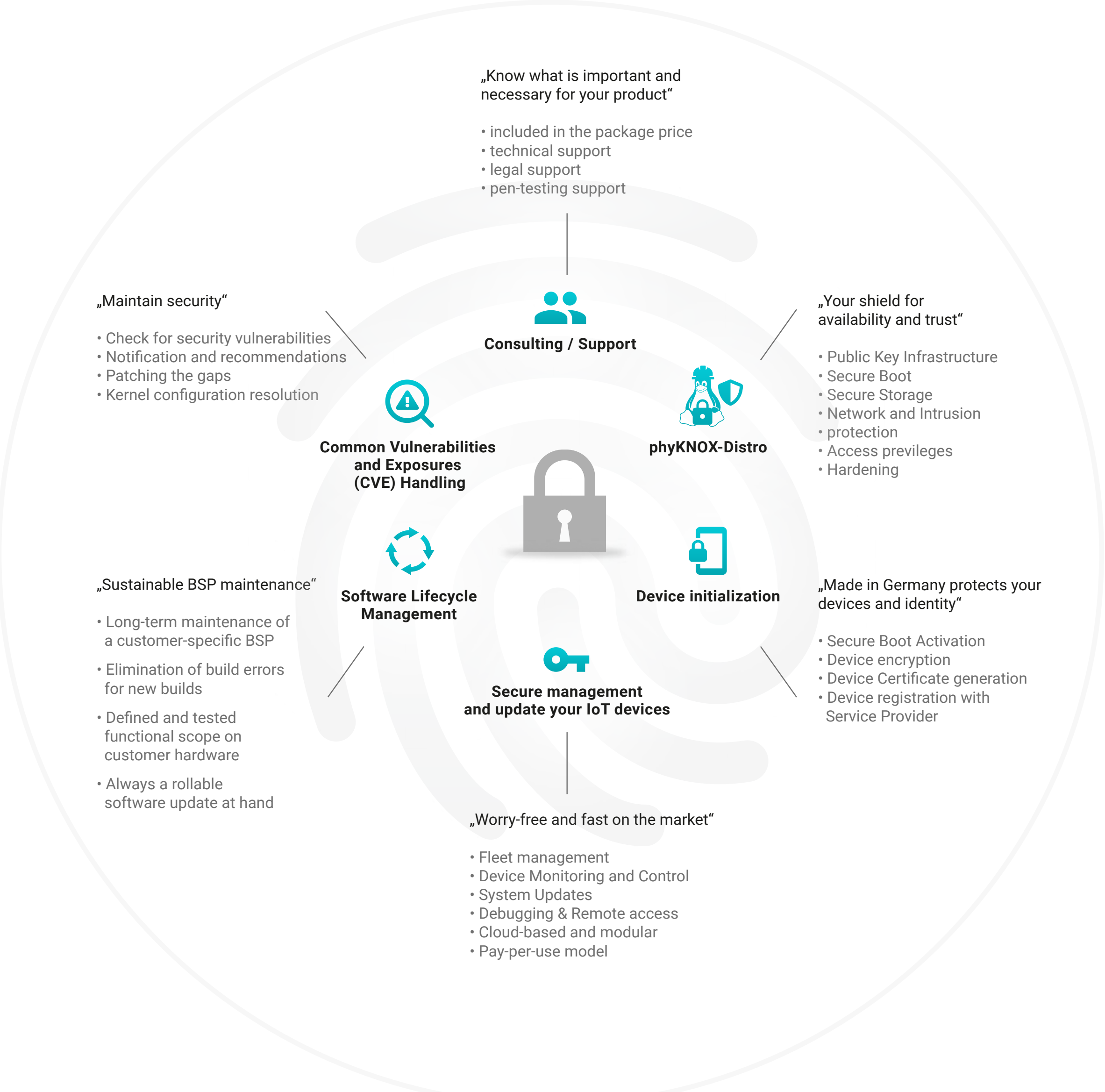
System protection

There are many reasons why you should take care of the protection of your System at the beginning of development. These reasons include project risk, attack risk, time to market, cost savings, focus on in-house expertise, protection against extortion or other misuse, etc.

What can be protected: Knowledge, image, monetary data, secret data, and compliance with legal requirements.

Your systems can benefit from:

- Secure data acquisition and transmission
- Know-How protection and data security on the device
- Encrypted personal data and secured connection to servers (on the Internet)
- Protection against device tampering and misuse
- Fulfillment of legal requirements - compliance



„Know what is important and necessary for your product"

- included in the package price
- technical support
- legal support
- pen-testing support

„Maintain security"

- Check for security vulnerabilities
- Notification and recommendations
- Patching the gaps
- Kernel configuration resolution

„Your shield for availability and trust"

- Public Key Infrastructure
- Secure Boot
- Secure Storage
- Network and Intrusion protection
- Access previleges
- Hardening

„Sustainable BSP maintenance"

- Long-term maintenance of a customer-specific BSP
- Elimination of build errors for new builds
- Defined and tested functional scope on customer hardware
- Always a rollable software update at hand

„Made in Germany protects your devices and identity"

- Secure Boot Activation
- Device encryption
- Device Certificate generation
- Device registration with Service Provider

„Worry-free and fast on the market"

- Fleet management
- Device Monitoring and Control
- System Updates
- Debugging & Remote access
- Cloud-based and modular
- Pay-per-use model

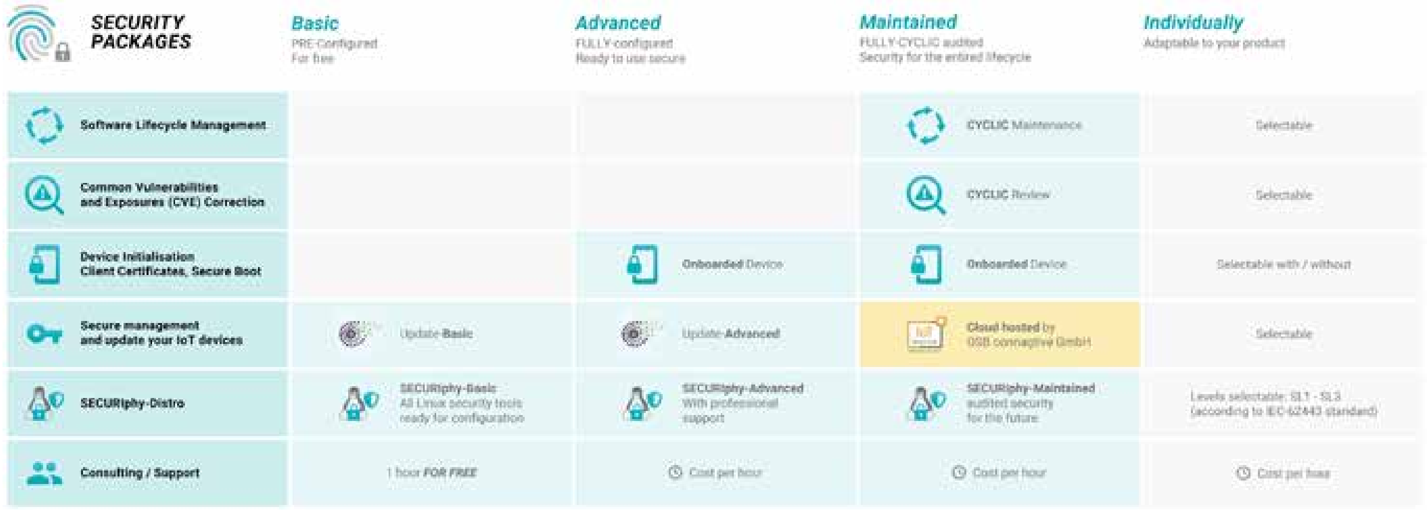
Consulting / Support
Common Vulnerabilities and Exposures (CVE) Handling
phyKNOX-Distro
Software Lifecycle Management
Device initialization
Secure management and update your IoT devices

Our offers for different security levels

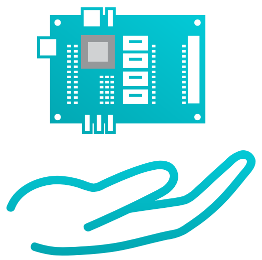
The table below provides an overview of the available security packages. The packages were developed based on extensive experience and cover a large number of typical application scenarios. When compiling the offerings, we have ensured that as much functionality as possible is usable, the offerings offer a high level of security, systems can be maintained over the long term, an offer can be put together individually, and these offers receive optimal professional support in the form of technical assistance with projects. What is important here is the clear structuring between finished components and customer-specific adaptations, which always lead to costs.

WE HAVE PUT TOGETHER FOUR SECURITY OFFERS

Our basic offer is free of charge, and you can use all of our hardware, you can use all of our upstream services. In the advanced offer how we can help you individually to achieve a higher level of security. The maintained offer shows how your system can be kept secure over a longer period of time.



SECURITY PACKAGES	Basic PRE-configured For free	Advanced FULLY-configured Ready to use secure	Maintained FULLY-CYCLIC audited Security for the entired lifecycle	Individually Adaptable to your product
Software Lifecycle Management			CYCLIC Maintenance	Selectable
Common Vulnerabilities and Exposures (CVE) Correction			CYCLIC Review	Selectable
Device Initialisation Client Certificates, Secure Boot		Onboarded Device	Onboarded Device	Selectable with / without
Secure management and update your IoT devices	Update-Basic	Update-Advanced	Cloud hosted by OSB connagtive GmbH	Selectable
SECURIphy-Distro	SECURIphy-Basic All Linux security tools ready for configuration	SECURIphy-Advanced With professional support	SECURIphy-Maintained audited security for the future	Levels selectable: SL1 - SL3 (according to IEC-62443 standard)
Consulting / Support	1 hour FOR FREE	Cost per hour	Cost per hour	Cost per hour



In practice, reaching even the first safety level is already a significant improvement in protecting your product.
This level can prevent security gaps caused by application errors. DIN 62443, as the basis for the assessment of security levels, is also suitable for classification according to the ESCO Cybersecurity Act, which has been introduced in 2020 for manufacturers of technical devices.

Our Offer
Consulting and Support

At PHYTEC, we can advise you on an individual basis on security issues relating to your project. Even the choice of controller has an influence on the available security features of your end product. We are happy to support you in the selection of the controller and possible additional modules. Together, we can determine the necessary protective measures for your product.

CONCEPTS

The concepts provide a comprehensive overview of the subject matter and indicate which topics are taken into account.

- **Legal aspects** - standards and guidelines - what does the law require?
- **Basics** (security pyramid) - from the module to the runtime - Which protection measures are available?
- **Security by Design** - Developing secure products - How is security considered in the product development process?
- **System security** - Analysis and implementation – Security requirements
- **Secure initialization** - Security features in production - How do your keys get access to the module?
- **Software Lifecycle Management** - Software maintenance and updates after delivery - How do you provide your product

The concepts of security are based on confidentiality and on individually adapted concepts.

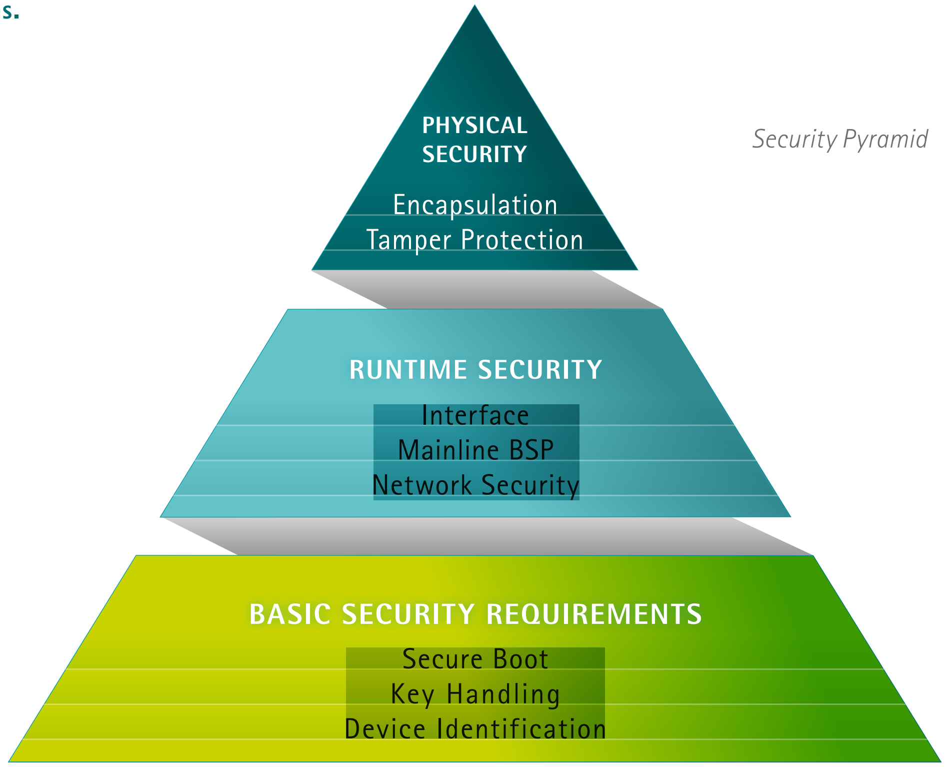
We are also happy to offer you customizable workshops and project consulting. Start with an expert discussion:
www.phytec.eu/en/expertengespraech

CONSULTATION

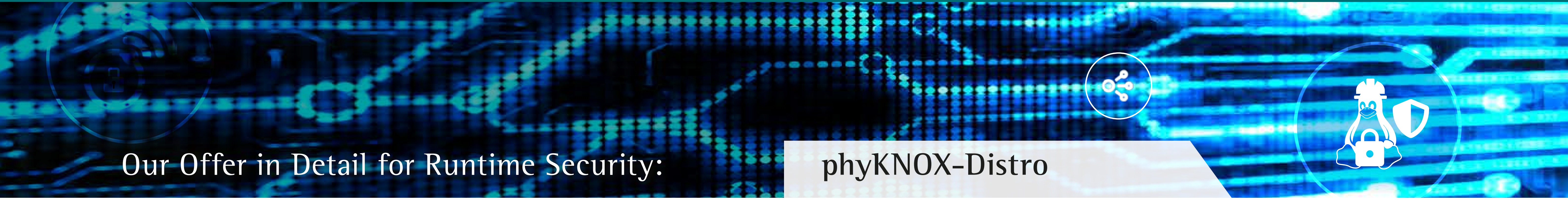
Many things can already be realized with the features of the controller, peripherals, memory, and operating system. We use solutions from different hardware manufacturers. For software, we rely on open source solutions. Our starting point is the knowledge of these features and the concepts and solutions behind security.

There are different solutions depending on the application:
- Secure-Boot ensures that only trustworthy software is executed on your module
- Depending on the application, the use of crypto chips / secure elements is recommended for the storage of keys and certificates (key handling)
- A unique identity may be required to identify your devices on networks
- When communicating via the network, we recommend the use of TLS for encryption
- The use of Mainline Linux allows for the long-term care of the product

All possible measures to defend against attacks can be roughly divided into three areas.



Security Pyramid



Our Offer in Detail for Runtime Security:

phyKNOX-Distro

YOUR PROTECTIVE SHIELD FOR AVAILABILITY AND TRUST

The PHYTEC-BSP is already equipped with many features that you can use to secure your product. The **phyKNOX-Distro** activates corresponding security features in the Board Support Packages. For example, if Secure Boot is activated, all images are signed and the boot loader is configured so that no unsigned images can be started. Here is an excerpt of the settings made during activation.

Our know-how for you
Expert talk free of charge

IT'S LIKE A PUZZLE

Your new project is in pieces in front of you, but which processes and interfaces are target-oriented? You are stuck in the middle of the project, but at one point? A puzzle is just a game. A PHYTEC expert will help you with your projects that have market-ready products in their sights.

PHYTEC embedded experts bring you further in your projects in an advisory capacity, because they...

- give a new perspective on things
- ask questions that help you move forward
- give structure to your project
- have years of experience
- are specialists in their field
- grow with challenges

Six experts are available to you on six specialist topics.

More info and all experts at a glance,
including direct appointment by calendar:
https://www.phytec.eu/en/expertengespraech

	phyKNOX-Distro **Basic** SL 1 / SL 2	phyKNOX-Distro **Advanced** SL 2 / SL 3	phyKNOX-Distro **Maintained** SL 2 / SL 3	phyKNOX-Distro **Individual**
General	Processing of slightly sensitive data such as measurement data or control data, where no high damage occurs in case of manipulation. The failure of a few devices has **no** influence on the overall system	Processing of sensitive data – control data, measurement data or personal data, where sub-sequent damage can occur in case of manipulation or the device takes over control tasks The failure of a few devices has an impact on the entire system		Level individually selectable
Development Support Maintained by SLCM with new kernel and Yocto versions and regular LTS patches		Public key infrastructure generation and action concept. Use of hardware secure modules		individually selectable
Basic Security Secure Boot	Authenticated Boot (Secure Boot)	Authenticated Boot (Secure Boot) Measured Boot (TPM)		individually selectable
Secure Key Storage	Trusted Platform Module Support **Basic Support** Trusted Execution Environment **Basic Support**	Trusted Platform Module Support **Advanced Support** Trusted Execution Environment **Advanced Support**		individually selectable
Secure Storage	Encrypted Root File System integrety (Data Errors)	Read only Filesystem encrypted partial Filesystem authenticated Filesystem (Manipulation detection)		individually selectable
Hardening	depend on Machine Features	advanced hardening		individually selectable
Runtime Security Secure Updates	RAUC Update Client offline Update (USB)	RAUC Update Client Network Update with Hawkbit	Feature support for the IOT suite from our partner OSB connagtive GmbH	individually selectable
Remote Access		supported	with IOT Suite	individually selectable
Network Security		Access control Firewall Policies WLAN / Bluetooth Configuration wireguard or VPN Configuration		individually selectable
Intrusion Protection		Access monitoring adapted to Use Case		
Access Control	exemplary use of individual passwords	adapted to Use Case use of tokens or keys		individually selectable
Device Monitoring			with IOT Suite	individually selectable
Casting		optional		individually selectable
Maintenance Maintained by SLCM with new kernel and Yocto versions and regular LTS patches			Check for function in conjunction with SLCM and CVE analysis	individually selectable

Security Offers

Our offer in detail
Device initialization – our concept

MADE IN GERMANY PROTECTS YOUR DEVICES AND YOUR IDENTITY

Most methods for securing devices and software are based on asymmetric cryptography using a connected public key infrastructure (PKI). To do this, you often need a different number of certificates, with public and private keys. Managing and protecting these certificates and private keys is a big challenge. The private keys must be protected throughout their entire lifecycle.

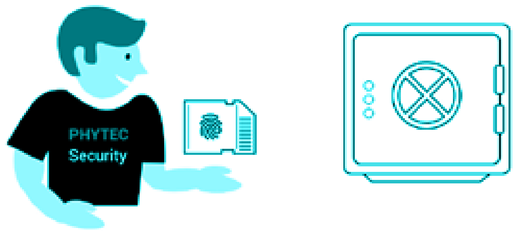
PHYTEC is your partner for these tasks and can guarantee the security of your private keys and other secrets with its production concept.

PARTNERSHIP BUILDS TRUST

PHYTEC you can trust! As a reliable partner for the implementation of your business ideas, we make protecting your secrets a top priority. We ensure the encrypted and verified transmission of your information for the realisation of your projects.

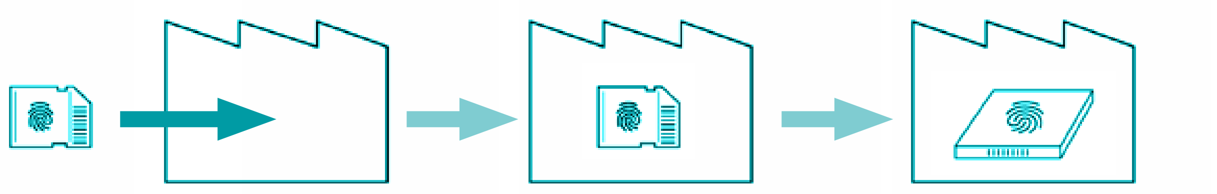
SECURE STORAGE

We protect your company secrets throughout the entire product lifecycle. We ensure safe storage on a specially developed system that is not connected to the company network. Strict access controls ensure maximum security.



- Strict access controls
- Not on the company network
- Physically separated network connection to production (software installation)

SAFE INTRODUCTION INTO THE PRODUCT



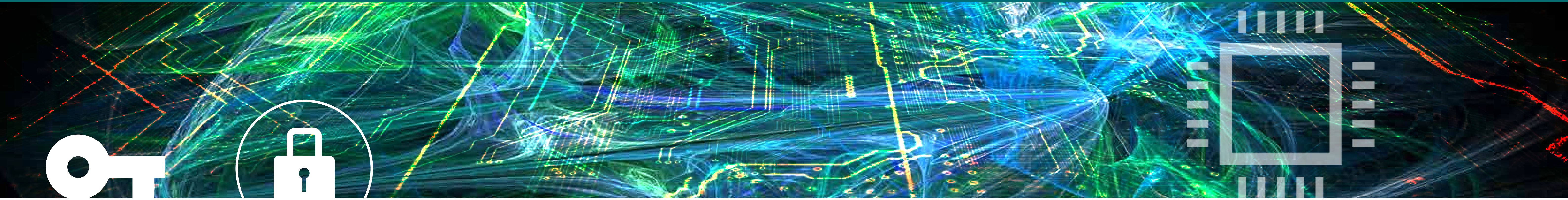
To ensure safe device initialization, PHYTEC has set up the implementation of a safe initialization zone in the new production facilities.

All safety-relevant functions of your device are activated within this safety zone. The use of special hardware security modules (HSM) during the initialization process ensures that your secrets remain confidential. The transfer of cryptographic keys to your end device takes place in the security zone with special access controls. This is how we ensure the highest level of security: whether it's patent-protected software, cryptographic keys for checking software updates, or certificates for unique device identification on the Internet: We bring your solutions securely to your product!

- No direct access to private keys in the test environment
- Use of HSM modules to protect private keys
- Physically independent network for the entire process

PROTECT YOUR PRODUCT UNTIL DELIVERY

We take care of the protection of your products during the entire production process and during storage, after installation of your customer software. We design the procedure up to the agreed delivery time according to your requirements.



Our offer in detail
Securely manage and update your IoT devices

COMPARISON OF RAUK/HAWKBIT FUNDAMENTALS OFFERING AND THE IOT SUITE

Offer RAUC and hawkBit
- All technical requirements to develop your own update and device management system
- Free of charge

Do-it-yourself
With the combination of RAUC as a secure update client and the use of hawkBit as an update server, all technical requirements for the self-hosted development of an update and device management system.

OSB offer with the IOT Suite
- Everything ready
- Customization and maintenance can be ordered from the partner
- No investment crisis

All-in-one IoT Suite
The partnership with OSB connagtive allows to build on already existing solutions. With the IoT-Suite, a ready-to-use system with many useful features is available without own investment risk, but with the possibility for individual adaptations and the saving of years of development work.

Test the IOT Suite as part of our kit offer.

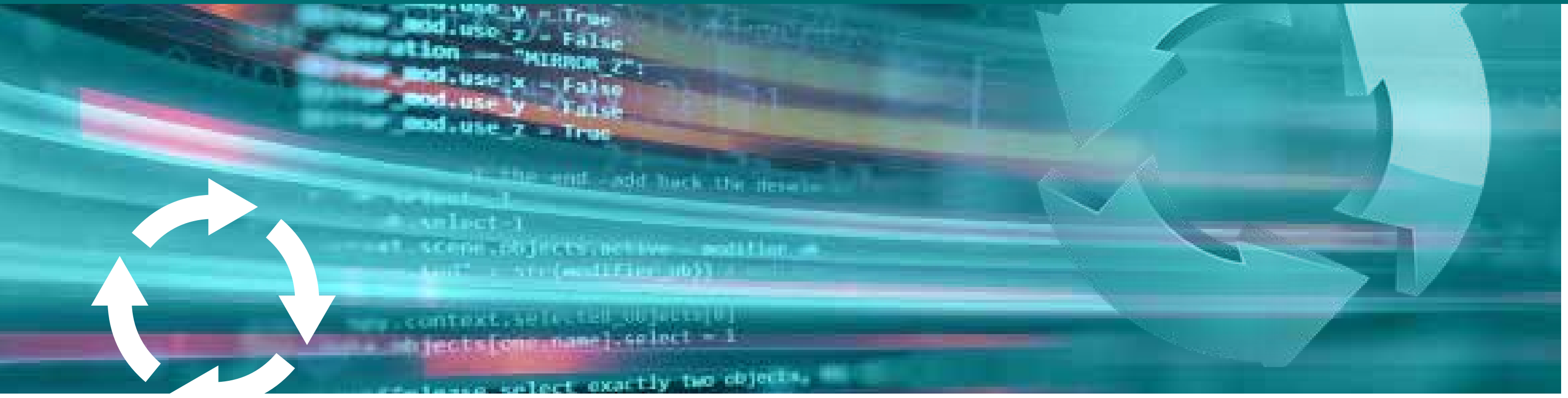
PHYTEC
Update + Device Management Kit
IoT Device Management for Your Cutting Edge
IoT
Device Suite
EMBEDDED SECURITY

Scan QR code now:
www.phytec.eu/en/produkte/development-kits/update-und-devicemanagement-kit/?lang=en/

COMPARISON OF THE DO-IT-YOURSELF AND THE ALL-IN-ONE IOT SUITE SOLUTION

Provided by	Feature	Do It Yourself Rauc & Hawkbit	All in One IOT Device Suite
PHYTEC	Update Client	⊕	⊕
	Update Server	⊕	⊕
	Automatic Onboarding	⊕	⊕ (optional)
PHYTEC / IOT Suite	Secure Connection	⊕	⊕⊕
	Identity sharing with foreign services	⊖	⊕ (optional)
IOT Suite connagtive	Update of partitions or Differential (Blockbased)	⊕	⊕
	Transparently manage large Fleets	⊕	⊕⊕
	Lucid Dashboard	⊕	⊕⊕
	Device Health and Status Information	⊖	⊕ (optional)
	Signed Update Images	⊖	⊕ (optional)
	SIM Card Management wherever SIM	⊖	⊕ (optional)
	Remote Maintenance Access	⊖	⊕ (optional)
	Device grouping	⊕	⊕ (optional)
	Worldwide Hosting	⊖	⊕ (optional)
	Scheduled roll outs	⊖	⊕ (optional)
PHYTEC / embedded data	Edge data visualization server	⊖	⊕ (optional)
	Sensor Data Aggregation	⊖	⊕ (optional)
embedded data	Process data transfer	⊖	⊕ (optional)
	Process data visualization	⊖	⊕ (optional)

We help you choose the right system for your project:
contact@phytec.de
www.phytec.eu/en/startseite/



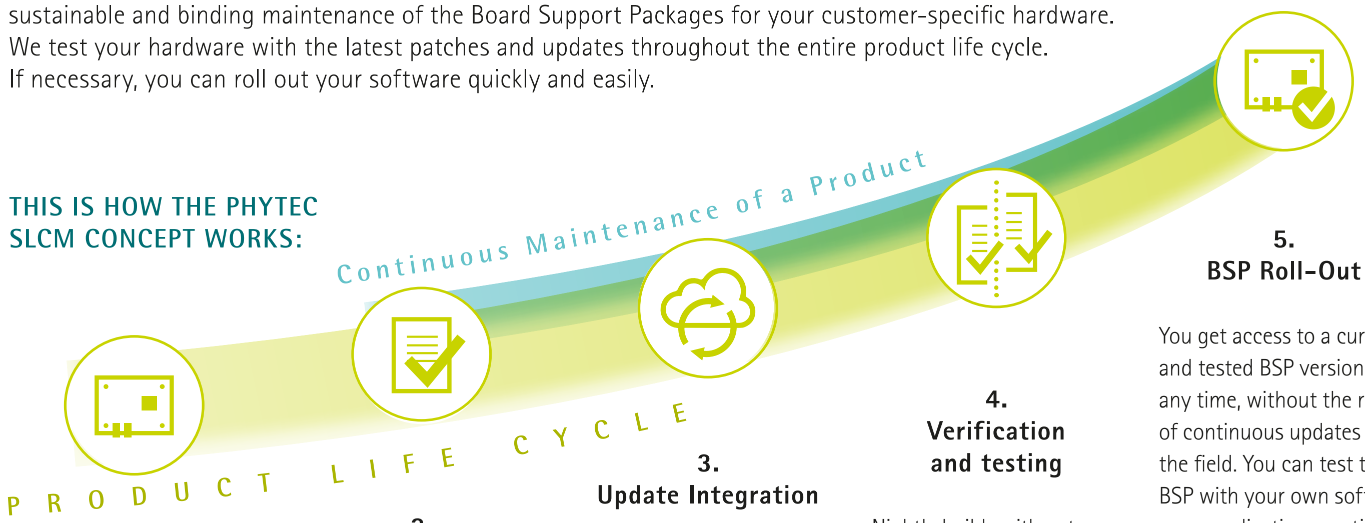
Our offer in detail
Software Lifecycle Management

YOU DEVELOP YOUR PRODUCTS FOR A LONG LIFE CYCLE – YOUR SOFTWARE TOO?

Security and data protection requirements are increasing – as are the number of attacks, security vulnerabilities and identified risks. You have to face these ever-changing security threats and ensure that your systems can be updated when they are connected to the Internet. The current IEC 62443 standard, for example, also requires this in the Patch Management in the Industrial Automation Control System Environment section.

The PHYTEC Software Lifecycle Management Service supports you in this. Take advantage of our offer for sustainable and binding maintenance of the Board Support Packages for your customer-specific hardware. We test your hardware with the latest patches and updates throughout the entire product life cycle. If necessary, you can roll out your software quickly and easily.

THIS IS HOW THE PHYTEC SLCM CONCEPT WORKS:



1. Development of your BSPs

We develop a customer-specific BSP for your PHYTEC hardware, based on the preliminary work of the standard development. We integrate hardware and BSP into our test farm and the CI system.

2. Roadmap planning

Together with you, we create an update strategy for your product and determine the frequency of updates. In general, we agree on annual major updates of the Yocto Project and biannual updates of the LTS kernel version.

3. Update Integration

Two BSP statuses are maintained in parallel. The first is an up-to-date version of your BSP, which we constantly supply with security and bug fixes over an agreed period of time. The other is a version in which we continuously update your BSP to the latest development status of the Yocto Project and Linux kernel. This provides a perfect basis for your next stable software release.

4. Verification and testing

Nightly builds with automatic tests quickly detect and resolve conflicts with your BSP. At the same time, we continuously check that the BSPs comply with your specifications. All results are recorded for you in test protocols.

5. BSP Roll-Out

You get access to a current and tested BSP version at any time, without the risk of continuous updates in the field. You can test the BSP with your own software applications routinely or as soon as a relevant vulnerability is detected, and play it out promptly.

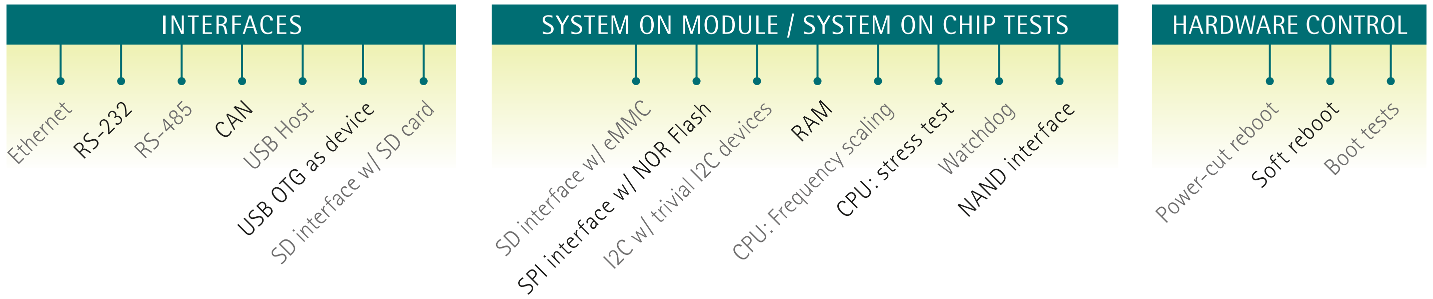
The RAUC Robust Auto-Update Controller, which is prepared in our BSPs, supports you in this. In addition, we provide you with updates of your BSP including current kernel and Yocto versions according to the agreed strategy.

General Conditions

Prerequisites for software lifecycle management are the use of a Mainline-Linux based BSP and the existence of a BSP specification that covers the entire functionality of the platform. An automated test environment is used to test the complete functionality of the system according to the BSP specification. The tests primarily include the interfaces, drivers and connections created on the boards. Customer applications are usually not included in the test.

The standard tests include "common" interfaces according to the graph below. Special interfaces or special protocols can be added individually by extending the test specification; this may require the creation of special test hardware. For testing, the Jenkins-based Continuous Integration System is linked to the test environment for automatic hardware testing. This makes the setup ideal for the continuous integration of standard board support packages and customized BSPs.

STANDARD TEST FOR CUSTOMIZED HARDWARE AND BSPS



INTERFACES
- Ethernet
- RS-232
- RS-485
- CAN
- USB Host
- USB OTG as device
- SD interface w/ SD card

SYSTEM ON MODULE / SYSTEM ON CHIP TESTS
- SD interface w/ eMMC
- SPI interface w/ NOR Flash
- I2C w/ trivial I2C devices
- RAM
- CPU: Frequency scaling
- CPU: stress test
- Watchdog
- NAND interface

HARDWARE CONTROL
- Power-cut reboot
- Soft reboot
- Boot tests

A positive side effect of the setup is the clear separation of BSP, middleware and application software. This allows the individual layers to be handled individually if required, without errors resulting from dependencies not taken into account.

Deployment MADE EASY!

We facilitate the roll-out of your software into the field by preparing the RAUC Robust Auto-Update Controller in all current BSPs. The update client ensures the reliable installation of signed BSP updates on the embedded systems and is supported by Yocto in the meta-rauc layer. BSP updates can be created, checked and modified on the host system using the tool.

PHYTEC supports you both in implementing the update mechanisms and in creating the appropriate infrastructure – from RAUC configuration and setting up cloud services to protecting the hardware from installing malicious software.

STRUCTURE OF THE BSP LAYERS		
CUSTOMER APPLICATION Yocto Project	• meta-cust etc.	Care provided by the customer
TESTS	Optional service from PHYTEC	
BSP-SPECIFICATION		Required for SLCM
Yocto Project	• meta-ksp • poky • meta-openembedded • meta-phytec • meta-yogurt • meta-rauc • meta-qt5	Care provided by PHYTEC

Benefit from our further services!

- Hardening & Secure Boot
- Security consulting for hardware & software design
- Key and certificate handling at our production facility in Germany
- Cloud platforms for the roll-out of updates

Talk to us about your individual offer for software lifecycle management!

contact@phytec.de
+ 49 (0) 6131/ 9221-32

Our offer in detail
Common Vulnerabilities and Exposures analysis (CVE)

A security vulnerability represents a threat to the security of a computer system. There is a risk that the vulnerability can be exploited and the affected computer system compromised.

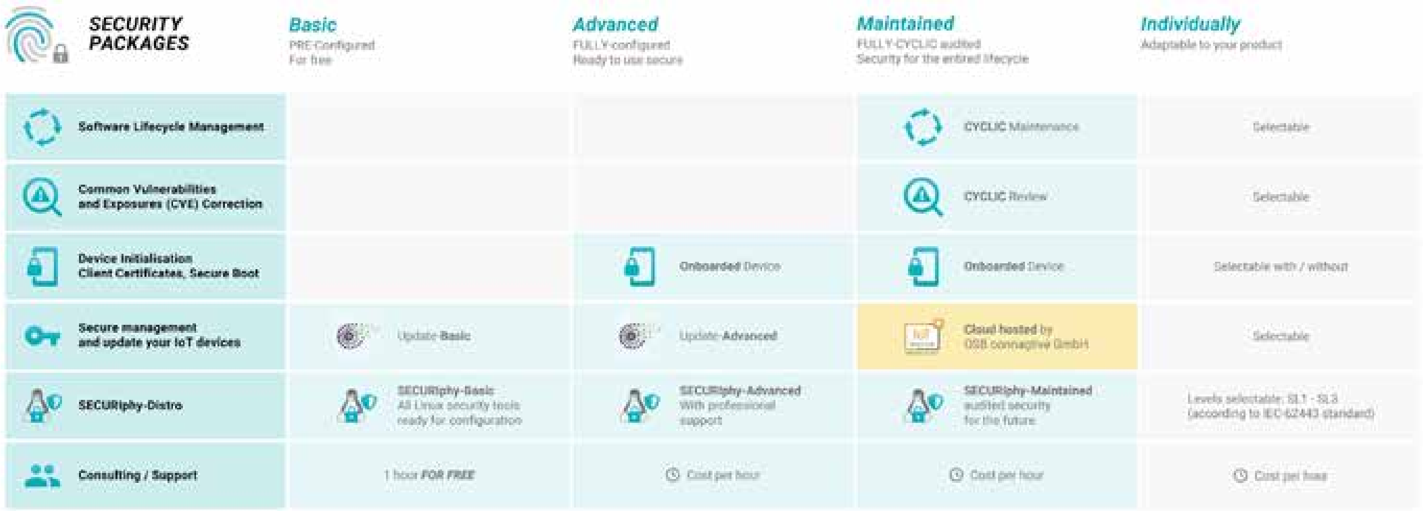
Among other things, security vulnerabilities arise from inadequate protection of an embedded device against attacks from the network and from programming errors in the operating system, services or middleware operated on the system. However, errors in the hardware can also lead to security vulnerabilities.

Security vulnerabilities are maintained and evaluated by Mitre Corporation using a referencing system. In our service we also consult other sources in order to be able to react quickly.

Benefit from our security services throughout the lifecycle of your products.

	CVE **Basic**	CVE **Advanced**	CVE **Maintained**	CVE **Individual**
Intended use	as a basis for own developments	as proof for an audit or at the end customer	To keep an eye on one's own image in order to be able to react quickly to security gaps	For applications in critical infrastructure we recommend the cooperation with our specialized partner
Can be combined with other PHYTEC offerings	⊖	⊖	✓ with SLCM available patches can be applied directly	✓ with products from partner companies
Software scope	bootloader, kernel and middleware of a PHYTEC minimal image	bootloader, kernel and middleware of a defined customer image		
Number of checks	once when creating the image		cyclically once per day	selectable
Multiple sources as basis for evaluation	✓	✓	✓	✓
Examination of the active software parts with Kernel and U-boot (reduction of the CVEs)	✓	✓	✓	✓
U-boot and kernel config (if can be determined)	✓	✓	✓	✓
CVE Summary Report	✓	✓	✓	✓
REST API access	⊖	⊖	✓	✓
CVE filtering by CVSS score or attack vector	⊖	⊖	✓	
Recommended action	⊕	generally determined according to criteria		⊕ ⊕ according to use case and application
Notification when new CVEs are found	⊖	⊖	✓	✓
Provision of available patches	⊖	⊖	✓	✓

Always the right level of security for your product.



SECURITY PACKAGES	Basic PRE-Configured For free	Advanced FULLY-configured Ready to use secure	Maintained FULLY-CYCLIC audited Security for the entired lifecycle	Individually Adaptable to your product
Software Lifecycle Management			CYCLIC Maintenance	Selectable
Common Vulnerabilities and Exposures (CVE) Correction			CYCLIC Review	Selectable
Device Initialisation Client Certificates, Secure Boot		Onboarded Device	Onboarded Device	Selectable with / without
Secure management and update your IoT devices	Update-Basic	Update-Advanced	Cloud hosted by OSB connagtive GmbH	Selectable
SECURIphy-Distro	SECURIphy-Basic All Linux security tools ready for configuration	SECURIphy-Advanced With professional support	SECURIphy-Maintained audited security for the future	Levels selectable: SL1 - SL3 (according to IEC-62443 standard)
Consulting / Support	1 hour FOR FREE	Cost per hour	Cost per hour	Cost per hour

PHYTEC

Security Embedded

Headquarters | Subsidiaries

Germany
PHYTEC Messtechnik GmbH
D-55129 Mainz
t +49 6131 9221-32
f +49 6131 9221-33
www.phytec.de

France
PHYTEC France SARL
F-72140 Sillé le Guillaume
t +33 2 43 29 22 33
f +33 2 43 29 22 34
www.phytec.fr

North America
PHYTEC America LLC
Bainbridge Island, WA 98110
t +1 206 780-9047
f +1 206 780-9135
www.phytec.com

India
PHYTEC Embedded Pvt. Ltd.
HSR Layout
Bangalore 560102
t +91 80 408670-46/49
www.phytec.in

China
PHYTEC Information Technology Co. Ltd.
Nanshan District, Shenzhen
518026 PRC
t +86 755 6180 2110
www.phytec.cn