PHYTEC

Immer das richtige Maß
an Security für Ihr Produkt.

Embedded Security

Security ist ein kontinuierlicher Prozess, der ihr Projekt von der Entwicklung bis zum End of Life in jeder sich veränderten Phase begleitet. Ausgangspunkt hierfür ist unsere langjährige Erfahrung in der Modulentwicklung und zu den unterschiedlichsten Sicherheitsanforderungen unserer Kundenprojekte.

Nutzen Sie unsere Expertise, um schneller und günstiger an Ihr Ziel zu kommen.
Sehen Sie Security als Chance, um sich vom Wettbewerb abzuheben.

Smarter. Faster. Easier.

Schutz von Systemen

Es gibt viele Gründe, warum Sie sich um den Schutz Ihres Systems zu Beginn der Entwicklung kümmern sollten. Zu diesen Gründen gehören Projektrisiko, Angriffsrisiko, Markteinführungszeit, Kosteneinsparungen, Konzentration auf das eigene Fachwissen, Schutz vor Erpressung oder anderem Missbrauch usw.

Was kann geschützt werden: Wissen, Image, geldwerte Daten, geheime Daten sowie die Erfüllung rechtlicher Anforderungen.

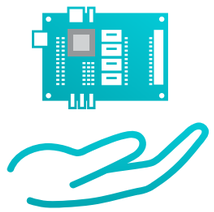
Ihre Systeme können davon profitieren durch:
- Sichere Datenerfassung und -übertragung
- Know-How-Schutz und Datensicherheit auf dem Gerät
- Verschlüsselte persönliche Daten und gesicherte Verbindung zu Servern (im Internet)
- Absicherung gegen Gerätemanipulation und -missbrauch
- Erfüllung gesetzlicher Anforderungen – Compliance

Unsere phyKNOX®-Angebote für verschiedene Securitylevel
Die nachstehende Tabelle gibt einen Überblick über die verfügbaren Sicherheitspakete. Die Pakete wurden nach umfangreichen Erfahrungen entwickelt und decken eine große Anzahl typischer Anwendungsszenarien ab. Bei der Zusammenstellung der Angebote haben wir darauf geachtet, dass möglichst viel Funktionalität nutzbar ist, dass die Angebote ein hohes Maß an Sicherheit bieten, dass die Möglichkeit besteht, Systeme langfristig zu warten, dass ein Angebot individuell zusammengestellt werden kann und dass Sie eine optimale fachliche Unterstützung in Form von technischer Hilfe bei Projekten erhalten. Wichtig ist dabei die klare Strukturierung zwischen fertigen Komponenten und kundenspezifischen Anpassungen, die immer zu Kosten führen.

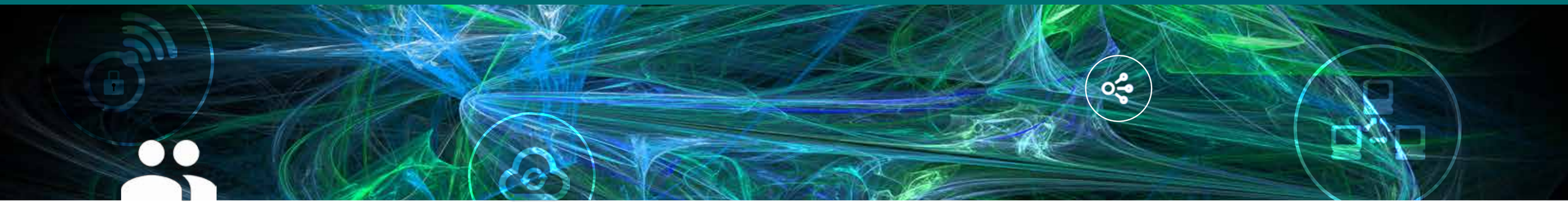
SECURITY PACKAGES	***Basic*** PRE-Configured kostenlos	***Advanced*** Mit professioneller Unterstützung	***Maintained*** Langfristig gepflegte Sicherheit	***Individual*** Anpassbar an Ihre Bedürfnisse
Software Lifecycle Management			**Zyklische BSP-Pflege**	frei wählbar
Common Vulnerabilities and Exposures (CVE) Behebung			**Zyklischer CVE-Scan**	frei wählbar
Geräteinitialisierung Client Certificates, Secure Boot		**inklusive**	**inklusive**	wählbar mit / ohne
Sicheres Management und Update Ihrer IoT-Geräte	Update-**Basic**	Update-**Advanced**	Update-**Advanced**	FOUNDRIES.IO, RAUC, Memfault
SECURIphy-Distro	**SECURIphy-Basic** Alle Linux-Securitytools bereits vorbereitet	**SECURIphy-Advanced** Mit professioneller Konfigurationsuntersützung	**SECURIphy-Maintained** Alle Linux-Securitytools langfristig gepflegt	frei wählbar
Consulting / Support	1 Stunde ***KOSTENFREI***	Kosten pro Stunde	Kosten pro Stunde	Kosten pro Stunde

WIR HABEN VIER SECURITY-ANGEBOTE GESCHNÜRT

Unser Basic-Angebot ist kostenlos, Sie können mit unserer Hardware alle Vorleistungen nutzen. Im Advanced-Angebot zeigen wir, wie wir individuell helfen können, ein höheres Maß an Sicherheit zu erreichen. Das Maintained-Angebot zeigt, wie Ihr System über einen längeren Zeitraum sicher gehalten werden kann.



In der Praxis ist schon das Erreichen des ersten Sicherheitslevels eine deutliche Verbesserung des Schutzes für Ihr Produkt. Durch dieses Level können Sicherheitslücken, die durch Anwendungsfehler entstehen, verhindert werden. Die DIN 62443, als Grundlage für die Einschätzung der Sicherheitslevel, ist auch geeignet, um eine Einstufung nach dem Cybersecurity Act der ESCO vorzunehmen, die ab 2020 für die Hersteller von technischen Deviceen eingeführt wurde.



Unser Angebot
Beratung und Support

Wir bei Phytec können Sie bei Security-Fragen zu Ihrem Vorhaben individuell beraten. Bereits die Wahl des Controllers hat Einfluss auf die verfügbaren Security-Features Ihres Endprodukts. Gerne unterstützen wir Sie bei der Auswahl des Controllers und möglichen Zusatzbausteinen. Wir bestimmen mit Ihnen gemeinsam die notwendigen Schutzmaßnahmen für Ihr Produkt.

KONZEPTE

Die Konzepte geben einen umfassenden Überblick über die Thematik und zeigen an welche Themengebiete berücksichtigt werden.

- **Rechtliche Aspekte** – Normen und Richtlinien
  Was schreibt der Gesetzgeber vor?
- **Grundlagen** (Security Pyramide) – vom Modul bis zur Laufzeit
  Welche Schutzmaßnahmen gibt es?
- **Security by Design** – Entwickeln von sicheren Produkten
  Wie wird Security im Produktentwicklungsprozess berücksichtigt?
- **Sicherheit im System** – Analyse und Umsetzung – Security-Anforderungen
- **Sichere Initialisierung** – Sicherheitsfeatures in der Produktion
  Wie kommen Ihre Schlüssel auf das Modul?
- **Software-Lifecyle-Management** – Softwarepflege und Updates nach Auslieferung
  Wie versorgen Sie Ihr Produkt mit Updates?

Die Security-Konzepte basieren auf Vertraulichkeit, ebenso wie auf individuell angepassten Lösungen.

Gerne bieten wir Ihnen auch individuell anpassbare Workshops und Projektberatung an. Starten Sie mit einem Expertengespräch:

www.phytec.de/expertengespraech/

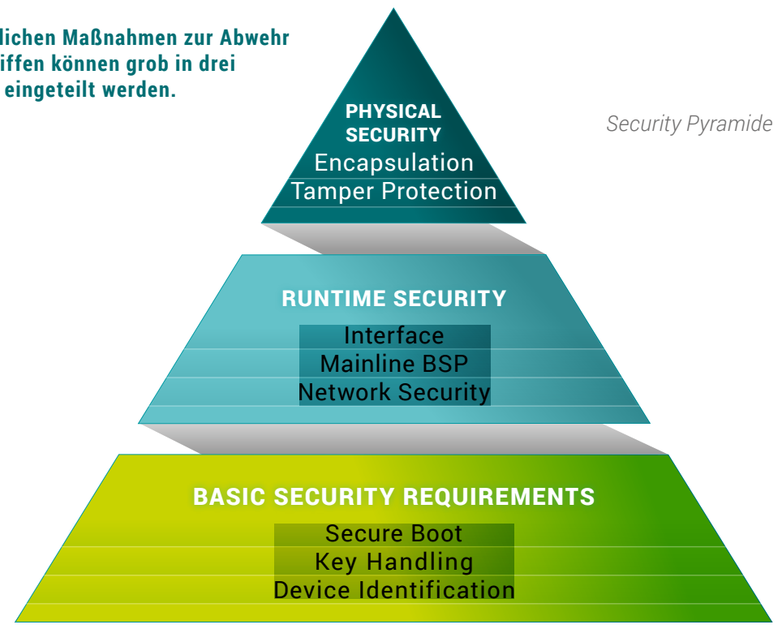
BERATUNG

Vieles kann schon mit den Features des Controllers, der Peripherie, Speicher und des Betriebssystems realisiert werden. Wir setzen Lösungen von unterschiedlichen Hardware-Herstellern ein. Bei Software setzen wir auf Open-Source-Lösungen. Ausgangspunkt ist das Wissen über diese Features und der sich hinter Security verbergenden Konzepte und Lösungswege.

Je nach Anwendungsfall gibt es verschiedene Lösungen:

- Mit Secure Boot wird sichergestellt, dass nur vertrauenswürdige Software auf Ihrem Modul ausgeführt wird
- Je nach Anwendungsfall empfiehlt sich die Verwendung von Krypto-Chips / Secure Elements zur Speicherung von Schlüsseln und Zertifikaten (Key-Handling)
- Für die Identifizierung Ihrer Geräte in Netzwerken kann eine eindeutige Identität erforderlich sein
- Bei der Kommunikation über das Netzwerk empfiehlt sich die Verwendung von TLS zur Verschlüsselung
- Die Verwendung von Mainline-Linux ermöglicht die langfristige Pflege des Produktes

Alle möglichen Maßnahmen zur Abwehr von Angriffen können grob in drei Bereiche eingeteilt werden.



Security Pyramide

Unser Angebot im Detail für Runtime Security: SECURIphy-Distro

IHR SCHUTZSCHILD FÜR VERFÜGBARKEIT UND VERTRAUEN

Das PHYTEC-BSP ist bereits mit vielen Funktionen ausgestattet, die Sie zur Absicherung Ihres Produktes verwenden können. Die phyKNOX-Distro aktiviert entsprechende Security Features im Board Support Package. Dabei werden z. B. bei Aktivierung von Secure Boot alle Images signiert und der Bootloader so konfiguriert, dass keine unsignierten Images mehr gestartet werden können. Hier ein Auszug der vorgenommenen Einstellungen bei Aktivierung.

Unser Know-How für Sie
Expertengespräch gratis

ES IST WIE BEI EINEM PUZZLE

Ihr neues Projekt liegt in Einzelteilen vor Ihnen, aber welche Prozesse und Schnittstellen sind zielführend? Sie stecken mitten im Projekt, aber an einer Stelle fest? Ein Puzzle ist nur ein Spiel. Bei Ihren Projekten, die marktreife Produkte im Visier haben, hilft ein PHYTEC-Fachmann.

PHYTEC Embedded Experten bringen Sie beratend in Ihren Projekten weiter, denn sie…

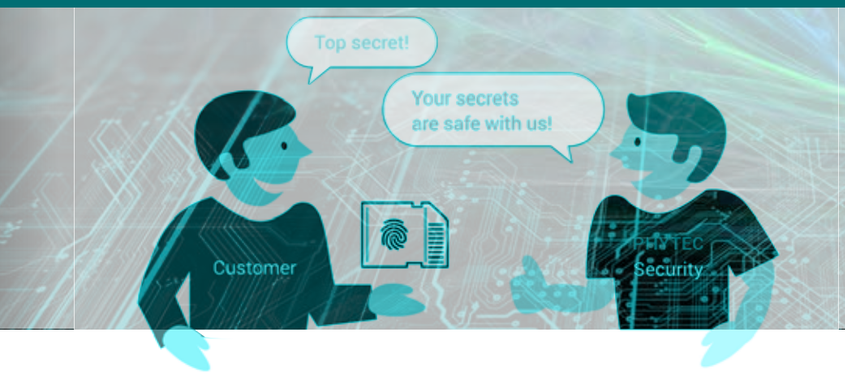
- geben eine neue Sicht auf die Dinge
- stellen Fragen, die voranbringen
- geben Ihrem Projekt Struktur
- haben jahrelange Erfahrung
- sind Spezialisten ihres Fachgebiets
- wachsen an Herausforderungen

Sechs Experten stehen Ihnen zu sechs Fachthemen zur Verfügung

Mehr Infos und alle Experten auf einen Blick,
inklusive direkter Terminvereinbarung per Kalender:

www.phytec.de/expertengespraech

	SECURIphy-Distro **Basic** SL 1 / SL 2	SECURIphy-Distro **Advanced** SL 2 / SL 3	SECURIphy-Distro **Maintained** SL 2 / SL 3	SECURIphy-Distro **Individual**
Generell	Verarbeitung leicht sensibler Daten wie Messdaten oder Steuerungsdaten, wo kein hoher Schaden bei Manipulation entsteht. Der Ausfall weniger Geräte hat keinen Einfluss auf das Gesamtsystem	Verarbeitung sensibler Daten – Steuerungsdaten, Messdaten oder personenbezogener Daten, wo Nachfolgeschäden bei Manipulation entstehen können oder das Gerät Steueraufgaben übernimmt Der Ausfall weniger Geräte hat einen Einfluss auf das Gesamtsystem		Stufe individuell wählbar
Development Support SLCM gepflegt mit neuen Kernel und Yocto Versionen und regelmäßige LTS		Public Key Infrastructure Erzeugungs- und Handlungskonzept Verwendung von Hardware Secure Modules		individuell wählbar
Basic Security Secure Boot	Authenticated Boot (Secure Boot)	Authenticated Boot (Secure Boot) Measured Boot (TPM)		individuell wählbar
Secure Key Storage	Trusted Platfom Module Support **Basic Support** Trusted Execution Environment **Basic Support**	Trusted Platfom Module Support **Advanced Support** Trusted Execution Environment **Advanced Support**		individuell wählbar
Secure Storage	Encrypted Root File System integrety (Data Errors)	Read only Filesystem encrypted partial Filesystem authenticated Filesystem (Manipulation detection)		individuell wählbar
Hardening	abhängig von den Eigenschaften der Maschine	erweitertes Hardening		individuell wählbar
Runtime Security Secure Updates	RAUC Update Client offline Update (USB)	RAUC Update Client Network Update mit Hawkbit	RAUC Update Client Network Update mit Hawkbit	individuell wählbar durch support von rauc, Mender.io, foundries oder anderen
Remote Access		supported	supported für SECURIphy-Advanced und SECURIphy-Maintained	individuell wählbar
Network Security		Zugriffsregelung: Firewall Richtlinien, WLAN / Bluetooth Configuration wireguard oder VPN Configuration		individuell wählbar
Intrusion Protection		Zugriffsüberwachung angepasst an Use Case		
Access Control	beispielhaft: Verwendung von individuellen Passwörtern	angepasst an Use Case Verwendung von Tokens oder Schlüsseln		individuell wählbar
Device Monitoring			supported für SECURIphy-Advanced und SECURIphy-Maintained	individuell wählbar
Vergießen		optional		individuell wählbar
Pflege SLCM gepflegt mit neuen Kernel und Yocto Versionen und regelmäßige LTS			In Verbindung mit SLCM und CVE Analyse auf Funktion prüfen	individuell wählbar



Sichere Geräteinitialisierung Provisioning

✔ SICHERE UMGEBUNG ✔ VERANTWORTUNGSVOLLER UMGANG MIT DATEN ✔ PRODUKTION IN MAINZ

Die meisten Methoden zur Absicherung von Geräten und Software basieren auf asymmetrischer Kryptographie unter Verwendung einer Public-Key-Infrastruktur (PKI). Hierbei benötigen Sie eine unterschiedliche Anzahl von Zertifikaten, bestehend aus öffentlichen und privaten Schlüsselpaaren. Die Verwaltung und der Schutz dieser Zertifikate und vor allem der privaten Schlüssel ist eine große Herausforderung. Die privaten Schlüssel müssen während des gesamten Lebenszyklus geschützt werden.

PHYTEC ist Ihr Partner für diese Aufgaben und kann mit seinem Produktionskonzept die Sicherheit Ihrer privaten Schlüssel und anderer Geheimnisse bei der Produktion/Software-einspielung mit übernehmen.

INITIALISIERUNG DES GERÄTS	ZERTIFIKATSERZEUGUNG UND GERÄTEREGISTRIERUNG
• Secure Boot-Aktivierung	Erstellung digitaler Schlüssel im sicheren Schlüsselspeicher (TPM, TEE, NXP SE050, ...)
• Initialisierung eines sicheren Schlüsselspeichers (TPM, SE050)	Erstellung von Client-Zertifikaten mit der Zwischenzertifizierungsstelle des Kunden (HSM, NitroKey, SmartCard, ...)
• Dateisystem / Verzeichnisverschlüsselung	Geräteregistrierung bei Cloud- / Dienstanbietern
• Deaktivierung von Funktionen (JTAG, Boot Fuses)	
• Software Programmierung MADE IN GERMANY	

Security Angebote

PARTNERSCHAFT SCHAFFT VERTRAUEN

PHYTEC können Sie vertrauen! Als zuverlässiger Partner bei der Umsetzung Ihrer Geschäftsideen steht für uns der Schutz Ihrer sensiblen Daten an erster Stelle. Wir sorgen für die verschlüsselte und verifizierte Übermittlung Ihrer Informationen zur Realisierung Ihrer Projekte.

SICHERE AUFBEWAHRUNG

Wir schützen Ihre Geheimnisse über den gesamten Produktlebenszyklus. Wir übernehmen die sichere Aufbewahrung in einem speziell entwickelten System, das nicht mit dem Firmennetzwerk verbunden ist. Strenge Zugriffskontrollen sorgen für maximale Sicherheit.

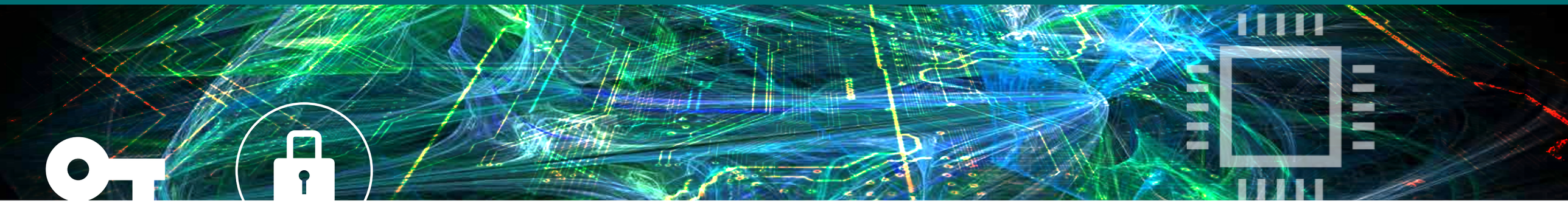
- **Strenge Zugangskontrollen**
- **Nicht im Firmennetzwerk**
- **Physisch getrennte Netzwerkverbindung zur Produktion (Softwareinstallation)**

SICHERE IMPLEMENTIERUNG IN DAS PRODUKT

- **Kein direkter Zugriff auf private Schlüssel in der Testumgebung**
- **Einsatz von HSM-Modulen zum Schutz privater Schlüssel**
- **Physikalisch unabhängiges Netzwerk für den gesamten Prozess**

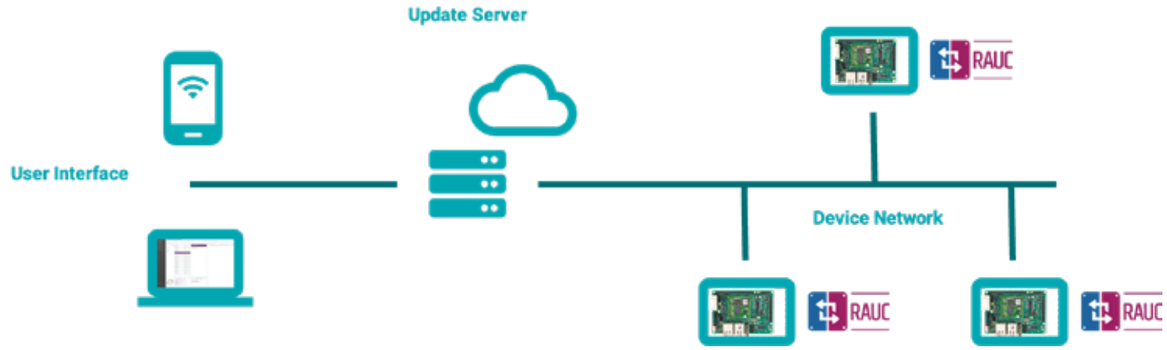
SCHUTZ IHRER PRODUKTE BIS ZUR AUSLIEFERUNG

Wir kümmern uns um den Schutz Ihrer Produkte während des gesamten Produktionsprozesses und während der Lagerung, nach der Installation Ihrer Kundensoftware. Das Verfahren bis zur vereinbarten Lieferzeit gestalten wir gemeinsam mit Ihnen und nach Ihren Vorgaben.



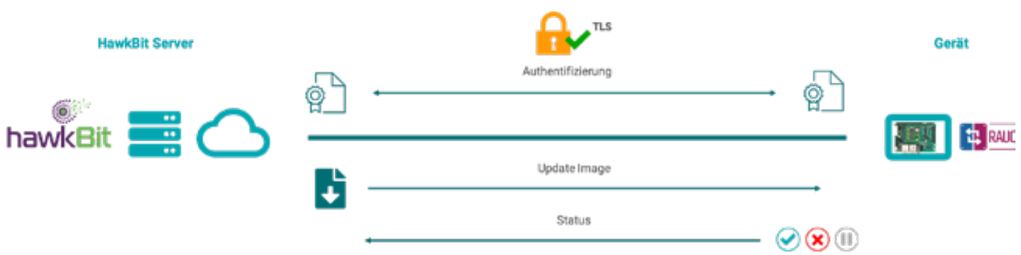
Unser Angebot im Detail
Sicheres Management und Update Ihrer IoT-Geräte

RAUC ist ein Update-Client, der auf Embedded Geräten läuft und den Aktualisierungsprozess Ihres Embedded Systems mit neuer Firmware verwaltet. Auf dem Host System können mit RAUC Update Bundles für das Embedded System erstellt, überprüft und geändert werden. Ziel ist es, mit RAUC eine solide und generische Basis für die verschiedenen kundenspezifischen Anforderungen zu schaffen, die bei der Entwicklung eines Update-Konzepts für Ihre Plattform zu berücksichtigen sind.



VORTEILE

- Übersicht des Gerätestatus und der Softwareversion
- Verwaltung von Update Bundles für unterschiedliche Gerätetypen
- Anbindung von externen Datenquellen (z.B. ERP)
- Schrittweises Ausrollen von Updates
- Keine Störung des laufenden Betriebs
- Ausfallsicherheit durch atomaren Updateprozess und redundantem A/B-System
- Updateprozesse individuell anpassbar
- Unterstütze Updatequellen (Ethernet, Wi-Fi, USB, ...)
- Open Source, lizenzkostenfrei und anbieterunabhängig



SICHERE KOMMUNIKATION ZWISCHEN SERVER UND GERÄT

- Gerät verbindet sich über TLS-Authentifizierung (Zertifikate erforderlich)
- Server sendet signiertes Update Bundle
- RAUC verifiziert Bundle mit lokal gespeichertem Zertifikat
- Nach erfolgreicher Verifikation wird das Bundle installiert
- RAUC sendet Statusinformationen zurück

USER INTERFACE	UPDATE SERVER	UPDATE CLIENT
• Graphisches User Interface zur visuellen Steuerung und Anzeige • REST-API zur Anbindung an eigene System und zur Automatisierung	• Server für die Aktualisierung von externen Geräten • Verwaltet und überwacht Update-Bundles für viele Geräte • Zeigt den Status des Aktualisierungsprozesses an • Läuft auf einem Server, lokalen PC oder als Cloud-Service	• Verwaltet den Software Aktualisierungsprozess • Ausfallsicheres Update durch A/B-System • Power cut Safe durch atomare Updates • Empfängt Update-Bundles über Ethernet, Wi-Fi, USB, SD... • Bundle Verschlüsselung • Adaptive Update
• Besitzt eine GUI und REST API	• Hawkbit ist der Standard Server bei den Realisierungen • Open Source • Entwickelt von der Eclipse Foundation	• Rauc ist der Standard Update Client bei PHYTEC • Ist Teil der PHYTEC Linux-Distribution • Open source • Developed von Pengutronix
Alternativen		
• Individuelle und erweiterte Graphische User Interface	• Fileserver zur Bereitstellung von Update Bundles • HTTPS Streaming für Adaptive Updates • Alternative Bereitstellung der verschlüsselten Update-Bundles ohne Server	• Client support von anderen Anbietern wie Mender.IO, foundries, swupdate möglich

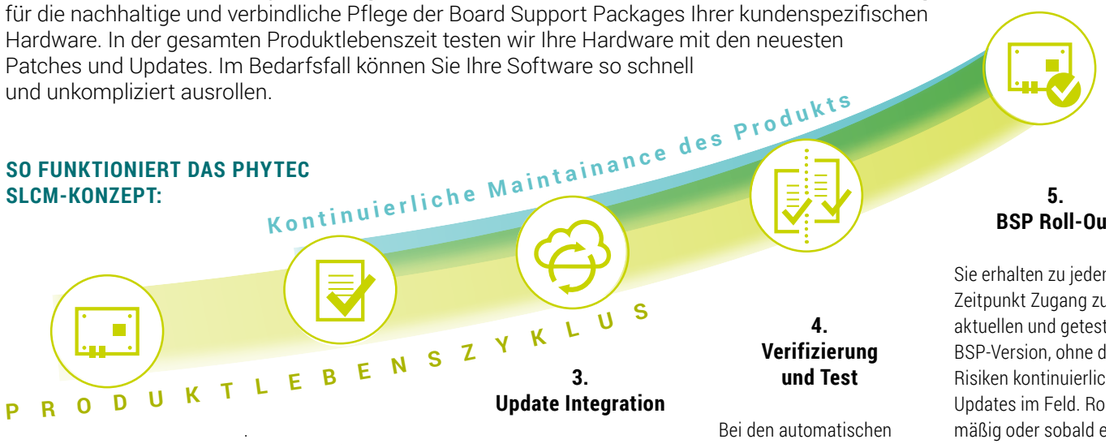
Unser Angebot im Detail
Software Lifecycle-Management

IHRE PRODUKTE ENTWICKELN SIE FÜR EINEN LANGJÄHRIGEN LEBENSZYKLUS – IHRE SOFTWARE AUCH?

Die Anforderungen an Sicherheit und Datenschutz steigen – und ebenso die Zahl der Angriffe, Sicherheitslücken und erkannter Risiken. Diesen stets verändernden Sicherheitsbedrohungen müssen Sie sich stellen und die Updatefähigkeit Ihrer Systeme gewährleisten, wenn Sie mit dem Internet verbunden sind. Das fordert beispiels-weise auch die aktuelle IEC 62443 Norm im Abschnitt Patch Management in the Industrial Automation Control System Environment.

Der PHYTEC Software Lifecycle Management Service unterstützt Sie dabei. Nutzen Sie unser Angebot für die nachhaltige und verbindliche Pflege der Board Support Packages Ihrer kundenspezifischen Hardware. In der gesamten Produktlebenszeit testen wir Ihre Hardware mit den neuesten Patches und Updates. Im Bedarfsfall können Sie Ihre Software so schnell und unkompliziert ausrollen.

SO FUNKTIONIERT DAS PHYTEC SLCM-KONZEPT:



1. Entwicklung Ihres BSPs

Wir entwickeln ein kundenspezifisches BSP für Ihre PHYTEC Hardware - aufbauend auf den Vorleistungen der Standard-Entwicklung. Hardware und BSP integrieren wir in unsere Testfarm und das CI-System.

2. Planung der Roadmap

Gemeinsam mit Ihnen erstellen wir eine Update-Strategie für Ihr Produkt und legen die Häufigkeit der Aktualisierungen fest. In der Regel vereinbaren wir jährliche Major Updates des Yocto Projects und im zweijährigen Rhythmus Updates der LTS Kernel-Version.

3. Update Integration

Parallel werden zwei BSP-Stände gepflegt: Eine aktuelle Version Ihres BSPs, das wir ständig mit Security- und Bug-Fixes über einen vereinbarten Zeitraum versorgen. Und eine weitere Version, bei der wir Ihr BSP kontinuierlich auf den aktuellsten Entwicklungsstand des Yocto Projects und Linux-Kernels bringen. Eine perfekte Basis für Ihr nächstes stabiles Software-Release.

4. Verifizierung und Test

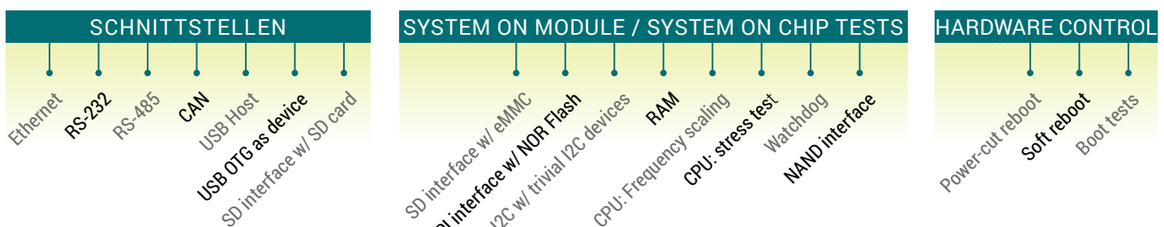
Bei den automatischen Tests mit Nightly-Builds werden etwaige Konflikte mit Ihrem BSP schnell erkannt und können zeitnah behoben werden. Gleichzeitig prüfen wir fortwährend die Übereinstimmung der BSPs mit Ihren Spezifikationen. Sämtliche Resultate werden für Sie in Testprotokollen festgehalten.

5. BSP Roll-Out

Sie erhalten zu jedem Zeitpunkt Zugang zu einer aktuellen und getesteten BSP-Version, ohne die Risiken kontinuierlicher Updates im Feld. Routinemäßig oder sobald eine relevante Sicherheitslücke erkannt wird, können Sie das BSP mit Ihren eigenen Software-Applikationen testen und zeitnah ausspielen. Dabei unterstützt Sie der RAUC Robust Auto-Update Controller, der in unseren BSPs vorbereitet ist. Darüber hinaus stellen wir Ihnen gemäß der vereinbarten Strategie Updates Ihres BSPs mit aktueller Kernel- und Yocto-Version zur Verfügung.

Rahmenbedingungen
Voraussetzung für das Lifecycle-Management der Software sind die Verwendung eines Mainline-Linux basierten BSPs und das Vorliegen einer BSP-Spezifikation, die die gesamte Funktionalität der Plattform umfasst. Es wird eine automatisierte Testumgebung verwendet, mit der die komplette Funktion des Systems entsprechend der BSP-Spezifikation geprüft werden kann. Die Tests umfassen in erster Linie die auf den Boards angelegten Schnittstellen, Treiber und Verbindungen. Kundenapplikationen werden in der Regel nicht in den Test aufgenommen. Die Standardtests umfassen „gängige“ Schnittstellen entsprechend der untenstehenden Grafik. Besondere Schnittstellen oder spezielle Protokolle können durch Erweiterung der Prüfspezifikation individuell aufgenommen werden; evtl. ist dafür die Erstellung spezieller Testhardware erforderlich.

Für die Tests ist das auf Jenkins basierende System für die Continuous Integration mit der Test-Umgebung für automatische Hardware-Tests verknüpft. Damit eignet sich das Setup optimal zur kontinuierlichen Integration von Standard-Board-Support-Packages sowie von kundenspezifisch angepassten BSPs.



Positiver Nebeneffekt des Setups ist die klare Trennung von BSP, Middleware und Applikationssoftware, mit der die einzelnen Schichten im Bedarfsfall individuell behandelt werden können, ohne dass sich Fehler durch nicht berücksichtigte Abhängigkeiten ergeben.

Deployment leichtgemacht!
Das Ausrollen Ihrer Software im Feld erleichtern wir durch die Vorbereitung des RAUC Robust Auto-Update Controllers in allen aktuellen BSPs. Der Update-Client sorgt für die zuverlässige Installation von signierten BSP-Updates auf den Embedded Systemen und wird von Yocto im meta-rauc Layer unterstützt. Auf dem Host-System können mittels des Tools BSP-Updates erstellt, geprüft und modifiziert werden.

PHYTEC unterstützt Sie sowohl bei der Implementierung der Updatemechanismen als auch beim Schaffen einer entsprechenden Infrastruktur – von der RAUC-Konfiguration über das Einrichten von Cloud-Services bis hin zum Schutz der Hardware vor dem Aufspielen von Schadsoftware.

PROFITIEREN SIE VON UNSEREN WEITEREN ANGEBOTEN!

- Hardening & Secure Boot
- Security-Beratung für Hardware- & Software-Design
- Schlüssel- und Zertifikatshandling im deutschen, rechtssicheren Raum
- Cloud-Plattformen für das Ausspielen der Updates

AUFBAU DER BSP-SCHICHTEN

KUNDENANWENDUNG Yocto Project	• meta-cust u.a.	Pflege durch den Kunden
TESTS	Optionaler Service von PHYTEC	
BSP-SPEZIFIKATION		für SLCM erforderlich
Yocto Project	• meta-ksp • poky • meta-openembedded • meta-phytec • meta-yogurt • meta-rauc • meta-qt5	Pflege durch PHYTEC

Sprechen Sie mit uns über Ihr individuelles Angebot für das Software Lifecycle-Management!

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

Unser Angebot im Detail
Sicherheitslücken Analyse (CVE)

Eine Sicherheitslücke stellt eine Bedrohung für die Sicherheit eines Computersystems dar. Es besteht das Risiko, dass die Sicherheitslücke ausgenutzt und das betroffene Computersystem kompromittiert werden kann.

Sicherheitslücken entstehen unter anderem durch den unzureichenden Schutz eines Embedded Devices vor Angriffen aus dem Netz sowie durch Programmierfehler im Betriebssystem, Diensten oder von Middleware, die auf dem System betrieben werden. Jedoch können auch Fehler in der Hardware zu Sicherheitslücken führen.

Sicherheitslücken werden durch die Mitre Corporation mittels eines Referenzier-Systems gepflegt und bewertet. Bei unserem Service ziehen wir noch weitere Quellen hinzu, um entsprechend schnell reagieren zu können.

Profitieren Sie von unseren Security Services im gesamten Lebenszyklus Ihrer Produkte.

	CVE **Basic**	CVE **Advanced**	CVE **Maintained**	CVE **Individual**
Verwendungszweck	als Basis für eigene Entwicklungen	als Nachweis für ein Audit oder beim Endkunden	Das eigene Image im Blick, um schnell auf Sicherheitslücken reagieren zu können	Für Anwendungen in Kritischer Infrastruktur empfehlen wir die Zusammenarbeit mit unserem spezialisierten Partner
Kombinierbar mit weiteren PHYTEC Angeboten	⊖	⊖	✓ mit SLCM können verfügbare Patches direkt angewendet werden	✓ mit Produkten von Partnerfirmen
Softwareumfang	Bootloader, Kernel und Middleware eines PHYTEC Minimalimages	Bootloader, Kernel und Middleware eines definierten Kundenimages		
Anzahl der Überprüfungen	einmalig beim Erzeugen des Images		zyklisch einmal pro Tag	wählbar
mehrere Quellen als Basis für Bewertung	✓	✓	✓	✓
Prüfung der aktiven Softwareteile bei Kernel und U-boot (Reduktion der CVEs)	✓	✓	✓	✓
U-boot und Kernel Config (wenn ermittelbar)	✓	✓	✓	✓
CVE-Zusammenfassungsbericht	✓	✓	✓	✓
REST API Zugriff	⊖	⊖	✓	✓
CVE-Filterung nach CVSS-Score oder Angriffsvektor	⊖	⊖	✓	
Handlungsempfehlung	⊕	allgemein nach Kriterien ermittelt		⊕⊕ nach Use-Case und Einsatzgebiet
Benachrichtigung bei neuen CVEs	⊖	⊖	✓	✓
Bereitstellung verfügbarer Patches	⊖	⊖	✓	✓

Immer das richtige Maßan Security für Ihr Produkt.

SECURITY PACKAGES	Basic PRE-Configured kostenlos	Advanced Mit professioneller Unterstützung	Maintained Langfristig gepflegte Sicherheit	Individual Anpassbar an Ihre Bedürfnisse
Software Lifecycle Management			Zyklische BSP-Pflege	frei wählbar
Common Vulnerabilities and Exposures (CVE) Behebung			Zyklischer CVE-Scan	frei wählbar
Geräteinitialisierung Client Certificates, Secure Boot		inklusive	inklusive	wählbar mit / ohne
Sicheres Management und Update Ihrer IoT-Geräte	Update-**Basic**	Update-**Advanced**	Update-**Advanced**	FOUNDRIES.IO, RAUC, Mender
SECURIphy-Distro	**SECURIphy-Basic** Alle Linux-Securitytools bereits vorbereitet	**SECURIphy-Advanced** Mit professioneller Konfigurationsuntersützung	**SECURIphy-Maintained** Alle Linux-Securitytools langfristig gepflegt	frei wählbar
Consulting / Support	1 Stunde ***KOSTENFREI***	Kosten pro Stunde	Kosten pro Stunde	Kosten pro Stunde

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