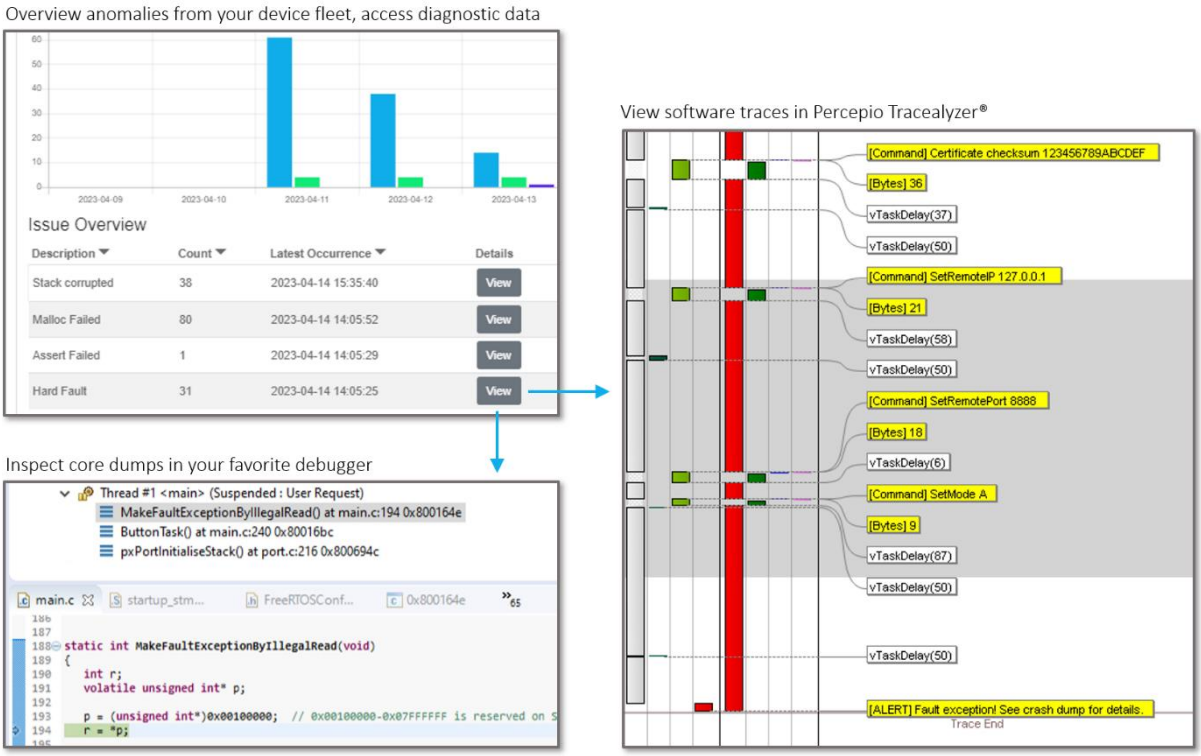
ZUR SOFORTIGEN VERÖFFENTLICHUNG



Bildunterschrift: Percepio DevAlert sorgt für umfassende Observability von Software-Anomalien in Edge-Devices im großflächigen Einsatz, wobei das Dashboard (oben links) einen Überblick und den einfachen Zugriff auf Debugging-Informationen wie etwa Core Dumps (unten links) und System-Traces (rechts) liefert.

Hochauflösendes Bild verfügbar auf: https://percepio.com/press/photos/DevAlert-2.0.png

Percepio® DevAlert® 2.0 bringt uneingeschränkte Edge-Observability für den Embedded-Software-Test und das Fern-Debugging großer Stückzahlen von Geräten im Feld

Västerås, Schweden, 29. November 2023 *** Percepio AB, führender Anbieter von Observability-Lösungen für Embedded-Software, gibt die umgehende Verfügbarkeit von Percepio DevAlert Version 2.0 bekannt.

Percepio DevAlert ist eine cloudbasierte Observability-Lösung, die eine Rückkoppelschleife zwischen Gerätebeständen und den zuständigen Produktteams bereitstellt. Mit DevAlert können Produktteams Abstürze, Fehler und andere Software-Anomalien während der Systemtests, in Feldversuchen oder im Betrieb beim Kunden umgehend detektieren und detaillierte Diagnoseinformationen einholen, um für rasche Abhilfe zu sorgen. DevAlert ist eigens für kleine Edge-Prozessoren und IoT-Mikrocontroller konzipiert, die RTOS-basierte Software verarbeiten und bei denen Sicherheit, Datenschutz, Transparenz und Skalierbarkeit im Vordergrund stehen. Software ohne Cloudanbindung lässt sich unterstützen, indem die Daten über einen lokal angeschlossenen Hostcomputer weitergeleitet werden – beispielsweise bei der Überwachung von Systemtests oder durch Anschließen eines Laptops im Rahmen des Kundendiensts. Auf diese Weise eignet sich

DevAlert für jegliche Embedded-Software, und es wird lediglich eine serielle Schnittstelle oder ein Debug Probe benötigt.

DevAlert 2.0 wartet mit deutlich verbesserten Diagnosefunktionen auf, darunter Core Dumps für das Debugging von Quellcode für Geräte mit Arm Cortex-M-Prozessoren. Dies macht es möglich, Abstürze, Fehler oder Cybersecurity-Anomalien aus der Ferne und in allen Einzelheiten zu analysieren, was den Funktionsaufruf-Stack, Parameter und Variablen sowie die Ausgabe des Quellcodes einschließt. Zusammen mit den schon bisher gebotenen Features zum Erfassen von Tracealyzer®-Traces zum Aufdecken von Anomalien sowie dem kürzlich hinzugefügten Tracealyzer SDK für kundenspezifische Trace-Integrationen (siehe hierzu diese Pressemeldung), ergibt dies eine uneingeschränkte Observability für beliebige Embedded-Software – ob diese nun auf einem Echtzeit-Betriebssystem (Real-Time Operating System, RTOS) oder als Bare-Metal-Applikation läuft. Auch wenn DevAlert bislang noch nicht auf Linux-basierten Geräten getestet wurde, ist die Plattform dafür ausgelegt, in naher Zukunft auch Linux-Support bieten zu können.

Die neue DevAlert-Lösung kann ebenfalls genutzt werden, um Verfälschungen des Stack-Inhalts mit gängigen Compiler-Features zu detektieren, und ein Beispiel für den GCC-Compiler gehört zum Lieferumfang. In Verbindung mit den Core Dumps lassen sich nicht nur gefährliche Pufferüberlauf-Probleme detektieren, sondern zur Inspektion der Daten können auch die verfälschten Stack-Inhalte erfasst werden. Hierdurch ist es möglich, nicht nur Code-Injection-Attacken in sämtlichen Einzelheiten aufzudecken, sondern auch solche Pufferüberläufe, die zwar unbeabsichtigt sind, aber dennoch gravierende Sicherheitslücken darstellen.

> *„Software-Observability ist wegen der zunehmenden Cyber-Bedrohungen und der ständig wachsenden Software-Komplexität, die schwer greifbare Bugs und Schwachstellen zur Folge hat, von immer größerer Bedeutung für das Vertrauen in digitale Systeme. Abgesehen von der Cloud, gilt dies insbesondere auch für Edge-Devices, die unvorhersehbaren Umgebungseinflüssen sowie physischen Attacken ausgesetzt sind und zahlreiche Angriffsflächen bieten. Diese Geräte sind teils mit CAN-Bussen, UARTs, JTAG-Debug-Ports und verschiedenen weiteren Schnittstellen ausgestattet sind, bei deren Design das Thema Cybersicherheit noch keine Rolle spielte.*
>
> *Percepio befasst sich seit vielen Jahren schwerpunktmäßig mit der Observability von Embedded-Software – beginnend mit Tracealyzer für die lokale Observability während der Entwicklungsphase. Die erste Version von DevAlert dehnte dies auf die tracebasierte Observability großer Stückzahlen im Einsatz befindlicher Geräte aus. Mit DevAlert 2.0 nun vollziehen wir den nächsten Schritt, indem wir den Anwendern das Einholen beliebiger Arten von Gerätedaten ermöglichen – darunter beispielsweise Core Dumps für das Debugging von Quellcode, aber auch kundenseitig definierte Daten wie etwa Device Logs, Network Logs, Sensordaten, Bilder und Audiodaten. Dies ebnet den Weg zu einer wirkungsvollen Edge-Device-Observability und ist das letzte bisher noch fehlende Element zum Erzielen einer echten Full-Stack-Observability, die sich bis ganz an die Außengrenzen eines Systems erstreckt",* erläutert Dr. Johan Kraft, CTO und Gründer von Percepio.

DevAlert 2.0 wurde von Sensorbee AB integriert, einem Anbieter IoT-basierter Lösungen zur Überwachung der Luftqualität.

> *„Für uns ist es sehr wichtig, neue Funktionalität schnell umzusetzen – von der Anforderung durch den Kunden bis zum Einsatz im Feld. DevAlert hilft uns, das Wachstum unseres Unternehmens anzukurbeln, da wir neue Funktionalitäten nicht nur schneller, sondern auch in*

der von unseren Kunden erwarteten Qualität ausliefern können“, berichtet David Löwenbrand, CEO von Sensorbee AB.

Ein Videointerview finden Sie unter https://vimeo.com/manage/videos/879338662.

Erweiterbarkeit, Datenkontrolle und Privatsphärenschutz durch Integration von Desktop-Tools

DevAlert 2.0 verbindet den Komfort und den reibungslosen Workflow eines anbieterseitig gehosteten Clouddiensts mit der Erweiterbarkeit, der Vertrautheit und dem Datenschutz lokaler Desktop-Tools.

Seit seiner Einführung bietet DevAlert eine datenschutzfreundliche Lösung nach dem „Bring Your Own Storage“-Prinzip, bei der die Kunden die vollständige Kontrolle über die Speicherung ihrer Diagnosedaten behalten und zu keiner Zeit sensible Gerätedaten oder geistiges Eigentum wie etwa Firmware-Images in den Clouddienst hochladen müssen. DevAlert 2.0 intensiviert die Fokussierung sogar noch durch die Bereitstellung eines separaten Desktop-Clients, mit dem die Anwender ihren eigenen privaten Datenspeicher konfigurieren können, um die volle Kontrolle zu haben und den Schutz der Privatsphäre zu gewährleisten. Der Client erlaubt den Anwendern außerdem den Anschluss eigener, desktopbasierter Diagnosewerkzeuge wie etwa Debugging-Tools und individueller Skripte und ruft jeweils das richtige Tool auf, wenn auf dem DevAlert-Dashboard ein Download-Link angeklickt wird.

Für Arm Cortex-M-Systeme ist die Integration mit GDB bereits enthalten, während die Unterstützung für andere Plattformen auf Anfrage realisiert werden kann.

Dazu erklärt Dr. Johan Kraft, CTO und Gründer von Percepio: *„Das neue Design machte es notwendig, zutiefst widersprüchliche Anforderungen miteinander in Einklang zu bringen, indem einerseits noch detailliertere Daten aus den Geräten abgerufen werden, ohne andererseits Abstriche an der Kontrolle und dem Schutz der Kundendaten zu machen. So ist zum Sichten von Core Dumps stets der Zugriff auf das richtige Firmware-Image notwendig, also auf sensibles Intellectual Property, das den privaten Bereich des Kunden eigentlich niemals verlassen sollte. Wir haben mit DevAlert 2.0 deshalb unser ‚Bring Your Own Storage‘-Design so verallgemeinert, dass wir den Datenschutz sicherstellen und gleichzeitig beliebige Arten von Device-Daten unterstützen können. Auf das Anklicken eines Download-Links im DevAlert-Dashboard hin werden automatisch die richtigen Daten in das richtige Desktop-Tool auf dem lokalen System geladen, ohne dass der private Bereich jemals verlassen wird. Wenn in der Software beispielsweise eine Anomalie entdeckt wird, können die Traces in Tracealyzer gesichtet werden, Core Dumps im bevorzugten Debugger, Daten von Bildverarbeitungssystemen in einem Image Viewer, Netzwerkanforderungs-Daten in einem Protokollanalyzer-Tool oder das neueste Device Log in dem bevorzugten Texteditor.“*

DevAlert 2.0 wurde in Zusammenarbeit mit mehreren Pilotkunden entwickelt, die die neue Lösung für den Praxiseinsatz in eigene Produkte integrieren wollen.

Weitere Informationen finden Sie auf https://percepio.com/devalert.

Ein Demo-Video gibt es hier: https://vimeo.com/manage/videos/877536941

Interview mit Sensorbee: https://vimeo.com/manage/videos/879338662

Über Percepio
Percepio® bietet über den gesamten Produktlebenszyklus hinweg Observability für kritische Edge-Software, um OEM und Betreibern ein schnelles, verlässliches Deployment intelligenter Systeme zu

ermöglichen und die Risiken bei der Produkteinführung bzw. OTA-Updates zu minimieren. Während der Applikationsentwicklung sorgt Percepio Tracealyzer® mit Software-Tracing und fortschrittlicher Visualisierung für die nötige Echtzeit-Observability, was die Markteinführung beschleunigt und die Qualität der Software bei deren Einführung verbessert. Sowohl in den Systemtests als auch nach dem Deployment bietet Percepio DevAlert® geschützte Observability-Funktionen, um der Produkteinführung die Risiken zu nehmen und eine fortlaufende Verbesserung der Zuverlässigkeit, Sicherheit und Performance des jeweiligen Produkts zu erzielen. Die Technologie lässt sich auf umfangreiche Gerätebestände skalieren und in beliebige Edge-Prozessoren integrieren – von kleinen IoT-Knoten bis hin zu leistungsstarken Multicore-SoCs. Percepio kooperiert mit führenden Anbietern von Prozessoren und Betriebssystemen im Embedded-Systems- und IoT-Bereich, darunter beispielsweise Arm, Infineon, NXP Semiconductors, STMicroelectronics, Renesas Electronics, Wind River Systems und Amazon Web Services. Weitere Informationen finden Sie auf percepio.com.

* * *

Leseranfragen
Percepio AB
Mike Skrtic
Tel: +46 76 003 0080
mike.skrtic@percepio.com
percepio.com

Pressekontakt
PRismaPR
Monika Cunnington
Tel: +44 20 8133 6148
monika@prismapr.com
prismapr.com