Percepio Device Firmware Monitor™

The Next Step in IoT Software Quality Assurance

Let's face it – we can never be certain that any firmware is free of bugs. On average, 5% of the original bugs remain in the production code, despite all verification efforts. This can mean hundreds of bugs in the shipped product. Some are perhaps insignificant or very unlikely, but you can't know for sure. Testing can't cover all possible paths through the code; there are simply far too many. Complementary verification methods like static analysis will certainly help, but each method has their limitations. For instance, the real-time behavior is typically not visible in the source code and therefore not addressed by most verification methods. You can always spend more time and money on verification, but the effort needed to find the last remaining bugs tends to increase exponentially and development projects have time and budget constraints to meet.

The real test comes when thousands of people starts using your product, in ways you never anticipated. Will it stand the test of reality? Missed bugs may at the very least irritate your customers, damage your reputation and hurt sales. In some cases, bugs may even lead to accidents, product recalls and legal action.

The rise of Internet-of-Things (IoT) increases the quality assurance challenges even further, but also provides a new remedy – Over-The-Air (OTA) software updates. If you fix the problem and update the shipped devices quickly, your customers will be more satisfied and might not even notice the issue. The faster you can deploy an OTA software update that fixes the problem, the fewer customers will notice it.

However, you cannot fix bugs that you are not aware of. Automatic feedback is needed to make developers aware of firmware issues in deployed products.

Enter Percepio Device Firmware Monitor (DFM), a ground-breaking new cloud service for IoT product organizations that provides awareness of missed bugs and speeds up resolution.

DFM notifies the firmware developers within seconds after an error has been detected and provides diagnostic information about the issue, including a trace for Percepio Tracealyzer. This shows you what was going on in your code when the error occurred, making it far easier to understand the problem and quickly find a solution.

Without automatic feedback, you actually rely on your end users to report any issues, a responsibility they have not agreed to. Then you might not hear about the issues until it's too late, when many customers have already been affected. Moreover, your end users can't be expected to provide sufficiently detailed information for you to quickly identify and solve the problem. A vague error report like "the screen went black" may require weeks of guesswork until you find a likely cause, and even then, you still don't know if really you solved the right problem. Imagine how much troubleshooting time that could be saved if you instead had access to detailed diagnostic information about every issue in the production software.

https://percepio.com

DFM is designed to leverage existing secure solutions for cloud connectivity, storage and OTA updates. Percepio DFM initially supports Amazon Web Services (AWS IoT Core) and Amazon FreeRTOS, but support for additional platforms is planned and can be provided on request.

Information Flow

The information flow starts in the error handling code of the IoT device, such as sanity checks and fault exception handlers. By calling the DFM firmware agent from these locations, firmware issues are uploaded as "alerts" to the customer's cloud account. Alerts may include an error message and any other information of interest to the developers for the specific issue, such as software states variables and hardware registers. Depending on the severity of the issue, the alert is either uploaded directly or after a device restart, once the connection has been restored.

The alert also includes a trace of the most recent software events prior to the issue, which is recorded automatically by the DFM agent. This tracing technology builds on 15 years of experience in RTOS tracing and is 4-8x more memory efficient than traditional RTOS tracers – only 4 KB is needed to store a trace containing up to 1000 software events. The efficient trace encoding is very important for two reasons - it allows for collecting traces of sufficient length even from memory-constrained IoT systems and it minimizes the cloud-side operational costs of DFM messaging and storage.
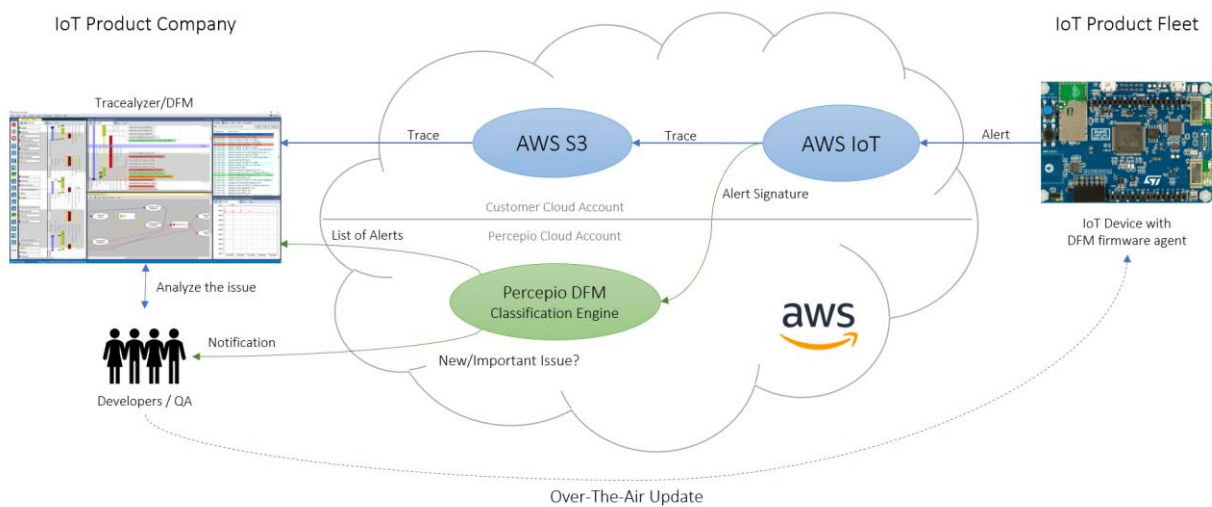
The alerts from the DFM firmware agent are uploaded to the customer's cloud service (AWS IoT Core), which is configured to store the alerts (Amazon S3) and also to notify the Percepio DFM Classification Engine. This service is the core of the DFM solution and runs in Percepio's AWS account. It is responsible for classification, statistics and

> "Percepio's Device Firmware Monitor is a game-changer in that it enables instant feedback from systems deployed in the field, to ensure your firmware quality is constantly improving"
>
> **Jack Ganssle, The Embedded Muse.**

notifications to the developers. It also offers configuration options for DFM, e.g., in what conditions notifications should be sent and where to send them.

The software trace never leaves the customer's cloud account. Only an anonymized signature of the issue is provided to the Percepio DFM Classification Engine and this information is completely transparent and configurable for the customer.

When the developers receive a notification about a new DFM alert, they can access the alerts and traces directly from Percepio Tracealyzer. The DFM Dashboard in Tracealyzer shows the recent alerts and allows for high-level analysis, e.g. if a certain issue was fixed by your latest firmware version. Moreover, the traces can be opened directly from the DFM Dashboard, thanks to built-in integration with Amazon S3.

> "Percepio's Device Firmware Monitor is early to the market and original. IoT developers need this sort of direct feedback from their deployed systems."
>
> **William E. Lamie, President, Express Logic**

Cloud-Side Operational Costs

DFM does not generate any data traffic unless an issue is detected, so if you don't have any missed bugs in your code, there is no DFM activity that drives cost. You need to store the alerts for some time, but due to the small amount of data per alert (typically 5 KB) and today's cheap cloud storage, this is a negligible cost. Especially when compared to the value of the provided information. Say that you have a large fleet of one million devices, with a lot of firmware issues – say 1 alert per device and week on average, and each alert is 5 KB. This would produce about 260 GB per year. Storing this data for a year would cost about $72, assuming Amazon S3 standard storage. But since most data can be deleted after a short time, e.g. duplicates of the same issue from different devices, the storage needed can be reduced to a fraction of this level.

Sending out OTA updates in response to DFM alerts can be a significant cost for large fleets, but this must be compared to the alternative cost of letting the bug remain unfixed, e.g. damaged customer experience, reduced product sales, or even accidents and legal action. How much would that cost? And, in case of minor issues, you can wait and see if more issues are reported, and then issue a single update with all corrections.

Learn More

Does this sound interesting? Please contact us at info@percepio.com. We are looking for early adopters to provide feedback. By joining our pilot program, you get free usage of the Percepio DFM service!

Percepio Device Firmware Monitor will be demonstrated in public for the first time at Embedded World 2019, in Percepio's stand 4-305. Welcome!

Copyright © 2019, Percepio AB

https://percepio.com