



Secure and Automated Updates for Embedded Linux

Objectives

- Understand the challenges of updating embedded Linux devices
- Automate the update process for embedded Linux devices using Mender
- Set up and configure a Mender server
- Deploy updates to devices using Mender, and monitor their progress.
- Use advanced Mender features such as rollback, A/B updates, and update channels to improve update reliability and flexibility.
- Integrate Mender with cloud providers such as AWS and Azure for OTA updates, and use delta updates to reduce update sizes and bandwidth usage.

Labs are conducted on target boards, that can be:

Dual Cortex/A7-based "STM32MP15-DISCO" boards from STMicroelectronics.

Quad Cortex/A9-based "SabreLite" boards from NXP.

Quad Cortex/A53-based "imx8q-evk" boards from NXP.

Course Environment

- Theoretical course
 - PDF course material (in English) supplemented by a printed version for face-to-face courses.
 - Online courses are dispensed using the Teams video-conferencing system.
 - The trainer answers trainees' questions during the training and provide technical and pedagogical assistance.
- Practical activities
 - Practical activities represent from 40% to 50% of course duration.
 - Code examples, exercises and solutions
 - For remote trainings:
 - ▶ One Online Linux PC per trainee for the practical activities.
 - ▶ The trainer has access to trainees' Online PCs for technical and pedagogical assistance.
 - ▶ QEMU Emulated board or physical board connected to the online PC (depending on the course).
 - ▶ Some Labs may be completed between sessions and are checked by the trainer on the next session.
 - For face-to-face trainings:
 - ▶ One PC (Linux ou Windows) for the practical activities with, if appropriate, a target board.
 - ▶ One PC for two trainees when there are more than 6 trainees.
 - For onsite trainings:
 - ▶ An installation and test manual is provided to allow preinstallation of the needed software.
 - ▶ The trainer come with target boards if needed during the practical activities (and bring them back at the end of the course).
- Downloadable preconfigured virtual machine for post-course practical activities
- At the start of each session the trainer will interact with the trainees to ensure the course fits their expectations and correct if needed

Prerequisite

- Embedded Linux Build (see our [D1 - Embedded Linux with Buildroot and Yoctocourse](#))
- Building a Linux Embedded image using Yocto (see our [Y1 - Yocto Project Developmentcourse](#))
- Preferably knowledge of Advanced Yocto Project usage and adaptation (see our [Y2 - Yocto Project Expertcourse](#))

Target Audience

- Any embedded systems engineer or technician with the above prerequisites.

Evaluation modalities

- The prerequisites indicated above are assessed before the training by the technical supervision of the trainee in his company, or by the trainee himself in the exceptional case of an individual trainee.
- Trainee progress is assessed in two different ways, depending on the course:
 - For courses lending themselves to practical exercises, the results of the exercises are checked by the trainer while, if necessary, helping trainees to carry them out by providing additional details.
 - Quizzes are offered at the end of sections that do not include practical exercises to verify that the trainees have assimilated the points presented
- At the end of the training, each trainee receives a certificate attesting that they have successfully completed the course.
 - In the event of a problem, discovered during the course, due to a lack of prerequisites by the trainee a different or additional training is offered to them, generally to reinforce their prerequisites, in agreement with their company manager if applicable.

Plan

FIRST DAY

Introduction to the update process using Mender

- Overview of the challenges of updating embedded devices
- Update options
 - Locally
 - Remotely
 - Over-the-air (OTA)
- Update risks
- Benefits of using Mender
- Introduction to the Mender architecture
- Mender update strategies
- How mender fits into the overall update process

What to update

- Identifying what needs to be updated on your devices
- Local updates vs OTA updates
- Robust system updates
- Application updates
- Proxy deployments

Mender server

- Installing and configuring a Mender server
- Setting up a Mender server and integrating it with your build system
- Connecting Mender to your build system and creating update artifacts
- Signing update artifacts for security

Exercise: Setting up a Mender server

Deploying updates to devices

- Deploying updates to devices
- Deploy an application update
- Deploy a system update
- Deploy a container update

Exercise: Deploying an update to a device using Mender

Mender artifacts

- The concept of Mender artifacts
- The role of artifacts in the update process
- The different types of artifacts
- Create an update Artifact

Exercise: Create and use artifacts

SECOND DAY

Advanced Mender features

- Using rollback to revert to a previous version if an update fails
- Implementing A/B updates to minimize downtime during updates
- Managing multiple update channels for different groups of devices
- Making updates robust and secure

Exercise: Rollback to revert to a previous version

Delta updates and the integration with cloud providers

- Introduction to delta updates
- Reduce update sizes and bandwidth usage
- Integrating Mender with AWS and Azure for OTA updates

Exercise: Update device OTA using AWS

Monitoring the update process and troubleshooting issues

- Understanding Mender's logging
- Mender's built-in monitoring capabilities
- Deployment status reports
- Debugging update issues and identifying root causes
- Test updates before deploying

Exercise: Debug and monitor update

Customizing Mender for your specific use case

- Extending Mender with custom scripts and plugins
- Integrating Mender with your existing deployment tools and processes
- Best practices for optimizing the Mender update process for your environment

Exercise: Extending Mender with custom scripts

Securing the update

- Best practices for securing the update process
- Security considerations for remote management
- Ensuring the integrity and authenticity of update artifacts
- Protecting against attacks on the update process
- Tips for hardening your Mender deployment against threats

Renseignements pratiques

Inquiry : 2 days