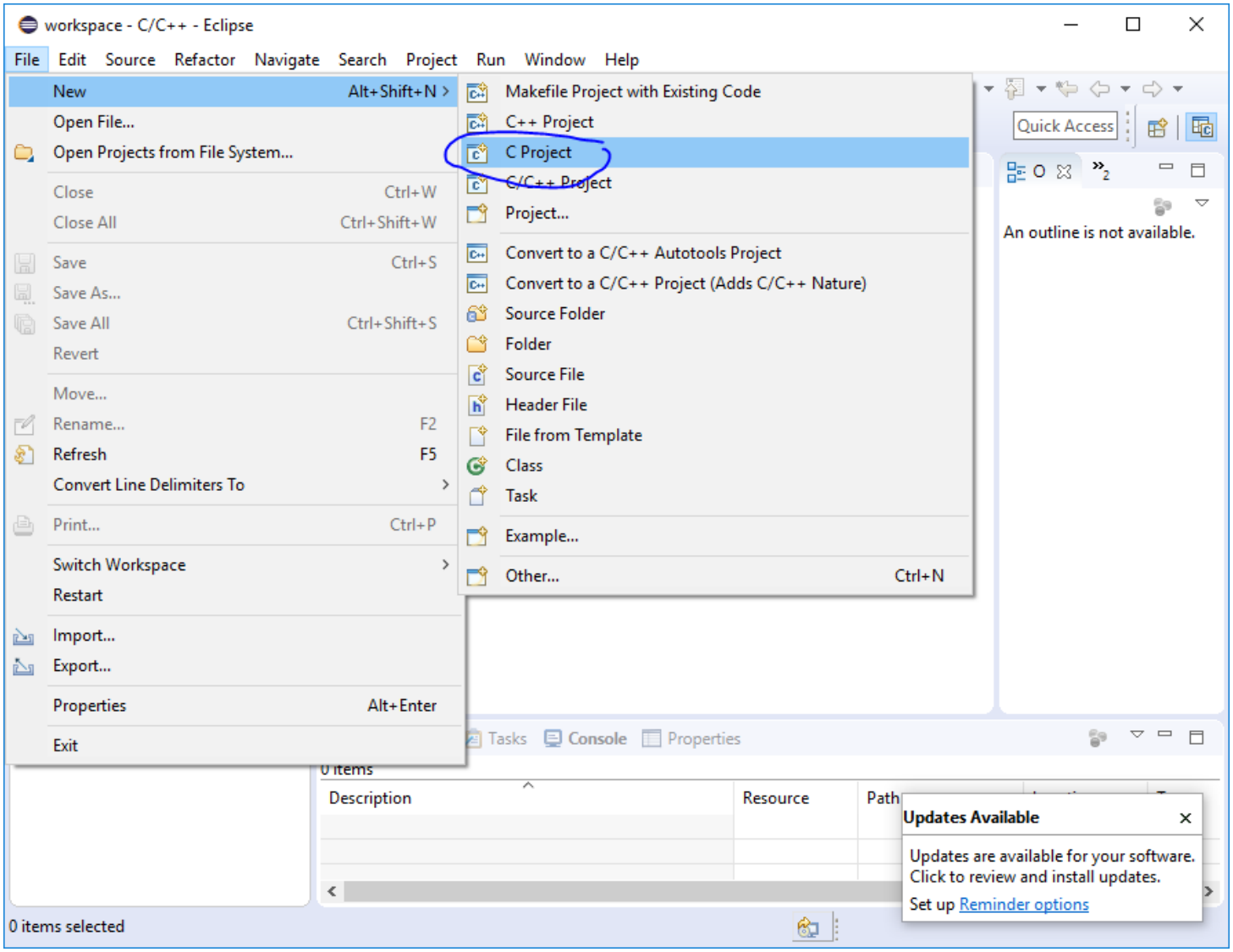
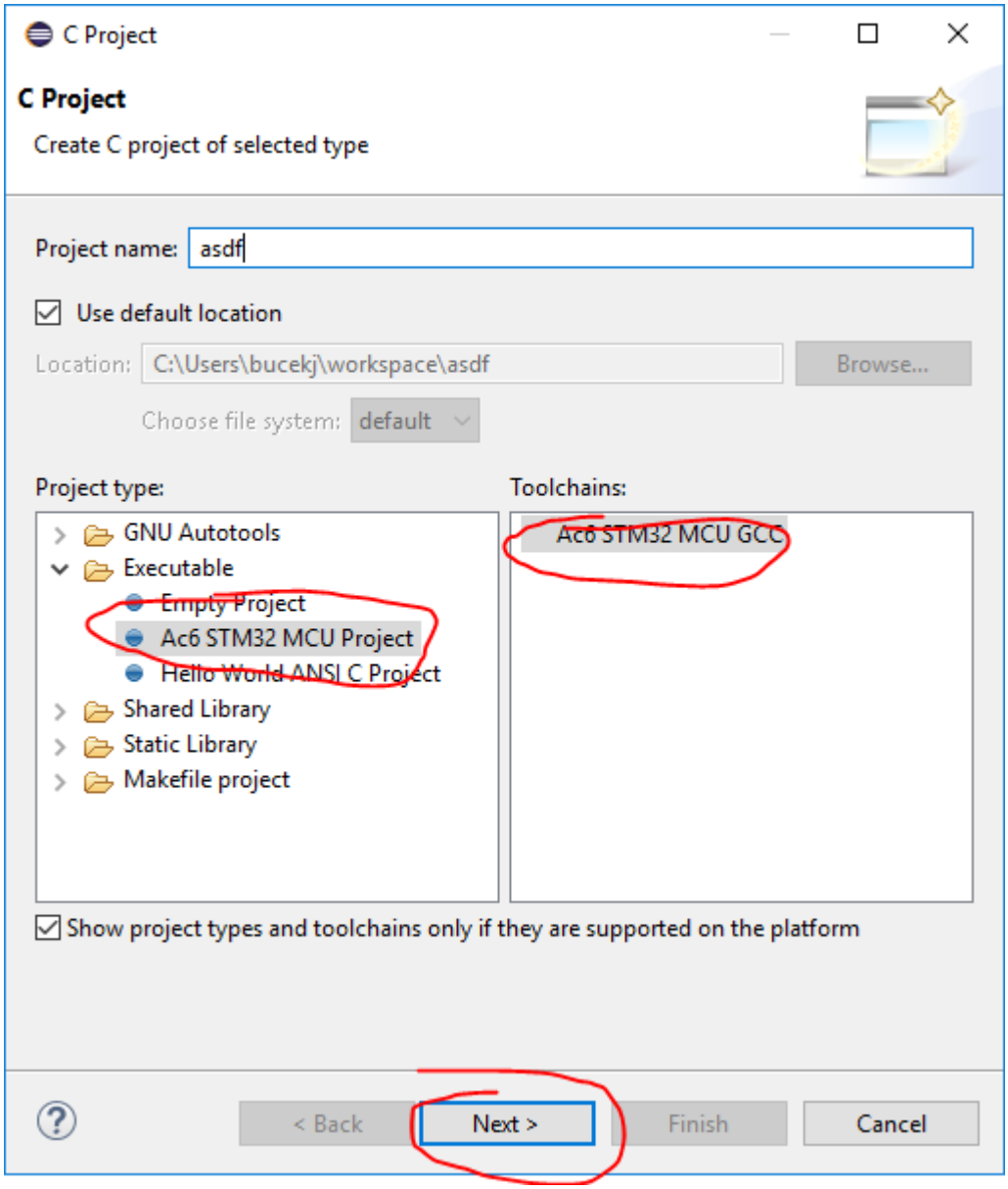
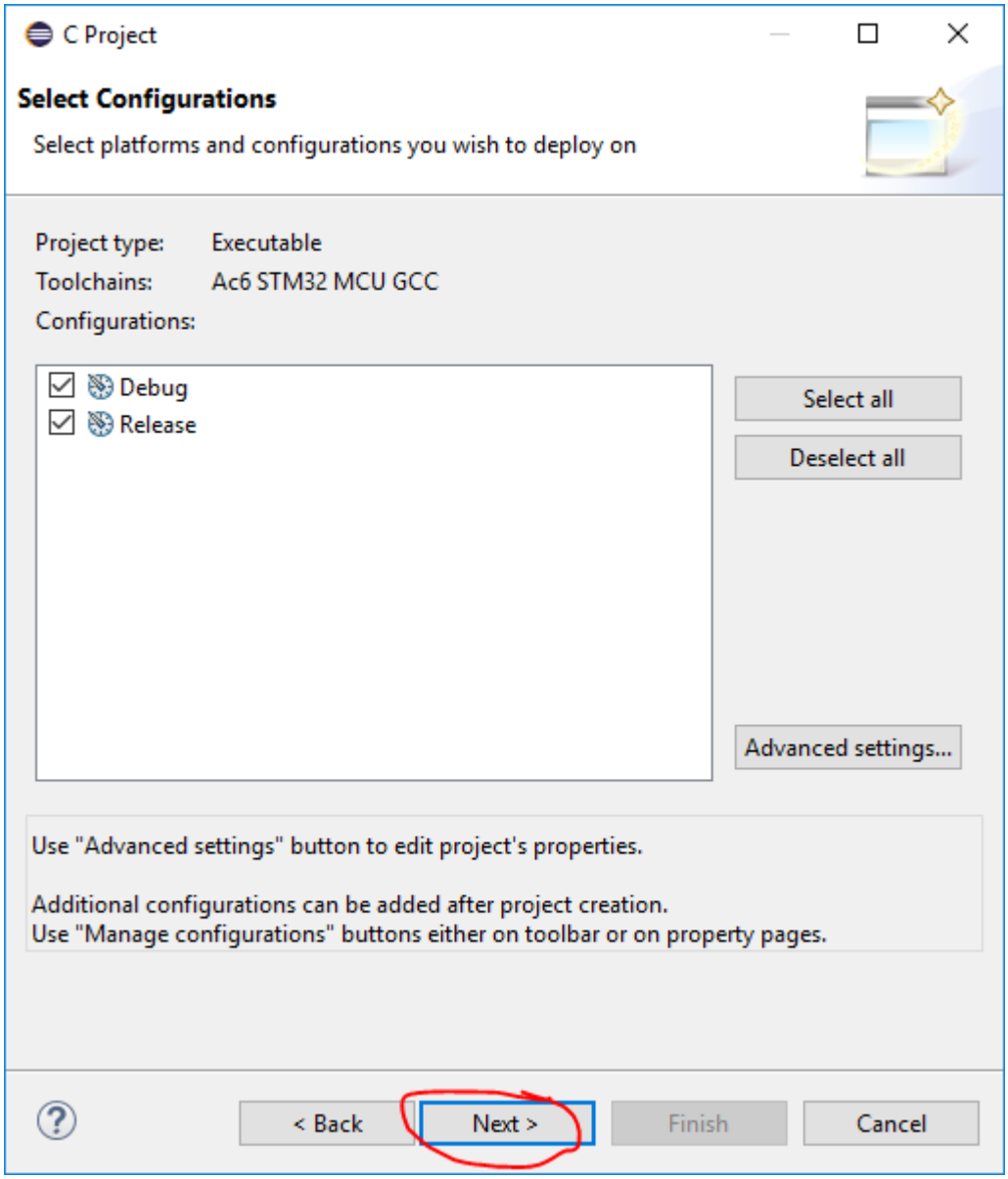
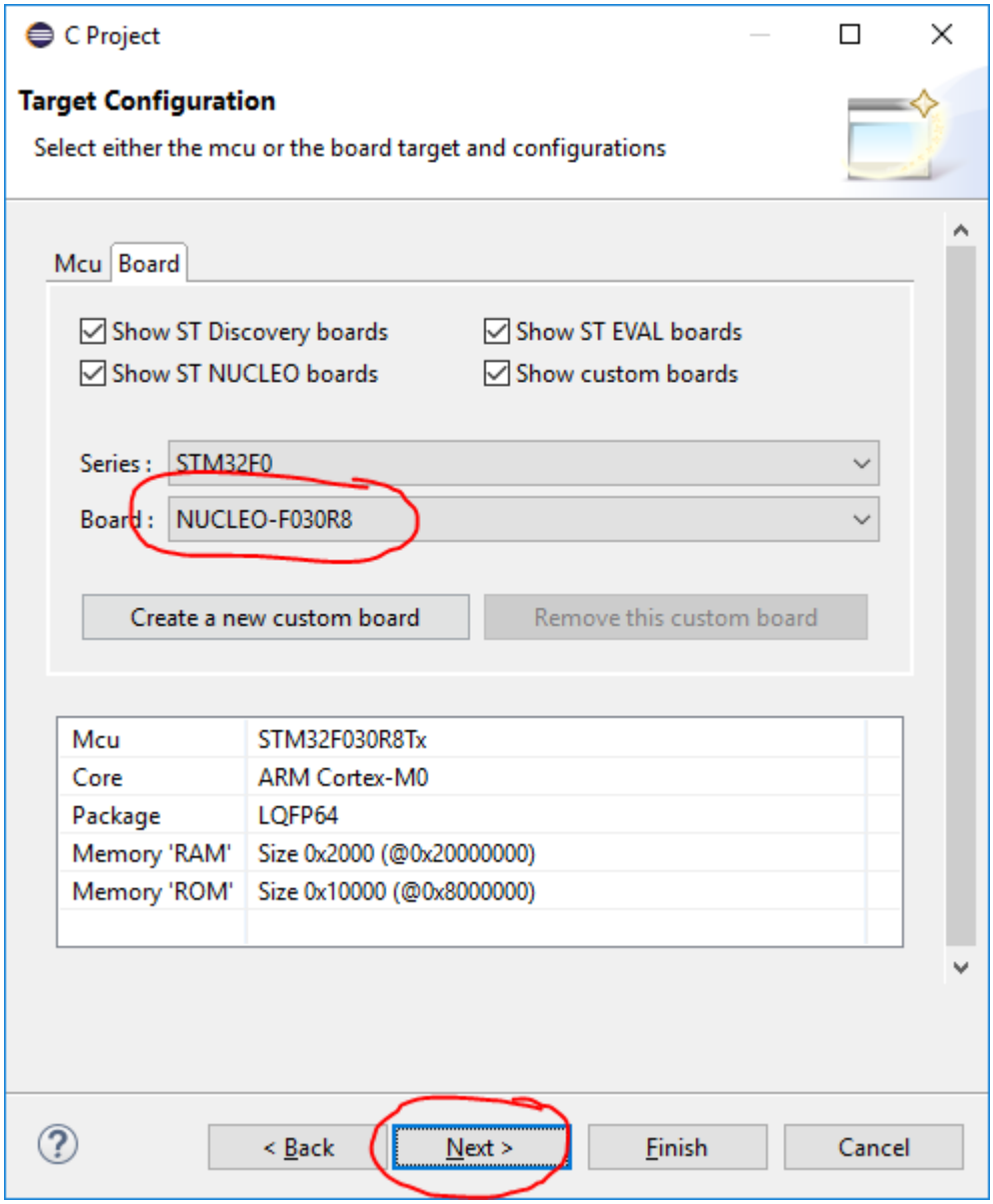
07. Testování AES na mikrokontroléru ARM

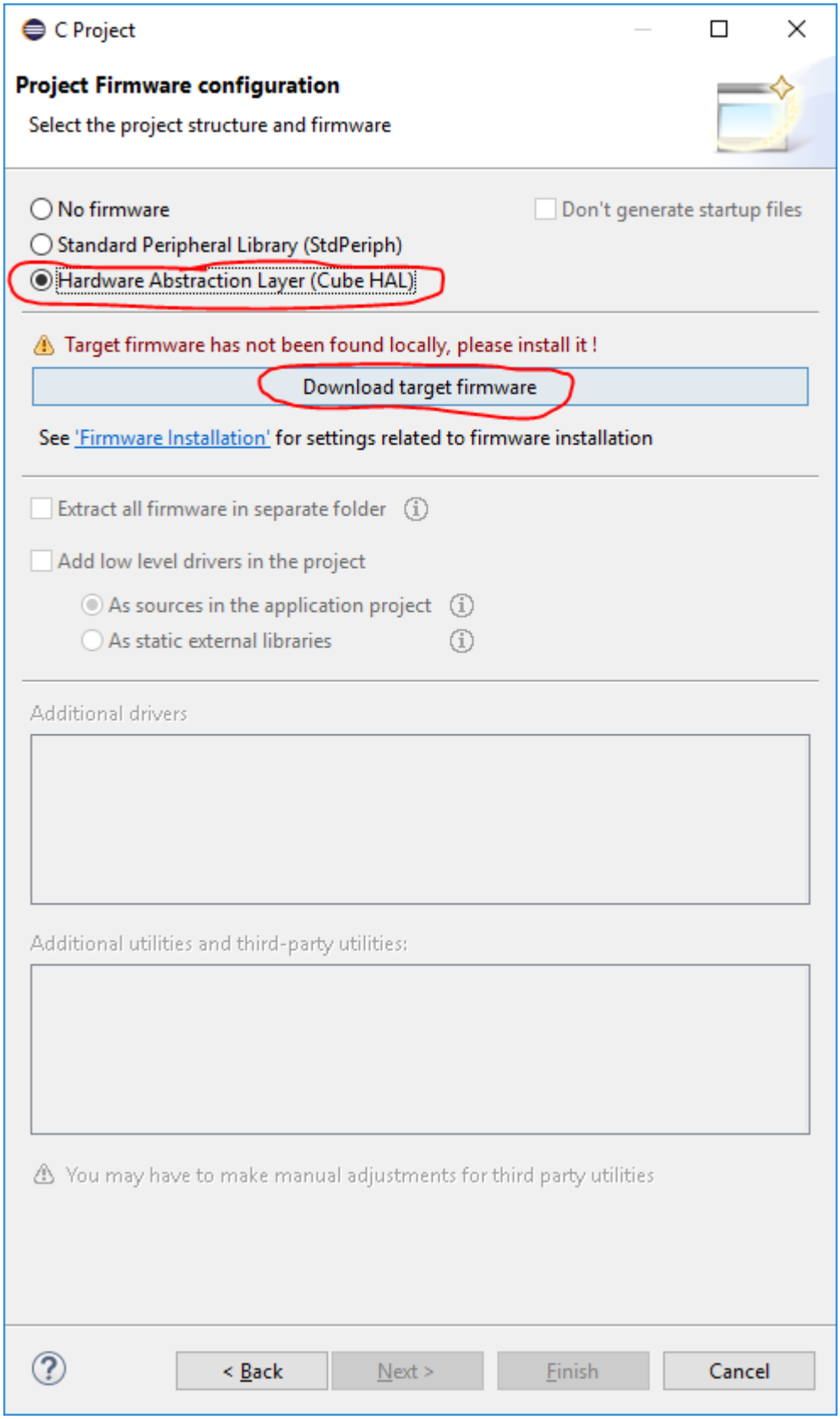
- Na **Windows** v učebně je nainstalován **System Workbench for STM32**
- Pokud máte u sebe (Windows nebo Linux) nainstalován Eclipse, můžete do něj doinstalovat pluginy z následujícího repozitáře: http://ac6-tools.com/Eclipse-updates/org.openstm32.system-workbench.update-site-v2
    - (návod pouze pro přihlášené na openstm32.org) http://www.openstm32.org/Installing%2BSystem%2BWorkbench%2Bfor%2BSTM32%2Bfrom%2BEclipse
- Otestujte na přípravku STM32 Nucleo-F030R8 dvě varianty implementace AES:
    - Jednoduchou přímočarou implementaci
    - Optimalizovanou implementaci pomocí T-boxů
    - Změřte čas provádění rozumného počtu iterací (např. 10000) a přepočtěte na trvání 1 AES
    - Porovnejte, kolikrát je PC rychlejší než tento mikrokontrolér
        - Pro získání času můžete použít funkci `HAL_GetTick()`, která vrací aktuální počet tiků (výchozí jednotka je ms)
    - Potřebujete kód pro **komunikaci pomocí sériové linky** (USB převodník je součástí přípravku).
        - Archiv se zdrojovými soubory (../files/nucleo_serial.zip)

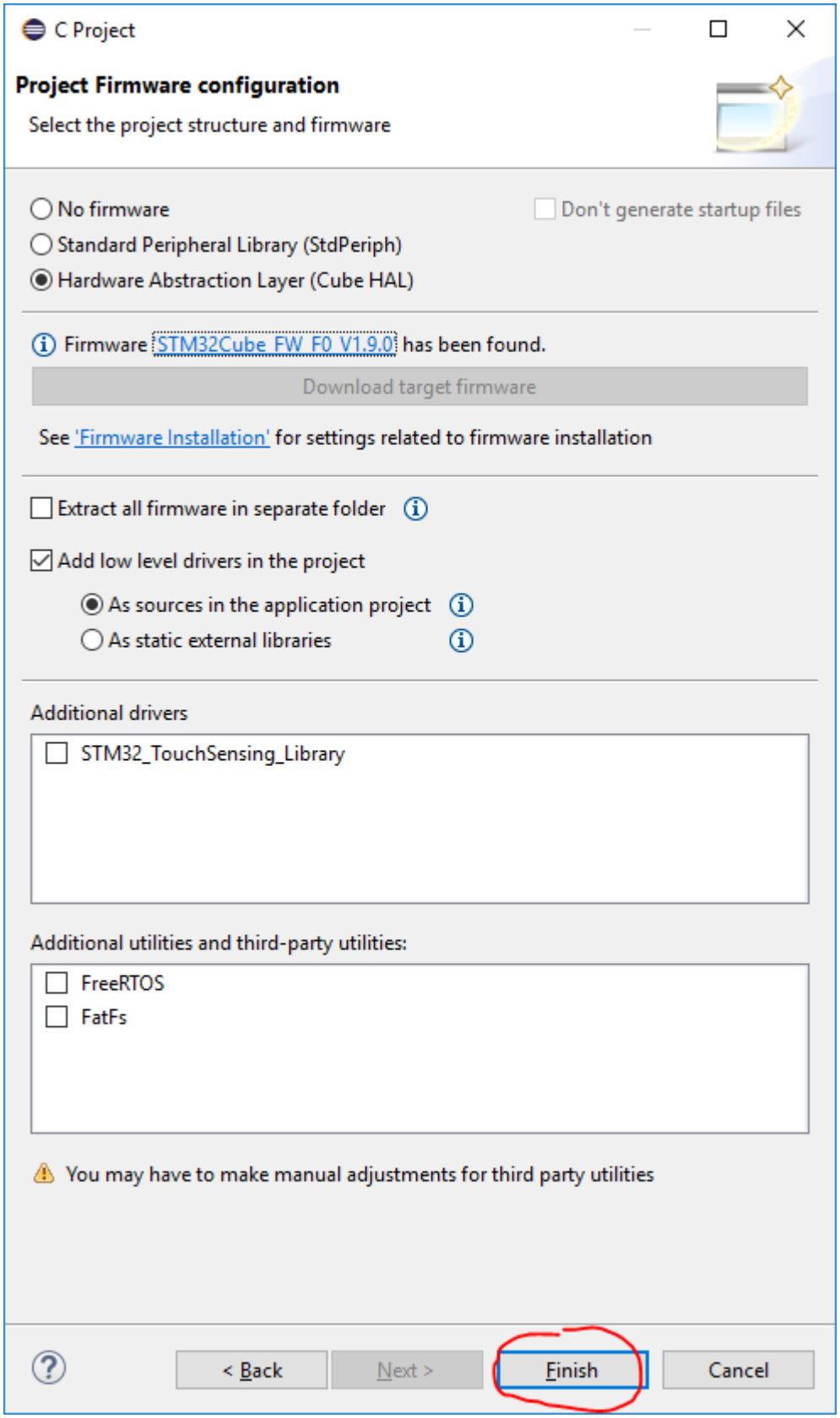

workspace - C/C++ - Eclipse
File Edit Source Refactor Navigate Search Project Run Window Help
New Alt+Shift+N
Open File...
Open Projects from File System...
Close Ctrl+W
Close All Ctrl+Shift+W
Save Ctrl+S
Save As...
Save All Ctrl+Shift+S
Revert
Move...
Rename... F2
Refresh F5
Convert Line Delimiters To
Print... Ctrl+P
Switch Workspace
Restart
Import...
Export...
Properties Alt+Enter
Exit
Makefile Project with Existing Code
C++ Project
C Project
C/C++ Project
Project...
Convert to a C/C++ Autotools Project
Convert to a C/C++ Project (Adds C/C++ Nature)
Source Folder
Folder
Source File
Header File
File from Template
Class
Task
Example...
Other... Ctrl+N
Quick Access
An outline is not available.
Tasks Console Properties
0 items
Description Resource Path
Updates Available
Updates are available for your software.
Click to review and install updates.
Set up Reminder options
0 items selected


C Project
C Project
Create C project of selected type
Project name: asdf
Use default location
Location: C:\Users\bucekj\workspace\asdf
Browse...
Choose file system: default
Project type:
Toolchains:
GNU Autotools
Executable
Empty Project
Ac6 STM32 MCU Project
Hello World ANSI C Project
Shared Library
Static Library
Makefile project
Ac6 STM32 MCU GCC
Show project types and toolchains only if they are supported on the platform
< Back
Next >
Finish
Cancel


C Project
Select Configurations
Select platforms and configurations you wish to deploy on
Project type: Executable
Toolchains: Ac6 STM32 MCU GCC
Configurations:
Debug
Release
Select all
Deselect all
Advanced settings...
Use "Advanced settings" button to edit project's properties.
Additional configurations can be added after project creation.
Use "Manage configurations" buttons either on toolbar or on property pages.
< Back
Next >
Finish
Cancel


C Project
Target Configuration
Select either the mcu or the board target and configurations
Mcu
Board
Show ST Discovery boards
Show ST EVAL boards
Show ST NUCLEO boards
Show custom boards
Series :
STM32F0
Board :
NUCLEO-F030R8
Create a new custom board
Remove this custom board
Mcu
STM32F030R8Tx
Core
ARM Cortex-M0
Package
LQFP64
Memory 'RAM'
Size 0x2000 (@0x20000000)
Memory 'ROM'
Size 0x10000 (@0x8000000)
< Back
Next >
Finish
Cancel


C Project
Project Firmware configuration
Select the project structure and firmware
No firmware
Don't generate startup files
Standard Peripheral Library (StdPeriph)
Hardware Abstraction Layer (Cube HAL)
Target firmware has not been found locally, please install it !
Download target firmware
See 'Firmware Installation' for settings related to firmware installation
Extract all firmware in separate folder
Add low level drivers in the project
As sources in the application project
As static external libraries
Additional drivers
Additional utilities and third-party utilities:
You may have to make manual adjustments for third party utilities
< Back
Next >
Finish
Cancel



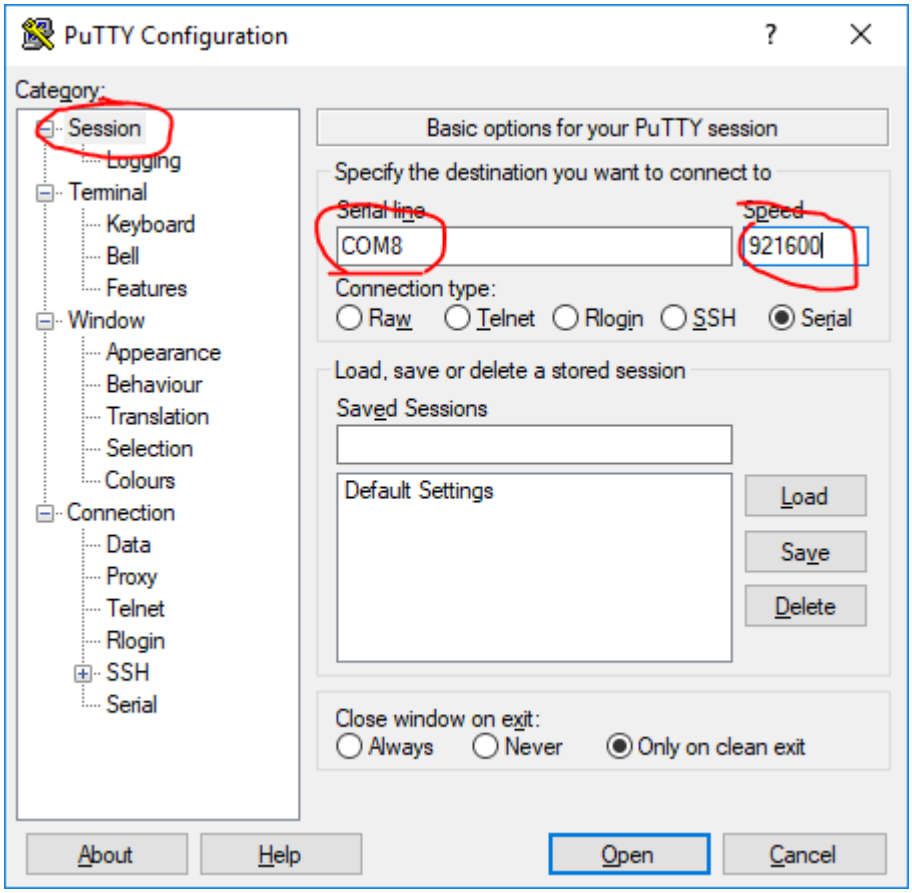
Communication with the device:

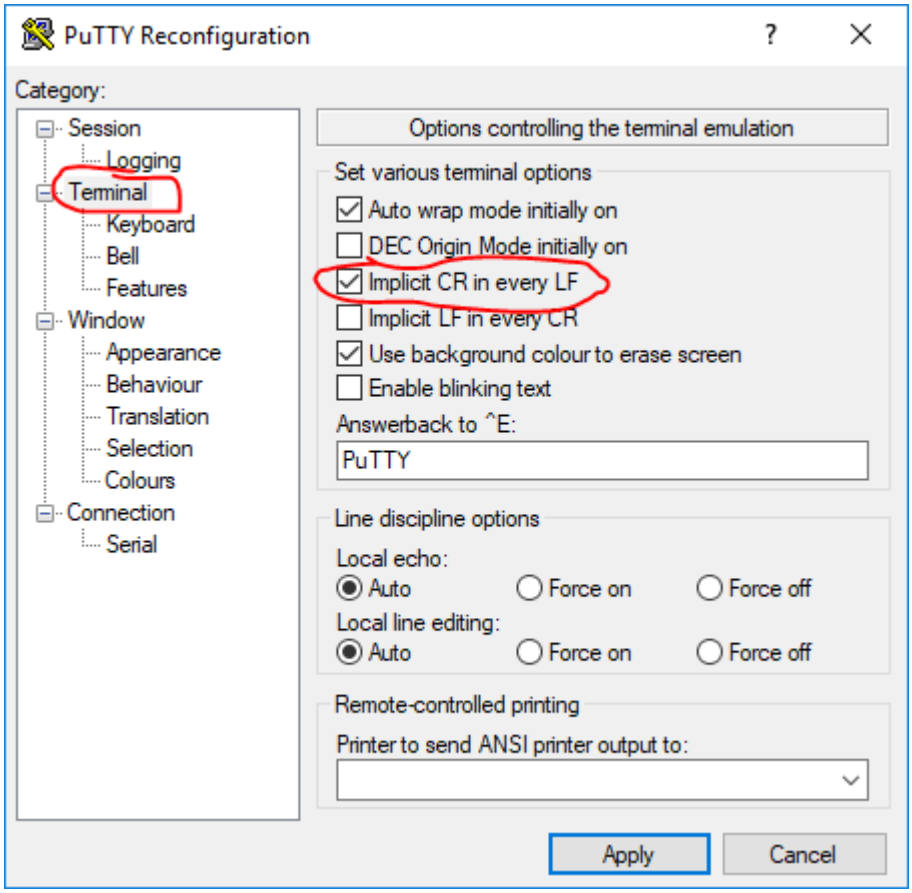
Komunikace s přípravkem:

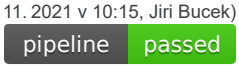
Na Windows i Linuxu funguje PuTTY, na linuxu navíc z příkazové řádky i např. miniterm:

```
miniterm --eol LF /dev/ttyACM0 921600
```

Přesné číslo portu (COM?, ttyACM?) záleží na konkrétním počítači.






pipeline
passed