

Base de Conhecimento > Products > How can you check whether the binary firmware file was copied correctly from Hirschmann to your computer?

How can you check whether the binary firmware file was copied correctly from Hirschmann to your computer?

- 2024-09-19 - Products

Hirschmann provides zipped folders for firmware. Within the folder you find the binary and an additional file with the hash value of the binary.

E.g. HiOS-MSP-06102.bin-sha256.txt contains one line:

"8e98dd3098f455390734547c015d076a051affeb66cb3ae2ad7f8d7799b6c0c8 *HiOS-MSP-06102.bin".

Calculating the SHA256 hash of the binary shall deliver the same value like in the txt file, if not a bit error occured during the copy process.

How can you calculate the hash?

- Win Windows 7 you can install the Powershell 4 (Windows 10 already contains the Powershell).
 - With command "get-FileHash -Algorithm SHA256 <file name>" you get the SHA256 hash value of the file.
- Another program for this calculation is "HashCheck Shell Extension"

Please note: this process has nothing to do with security, it's just to detect damaged files after copy process. Is it worth checking it? Only when a firmware update fails and you don't know a better reason.

Why does Hirschmann now use SHA256 algorithm instead of MD5 like with previous firmware releases? - Because people might have read about MD5 and SHA1 not being secure anymore, thus being unsettled and keeping us busy with phone calls. Again: MD5 offers the same without any drawback in this case.