Smart home and building solutions.
Global. Secure. Connected.

FIRMWARE UPDATE via KNX RF

Requirements and Solution

Christian Gossé
Actimage - Gossé&Tech Tapko

Some information

Christian Gossé, the KNX-RF & EASY KNX expert Joins Actimage GmbH, a German company specialized in Software Data Intelligence.

Combining mobile and cloud with embedded and IoT areas, Actimage GmbH is extending its expertise further by including the KNX technology into its core business. This is a new challenge for the company specializing in digital solutions for the last 23 years.

actimage | digital intelligence

Today, he works for Actimage GmbH as a Business Manager and grabs the chance to share his KNX know-how with the team. The KNX communication protocol stack, device system software and development standards are now no secret for Actimage GmbH.

TAPKO GOSSÉ & TECH

Gossé&Tech Tapko still continues to provide KNX technologies, but all dedicated software developments are now managed by Actimage GmbH.

Agenda

1. Requirements
2. Principles of Firmware Update via RF (**O**ver **T**he **A**ir)
3. Transfer of Firmware's images
4. OTA images description
5. OTA server
6. OTA Client
7. OTA services
8. OTA examples
9. Conclusion

KNX Requirements

2.6.3.5 Firmware update

KNX devices that support KNX Data Security shall foresee the possibility of a firmware update. This shall allow that shortcomings and bugs in the implementation of KNX Data Security can be corrected in the installed devices.

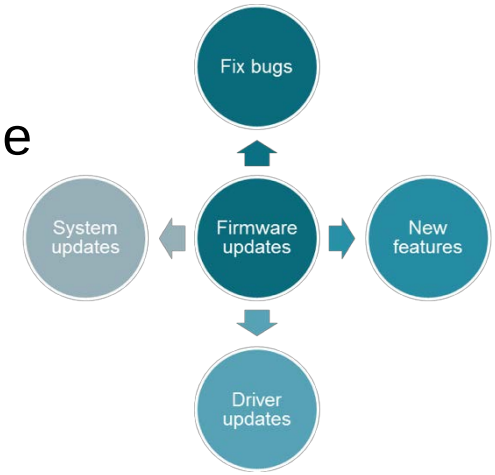
- The means for accomplishing a firmware update are implementation specific.

  EXAMPLE 30 This can be a Device Configuration App in ETS; this can be a stand-alone tool; this can be performed over the bus using KNX Standard services and Management Procedures or manufacturer specific services; this can be done locally on the device.
- The target of the firmware (security algorithm bugs, parameters, algorithms change, other KNX stack code, other software in the device…) is not fixed.
- There are no requirements towards the hardware resources (like memory size) of the firmware update.

KNX Association will not oblige a KNX manufacturer to provide and deploy a firmware, also not after a certain time, like after detection of any need for this or after the approval of any system extension. New devices brought onto the market shall however reflect the current state of the KNX security specifications – 6 months after publication of the AS version.

Device and Project Requirements

- OTA download shall not interrupt Application runtime



- OTA download may be organized in 2 steps
  1. Download of new firmware
  2. Switch to new download firmware

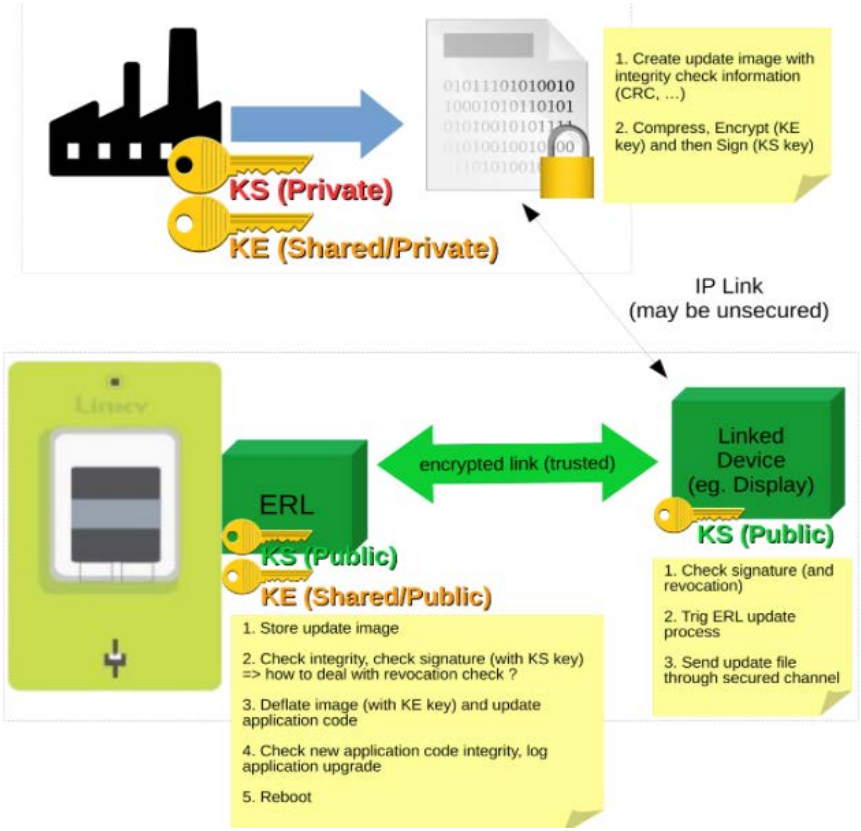
- As receiver may be multi-MCU device, the download could handle multi firmware updates. This packet of binaries is called “OTA image”

Principles

- Use the KNX RF to download new firmware binaries Over The Air (OTA)
- The update sequence is always started from a tool (OTA client) and not the device (OTA server)
- The OTA client has the new image and all the sequence is triggered by the OTA client
- Execution of procedure implies that a secured link, using Easy push-Button KNX configuration is existing (AN169 Secure P Mode Configuration) between the OTA client and OTA server.
- Encryption and Authentication shall be used for the image download

Transfer of image

- The image is build in factory with a CRC (to check integrity)
- The image is transferred to the local client via internet with standard secured protocol.
- The OTA client gets a request from cloud platform to update the device
- OTA client start a update procedure with the OTA client
- OTA Server accepts or not the download (negative in case another update is in progress)



Transfer of image

- The OTA transfer can be interrupted and resumed. No timing constraints.
- The OTA image is downloaded using KNX services and shall take care of RF Duty Cycle.
- The only request is to keep sequence of continuous packets

Description of image

- Generic for mono MCU or multi MCU update

Update file offset (bytes)	+0	+1	+2	+3
0	CBC-MAC			
4	File format version	Reserved		Nb App descs
8	Reserved	App-ID #1		
12	App #1 length in bytes in update file			
16	Reserved	App-ID #2		
...	App #2 length in bytes in update file			
...	... App # ...			
(App #1 Offset) ...	Enc'd	Desc Version	Reserved (Update flags, ... ?)	
...	Version Major	Version Minor	Version Build	Hardware compatibility
...	Container Type	... (the whole container is encrypted if 'Enc'd' bit is set)		
(App #2 Offset) ...	Enc'd	Desc Version	Reserved (Update flags, ... ?)	
...	Version Major	Version Minor	Version Build	Hardware compatibility
...	Container Type	... (the whole container is encrypted if 'Enc'd' bit is set)		
(App #... Offset) ...	... App # ...			
End Of File				

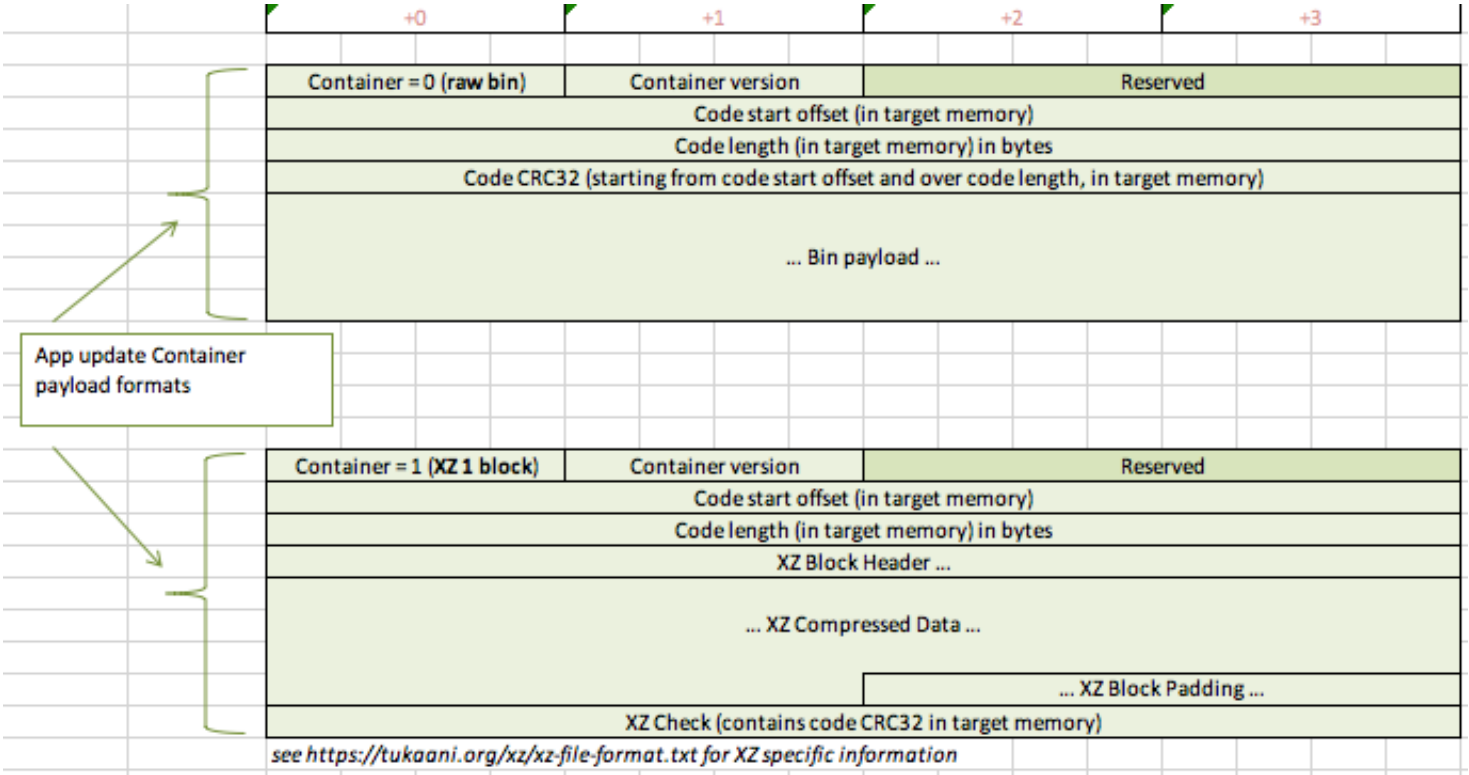
Index table
- Entries listed in order of appearence in the file (meaning growing offsets)

App #1 update description and payload

App #2 update description and payload

Description of image

- With Bin or Compressed Data



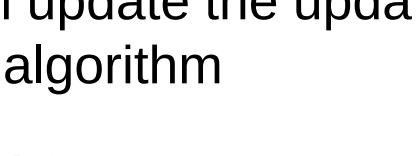
Description of image

Firmware_ARM.bin	03/06/2018 14:40	BIN File	263 KB
Firmware_ARM_And_KNX_compressed.upd	26/06/2018 12:03	UPD File	187 KB
Firmware_ARM_And_KNX_uncompressed.upd	26/06/2018 12:03	UPD File	308 KB
Firmware_ARM_compressed.upd	26/06/2018 12:03	UPD File	168 KB
Firmware_ARM_uncompressed.upd	26/06/2018 12:03	UPD File	263 KB
Firmware_KNX.bin	28/03/2018 10:59	BIN File	45 KB
Firmware_KNX_compressed.upd	26/06/2018 12:03	UPD File	19 KB
Firmware_KNX_uncompressed.upd	26/06/2018 12:03	UPD File	45 KB

308 KB to 187 KB => compression = 1,64 compression ratio= 39,2%
45 KB to 19 Kb => compression = 2,36 compression ratio= 57,6%

OTA Server Structure

- Bootloader : software able to launch RTOS, Updater
- Updater : module that can expand and check an image
- Updater Helper : module that can update the updater in case of change of compression or MAC algorithm
- Application :
  - KNX Stack
  - functional application
  - Other Protocol Stack



The Application shall always be able to download a new image

OTA Server Structure

- All configuration data and security “counters” must be kept in a specific memory storage that is not lost during OTA procedure.
- In case of modification of these data structures, it is up to the new application to updates these data.

OTA Client Structure

- The USB RF module to be used in any gateway was linked to the OTA client using Enhanced Push-button configuration
- Via a USB RF Push-button module connected to a Python Client
- Dedicated API : services to access KNX “P2P” services, properties (array of logs or parameters of application)

The Application shall always be able to download a new image

OTA Download services

- Via Function properties command(tested based on SystemNetworkParameterWrite) using Function property response via a private property.

- ***SYNC FACK***

This service is used to Synchronise the OTA acknowledge mechanism

00	Num Seq

- ***NEW_FILE***

This service is used to start the transfer of a new image. The CBCMac is used to identify the image between the beginning and the end of the transfer.

This will request the ERL to erase the Flash memory used for the transfer of the image.

01	Num Seq	Image CBCMAC	Image Size

- ***PACKET_CHUNK***

This service is used to transfer a bloc of data from the image. It must be done in sequence by increasing the offset. Any telegram with a sequence number smaller than the last received will just accept it without checking the received .

02	Num Seq	Len	Offset	Data [0]	…	Data [len-1]

OTA Download services

- ***END_OF_FILE***

To be sent at the end of the download to indicate to the ERL that it has to prepare the images for updating the different images.

03	Num Seq	CBCMAC of image

- ***ACTIVATE***

Request the ERL to use the new images, by doing a reset.

04	Num Seq	Action	CBCMAC image

OTA Download Tricks

- RF for concerned secure devices shall be RF-Multi and then providing FastAcknowledge is mandatory. The AckFrame format from the FunctionPropertyCommand coming from OTA Client is counted in the the OTA Client Dutycycle
- Function Property Response is replaced by the some values of the field Info in FastAcknowledge (one range of the future use [0101 rrrr] is not more future but this hasn't be proposed and agreed anywhere) rrrr=Num Seq.

6.6.4.4 Ack Frame format

The Ack Frame shall always be sent on the same RF channel as the Frame that it acknowledges.

The format of the Ack Frame shall be as specified in Figure 44.

Short Preamble	Synchro	KNX Ctrl	Info	CRC
18 chips	6 chips	1 octet	1 octet	2 octets

Figure 44 - Ack Frame format

- **Info**

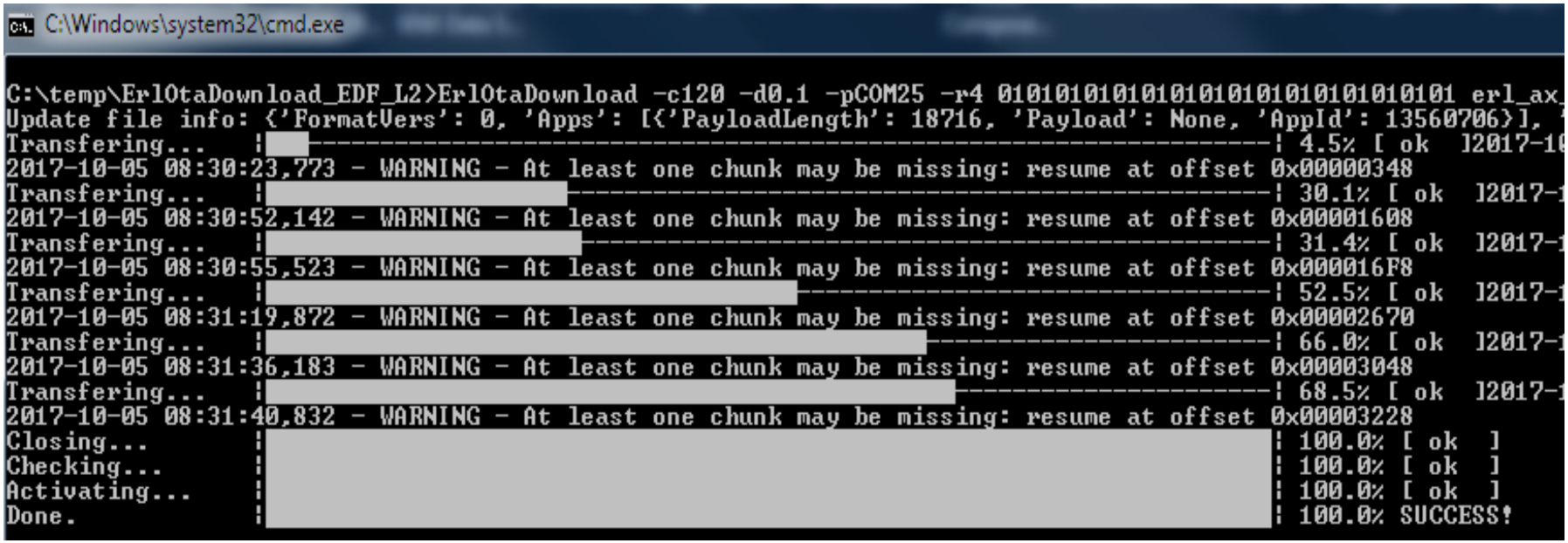
Encoding: 00h (Default value if not used. Otherwise optional values below shall be used)
0 rrr rrrr: Value:

- 000 x rrrr : RSSI value
  Reception level is calculated by [-113 dBm + 3 × RSSI Value (1 to 31)].
  If RSSI value = 31 the reception level is ≥ -20 dBm
- 0 01 r rrrr : Temperature (internal of the device, board temp)
- 0 10 r rrrr : Reserved for future use
- 0 11 r rrrr : Reserved for future use

OTA Download example

Device with 2 MCUs :

- ARM core for KNX Application and Zigbee Stack (Binary = 268Ko)
- KNX RF on SOC (Mcu + Sub GHz Transceiver). (Binary = 43Ko)

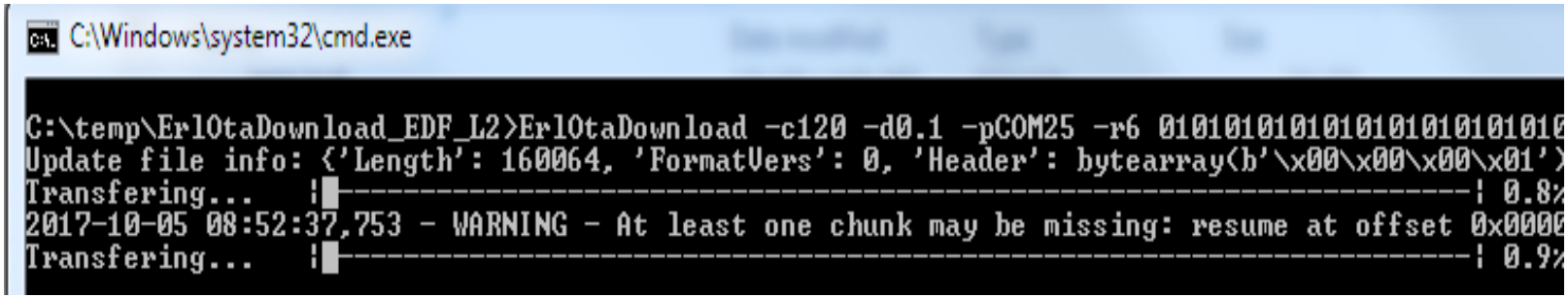


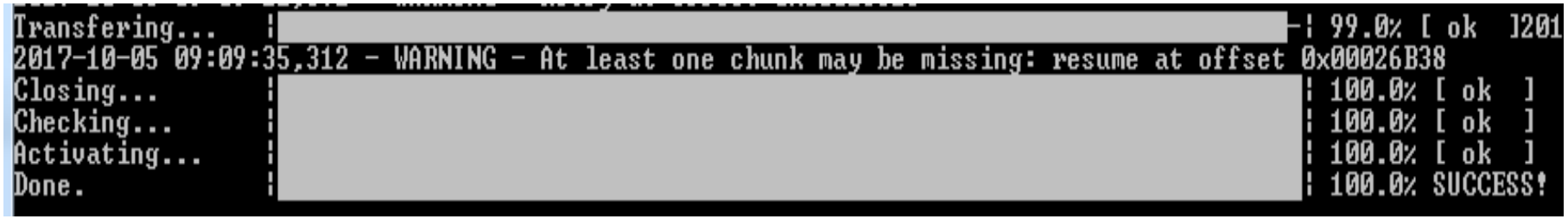
1 minute and 17 second for 18716 bytes (43Ko from KNX secondary MCU)

OTA Download exemple

Device with 2 MCUs :

- ARM core for KNX Application and Zigbee Stack (Binary = 268Ko)
- KNX RF on SOC (Mcu + Sub GHz Transciever). (Binary = 43Ko)





18 minutes for 160048 bytes (268Ko from KNX secondary MCU)

OTA Download example

Time to update ARM flash around 4-5 seconds
Time to update secondary KNX Mcu around 40 seconds

Maximum service update time when Application is not running = 1 minute

With this solution, update may take long time because we are using KNX RF protocol, But Runtime ”Out of Service” is only 1 minute.

Conclusion

- OTA has been deployed on 4 KNX RF Multi Secured -Devices
- Mechanism to ‘undo’ an update on the OTA server is not described and not implemented in all implementation due to memory size.
- It has been used during Field Test to update Application features on 100 devices without failure.
- An option to enable “Broadcast” update using is under consideration but could be complex on RF due to RF transmission possibilities.

Thanks.

Christian Gossé

Business Manager/Actimage – CEO/Gossé&Tech Tapko

+49 173 5390194

christian.gosse@actimage.com

For general questions:
info@knx.org – www.knx.org

Smart home and building solutions.
Global. Secure. Connected.

Join **us**
www.knx.org