HISTORY

Rev	Date	Comment	Author
A	10-Mar-2020	Initial	Thomas Wiedebusch
B	09-Jun-2020	Summarized review results	Thomas Wiedebusch

Copyright © 2020 by
SENSUS GmbH

REVIEWS

Rev	Date	Reviewer	Department
A	13-May-2020	Raymond Savarda	Product Security
A	13-May-2020	Rudolf Krupp	
A	13-May-2020	Jens Schulz	Marketing
A	13-May-2020	Andreas Pfeiffer	R&D
A	13-May-2020	Roland Drahbesch	Software Development
A	13-May-2020	Jörg Lachenmayer	R&D FW
A	29-Apr-2020	Frost Alex	R&D FW
A	13-May-2020	Dr. Joachim Baumann	
A	13-May-2020	Jörn Gögge	
A	13-May-2020	Jörn Vorwahl	
A	13-May-2020	Michael Schneider	

 Copyright ©2020 by SENSUS GmbH

LIST OF CONTENTS

1 General Part 6
1.1 Introduction 6
1.2 Document Content 6
1.3 System Overview 6
2 Prerequisites 7
2.1 Required SW 7
2.2 FW-Update Builder 7
2.2.1 LaaDB Content 7
2.2.2 LuDB Content 7
2.3 FW-Update Loader 7
2.3.1 Required HW 7
3 FW-Update Procedure 8
3.1 Update Demand Identification 8
3.2 Device List Generation 8
3.3 FW-Update Builder 8
3.3.1 Update Capability Verification 9
3.3.2 Password Collection 9
3.3.3 FW Collection 9
3.3.4 FW-Update SW Download 9
3.3.5 Key Generation 10
3.3.6 Encryption/Decryption 11
3.4 Key Exchange 11
3.5 Cordonel FW-Update Execution 11
3.5.1 Error Handling During Update 12
3.6 Update Procedure Failed Status 12
3.7 Order Closure 12
4 Security Concerns 13
4.1 SW Time Limitation 13
4.2 SW Security Bypassing 13
4.2.1 NET Framework Disassembly 13
4.2.2 RAM Investigation of Executed SW 14
4.3 Communication Logging 14
4.3.1 Serial Port Scanner 14
4.3.2 IrDA Sniffer 14
5 Contacts 14

 Copyright ©2020 by SENSUS GmbH

LIST OF TABLES

Table 1.1 Abbreviations *5*
Table 5.1 Contacts *14*

LIST OF PICTURES

Picture 1.1 System Overview *6*
Picture 3.1 FW-Update Builder *8*
Picture 3.2 Key Generation *10*
Picture 3.3 Offline Update *11*
Picture 4.1 Vulnerable Area *13*

 Copyright ©2020 by SENSUS GmbH

ABBREVIATIONS

ABC	Application Binary Container, this is the application code called Firmware
ADF	Applications Description File, a list of binaries (applications) for a valid combination including versions and CRCs
Cordonel™	Water meter with ultra-sonic measurement, initial name GENESIS
CRC	Cyclic Redundancy Check, used as checksum used to validate a binary file
DB	Data Base
EMEA	European, Middle East and African market.
FW	Firmware, this is a combination of several applications combined to an ABC.
GENESIS	Legacy name for the Cordonel™
HW	Hardware
ID	Identification number
IE	Industrial Engineering
IrDA	Infrared Data Association, used as serial communication interface
LaaDB	Laatzen data base, production DB with process and device information
LED	Light Emitting Diode, used as serial communication interface
LuDB	Ludwigshafen data base, BSI certified password and radio-addresses generator and server in
MRD	Marketing Requirement Document
NA	North American market
PCB	Printed Circuit Board, here the Cordonel™ electronics
R&D	Research and Development
SW	Software
tbd	to be defined
TBF	Test Bench Framework, the entire SW for the test benches and meters
TSC	Technical Service Centre (reclamation)
UM	User Manual
VPN	Virtual Private Network
UPort	Naming of an interface converter from USB to RS485 4-wire from MOXA-Company

Table 1.1 Abbreviations

 Copyright ©2020 by SENSUS GmbH

1 General Part

1.1 Introduction

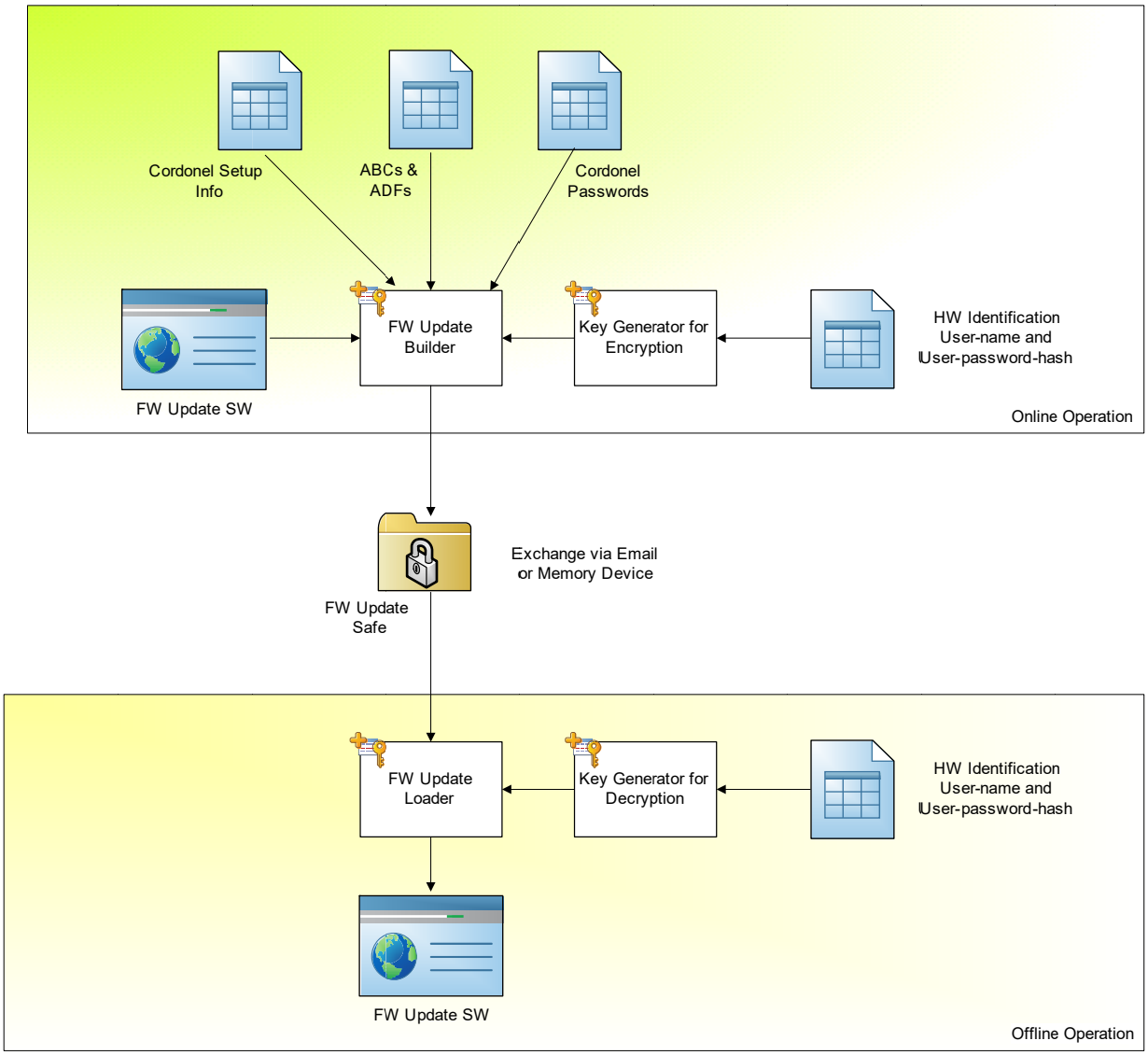
The Cordonel™ may need a FW update during life time. Before a secure process has been developed, an interim solution is needed to update the first samples. It is required being able to update the Cordonel™ offline without any connection to the SENSUS/Xylem network. For this process the IrDA interface shall be used.

1.2 Document Content

The document gives an overview of the FW-Update process. It covers the collection of necessary data, the encryption, the key-generation and exchange for the encrypted data container.

A special focus is being set to the security assessments to state the known risks as they are nowadays.

1.3 System Overview



Picture 1.1 System Overview

 Copyright ©2020 by SENSUS GmbH

2 Prerequisites

This chapter states the requirements needed before the "FW-Update SW" or the sub-modules can be used on a specific hardware.

2.1 Required SW

The Microsoft™ .NET framework 4.7.2 or higher has to installed on the PC.

2.2 FW-Update Builder

The FW-Update builder shall check the FW-Update capability, collect all data needed for the update process, build the encryption key and build the "FW-Update Safe".

Therefore the essential information is stored to several DBs being able to retrieve this information.

2.2.1 LaaDB Content

The LaaDB stores for each Cordonel™:

- ABC (Application-Binary-Container), this is the released and validated FW,
- ADF (Application-Description-File), this is the FW description file,
- PCB ID, HW identification, which can be read out from the Cordonel™ via NFC and IrDA,
- Meter ID, this can be a customer or SENSUS ID,
- Order number, giving information which production order is assigned to a specific device,
- Radio Address, needed to access the LuDB passwords and radio key,
- Cordonel™ core revision, the version which is installed on the product, history of installed FW, including the installed Metrology version, essential for update capability,
- History of registers setups,
- Meter size, needed for specific FW releases.

2.2.2 LuDB Content

The LuDB shall contain:

- Passwords level 7 per Cordonel, already implemented,
- Radio key, already implemented,
- Service technician Laptop identification (HW identification), NEW FEATURE,
- Service technician name and password hash, NEW FEATURE.

2.3 FW-Update Loader

The "FW-Update Loader" has to be installed on the Laptop which shall be used for the FW-Update process. This loader loads the "FW-Update Safe", decrypts it and executes the "FW-Update SW".

In fact an installation is here just a copy to a folder, the "FW-Update Loader" can be executed from any storage device as mobile application.

2.3.1 Required HW

To execute the "FW-Update SW" a special HW is needed to communicate via IrDA with the Cordonel™:

- Laptop with 1 free USB port, assigned to a user, HW identification needed,
- IrDA Interface with MOXA V2.0 (UPort 1130 with USB voltage converter 12V for IrDA head), this should be feasible to drive the current needed for the UPort.

 Copyright ©2020 by SENSUS GmbH

3 FW-Update Procedure

3.1 Update Demand Identification

On observed bugs or needed new features by R&D – IE or Customer – TSC a maintenance order has to be initiated. This step has to identify the FW with malfunctions and state the FW which solves the problem.

3.2 Device List Generation

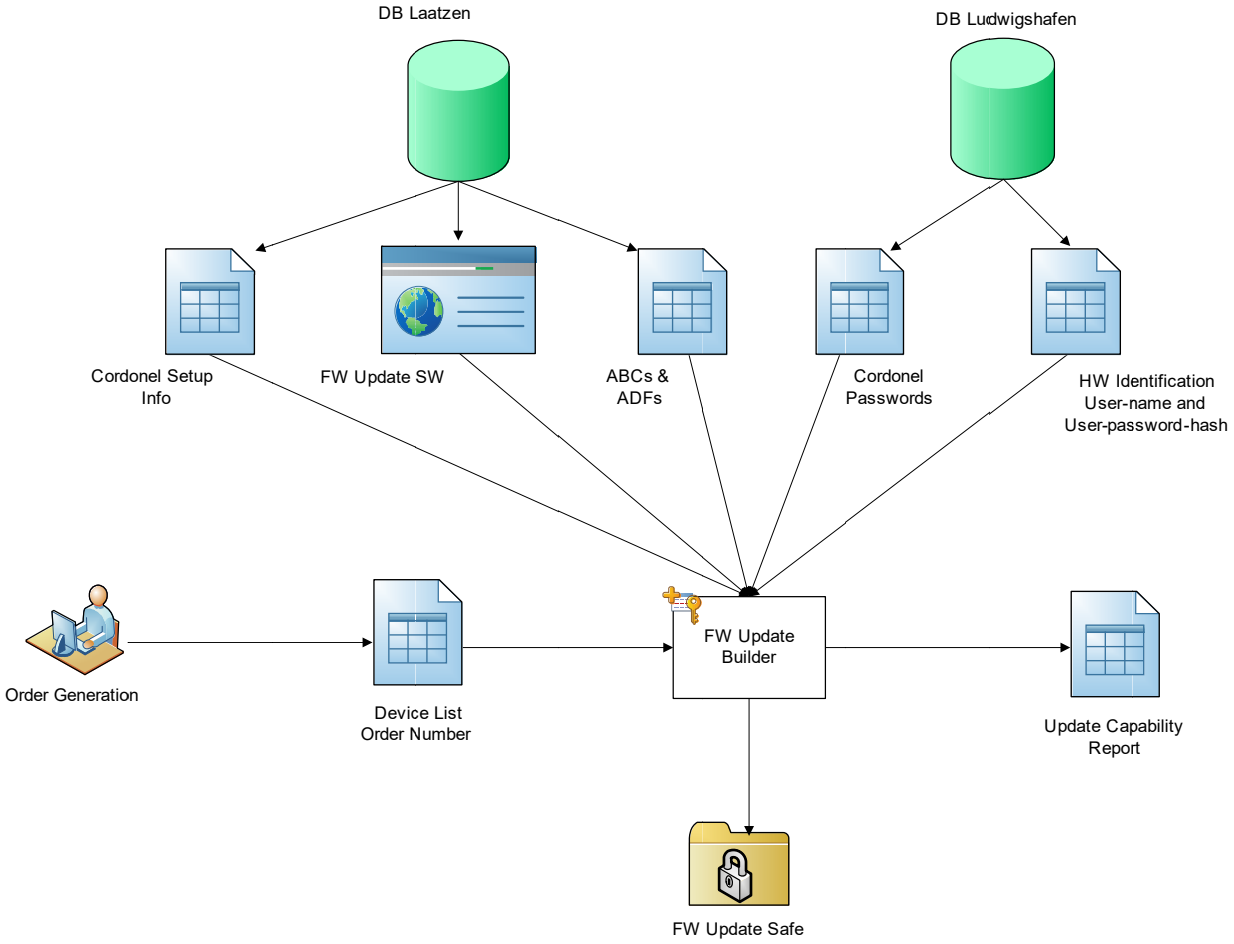
Out of the maintenance order, the "Device List" for the update candidates has to be built. This device list is essential for automatic collection of all data needed for the update. It should be delivered in machine readable format.

Useful might be an Excel™ spread sheet containing all devices for this update run identified by its PCB ID or Meter ID or, for EMEA, the Radio Address. The LaaDB has an entry which concatenates all these IDs and addresses.

Additionally the maintenance-technician has to be listed.

3.3 FW-Update Builder

The "FW-Update Builder" shall collect and verify all data needed to ensure an offline update of the group of Cordonels™ listed in the "Device List" [3.2 Device List Generation]. It shall build the "FW-Update Safe" which is an encrypted container to be delivered to the "FW-Update Loader".



Picture 3.1 FW-Update Builder

 Copyright ©2020 by SENSUS GmbH

The “FW-Update Safe” shall contain:

- FW-Update SW, this avoids installation of the SW to a Laptop and also has the smart advantage, that always the latest validated version will be used,
- Password level 7, per device identified by PCB ID,
- ADF and ABC, per device identified by PCB ID.

The “FW Update Safe” content is exclusively based on the PCB ID, because this ID can be read from the Cordonel™ via the communication interface. As the “Device List” can identify the device by PCB ID, Meter ID, Radio Address, the “FW-Update Builder” is going to select the according PCB ID.

3.3.1 Update Capability Verification

An update capability verification using the LaaDB shall be executed. Therefor the update list has to be fed to the “FW-Update Builder”.

Using the history information of the LaaDB it will be checked for each device the:

- Core Revision, not every Core Revision of the Cordonel™ can handle new FW releases,
- Metrology version, update will be denied if intended FW does not contain the identical metrology because the update of the metrology is forbidden,
- HW check for 433 or 868MHz, a FW is specifically for a dedicated radio frequency,
- HW revision check, if FW can be used with this specific PCB or HW,
- Meter size, each meter size has its own FW.

3.3.2 Password Collection

Login on LuDB with Token,

For each device:

- Use order number and radio address to collect password level 7.

3.3.3 FW Collection

For each device:

- Collection of ADF and ABC from LaaDB.

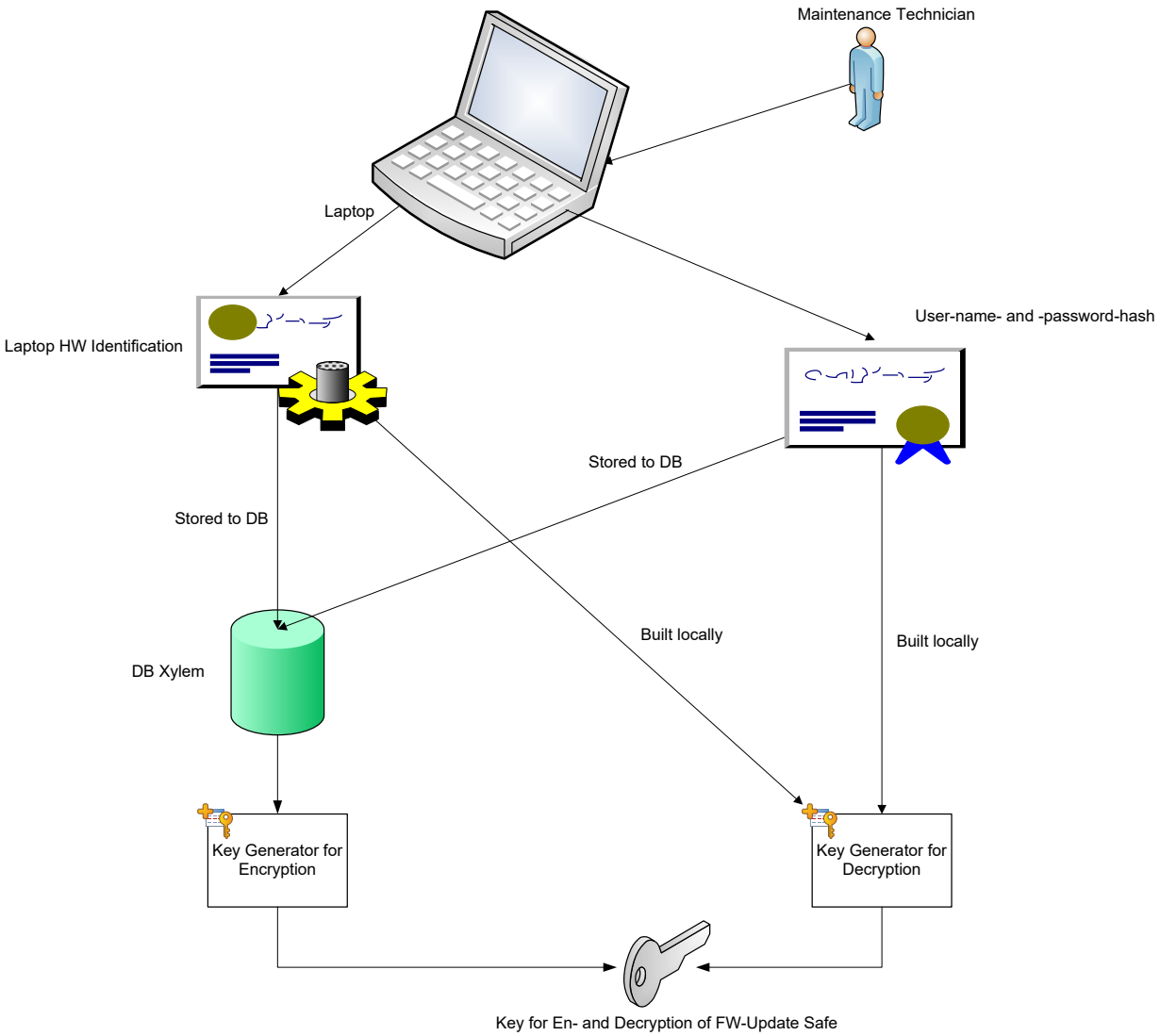
3.3.4 FW-Update SW Download

Specify actual “FW-Update SW” and download version from LaaDB.

 Copyright ©2020 by SENSUS GmbH

3.3.5 Key Generation

The key is required to encrypt and decrypt the “FW-Update Safe”. A user (maintenance technician) and a HW have to be assigned.



Picture 3.2 Key Generation

To build a generic key (AES256) and avoid an unsecure key exchange, the key shall be generated with the usage of information already attached to a specific HW and user without manual interaction:

- Locked on a specific HW, the Laptop of the service technician, stored and recovered from LuDB for the encryption process, built locally on decryption process,
- Assigned to user-name and user-password-hash, stored and recovered from LuDB for encryption process and built locally for decryption process.

Using the user-name and -password will bring some advantages and risks:

- The Xylem password policy will take care of the strength and also the expiration date of the password, the user-password-hash is stored on each device the user has been logged in as soon as he is connected to the network and therefore can be directly accessed by the “FW-Update Builder” and the “FW-Update Loader”,
- The risk and/or advantage is, that a password change will revoke the key validation,
- The key is temporary and nowhere stored in plain-text or encoded,

 Copyright ©2020 by SENSUS GmbH

- It is not needed to exchange the key on any unsecured channel.

3.3.6 Encryption/Decryption

The encryption shall use the generated key, a salt and an initialization vector randomly generated.

Therefore the AES-GCM from the open-source bouncy castle C# library to encrypt the data shall be used. This provides both authentication and encryption with a single Key.

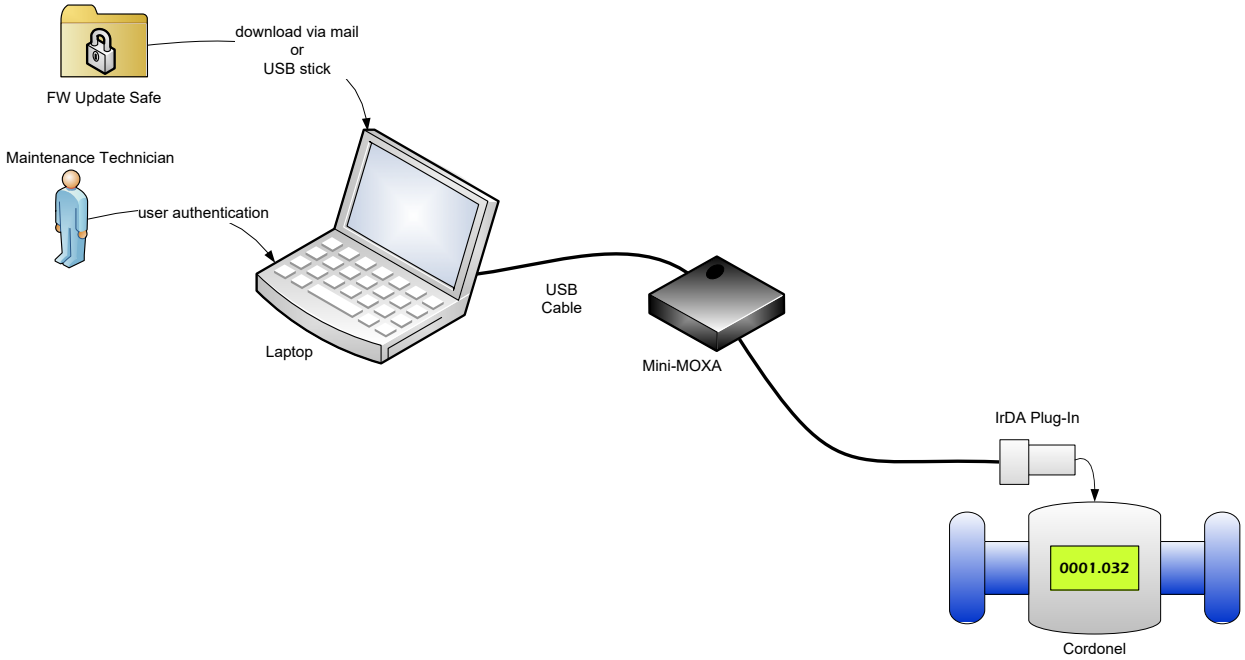
The salt shall be generated using the "System.Security.Cryptography.RNGCryptoServiceProvider" which is part of the .NET framework.

3.4 Key Exchange

Not needed according to chapter [3.3.5 Key Generation] if the key generation is based on HW identification and user-authorisation.

3.5 Cordonel FW-Update Execution

The "FW-Update Safe" has to be copied to the Notebook of the maintenance technician and the user has to login to the device.



Picture 3.3 Offline Update

The "FW-Update Loader" has to be started and the "FW-Update Safe" has to be loaded. Then the following processing steps shall be executed:

- Generate the key using the Laptop HW identification, the user-name and –password hash,
- Decrypt "FW-Update Safe", using the generated key, the salt and initialization vector from "FW-Update Safe",
- Start "FW-Update SW" out of "FW-Update Safe",
- Wait on user interaction to [START] the FW-update,
- Port Auto-Detection,
- Remote PCB ID from Cordonel,
- Load assigned ADF and ABC based on PCB ID,
- Execute update procedure,
- Avoid update of Metrology,
- Final check of update results, registers and password file,

 Copyright ©2020 by SENSUS GmbH

- Generate report, which has to be fed back to the LaaDB to keep the history up-to-date and close the order.

3.5.1 Error Handling During Update

On erroneous update the following interaction by the user is required:

- Artificial or natural light isolation,
- Check IrDA head positioning,
- Check the cabling,
- Check MOXA LED status,
- Start manual retries,
- tbd.

3.6 Update Procedure Failed Status

If the update procedure failed, then the old FW remains active.

The FW update failed if:

- The at least one application file is invalid, this will be checked by the bootloader of the Cordonel™ FW,
- Trigger upgrade execution failed.

3.7 Order Closure

Finally the order has to be closed and marked as executed. Therefore the LaaDB shall be updated with all required information for each updated Cordonel™:

- Installed Applications with versions and CRC,
- All register values which had been verified,
- Check if password file is valid (device secured).

All these information will automatically read back from the device and stored to a file without any manual interaction.

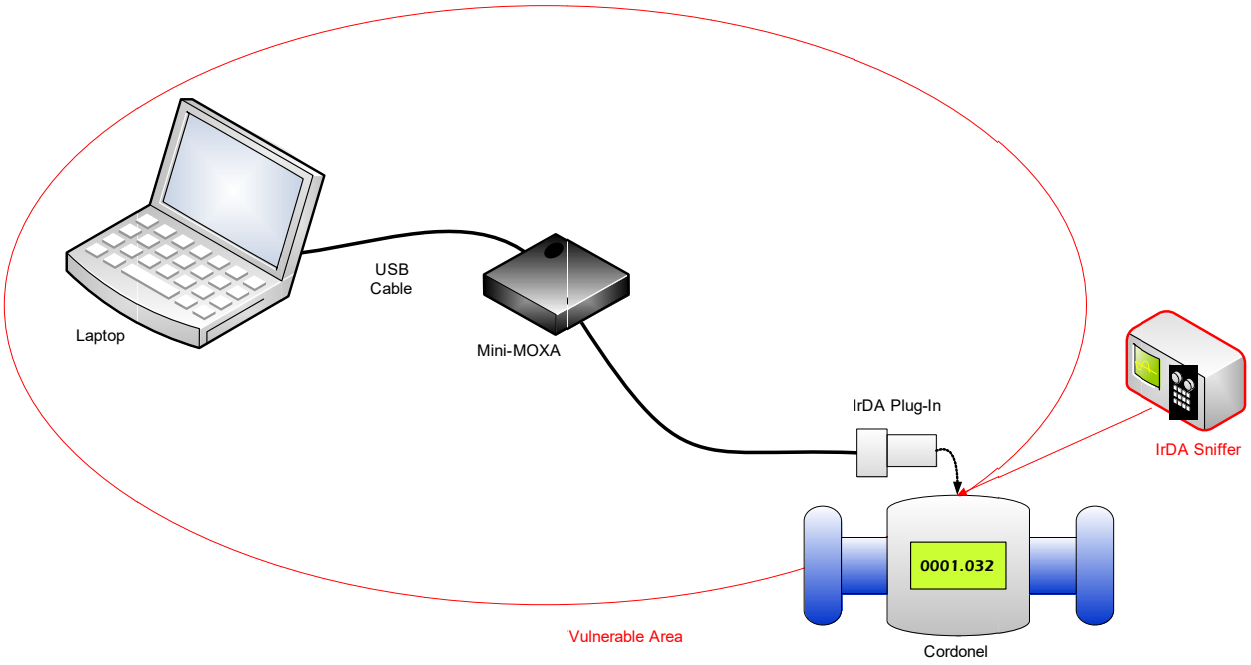
Meter history in LaaDB [2.2.1 LaaDB Content]:
Each Cordonel™ has an entire history of the production process including all register values at different production states and a history of the installed FWs. This is based on an individual identifier (Meter ID, PCB ID, radio address and/or order number). Additionally this data base contains a list of all released and approved FW versions (ABCs and ADFs) including identifications on which device (depending on size, radio frequency, PCB HW revision, metrology version and Cordonel™ Core Revision) this can be installed.

 Copyright ©2020 by SENSUS GmbH

4 Security Concerns

Even if this firmware update procedure is intended to be an interim solution for a short period, the risk assessment has to evaluate the security aspects of this solution.

As the SW can be seen as a security risk to access the Cordonel™ if the password has been compromised, it has to be avoided, that this SW can be used after it has been replaced by the commercial solution.



Picture 4.1 Vulnerable Area

To minimize the impact of this solution on security issues:

- A contract for the FW usage has to be made and signed by the user,
- A user manual shall be created,
- A user training has to be initiated.

4.1 SW Time Limitation

After the expiration time, it should be avoided, that the “FW-Update SW” can be executed.

4.2 SW Security Bypassing

Using one of the later mentioned methods to access the “FW-Update SW” code, it could be possible to use the “FW-Update SW” without the required access rights. The “FW-Update SW” is written in C# using the .NET framework from Microsoft™. On some code-lines the security verification like the license validation and the time limitation are executed. If these lines can be identified, it would be possible to bypass the validations.

4.2.1 NET Framework Disassembly

Because the .NET framework is using an intermediate language MSIL (Microsoft™ intermediate language), it is very simple to disassemble the “FW-Update SW” and use a development environment like MS Visual Studio™ to set breakpoints on a dedicated program line and change the validation.

 Copyright ©2020 by SENSUS GmbH

4.2.2 RAM Investigation of Executed SW

Soon the "FW-Update SW" is going to be executed, a RAM image can be taken to hijack the executable code and decompile or modify it.

4.3 Communication Logging

As the communication from the "FW-Update SW" and the Cordonel™ IrDA interface is not encrypted, this can be attacked on several access points. Here the password can be seen in "clear text" and all register accesses and protocols could be evaluated.

4.3.1 Serial Port Scanner

It could be possible to intercept the serial port communication with a serial port redirector. This software simulates a serial port, catches the communication and redirects it to the final hardware serial port.

4.3.2 IrDA Sniffer

A hardware IrDA interface can be used to monitor the communication by sniffing to the infra-red signals between the IrDA-Plugin and the Cordonel™ interface.

5 Contacts

Name	Function	Mail

Table 5.1 Contacts

 Copyright ©2020 by SENSUS GmbH