BMS for Drones and Small Systems, Incorporating Automotive Components

Iain Galloway

Drone Program Lead
Systems Innovation, CTO

October 2019 | Session #AMF-AUT-T3828

SECURE CONNECTIONS FOR A SMARTER WORLD

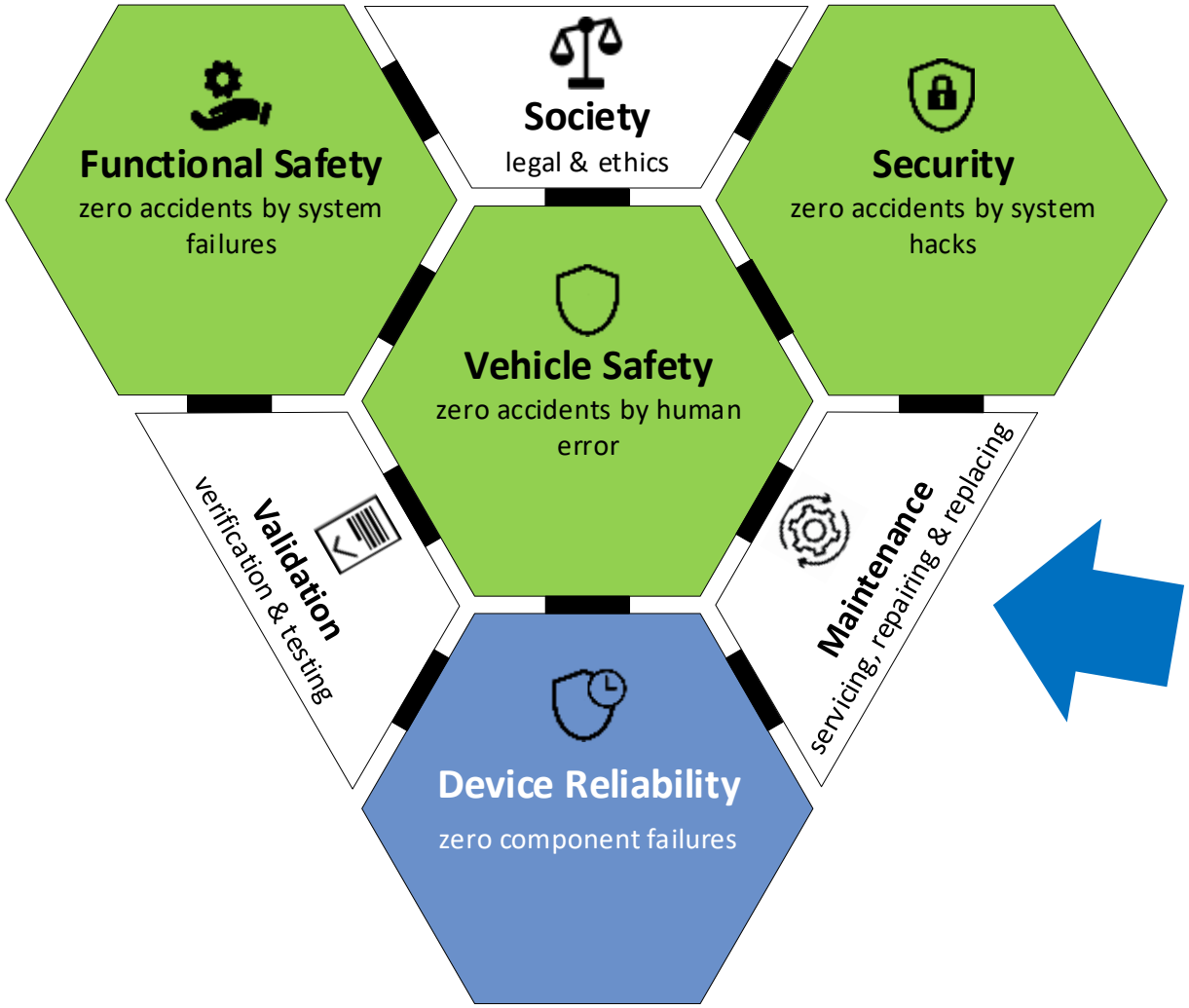
Welcome

- Drone Team at NXP?
- RDDRONE-BMS772
- Not quite the typical Ref Design
- Not “turn key complete” but rather a framework for open development
- Collaborative design process with Open Source drone community

Why this BMS

- Drone and Rover batteries may be abused for performance and not used like laptop or consumer batteries
- Limited ability to experiment
- Lack of non-proprietary battery health options
- Automotive grade*
- Other uses for this BMS
- Functional Playground for development
  - Universities, good enough BMS, security,

Elements of a Safe System



Monitoring, cycle counts and health of power system

Tricopter

Quadcopter

Hexacopter

Octocopter-Flat

Octocopter - Coax

Multicopter

Plane

Flying Wing

VTOL
Pusher Prop

Long Flight Duration

VTOL Transitioning Wing

Airship


Submarine


Delivery Rover


Boat

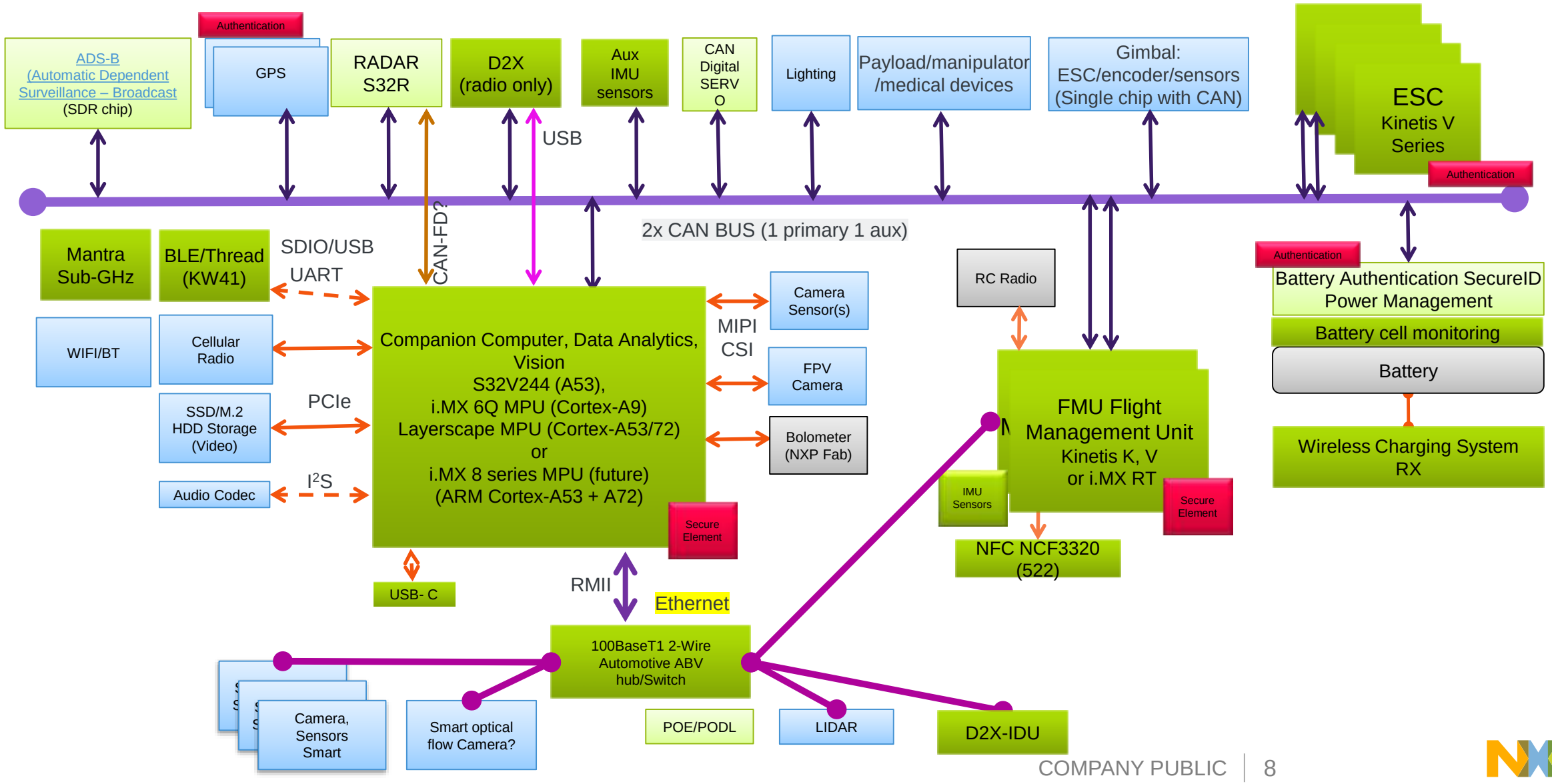

POLICE
Security


Lawnmower or Agricultural?

LuftTaxi
AirTaxi

VTOL reduction in greenhouse gas Emissions:
- 52% @60miles+ compared to ICE cars
- 6% @60 miles+ BEV
Starting for trips > 22 miles
https://www.nature.com/articles/s41467-019-09426-0

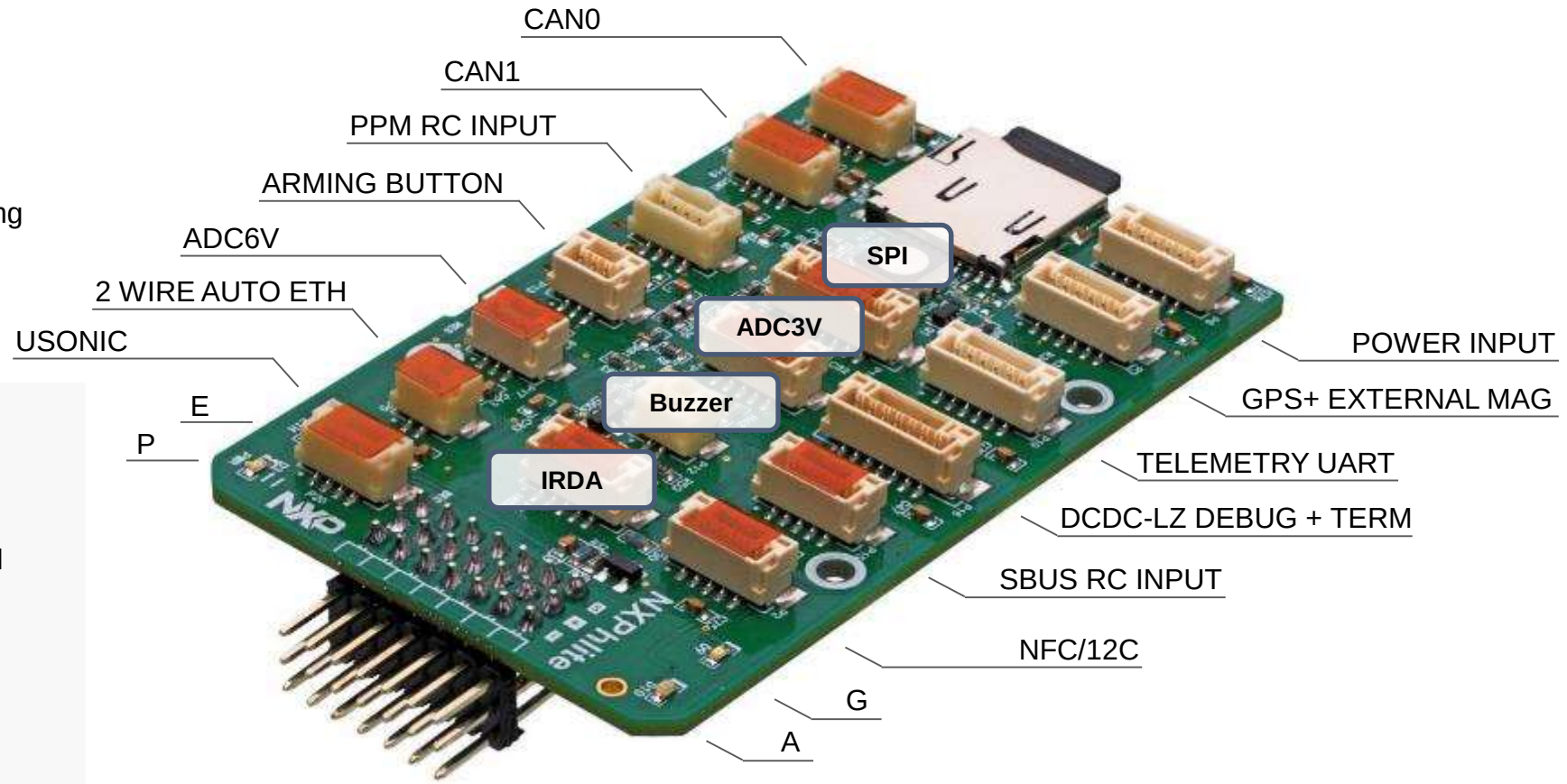
Industrial-Grade UAV – Modular with CAN and Ethernet



FMU Components

Vehicle Management Unit with Automotive Grade Components

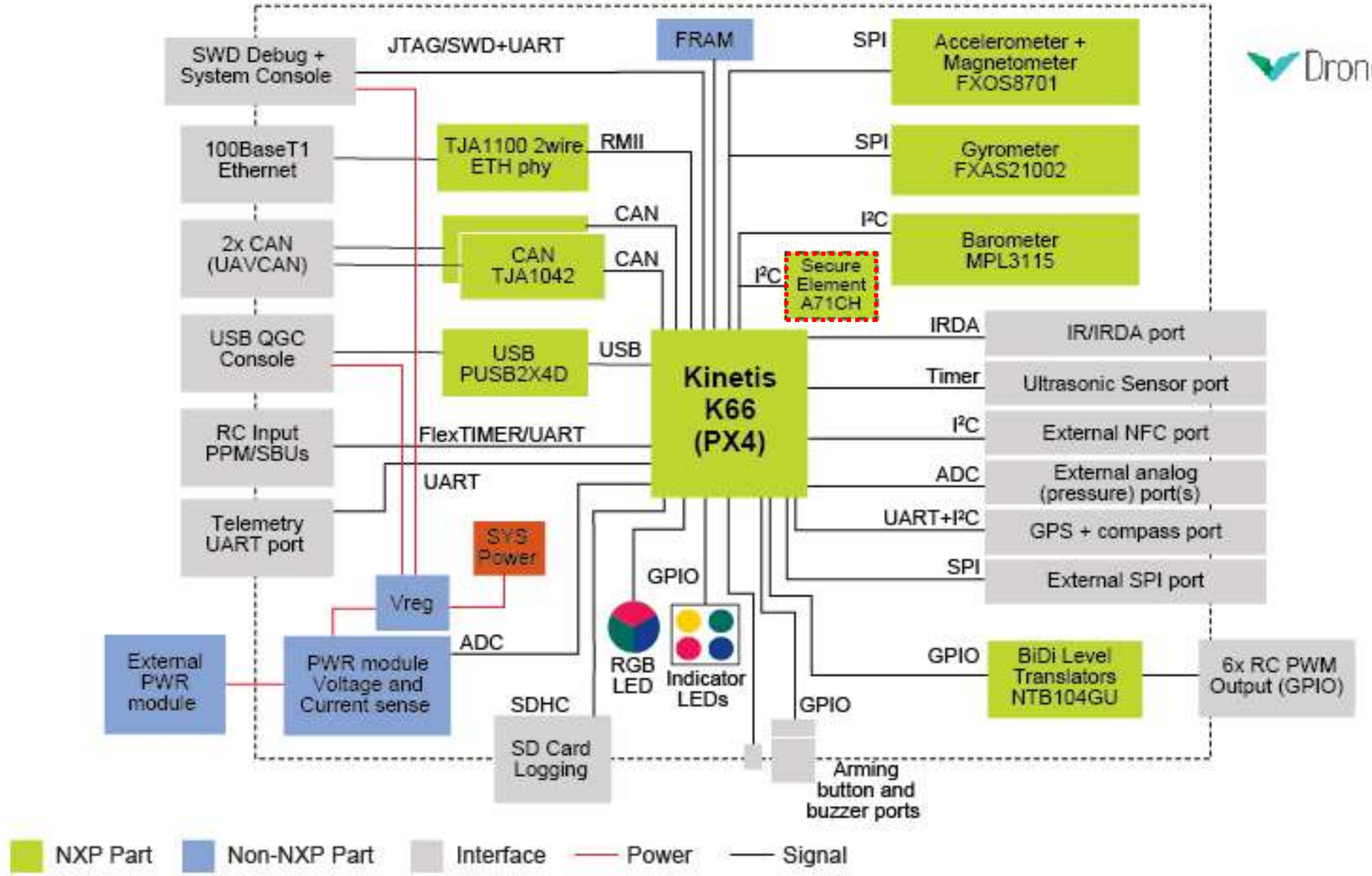
Supports required Drone interfaces:
RC input, PWM control output, GPS and Telemetry radios, Arming switch and beeper.



NXP differentiation by forward looking emphasis on:

- **CAN-FD** / UAVCAN peripheral enablement
- 100BaseT1 IEEE1588 **2-wire Ethernet**
- **Security and Authentication**

I HoverGames


SWD Debug + System Console
JTAG/SWD+UART
FRAM
SPI
Accelerometer + Magnetometer FXOS8701
Dronecode
100BaseT1 Ethernet
TJA1100 2wire ETH phy
RMII
SPI
Gyrometer FXAS21002
2x CAN (UAVCAN)
CAN
CAN TJA1042
CAN
I²C
Barometer MPL3115
I²C
Secure Element A71CH
USB QGC Console
USB PUSB2X4D
USB
Kinetis K66 (PX4)
IRDA
IR/IRDA port
Timer
Ultrasonic Sensor port
RC Input PPM/SBUs
FlexTIMER/UART
I²C
External NFC port
UART
ADC
External analog (pressure) port(s)
Telemetry UART port
SYS Power
UART+I²C
GPS + compass port
SPI
External SPI port
GPIO
Vreg
RGB LED
Indicator LEDs
External PWR module
PWR module Voltage and Current sense
ADC
GPIO
BiDi Level Translators NTB104GU
6x RC PWM Output (GPIO)
SDHC
GPIO
SD Card Logging
Arming button and buzzer ports
NXP Part
Non-NXP Part
Interface
Power
Signal

HoverGames Drone

Reference Design

- Complete low cost ‘hobby’ drone platform, but really an open design robot
- 500mm size big enough for easy experimentation
- Complete system to test new components such as motor controllers with UAVCAN or secure authentication of battery
- Reuse of components for ground rovers

PX4 is an Integrated Software Ecosystem

Vehicle Firmware	Communication MAVLINK MICRO AIR VEHICLE COMMUNICATION PROTOCOL	Ground Control Station QGroundControl	Hardware  pixhawk
Autonomy Vision based localization and avoidance	Middleware ROS2 2	API <dronecode/sdk>	 NXP RDDRONE FMUK66  Intel Aero

HoverGames Challenges

A complete autonomous vehicle development platform and infrastructure

- Coding challenges with larger societal impact theme
- INTERNAL
  - “First Flyers” 50 Teams, 200 participants, 30 countries
- EXTERNAL
  - 250 Teams , 1000 participants/followers

Smart BMS for Small Systems

Why this Project for PX4 Drones?

Dumb vs. Smart Batteries

Typically batteries contain no embedded controller or supervision system.

HoverGames drone KIT-HGDRONEK66 contains a Power Module Unit (PMU) that provides to the Flight Module Unit (FMU) an analog voltage and current measurement of the battery.

A PX4 FMU does its best effort to determine when the battery is drained based on current and voltage measurements over time.

Because frequency of measurement is low, and the analog measurement not very accurate, it is not possible to run a sophisticated algorithm to predict the State of Charge (SoC) of the battery accurately.

A smart battery embeds a controller that features several functions, such as cell voltage sensing, coulomb counting, current measurement, SoC calculation, cell balancing, protection, communication, etc.

RDDRONE-BMS772 (Automotive)

Battery Management for small systems

- Low Cost ~$20
- Up to 6S battery (25.2V)
- 90A continuous 200A peak
- Auto and consumer grade BOM
- CAN-FD/UAVCAN V1.0
- Secure authentication
- Secure event count and flags
- NFC for manifest log and settings
- S32K MCU development
- Dronecode Connector system
- HoverGames DCD-LZ debugger

RDDRONE-BMS772 Smart Battery Ref Design Features (1/2)

RDDRONE-BMS772 target features:

- Battery from 3s to 6s LiPo (or other) with stack voltage ranging from 6V to 26V
- Charge/Discharge current measurement up to 200A peak and 90A DC
- Cell balancing operation during charging
- Cell temperature measurement
- Ambient temperature range from -20°C to 60°C
- Battery shutdown in case of overcharging.
- DEEP SLEEP mode with <80µA leakage current
- Automatic SLEEP mode with <200µA current consumption

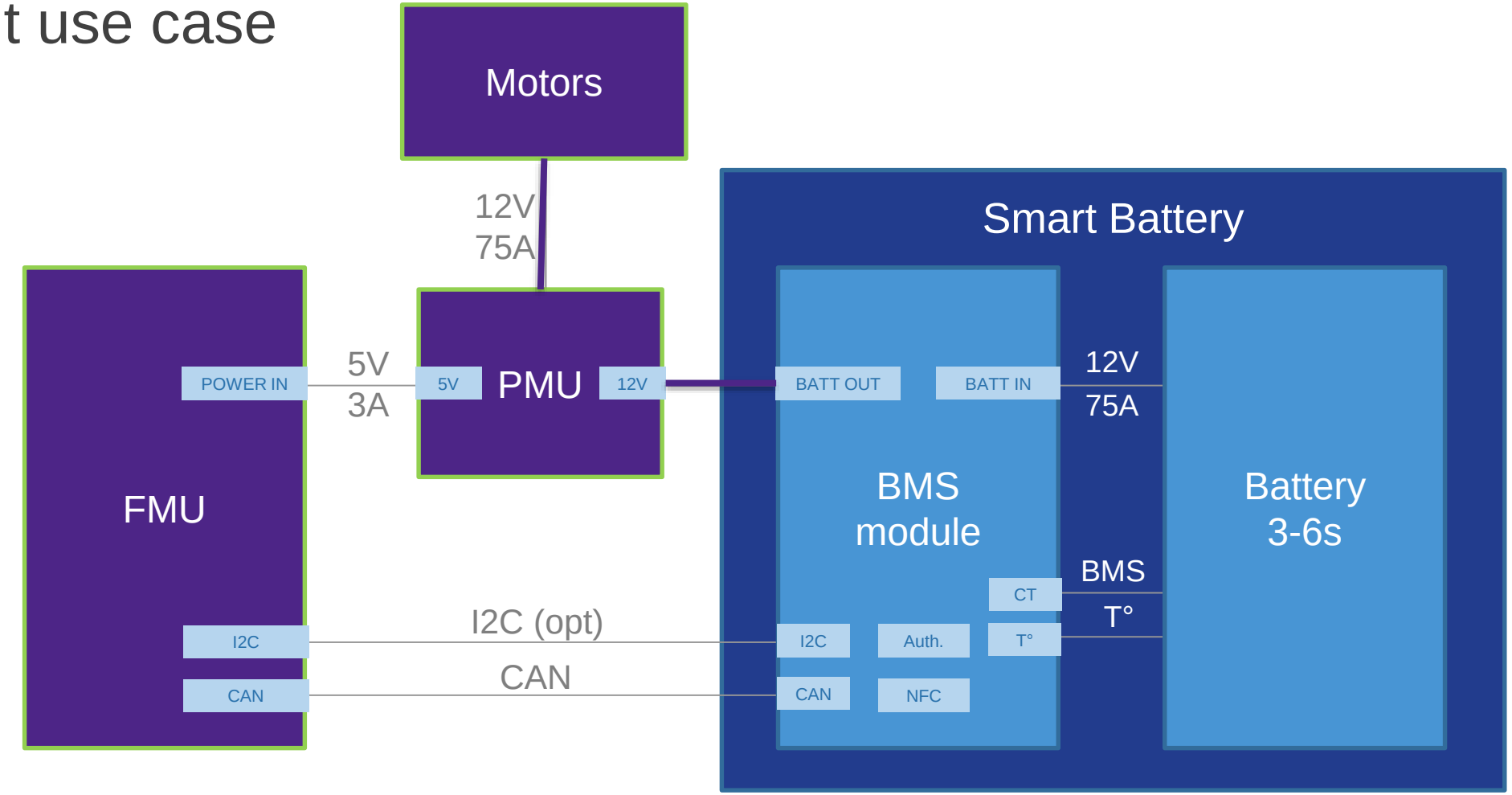
RDDRONE-BMS772 Smart Battery Ref Design Features (1/2)

RDDRONE-BMS772 target features:

- Authentication of the battery
- Diagnostics to verify the safe operation of the battery
- CAN communication following UAVCAN protocol every 100ms
- NFC communication with user to configure battery (shipping mode, number of cells, capacity, chemistry, etc.) and get main battery parameters (voltages, temperatures, currents, power, capacity, health, fault, etc.)
- SWD and JTAG debugging interface using J-Link Mini EDU shipped with HoverGames kit

Context: Our Smart Battery Architecture (1/2)

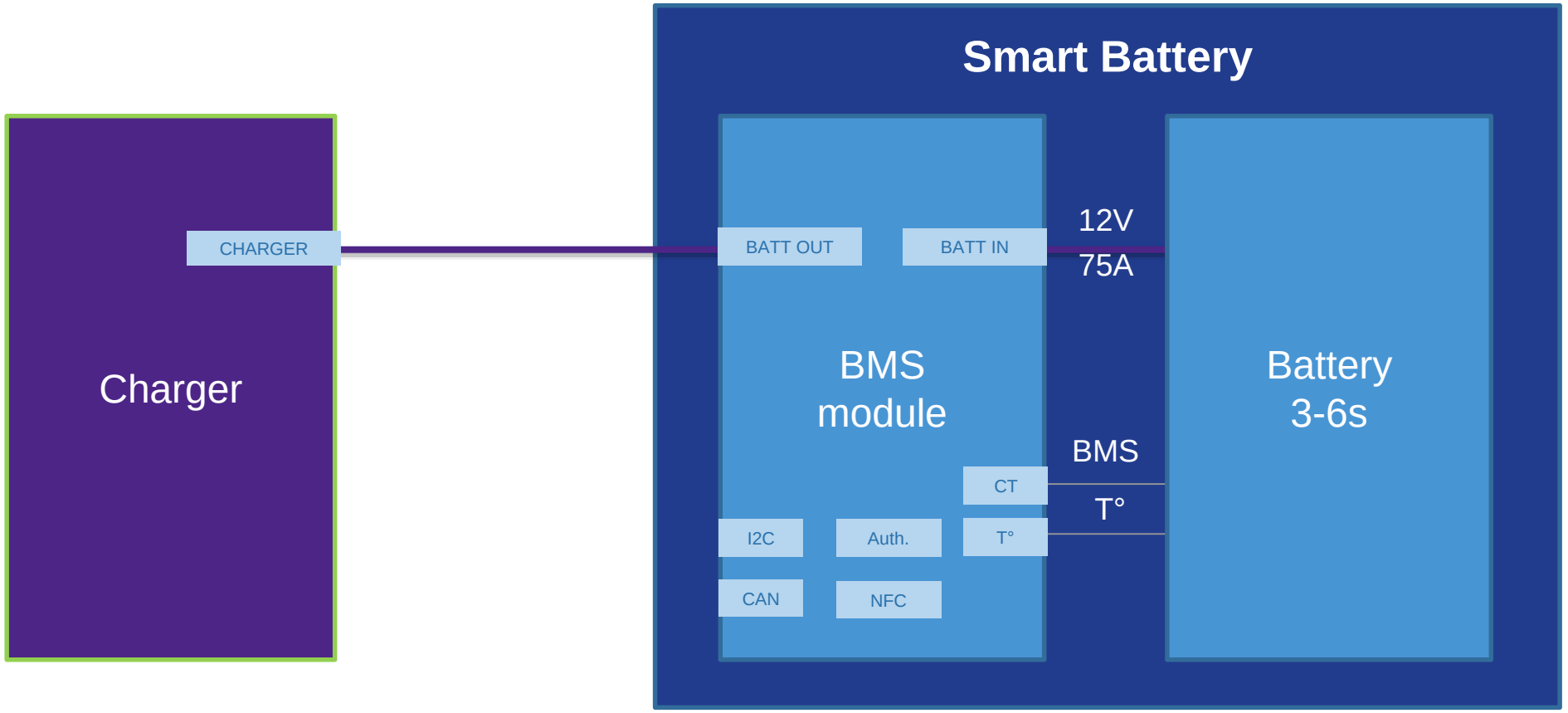
Flight use case



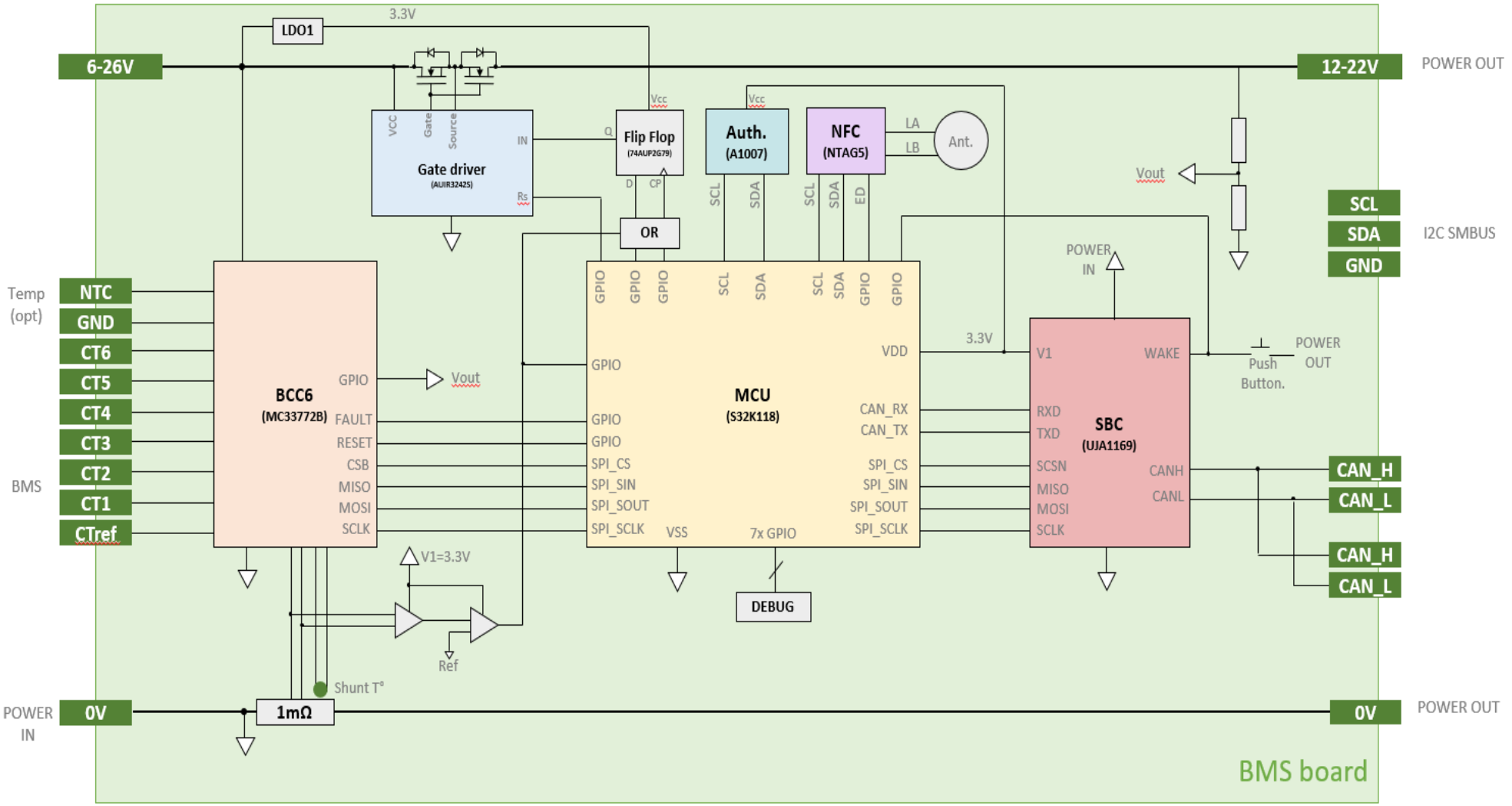
Context: Our Smart Battery Architecture (2/2)

Charge use case

- Charger can be simple power supply since balancing done at BMS level
- Protection of the battery from overcharging is done at BMS level

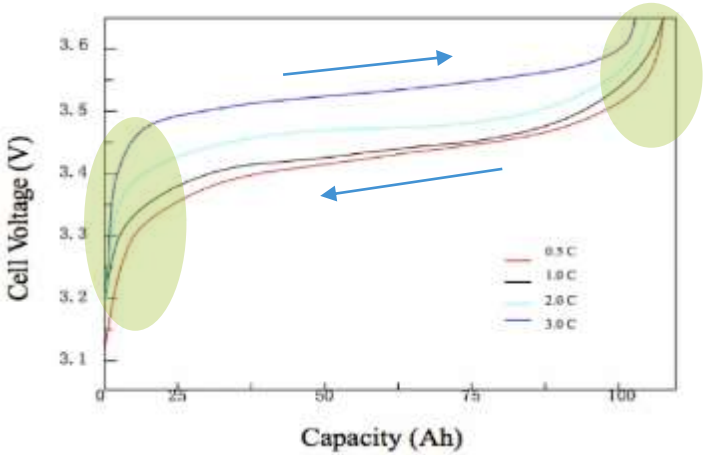
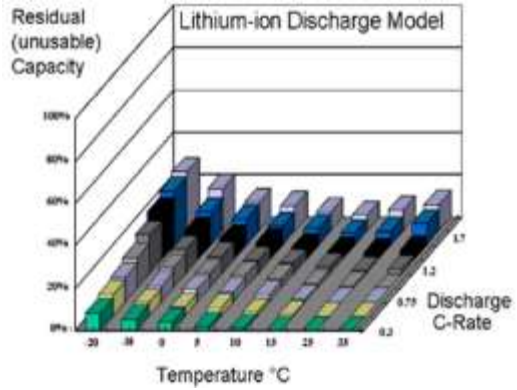
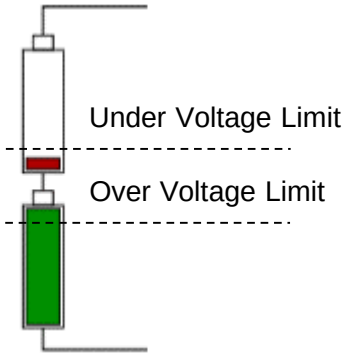


Block Diagram



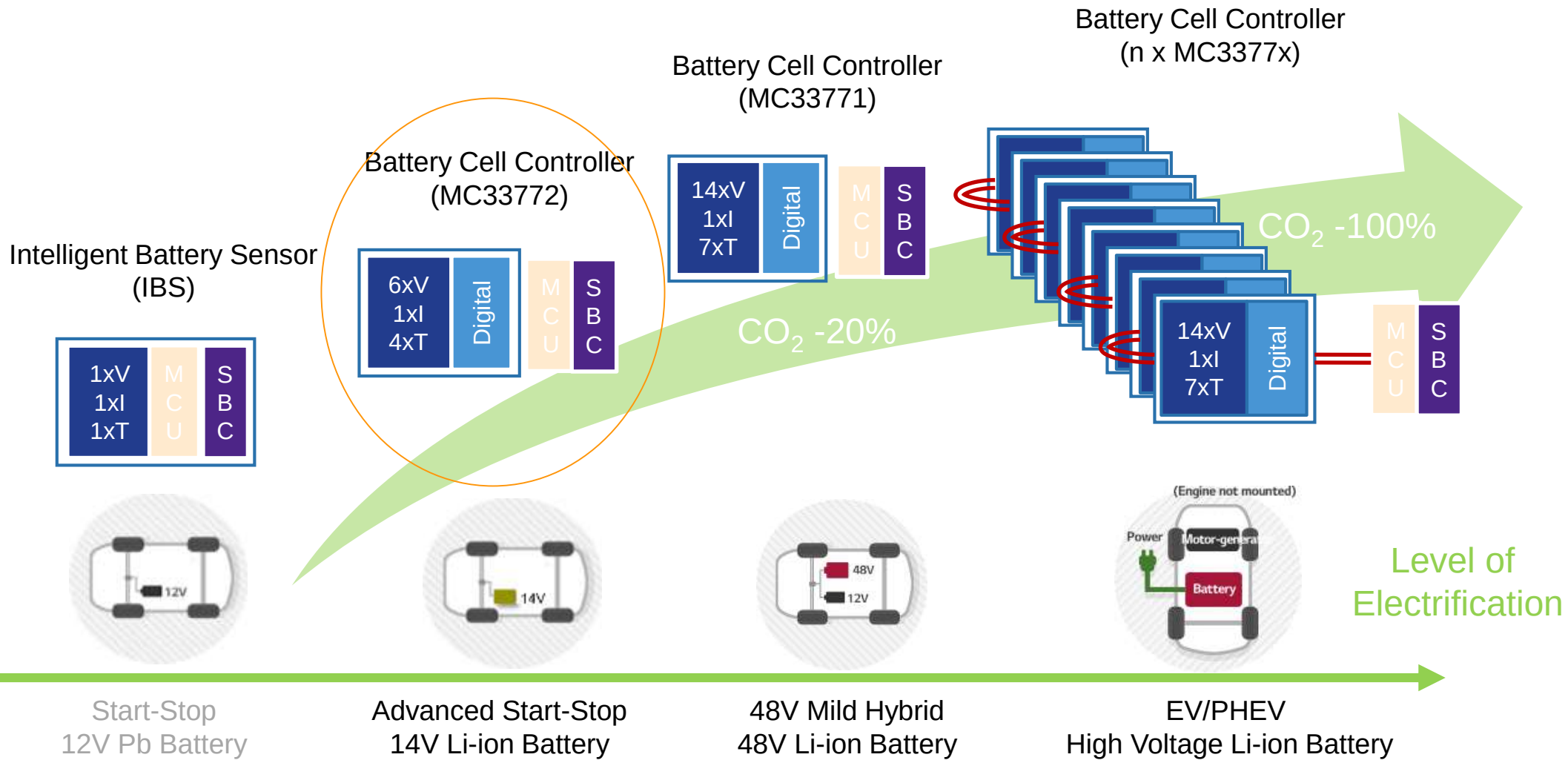
MC33771B, MC33772B
Analog Front End Key Features

Main Functions of BMS Systems

	Safety	Performance	Multi-Cell function
			
	Danger: • Over voltage • Extra heat • Unstable chemical stage • Thermal runaway=>fire/explosion • Low temperature charge	**Requirements:** • Safe & fast charging • Discharge optimization • State of charge (SOC) estimation • State of health (SOH) estimation	**Challenges:** • Up to hundreds of cells • Manufacture mismatch • Capacity degradation • Lifetime degradation
Key BMS Functions	V/I/T measurement	V/I/T measurement Coulomb counting Internal resistance calculation	Cell balancing

NXP's Scalable Battery Management Portfolio

Addresses all Battery Management Applications – maximizes HW/SW reuse



MC33772B – 6 Cell Battery Cell Controller AFE

High Performance Integrated Functions

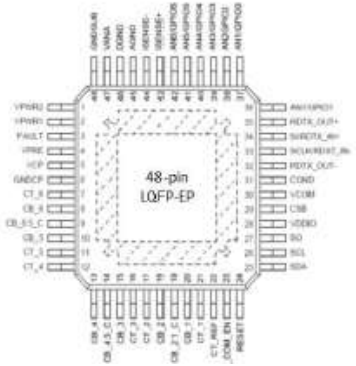
- Operating Voltage:
  - 5V ≤ VPWR ≤ 30V Operation, 42V Transient (for SPI communication)
  - 7V ≤ VPWR ≤ 30V Operation, 42V Transient (for TPL communication)
- Life-time guaranteed high accuracy 6 Cell Voltage Measurement Channels
- 4.0 Mbps SPI or Isolated 2.0 Mbps Differential Communication
- Integrated 300 mA Passive Cell Balancing per channel with dedicated timer
- Synchronized on-chip current measurement with ±0.5% accuracy (±1500A)
- Synchronized on-chip Coulomb Counter (also in low-power mode)
- 7 ADC/GPIO/Temperature Sensor Inputs
- Total Stack Voltage Measurement (0.5%)
- Addressable on Initialization
- 5.0V @ 5mA Reference Supply Output

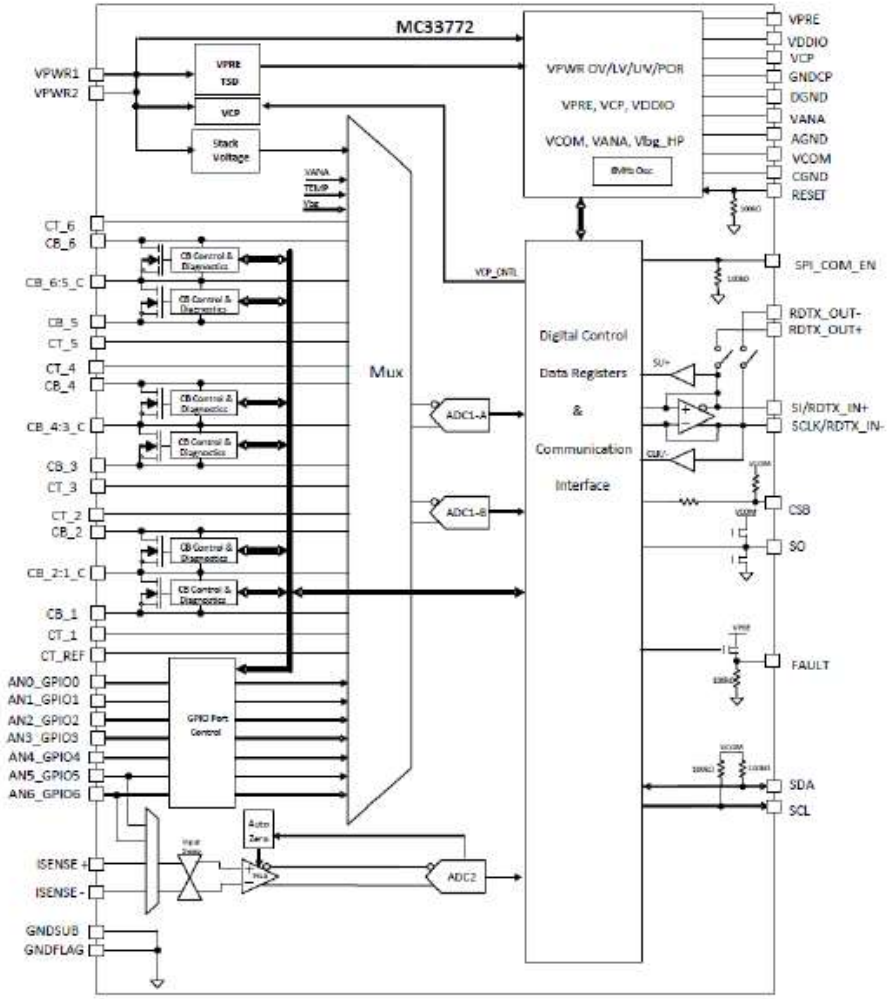
Comprehensive Integrated Functional Safety Features

- Designed to support ISO 26262, up to ASIL D safety capability
- Automatic OV/UV and temperature detection routable to fault pin
- Integrated sleep mode OV/UV and temperature monitoring
- OV/UV, Over/Under Temperature Fault Verification
- Detection of internal and external faults, as open lines, shorts, and leakages
- Integrated balancing diagnostics

Quality & Robustness

- AEC-Q100 Automotive Qualified
- Temp range:
  - -40°C to 125°C (for SPI communication)
  - -40°C to 105°C (for TPL communication)
- Operational Low Power Mode
- Hot Plug Capable
- EMC/ESD Robustness





Function Descriptions

Cell Measurement
(MC33771)

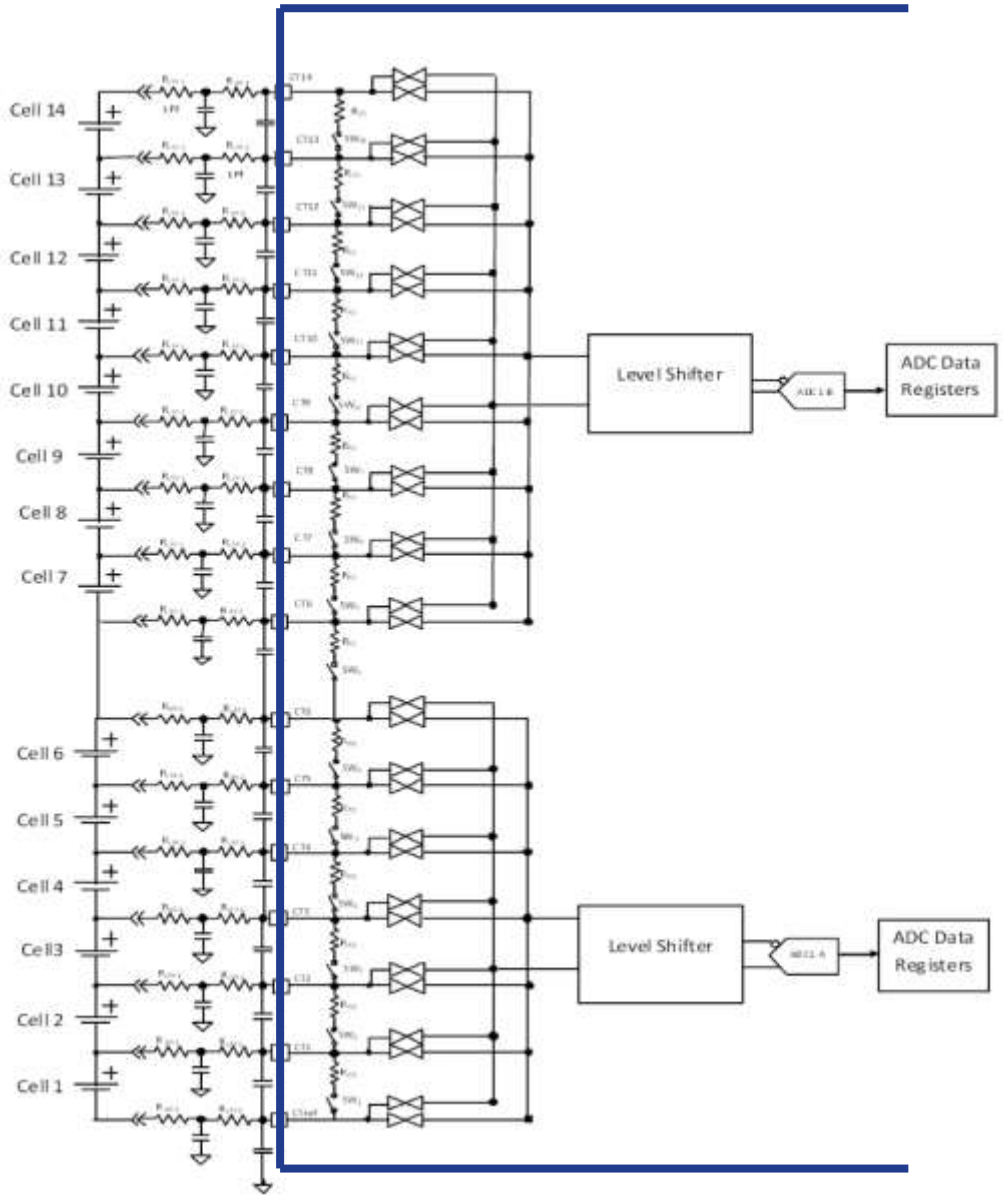
Two ADC's have selectable 13 up to 16-Bit to support measurement resolution versus acquisition speed requirements

Stack voltage measurement possible between VPWR & GND. Verify cell voltage sum equals stack voltage

Conversion command and measurement data are synchronized with Tag ID's

Selectable cell measurement thresholds for sleep mode wake up

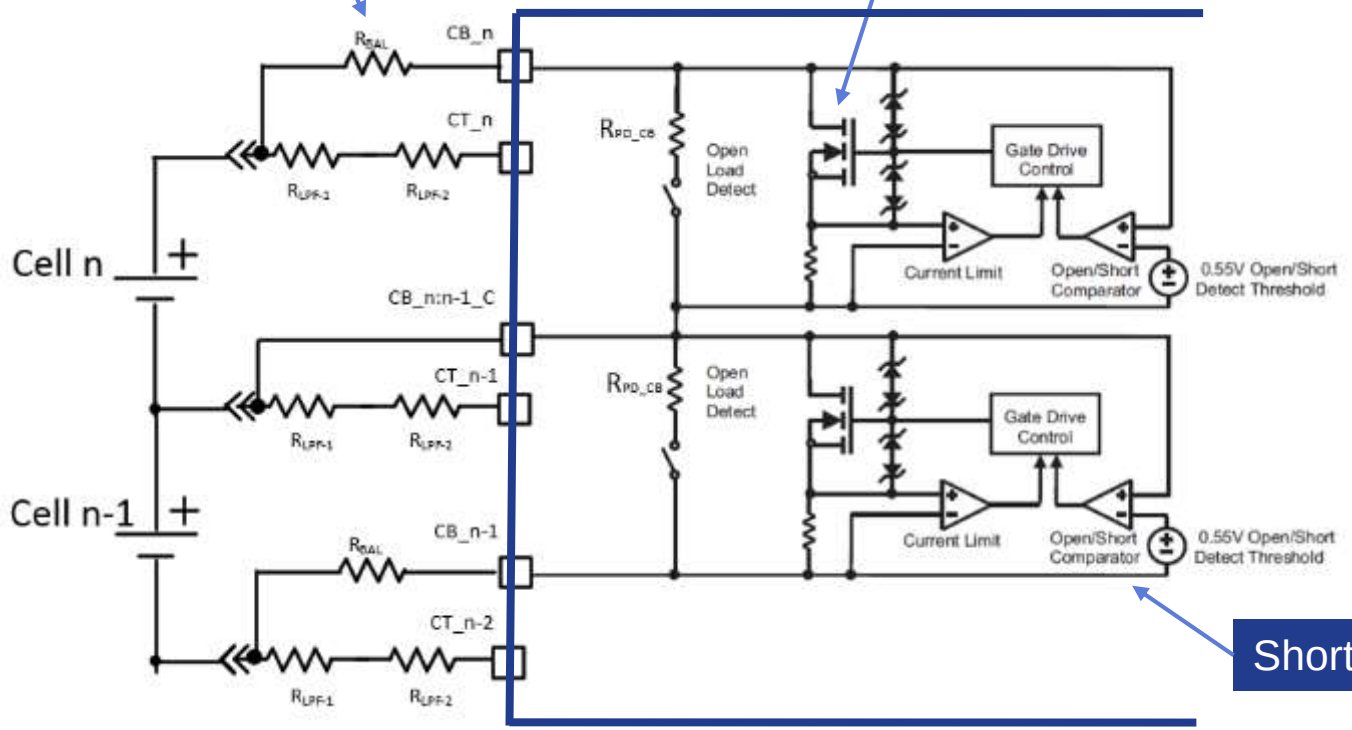
Measurement chain verification made available with separate internal references at cell inputs and ADC inputs



Cell Balancing

Energy dissipated across external resistor

300mA, 750mΩ Integrated MOSFET



Cell balance in sleep mode

Short & open detection

Cell balance timer 30sec-511min

Cell balance voltage thresholds

Cell balance auto pause during CT measurement

Current Measurement

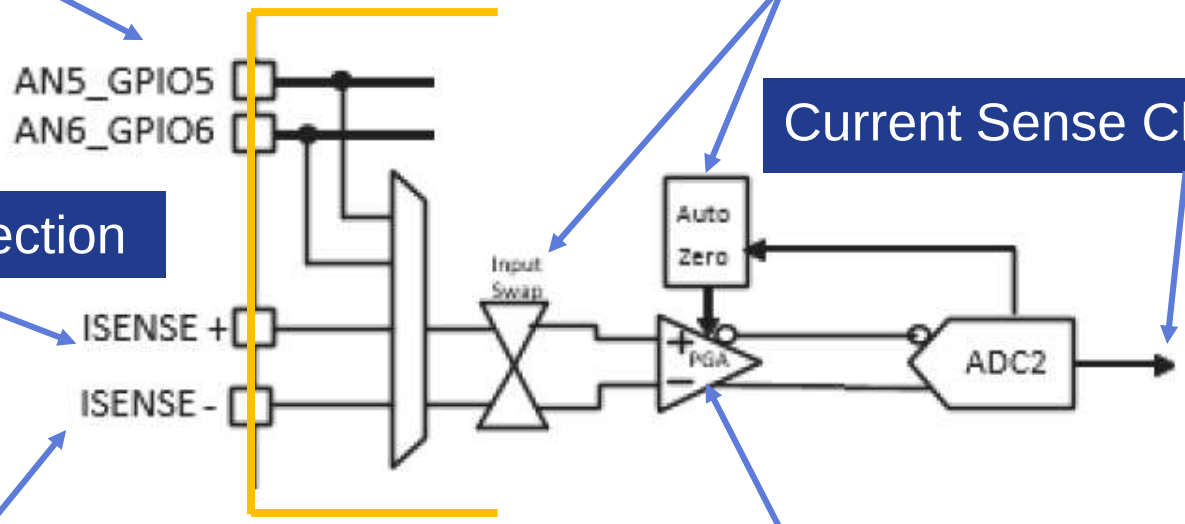
Measures current flowing in both directions

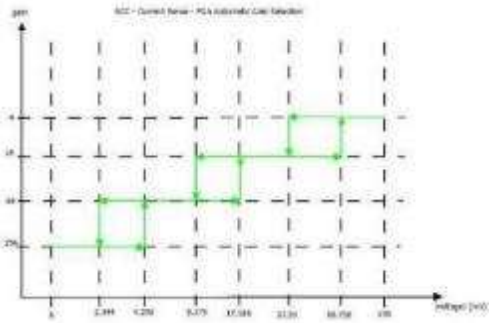
Redundant Current Sense Inputs

Acquisition Chain Offset Cancellation

Current Sense Channel Resolution 0.6µV/LSB

Open Pin Detection





±150mV Input Range

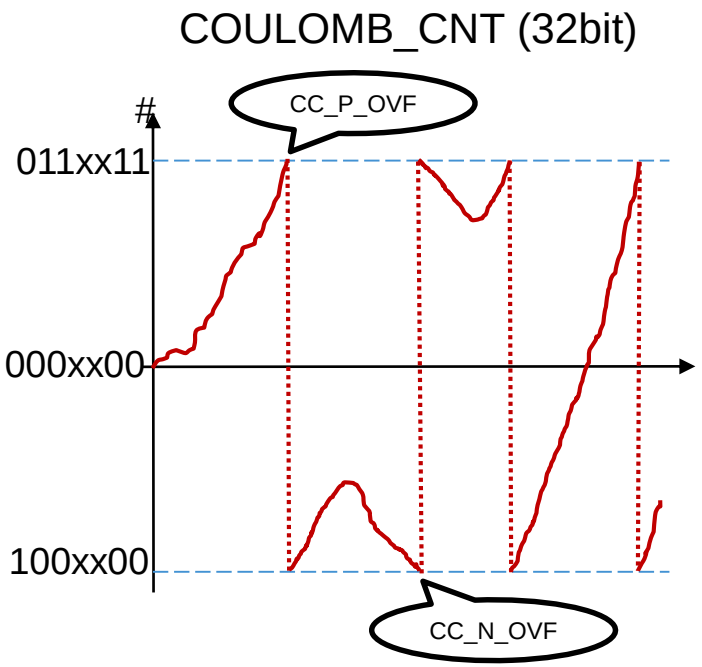
+/- 0.5 % Gain Error

+/- 0.5 uV Offset Error

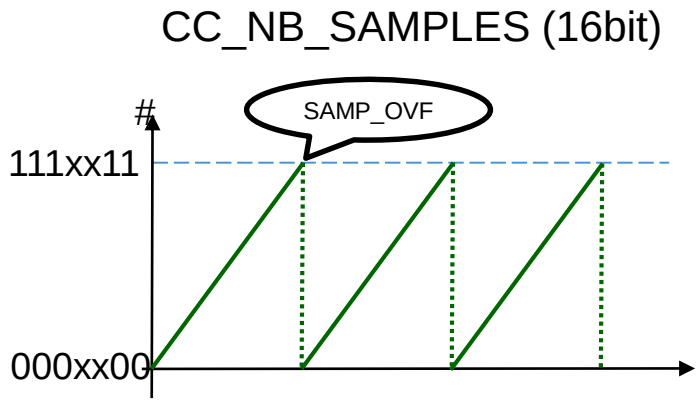
Automatic Gain Control: 4, 16, 64 & 256 (w/ hysteresis)

Coulomb Counter

Each successive continuous ADC acquisition is added to the CC accumulator



Each successive ADC acquisition Increments the CC number

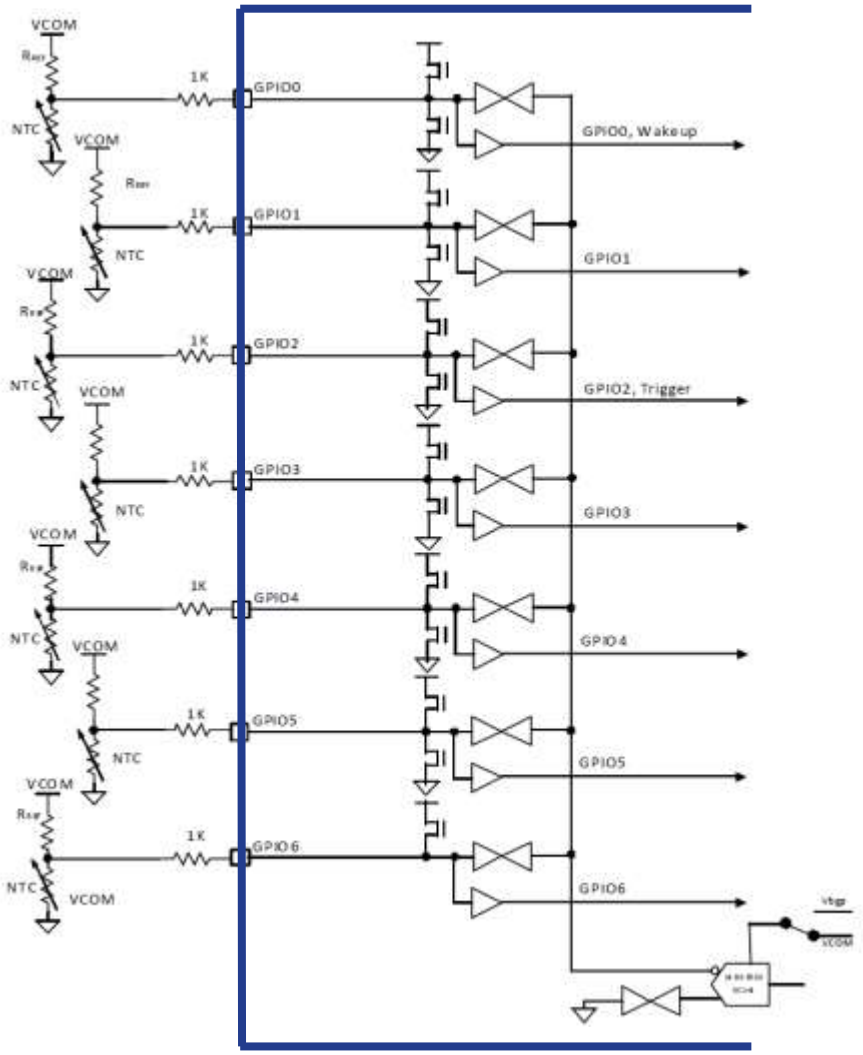


- Operates in normal & sleep modes
  - Normal mode: Continuous conversions
  - Sleep mode: Conversions based on cyclic timer setting
- Selectable coulomb counter threshold for sleep mode wakeup
- Selectable counting modes;
  - Overflow counter or
  - Clamp counter

$$Iave = Coulomb\_CNT \div CC\_NB\_Samples$$

$$\Delta Q = (I_{ave}) \times (t_{old} - t_{new})$$

Temperature / GPIO Measurement



	GPIO			Anx		ISENSE
GPIO Port	Std gpio	Wup& Daisy Chain	Convert Trigger	Absolute	Ratiometric	
0	X	X		X	X	
1	X			X	X	
2	X		X	X	X	
3	X			X	X	
4	X			X	X	
5	X			X	X	X
6	X			X	X	X

Open & short circuit detection

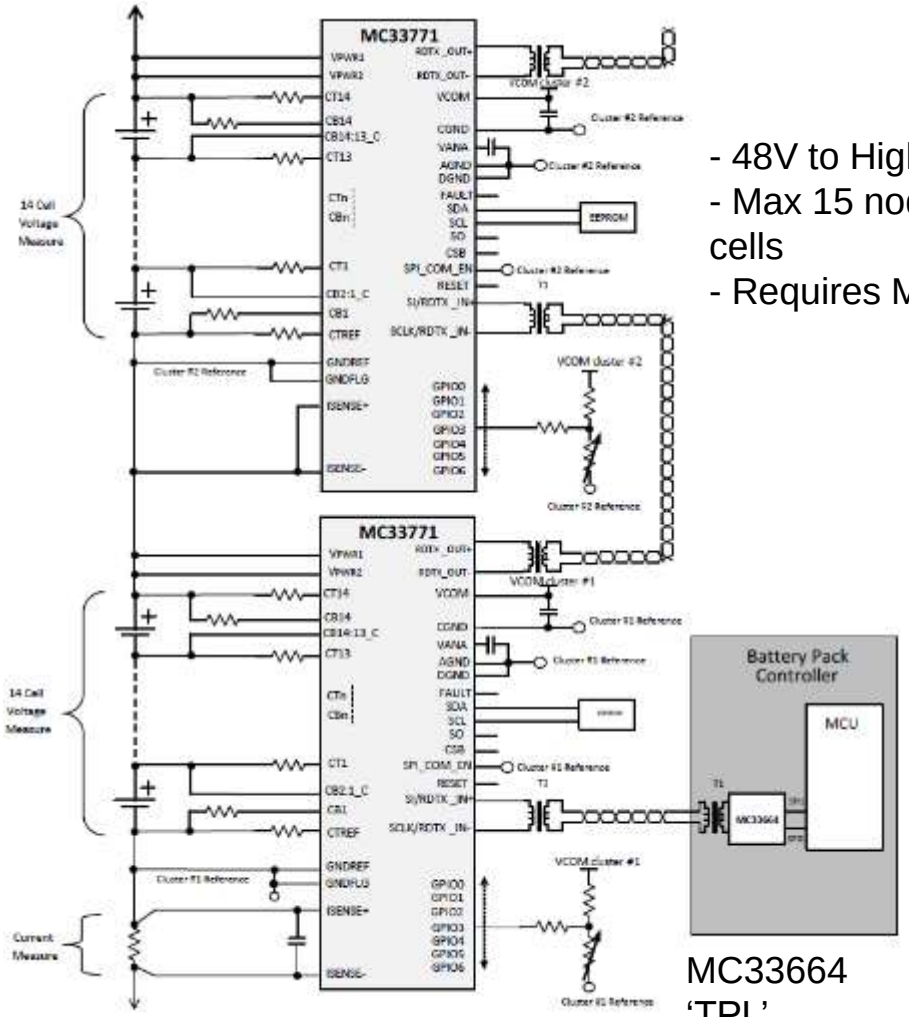
Selectable UT / OT thresholds with Fault output assertion

UT / OT functional verification

MC33771xB TPL Communication

MC3377xB – Connectivity Options

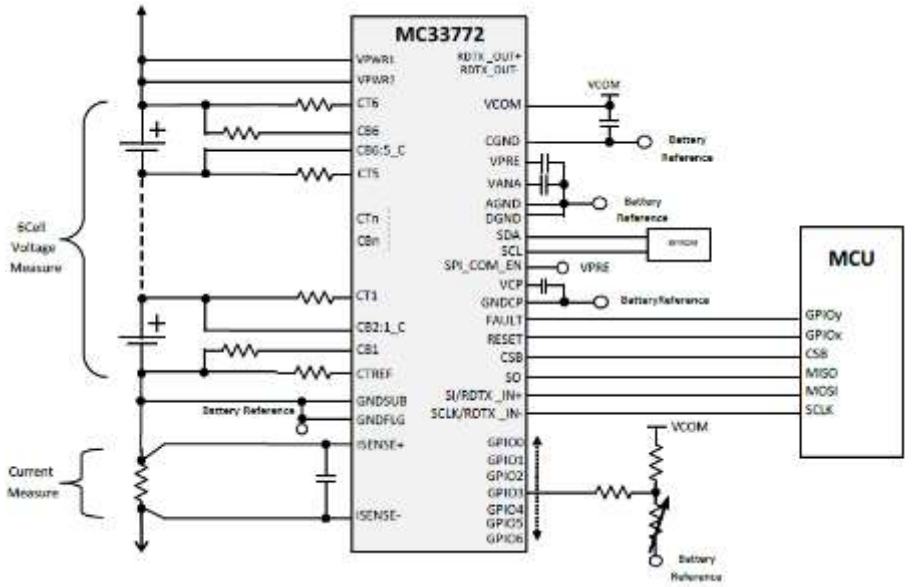
HV Daisy Chain Solution



- 48V to High Voltage
- Max 15 nodes / 210 cells
- Requires MC33664

MC33664 'TPL'

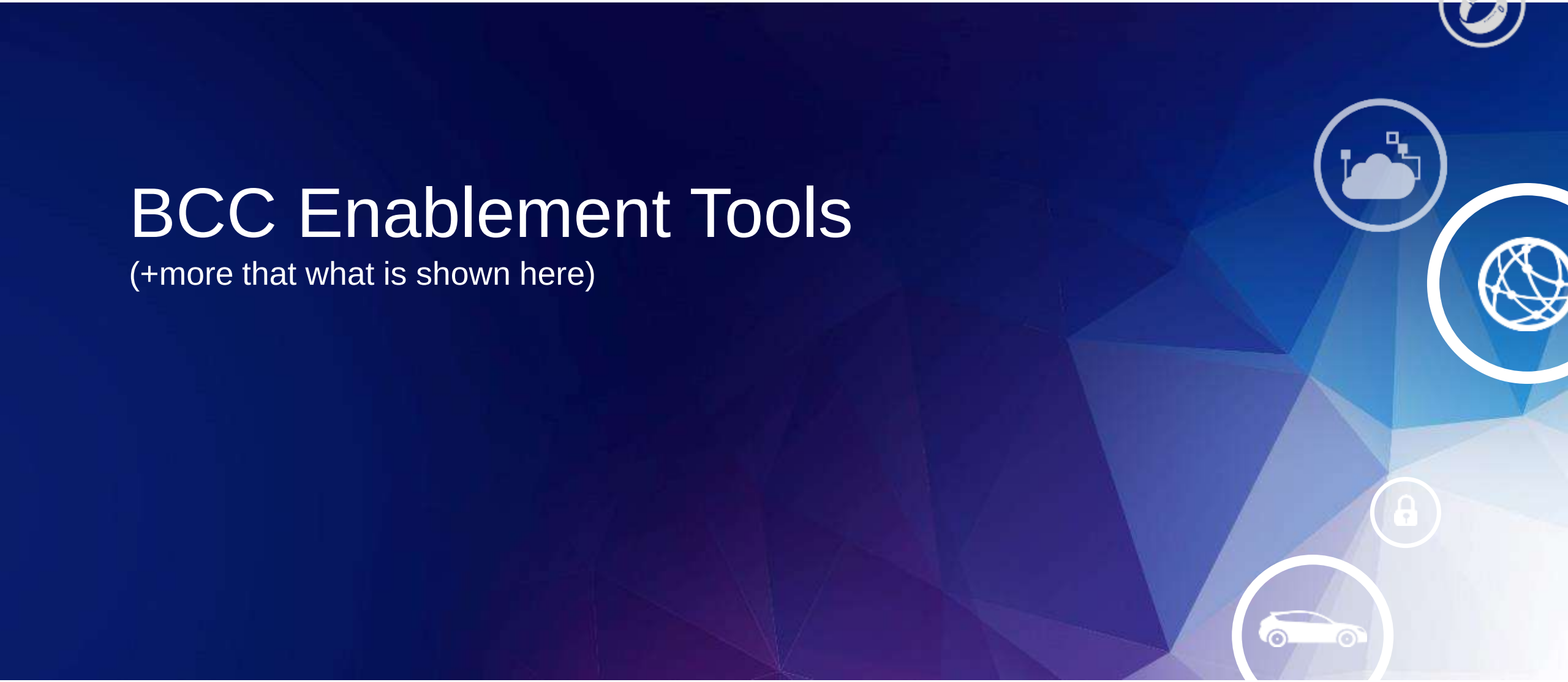
LV SPI Solution



- Typical 12v application

BCC Enablement Tools

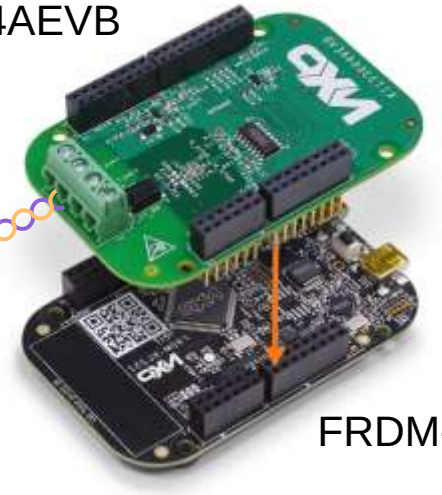
(+more that what is shown here)



http://www.nxp.com/products/automotive-products/energy-power-management/battery-management/battery-cell-controllers/14-channel-li-ion-battery-cell-controller-ic:MC33771?tab=Design_Tools_Tab

33771 / 33664 Evaluation Kit

KIT33664AEVB



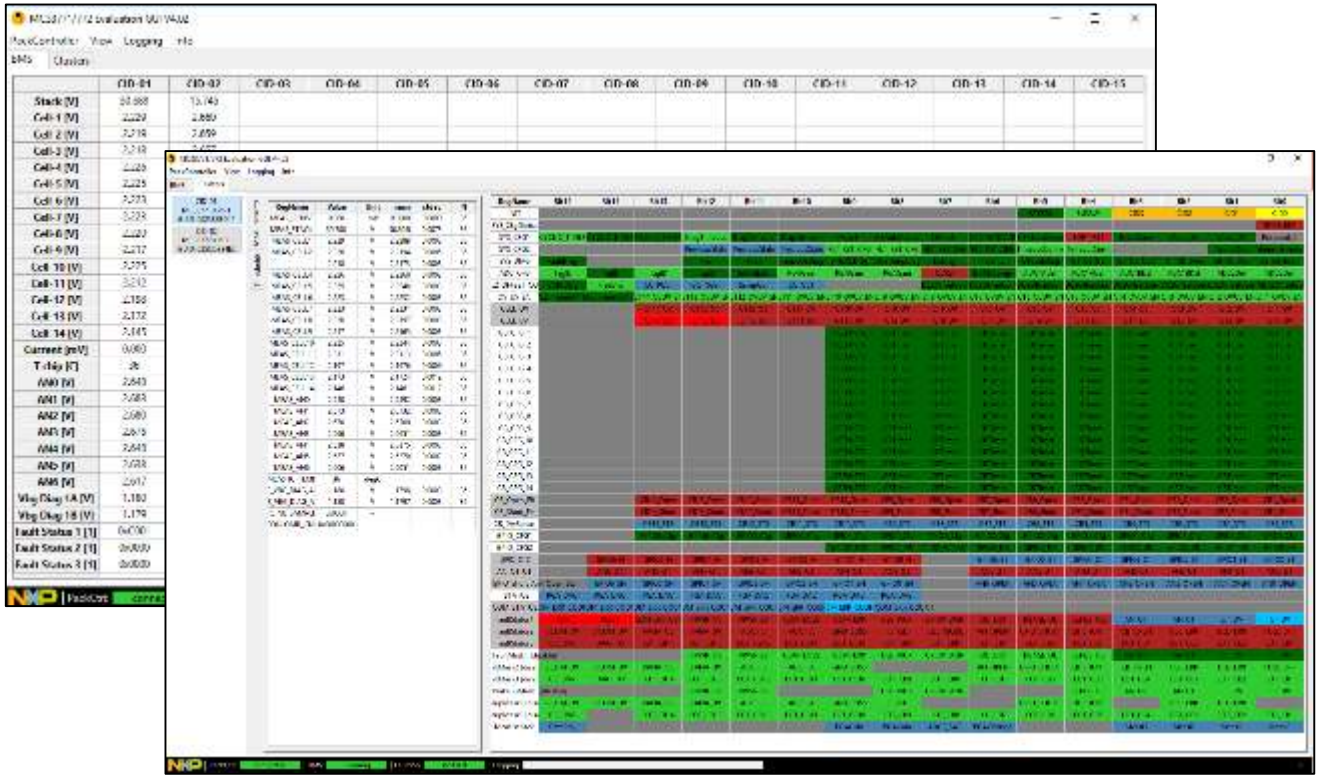
FRDM-KL25Z

KIT33771TPLEVB
KIT33771SPIEVB

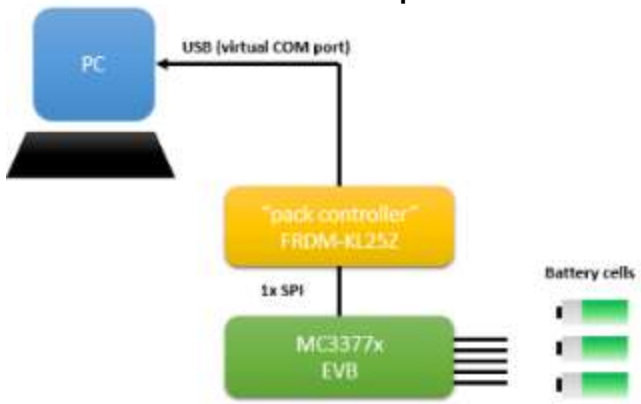
BATT-14AAAPACK

NXP BCC Evaluation GUI – With KL25Z Firmware

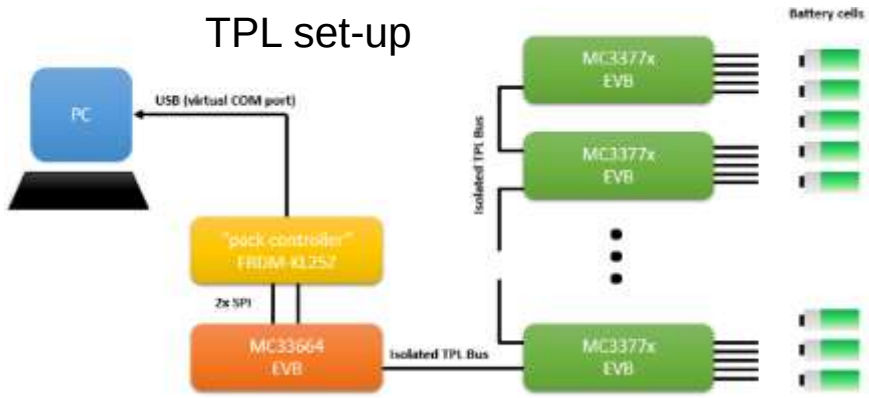
Supports KL25Z FW update if needed
Supports SPI communication
Supports TPL communication for daisy chain
Provide device registers configuration and measurements access



SPI set-up



TPL set-up



Battery Cell Controller Rev B – Analog Expert SW Driver

Function Name	Description
BCC_Init	Initializes the Battery Cell Controller device or devices (depends on configuration). It Assigns CID, initializes communication interface according to selected mode (classic SPI or TPL) and configures the device with predefined values from Processor Expert properties.
BCC_Deinit	Deinitializes the components used by Battery Cell Controller component. Note that this method does not reset the device.
BCC_WriteRegister	This method writes a value to addressed register of selected Battery Cell Controller device.
BCC_WriteGlobalRegister	This method writes a value to addressed register of all configured Battery Cell Controller devices. This method is available when communication mode is TPL.
BCC_ReadRegisters	This method reads a value from addressed register of selected Batter Cell Controller device.
BCC_Sleep	Set sleep mode of all Battery Cell Controller devices. MC33664TL goes to sleep mode automatically.
BCC_WakeUp	Sets normal mode of all Battery Cell Controller devices. MC33664TL goes to normal automatically.
BCC_StartConversion	Starts ADC conversion. It sets Start of Conversion bit and new value of TAG ID in ADC_CFG register. TAG ID is increment for each conversion. You can use method IsConverting to check conversion status.
BCC_IsConverting	Checks status of conversion defined by End of Conversion bit in ADC_CFG register.
BCC_GetRawMeasurements	Reads the measurement registers and returns raw values. You can use macros defined in header file to perform correct unit conversion.
BCC_GetAverageCurrent	Computes average current with use of the Coulomb counter. Restart of the Coulomb counter depends on settings of BCC (see "Action on Read CC" property).
BCC_GetStatus	Reads the status registers and returns raw values. List of read registers: CELL_OV_FLT, CELL_UV_FLT, CB_OPEN_FLT, CB_SHORT_FLT, CB_DRV_STATUS, GPIO_STS, AN_OT_UT_FLT, GPIO_SHORT_Anx_OPEN_STS, I_STATUS, PGA DAC, COM_STATUS, FAULT1_STATUS, FAULT2_STATUS, FAULT3_STATUS.
BCC_RunDiagnostic	Call internal diagnostic functions.
BCC_SoftwareReset	Resets Battery Cell Controller device using software reset. It enters reset via SPI or TPL interface.
BCC_HardwareReset	Resets Battery Cell Controller device using software reset. It enters reset via RESET pin. This method is available when RESET pin is enabled in properties ("Reset pin" set to Enabled).
BCC_SetGPIOOutput	Sets output value of Batter Cell Controller GPIO pin. This method is available when at least one GPIO is in output mode.
BCC_SetCBDrivers	Sets state of cell balancing drivers. It is designated to control all the drivers at once.
BCC_GetNtcCelsius	This method calculates temperature from raw value of MEAS_ANx register. You can use method GetRawMeasurements to get values of measurement registers. It uses precomputed values stored in BCC_NTC_TABLE table.

Analog expert SW driver details:

- Tools chain supported
  - S32 DS 2018.R1
  - S32 SDK EAR 0.8.6
- S32K144 Project examples
  - BCC6 / BCC14
  - SPI / TPL communication
  - Diagnostics / Measurements
  - Freemaster 2.0

Supported HW:

- S32K144EVB-Q100
- FRDM33664BEVB
- FRDM3377xBTPLEVB
- FRDM3377xBSPIEVB

Documentation:

- SW User’s Guide and readme file
- Programmers’ guide

S32K Automotive MCUs

S32K1 Automotive MCU Product Family

Scalable Single Platform

- 8K to 2M Flash
- HW and SW compatibility

→ ***Reduced R&D***

Superior Performance and Features

- Cortex M with FPU & DSP
- Best low-power
- Functional Safety- ASIL-B
- Security HW support
- CAN-FD, Ethernet, Audio
- FlexIO

→ ***Future proof designs***

Complete Software Solution

- S32 Design Studio
- Software Dev Kit (SDK)
- Autosar MCAL + OS

→ ***Reduced Time-to-Market***

From Drone program: NuttX POSIX RTOS now ported to support S32K

MCU Requirements for our BMS

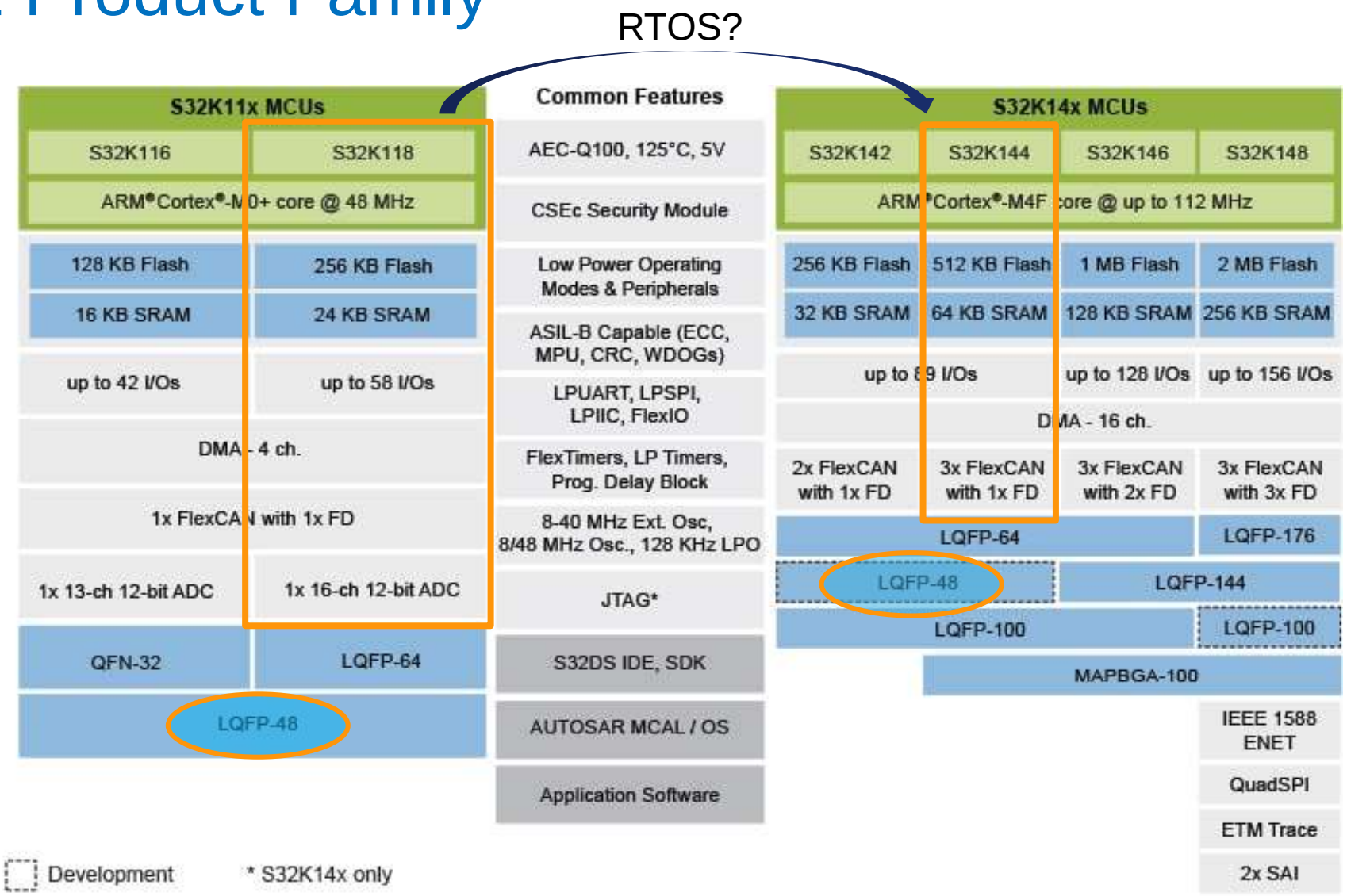
Interface requirements:

- SPI – interface with AFE
- CAN – interface with FMU
- I2C – optional for SM-Bus standard
- I2C - for NFC NTAG interface
- I2C – Authentication A1006/1007
- GPIO for LEDs switch etc.

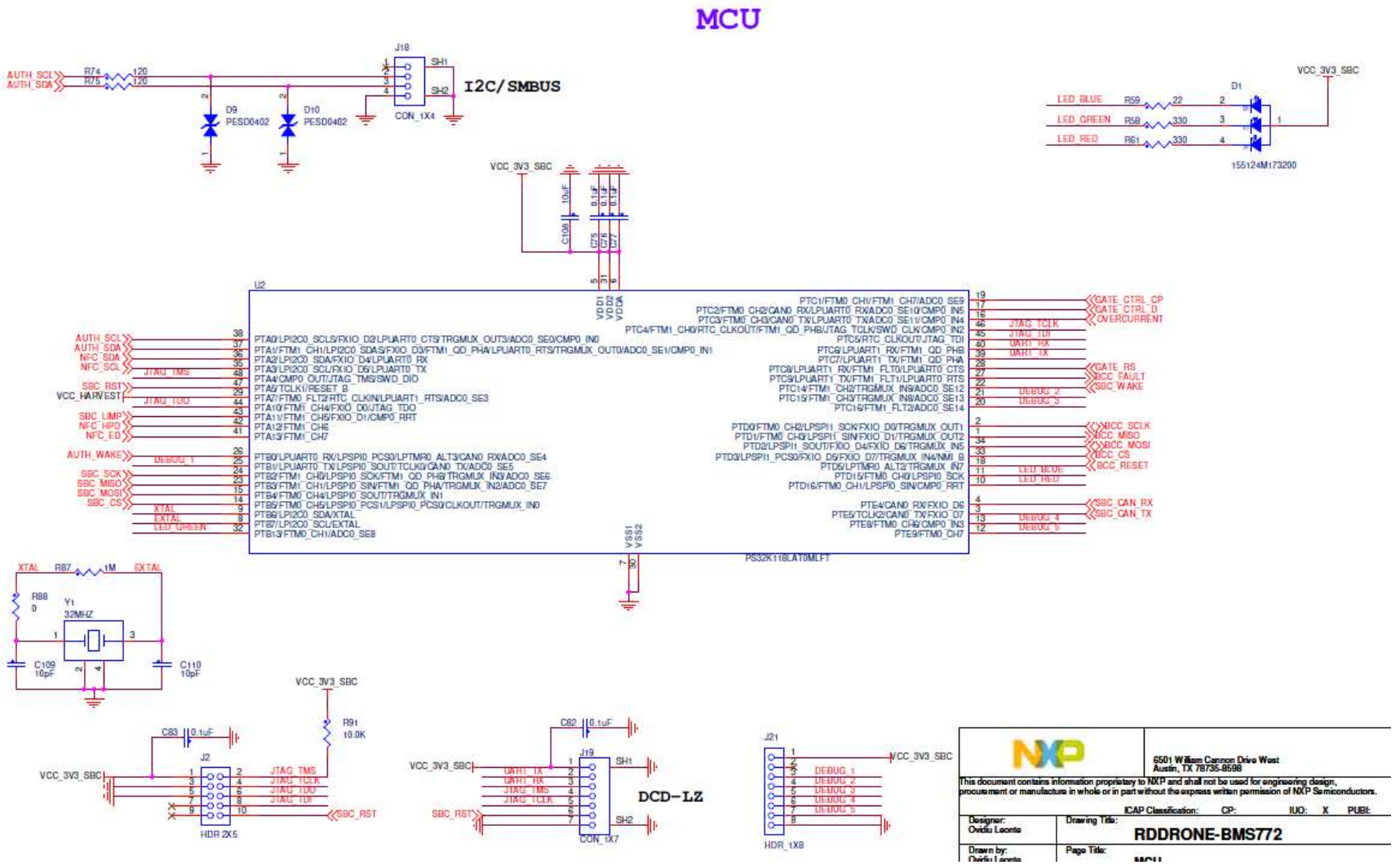
Possible Functions:

- Communication with AFE
- SOC estimation based on OCV and CC once every 100ms
- SOH estimation based on internal resistance and previous cycles or cycle counting
- Auto sleep mode and auto wake up function
- Diagnostics verifications for the AFE (once every second):
  - OV/UV detection and functional verification (SM01, SM03, SM07, SM34)
  - ADC functional verification (SM07)
  - CT leakage monitoring (SM04)
  - CT open line detection (SM02)
- Communication with FMU with UAVCAN protocol every 100ms (alternatively with SM-Bus I2C):
  - Battery stack voltage
  - Battery temperature
  - Battery current
  - Battery power
  - Battery remaining capacity (based on SOC and SOH information)
  - Battery fault status and battery information (manuf, S/N)
- Debug option with SWD (serial wire debug) (open, programming option, J-Link Mini EDU is shipped with HoverGames pack
- Industrial (Automotive optional BOM)
- Battery authentication with NFC
- Safety: no specific requirements, but use best practices

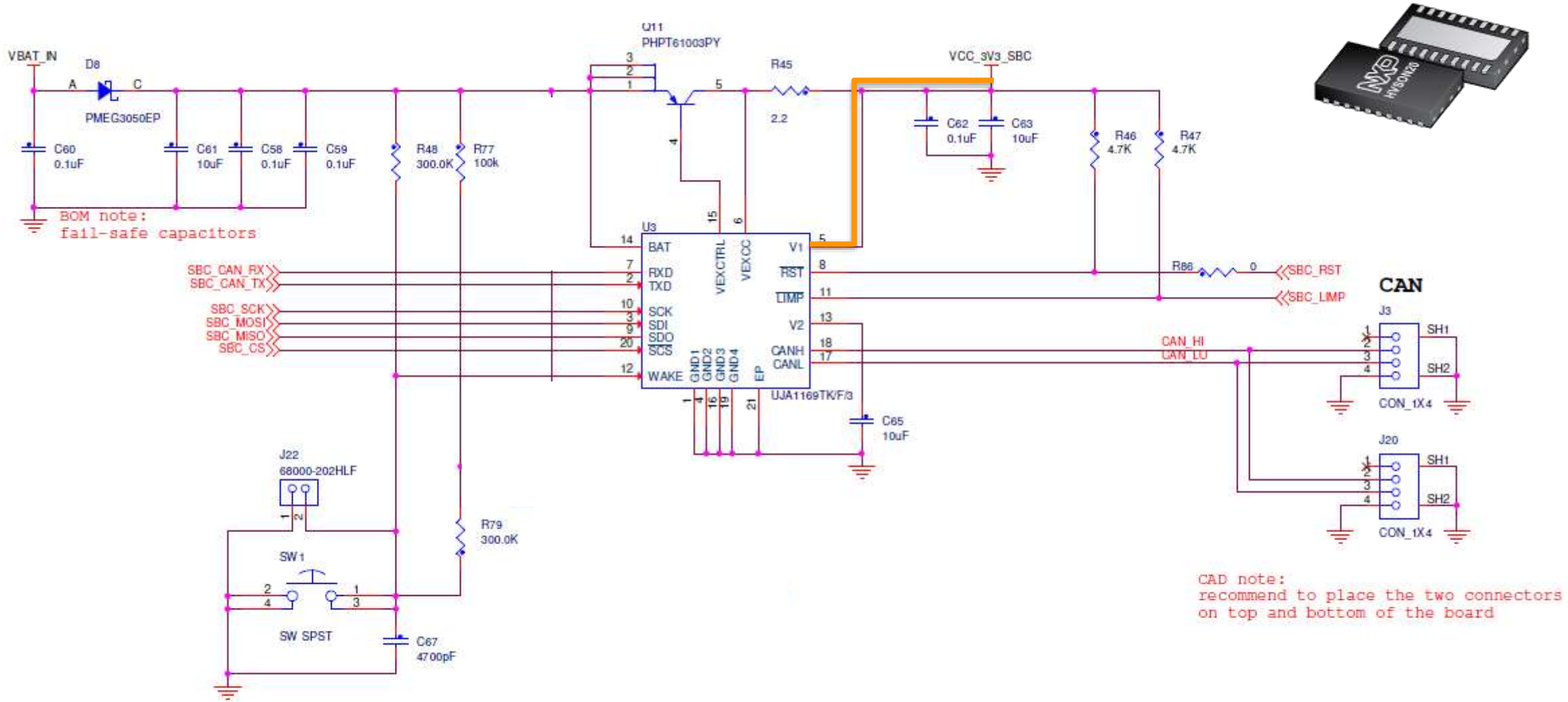
S32K1 Product Family



S32K1 Product Family



UJA1169 System Basis Chip


VBAT_IN
D8
PMEG3050EP
C60
0.1uF
C61
10uF
C58
0.1uF
C59
0.1uF
R48
300.0K
R77
100k
BOM note:
fail-safe capacitors
Q11
PHPT61003PY
R45
2.2
VCC_3V3_SBC
C62
0.1uF
C63
10uF
R46
4.7K
R47
4.7K
U3
BAT
RXD
TXD
SCK
SDI
SDO
SCS
WAKE
VEXCTRL
VEXCC
V1
RST
LIMP
V2
CANH
CANL
GND1
GND2
GND3
GND4
EP
UJA1169TK/F/3
SBC_CAN_RX
SBC_CAN_TX
SBC_SCK
SBC_MOSI
SBC_MISO
SBC_CS
R88
0
SBC_RST
SBC_LIMP
CAN_HI
CAN_LO
CAN
J3
J20
SH1
SH2
CON_1X4
C65
10uF
J22
68000-202HLF
SW1
SW SPST
R79
300.0K
C67
4700pF
CAD note:
recommend to place the two connectors
on top and bottom of the board

General

- ISO 11898-2:201x compliant 1 Mbit/s high-speed **CAN transceiver supporting CAN FD** active communication up to 2 Mbit/s
- Autonomous bus biasing according to ISO 11898-6:2013 and ISO 11898-2:201x
- Scalable 5 V or 3.3 V 250 mA low-drop voltage regulator for MCU supply (V1) based on external PNP transistor for thermal scaling
- CAN-bus connections are truly floating when power to pin BAT is off
- No ‘false’ wake-ups due to CAN FD traffic (in variants supporting partial networking)

Designed for automotive applications

- ±8 kV ElectroStatic Discharge (ESD) protection on the CAN-bus pins
- ±6 kV ESD protection according to IEC 61000-4-2 on pins BAT, WAKE, VEXT and the CAN-bus pins
- CAN-bus pins short-circuit proof to ±58 V
- Battery and CAN-bus pins protected against automotive transients according to ISO 7637-3
- Very low quiescent current in Standby and Sleep modes with full wake-up capability
- Leadless HVSON20 package with improved Automated Optical Inspection capability and low thermal resistance
- Dark green product (halogen free and Restriction of Hazardous Substances (RoHS) compliant)

Low-drop voltage regulator for 5 V/3.3 V microcontroller supply (V1)

- 5 V/3.3 V nominal output; ±2 % accuracy
- 250 mA output current capability
- Thermal management via optional external PNP
- Current limiting above 250 mA
- Support for microcontroller RAM retention down to a battery voltage of 2 V (5 V only)
- Undervoltage reset with selectable detection thresholds of 60 %, 70 %, 80 % or 90% of output voltage, configurable in non-volatile memory (5 V variants only)
- Excellent transient response with a small ceramic output capacitor
- Output is short-circuit proof to GND
- Turned off in Sleep mode

On-board CAN supply

- 5 V nominal output; ±2 % accuracy
- 100 mA output current capability
- Current limiting above 100 mA
- Excellent transient response with a small ceramic output capacitor
- Output is short-circuit proof to GND
- User-defined on/off behavior via SPI

Off-board sensor supply

- 5 V nominal output; ±2 % accuracy
- 100 mA output current capability
- Current limiting above 100 mA
- Excellent transient response with a small ceramic output load capacitor
- Output is short-circuit proof to BAT, GND and negative voltages down to -18 V
- User-defined on/off behavior via SPI

Power Management

- Standby mode featuring very low supply current; voltage V1 remains active to maintain the supply to the microcontroller
- Sleep mode featuring very low supply current with voltage V1 switched off
- Remote wake-up capability via standard CAN wake-up pattern or ISO 11898-6:2013 and ISO 11898-2:201x compliant selective wake-up frame detection including CAN FD passive support (/F versions only)
- Local wake-up via the WAKE pin
- Wake-up source recognition

System control and diagnostic features

- Mode control via the Serial Peripheral Interface (SPI)
- Overtemperature warning and shutdown
- Watchdog with Window, Timeout and Autonomous modes and microcontroller independent clock source
- Optional cyclic wake-up in watchdog Timeout mode
- Watchdog automatically re-enabled when wake-up event captured
- Watchdog period selectable between 8 ms and 4 s supporting remote flash programming via the CAN-bus
- LIMP output pin with configurable activation threshold
- Watchdog failure, RSTN clamping and overtemperature events trigger the dedicated LIMP output signal
- 16-, 24- and 32-bit SPI for configuration, control and diagnosis
- Bidirectional reset pin with variable power-on reset length; configurable in non-volatile memory to support a number of different microcontrollers
- Customer configuration of selected functions via non-volatile memory
- Dedicated modes for software development and end-of-line flashing

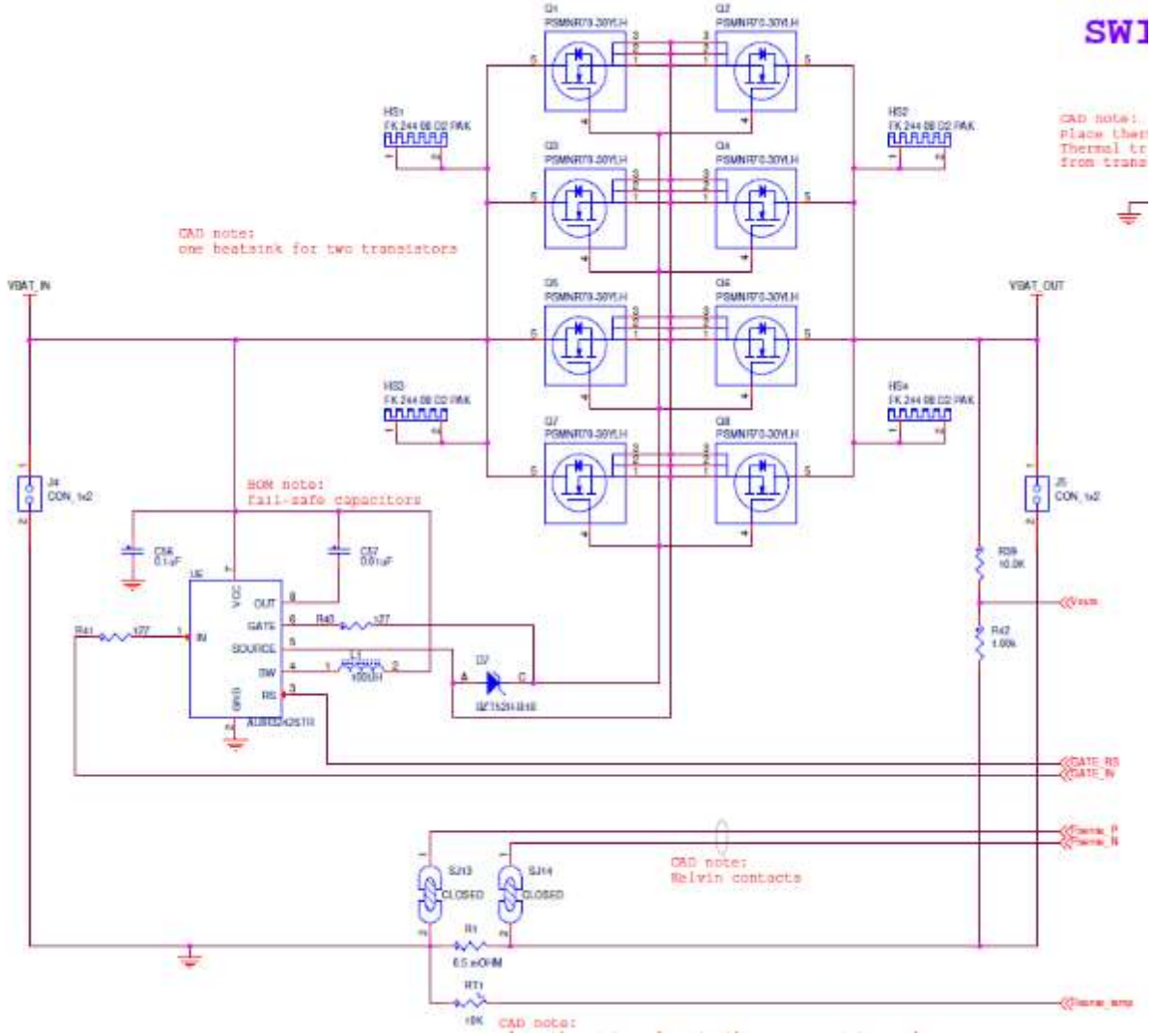
FETS and Gate Drive

FETs Switches & Gate Drive

- Design objective – Total System Low deep sleep current <80 uA
- Optional population of FETs relative to required current handling
- Bi-directional Charge/Discharge

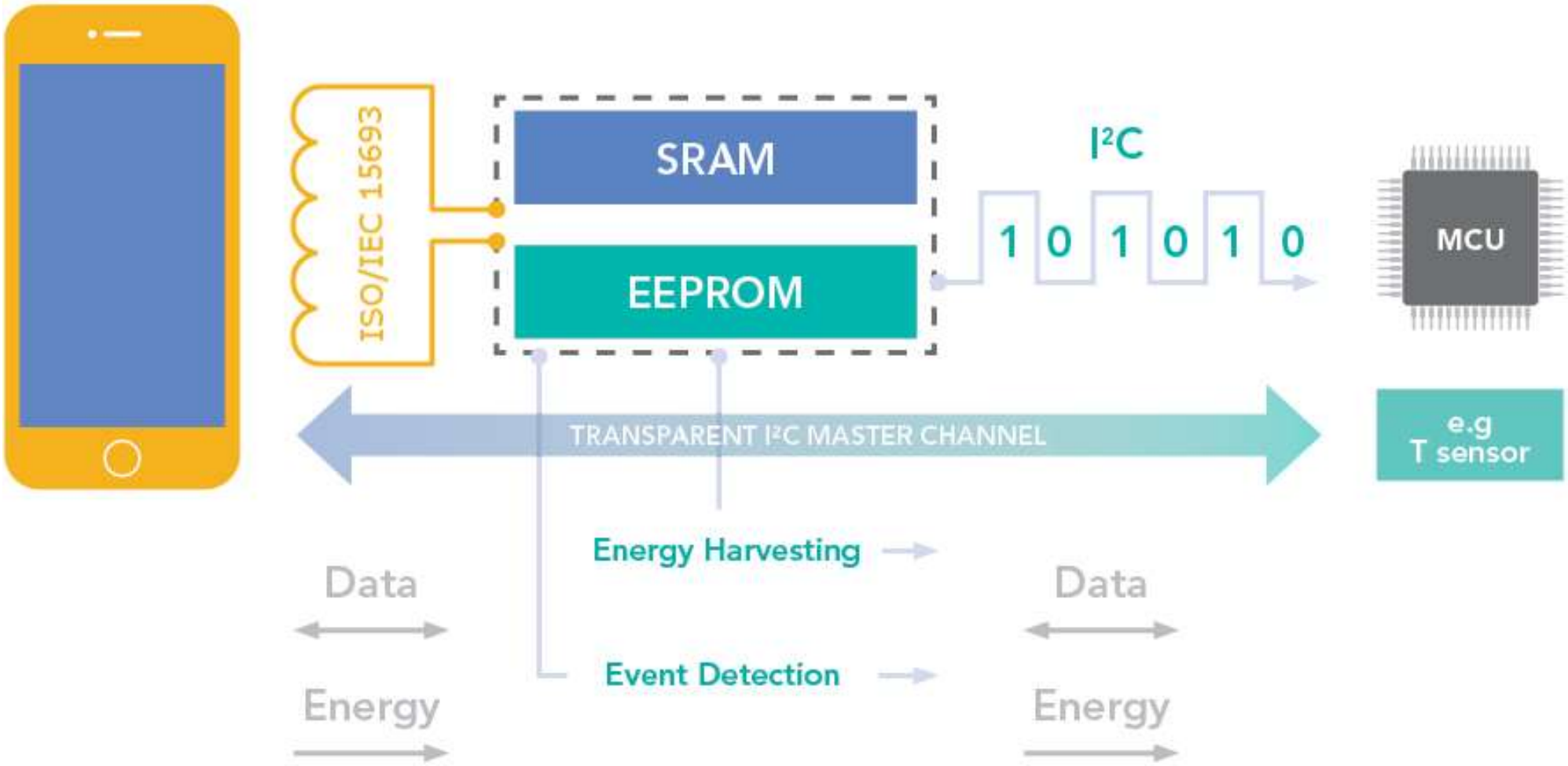
FET Switch & Gate Drive

nexperia

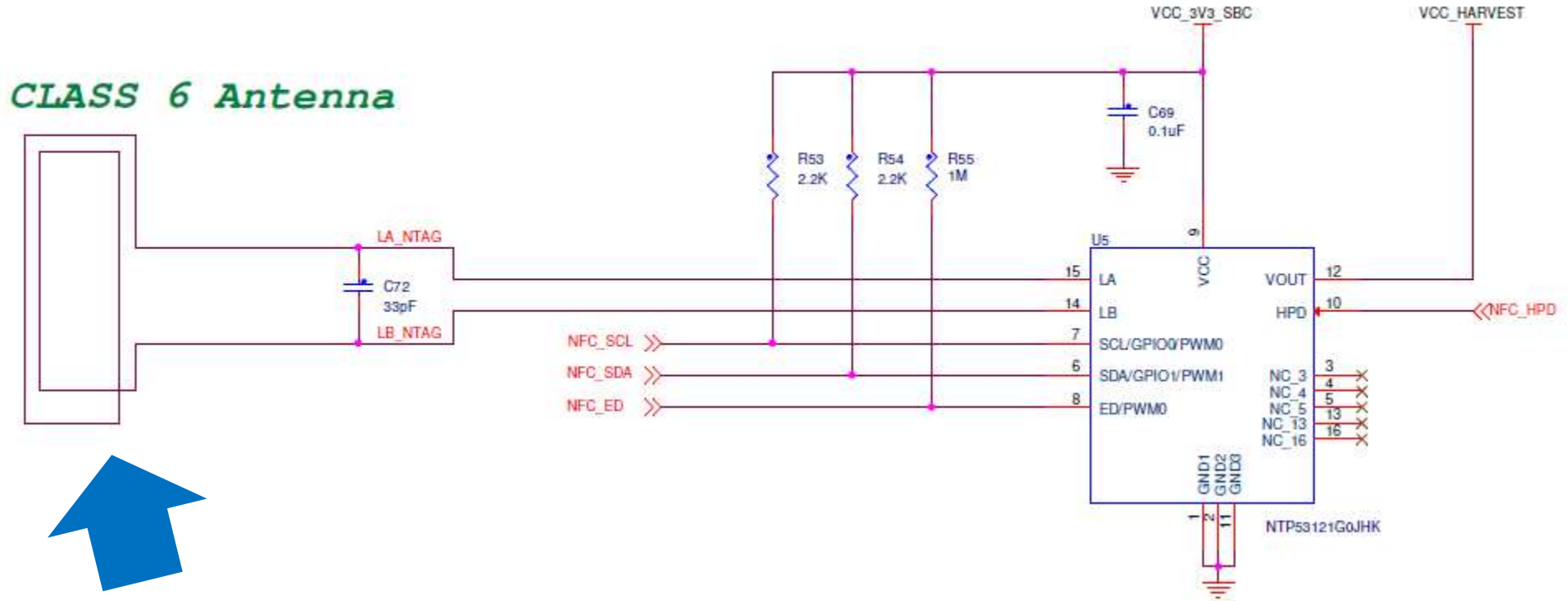


NFC: NTAG 5 Link

NFC: NTAG 5 Link



NFC – NTAG5 (+ i2C)

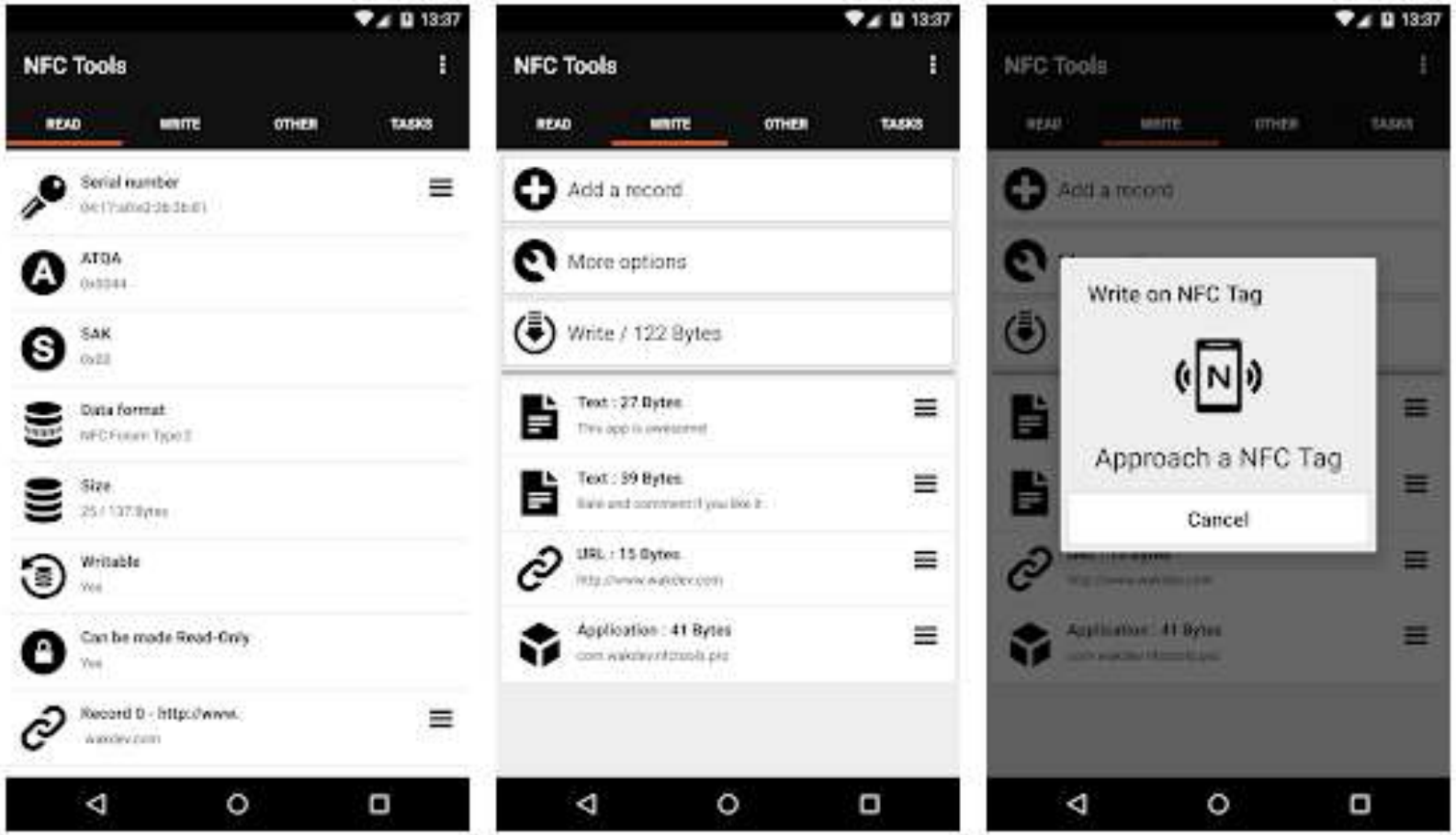


Larger antenna for improved coupling/power. Could also use ferrite wound coil

NFC – NTAG5 Usage in BMS

Identify battery serial number, group and pack, dates, charge state, health, logged faults, owner etc.

- HTTP record
  - No app needed!
- NDEF record
  - Set/clear deep sleep mode
  - Secure? Set/clear other parameters such as battery chemistry
- Pass through to secure element?

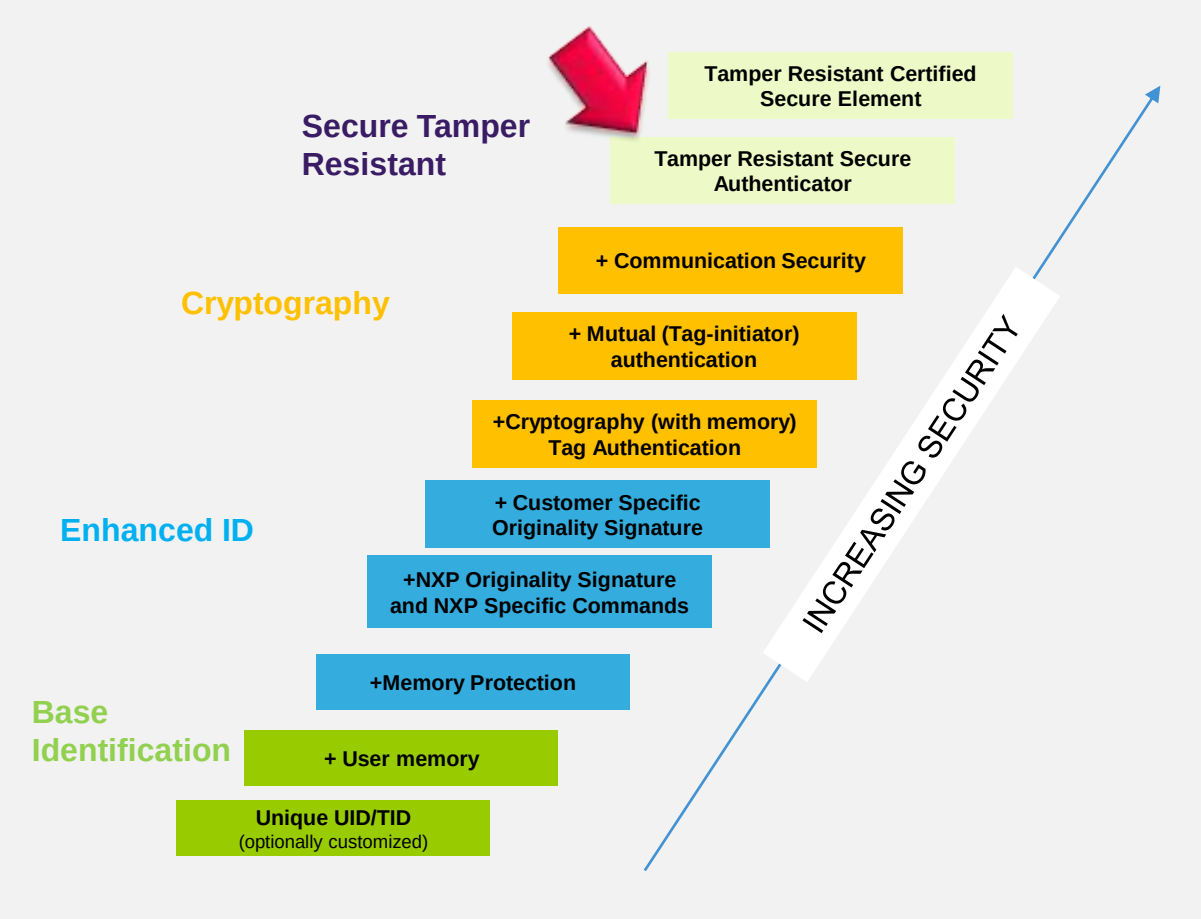


EdgeLock A1007
Secure Authenticator Product (Preview)

NXP Offers a Full Range of Authentication Solutions

The level and type of security depends on the nature of the product, the logistics channel and possible threats

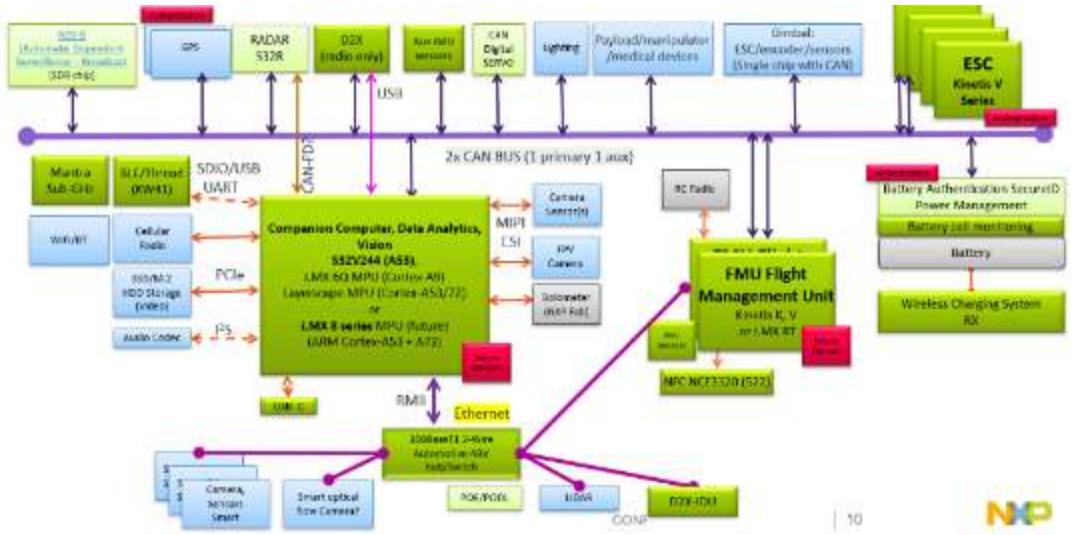
NXP products address a whole range of security requirements: from base level identification to physically secure tamper resistant cryptographic authentication through to independently certified Secure Elements for applications such as payment and e-government identification



Counterfeited Batteries and Chargers – Serious Problem

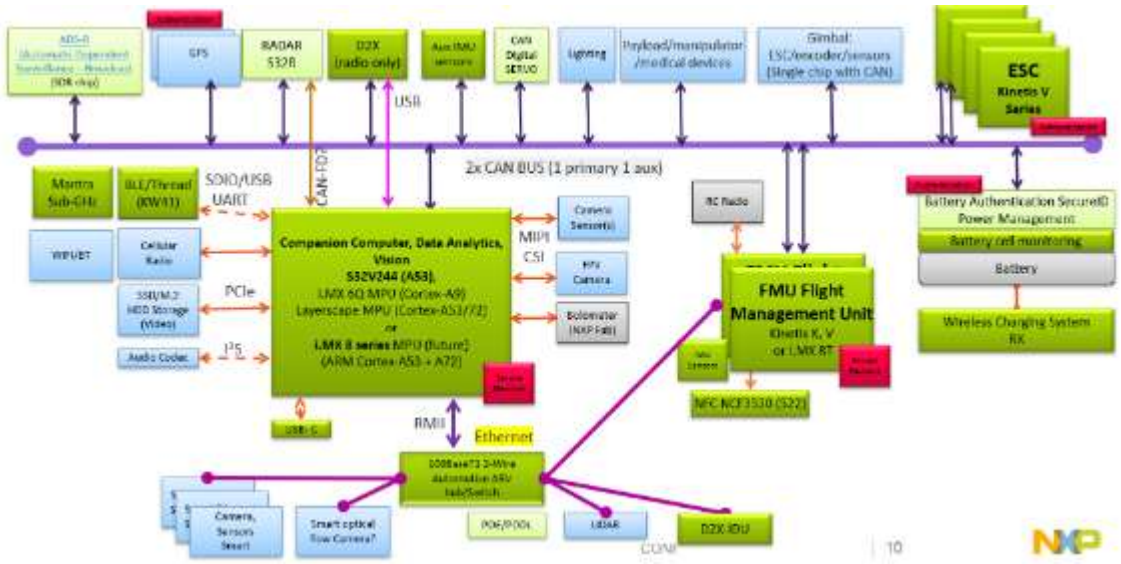
- Very common and difficult to identify
- Significant risk to consumers
- Risk to safety and product liability
- Risk to brand and revenue. Replaceable batteries, power banks, and all chargers are susceptible to counterfeit

Authenticating Autonomous Robot Modules



- Drones and other robotics are modular
- Each one can add risk to entire vehicle
- Modules may come from many sources
- Modules may be unintentionally replaced with
  - The wrong part for the vehicle
  - A counterfeit part
  - A part that has been damaged

Authenticating Autonomous Robot Modules



- Ecosystem of trusted parts
  - Embedded secure element is requirement to be a “Trusted 3rd party”
  - Enforce testing standards must agree to OEMs T&C’s and purchase authentication IC from partners
  - Insurance agencies see value in electronic manifest of components
  - Certification bodies are interested in digital certificates.

NXP Trust Provisioning Overview

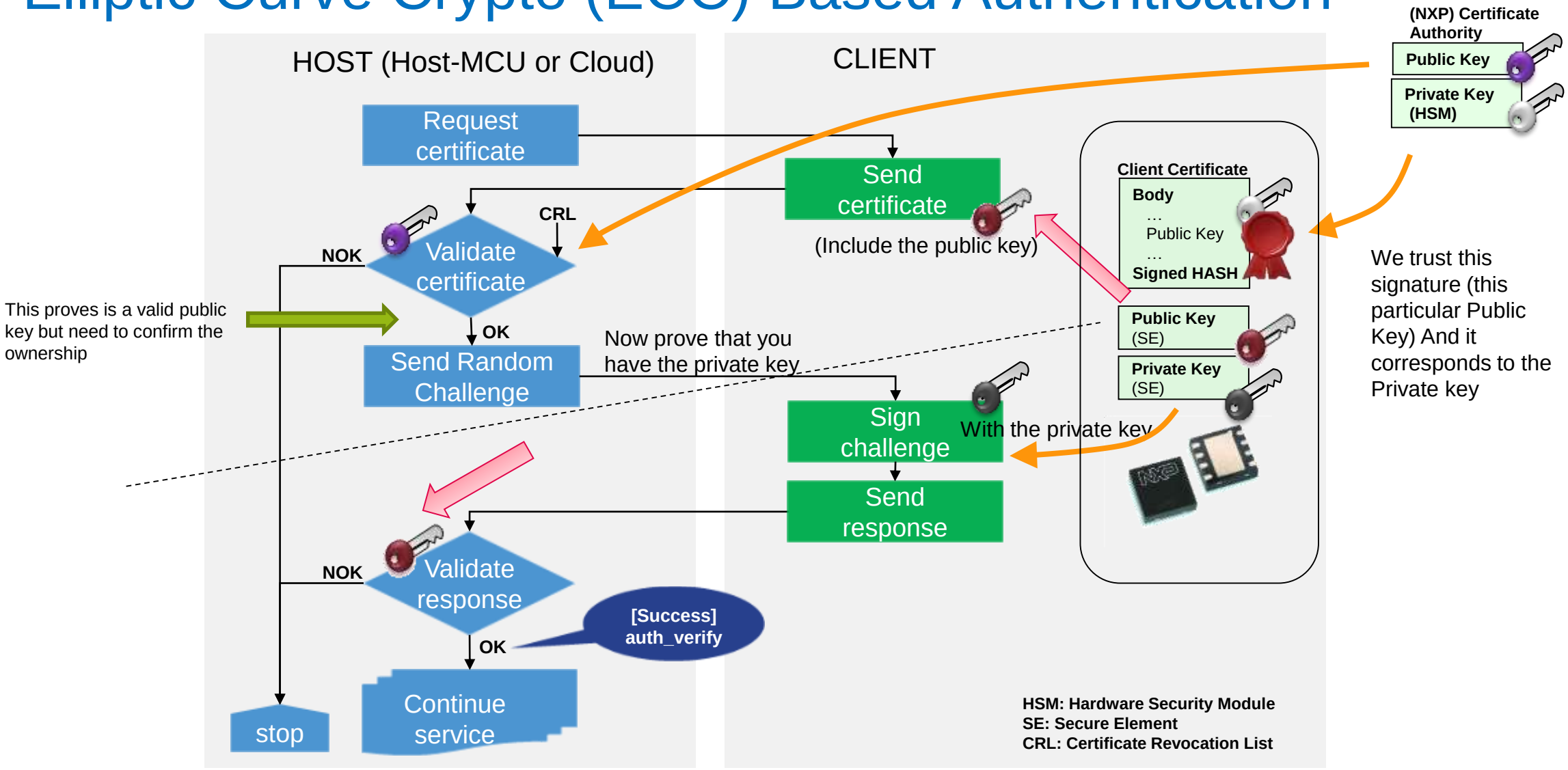
Creation of secret keys, certificates & personalization data in HSM

- Only **HSM**'s (Hardware Security Modules) with CC EAL5+ certification have access to Master secrets and unencrypted cryptographic objects

Insertion of key data into NXP chips during production

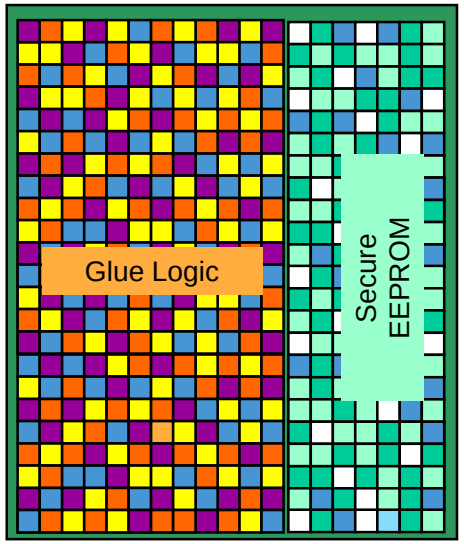
- Security sealed **Wafer Tester** allocates cryptographic objects into chips

Elliptic Curve Crypto (ECC) Based Authentication



NXP Key Value: Hardened Chip Attack Countermeasures

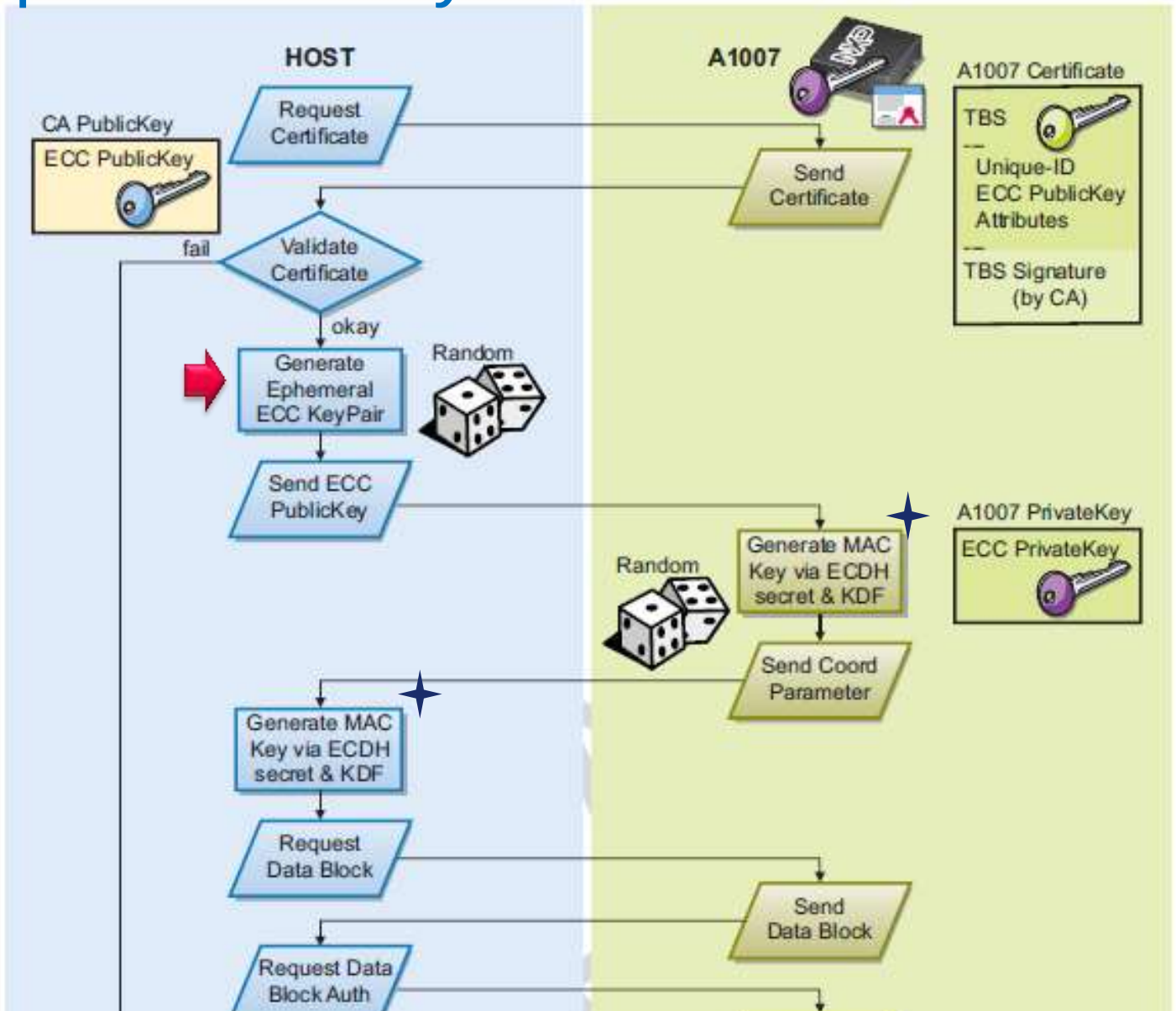
- Glue Logic
  - Function blocks are chopped up and randomly mixed
- Memory encryption, Memory scrambling
  - For unique placement of data for each IC
- Security routing on all metal layers
- Voltage sensors on the IC
- Active and passive shielding
- Protected true random number generator
- Secured Cores
  - Secured booting/secured mode control
  - Protection against pertinent fault attacks (robustness)
- Leakage attack countermeasures
  - Protection against timing analysis
  - Protection against Single Power Analysis (SPA), Differential Power Analysis (DPA), Electromagnetic Analysis (EMA)
  - Protection against Differential Fault Analysis (DFA)

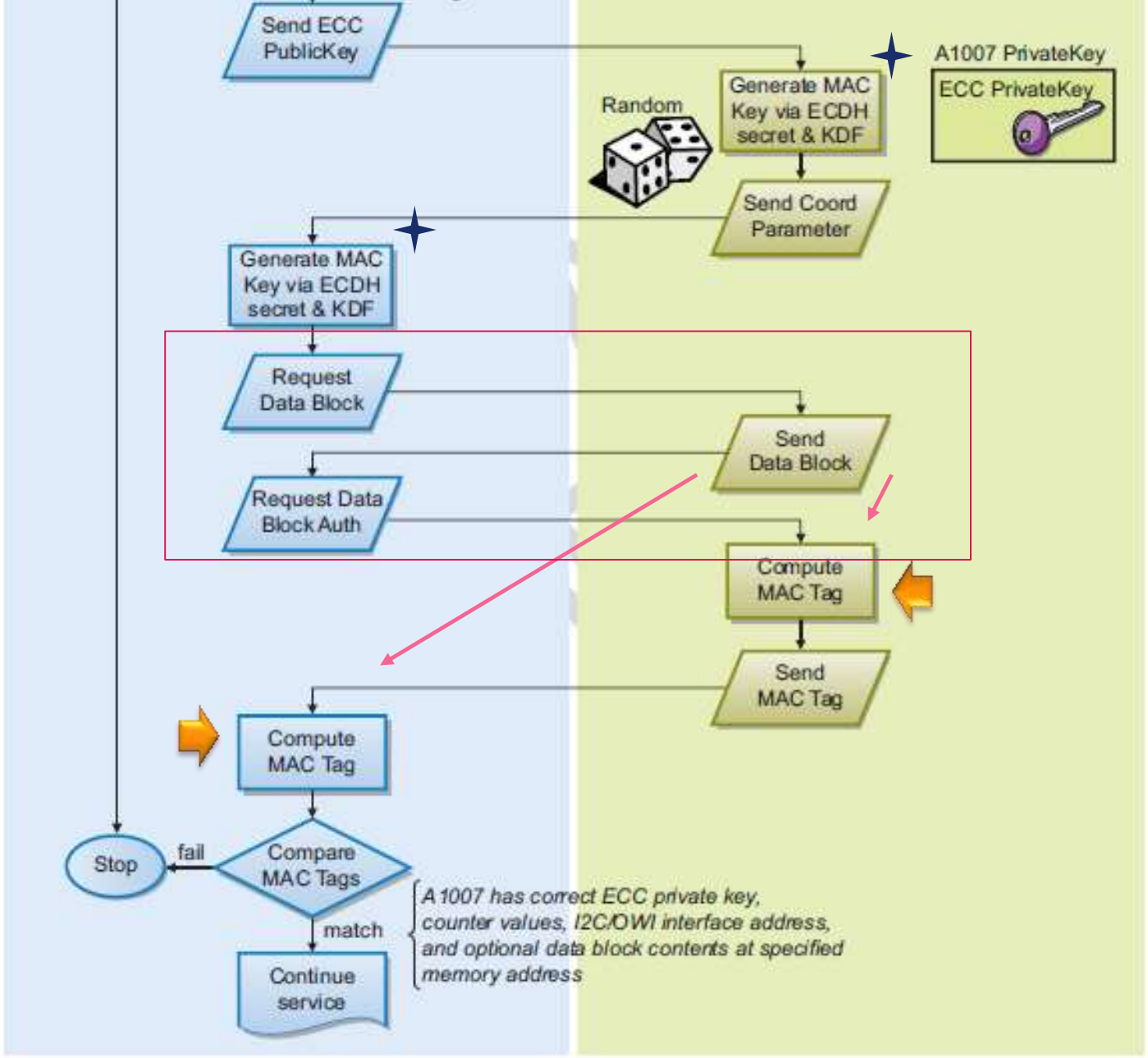


A1007 for Consumables

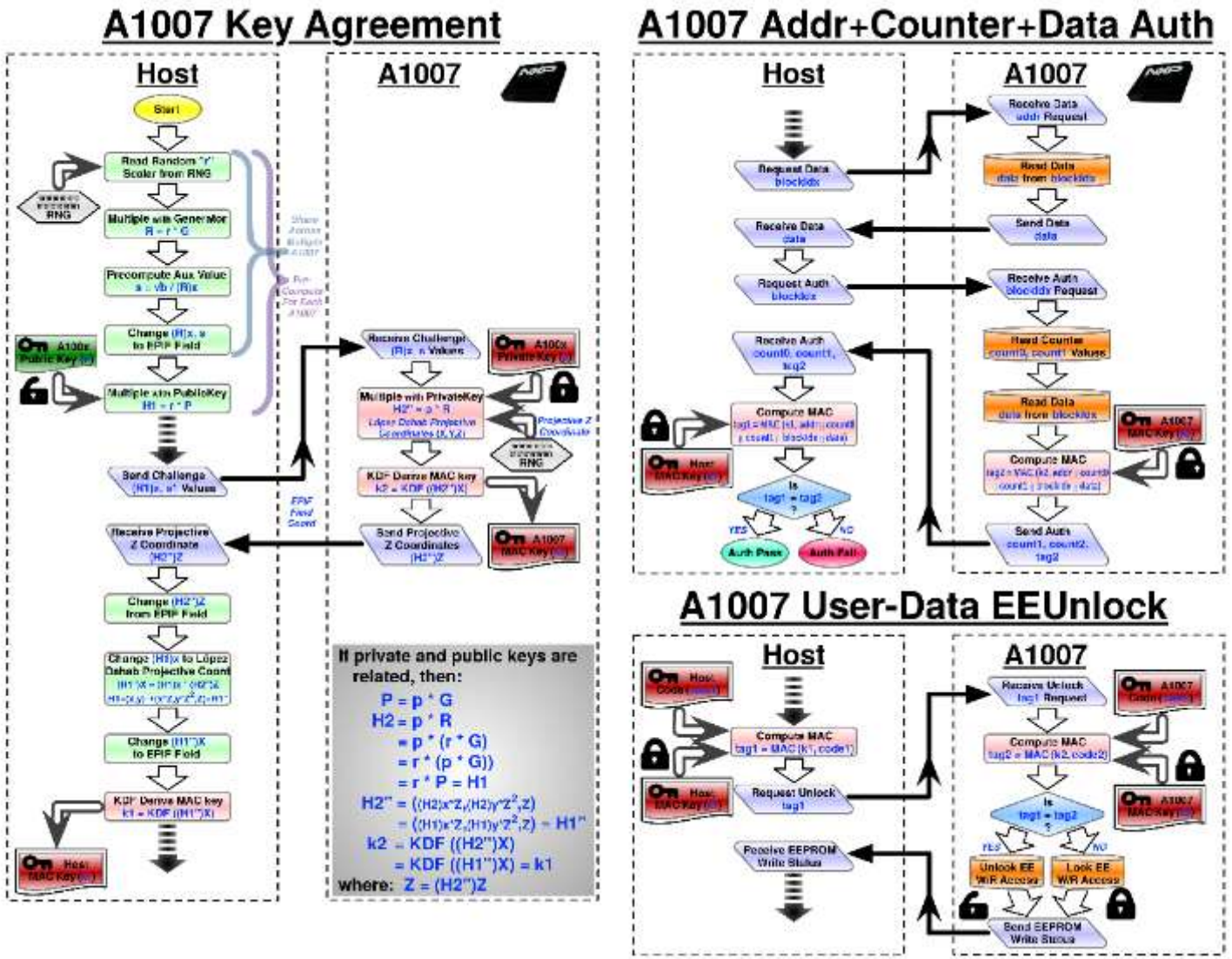
- No security IC needed on host side because of public key authentication (PKI)
  - Asymmetric public/private key Diffie-Hollman authentication protocol based on NIST ECC B-163 curve
  - Digitally signed certificates using ECDSA and NIST ECC P-224 curve
  - PRESENT cipher for locking user memory
- Features for consumables:
  - Two one-way counters
  - 16 non-resettable flags
  - Lockable user space
  - Kill-chip command
- Industry leading advanced security features include: TRNG, active shielding, security sensors, DPA/SPA, many more
- 8kbit EEPROM supports 2 certificates, system memory, and 4kbit for user needs
- Industry's lowest power (550uA max)
  - Deep sleep power < 1 uA at 1.8V Vdd
- Small footprint – available in HXSON6 2 x 2 mm package
  - CSP package - 1.3 x 0.94 mm WLCSP4
- Flexible Interfaces: 400 kbps I2C or one wired interface
  - OWI bus powered (no external Vdd needed)
  - OWI interface rated 8kV IEC61000-4-2 ESD protection

A1007 Ephemeral Key and MAC TAG

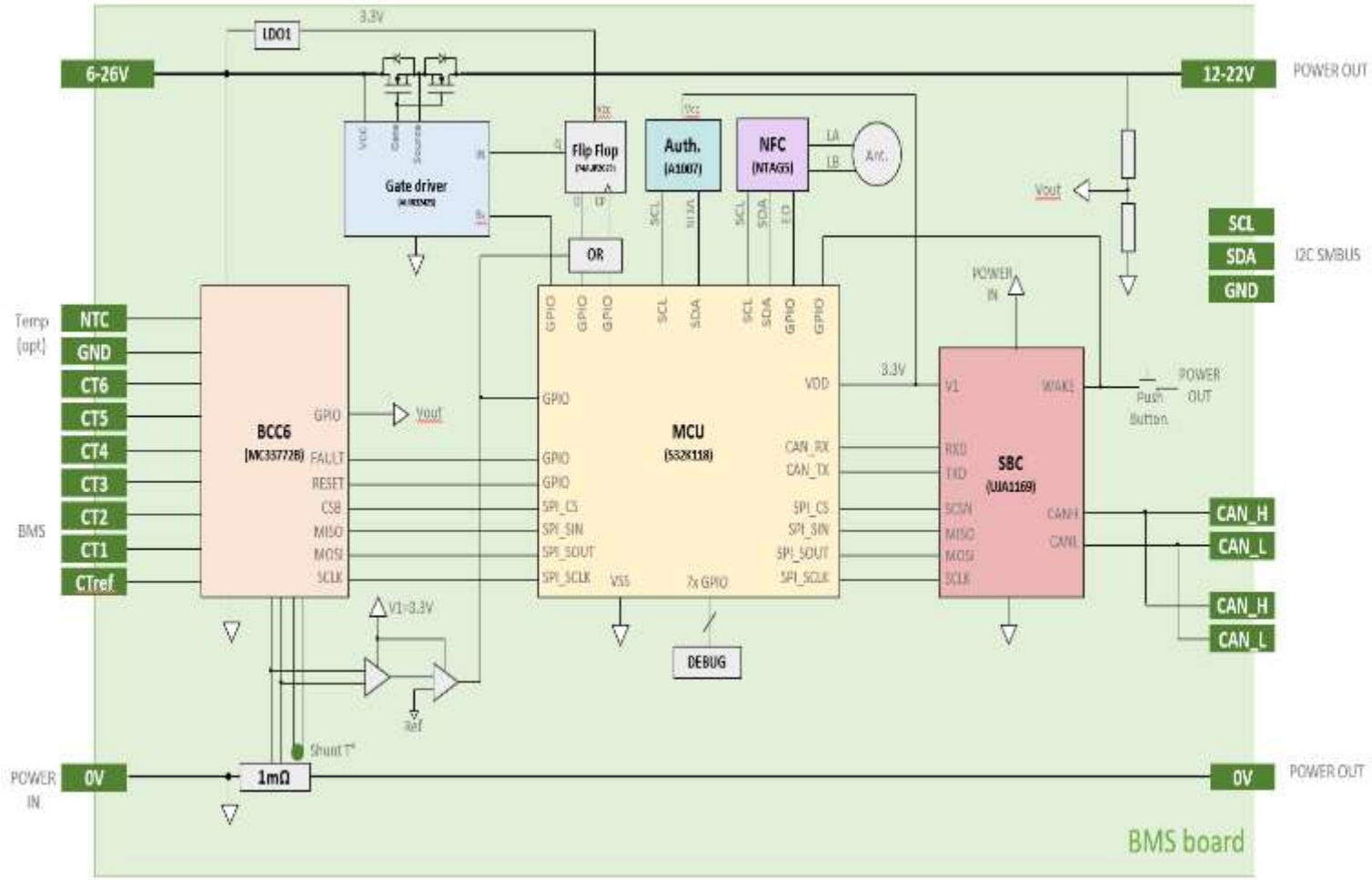


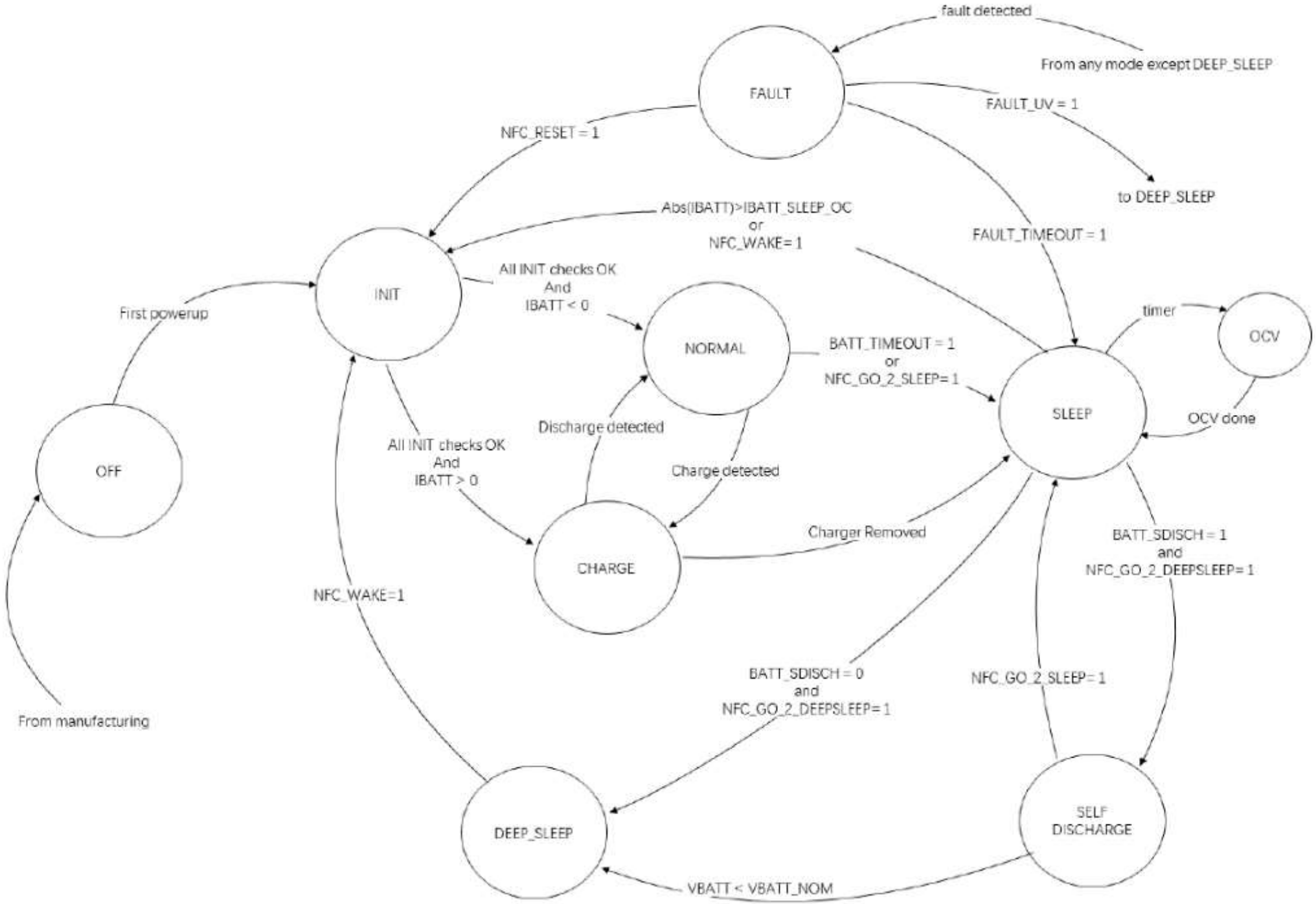

Send ECC PublicKey
A1007 PrivateKey
ECC PrivateKey
Random
Generate MAC Key via ECDH secret & KDF
Send Coord Parameter
Generate MAC Key via ECDH secret & KDF
Request Data Block
Send Data Block
Request Data Block Auth
Compute MAC Tag
Send MAC Tag
Compute MAC Tag
Stop
fail
Compare MAC Tags
match
Continue service
A1007 has correct ECC private key, counter values, I2C/OWI interface address, and optional data block contents at specified memory address

NXP Trust


A1007 Key Agreement
Host
A1007
Start
Read Random "r" Scaler from RNG
RNG
Multiple with Generator R = r * G
Precompute Aux Value
Change (R)x, z to EPIF Field
Multiple with PublicKey H1 = r * P
Send Challenge
Receive Challenge
Multiple with PrivateKey H2'' = p * R
KDF Derive MAC key
Send Projective Z Coordinates
Receive Projective Z Coordinate
Change (H2'')Z from EPIF Field
Change (H1)x to López Dahab Projective Coord
Change (H1'')X to EPIF Field
KDF Derive MAC key
If private and public keys are related, then:
P = p * G
H2 = p * R
= p * (r * G)
= r * (p * G)
= r * P = H1
H2'' = ((H2)x*Z,(H2)y*Z^2,Z)
= ((H1)x*Z,(H1)y*Z^2,Z) = H1''
k2 = KDF ((H2'')X)
= KDF ((H1'')X) = k1
where: Z = (H2'')Z
A1007 Addr+Counter+Data Auth
Host
A1007
Request Data
Receive Data
Request Auth
Receive Auth
Compute MAC
Is tag1 = tag2 ?
YES
NO
Auth Pass
Auth Fail
Send Auth
A1007 User-Data EEUnlock
Host
A1007
Compute MAC
Request Unlock
Receive EEPROM Write Status
Unlock EE W/R Access
Lock EE W/R Access
Send EEPROM Write Status

Software?


LDO1
3.3V
6-26V
12-22V
POWER OUT
Gate driver
Flip Flop
Auth.
(A1007)
NFC
(NTAG5)
Ant.
LA
LB
Vout
OR
SCL
SDA
GND
I2C SM/BUS
POWER IN
NTC
Temp (opt)
GND
CT6
CT5
CT4
CT3
CT2
CT1
CTref
BMS
BCC6
(MC33772B)
GPIO
FAULT
RESET
CS
MISO
MOSI
SCLK
MCU
(S32K118)
VDD
CAN_RX
CAN_TX
SPI_CS
SPI_SIN
SPI_SOUT
SPI_SCLK
VSS
7x GPIO
DEBUG
SBC
(UJA1169)
V1
WAKE
RXD
TXD
SCSN
CANH
CANL
Push Button
POWER OUT
CAN_H
CAN_L
V1=3.3V
ref
Shunt T°
1mΩ
0V
POWER IN
POWER OUT
BMS board


fault detected
From any mode except DEEP_SLEEP
FAULT
FAULT_UV = 1
to DEEP_SLEEP
NFC_RESET = 1
Abs(IBATT)>IBATT_SLEEP_OC
or
NFC_WAKE= 1
FAULT_TIMEOUT = 1
INIT
All INIT checks OK
And
IBATT < 0
NORMAL
BATT_TIMEOUT = 1
or
NFC_GO_2_SLEEP= 1
timer
OCV
First powerup
SLEEP
OCV done
Discharge detected
All INIT checks OK
And
IBATT > 0
Charge detected
OFF
Charger Removed
CHARGE
BATT_SDISCH = 1
and
NFC_GO_2_DEEPSLEEP= 1
NFC_WAKE=1
BATT_SDISCH = 0
and
NFC_GO_2_DEEPSLEEP= 1
NFC_GO_2_SLEEP= 1
From manufacturing
DEEP_SLEEP
SELF
DISCHARGE
VBATT < VBATT_NOM

Results: What is the Software Status?

Software drivers and initial API to:

- ✓ Acquire measurements
- ✓ Balance cells
- ✓ Open and close the MOSFETs
- ✓ Blink the LED
- ✓ Detect an overcurrent on the MCU
- ✓ Send measurements to an adapted Python GUI via CAN

In Discussion: What architecture to use for the application software?

- Bare Metal – lightest weight option but less flexible
- NuttX RTOS – align with DroneCode developers and reuse of modules
- Other RTOS – align with other NXP business

What's Next

- Q1' 2020
- Engagement with PX4 community and early adopter companies.
- Early access available
- Contact iain.galloway@nxp.com

www.hovergames.com

www.nxp.com/hovergamesdrones

SECURE CONNECTIONS
FOR A SMARTER WORLD