AN12148

S32K1xx and SBC in safety applications

Rev. 0 — November 2018 Application Note

by: NXP Semiconductors

Contents

1 Introduction

This application note provides an overview and general guidelines for automotive electronic applications based on NXP general purpose S32K1xx microcontroller family and NXP System Basis Chips that target the ISO 26262 functional safety standard. It provides a safety feature set overview of S32K1xx MCU family and corresponding SBC devices from NXP : UJA1169, UJA113x and FS4500 and gives guidelines for using this devices as a bundle in automotive safety applications rated according to ISO26262 level ASIL B, C and D.

NXP's ISO 26262 solutions, that form part of the SafeAssure program, help system manufacturers to easily achieve system compliance with functional safety standards by simplifying the system architecture.

2 S32Kxx family overview

S32K1xx is a scalable family of AEC-Q100 qualified 32-bit ARM® Cortex®-M4F and Cortex®-M0+ based MCUs targeted for general purpose automotive applications including safety applications for various domains.

This section describes the S32K1xx features that are of interest when integrating the device with a system basis chip.

2.1 SafeAssure program

S32K1xx family belongs to NXP's SafeAssure program SafeAssure products are conceived to simplify system level functional safety design and cut down time to compliance.

The S32K1xx series is developed according to ISO 26262 and has an integrated safety concept targeting an ISO26262 ASIL-B integrity level. The following documentation supports the integration of an S32K1xx chip into safety-related systems:

- Reference Manual (S32K1xxRM): describes the programming model and functionality of S32K1xx chips
- Data Sheet (S32K1xx): describes S32K1xx operating conditions as well as timing and electrical characteristics
- Safety Manual (S32K14xSM): describes the S32K14x safety concept and possible safety mechanisms (integrated in S32K14x, system-level hardware, or system-level software) as well as measures to reduce dependent failures
- Dynamic FMEDA: inductive analysis enabling customization of system-level safety mechanisms, including the resulting safety metrics for ISO 26262 (SPFM, LFM & PMHF) and IEC 61508 (SFF & Beta IC Factor)
- FMEDA Report: describes the FMEDA methodology and safety mechanisms supported in the FMEDA, including source of failure rates, failure modes, and assumptions during the analysis

2.2 S32K1xx family safety concept

The Objective of safety concept is to define how MCU ASIL targets will be achieved between a mix of on-chip HW safety measures and system level safety measures (HW/SW). In order to minimize additional software and module level features to reach this target, on-chip redundancy is offered for the critical components of the MCU:

- Core Selftest for M0+ (S32K11x) and M4 cores (S32K14x)
- ECC on RAM
- ECC on Flash
- Power Supply Monitoring
- Clock Monitoring
- Memory Protection Unit
- Internal Software Watchdog
- CRC Unit
- Register Protection
- Diversity of communication channels
- Diversity of digital and analog signal paths

2.3 Power supply requirements

Power diagram: S32K power supply is based on a single power supply (2.70–5.5 V) with full functional flash program/erase/read operations.

A detailed description of S32K Power Supply and decoupling guidelines can be found in Datasheet and Application note AN5426 “Hardware Design Guidelines for S32K1xx Microcontrollers”.

The diagram below provides a high level overview of power supply domains and connections on S32K1xx family.

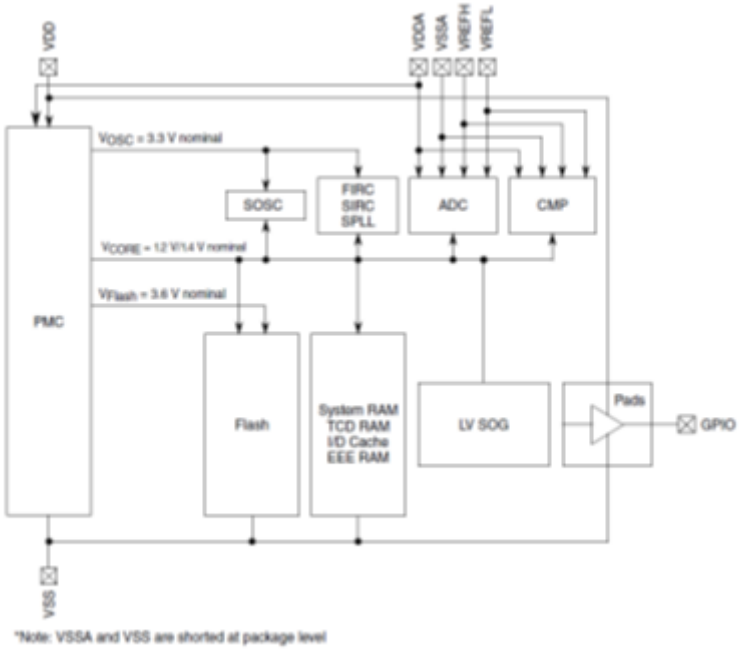

Figure 1. Power diagram

Table below shows the power Supply Pins and operating ranges.

Table 1. Power Supply Pins and operating ranges

Power Domain	Description	Operating Range [V]
VDD / VSS	Input Supply Voltage	2.7…5.5
VDDA / VSSA[1]	Analog supply voltage	2.7…5.5
VREFH[2] / VREL[3]	ADC reference voltage high/low	2.7…VDDA+0.1
VREFL - VSS	VREFL to VSS differential voltage	-0.1…+0.1
VDD -VDDA	VDD to VDDA differential voltage	-0.1…+0.1

1. Vssa is internally connected to Vss and no external connection is available.
2. Vrefh may be connected to the same potential as Vdda or may be driven by an external source to a level between the minimum Ref Voltage High and the Vdda. Potential in Vrefh should never exceed Vdda.
3. Connect VFREL to the same potential as Vssa.

2.4 Communication interfaces

There are three serial communication interfaces which are used together with SBCs: FlexCAN for CAN and optionally CAN-FD interface, Low Power UART, and Low Power Serial Peripheral Interface (LPSPI) and FlexIO module which is capable of supporting a wide range of protocols including UART, I2C, SPI . The FlexCAN module is a communication controller implementing the CAN Protocol Specification version 2.0B.

The LPUART module supports LIN Master mode, LIN Slave mode and UART mode. The LIN state machine is compliant to LIN 1.3, 2.0, 2.1 and 2.2 specifications.

DSPI module provides a synchronous serial bus for communication between the MCU and external peripheral devices, for example the SBCs UJA1169, UJA1132 and FS45.

2.5 S32K1xx family Power Management

2.5.1 Power Management Controller and Reset

PMC provides features POR, brown out detect, Low voltage reset (LVR) and low voltage detect supporting two low voltage trip points and interrupt. A dedicated and permanently enabled Power On Reset (POR) mechanism controls the V_{dd} supply, the internal flash supply, as well as the oscillator supplies. When power is initially applied to the MCU or when the supply voltage drops below the power-on reset re-arm voltage level (VPOR), the POR circuit causes a POR reset condition. After a POR event, the typical amount of time from the point VDD reaches 2.7 V to execution of the first instruction across the operating temperature range of the chip is 325 us.

When power is initially applied to the MCU or when the supply voltage drops below the POR detect voltage (VPOR), the POR circuit causes a POR reset condition.As the supply voltage rises, the LVD circuit holds the MCU in reset until the supply has risen above the LVD low voltage detect threshold (VLVD). Below diagram shows MCU operating conditions along with rising and falling POR and LVD threshols levels.

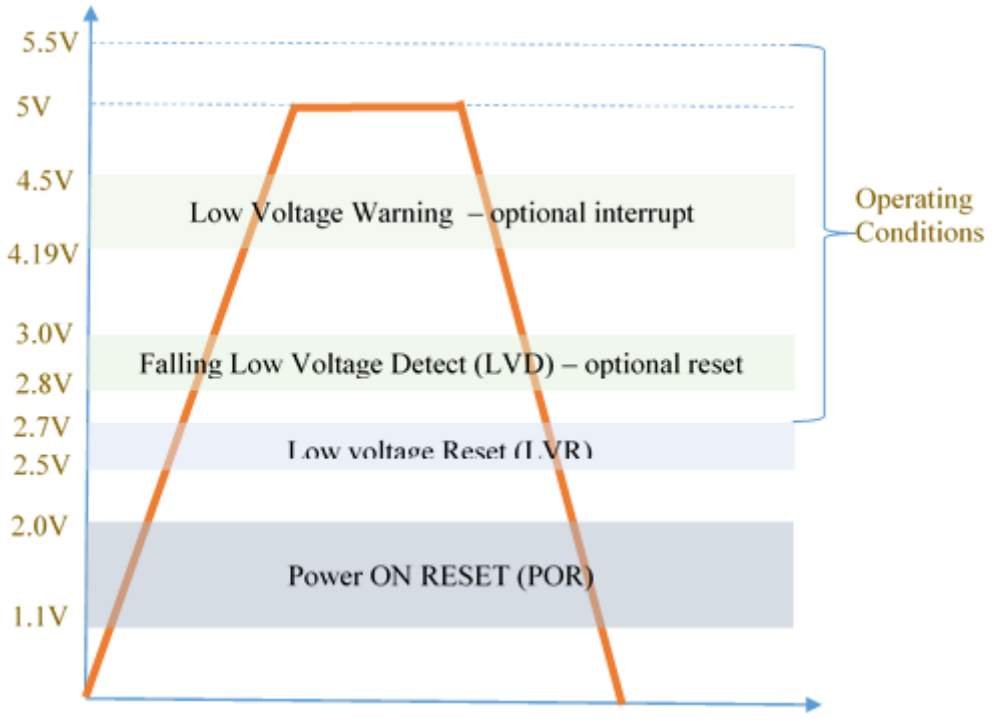

Figure 2. VDD supply LVR, LVD and POR operating requirements and reaction

Table below shows POR and low voltage monitoring options available on S332K1xx family along with reactions when specified threshold has been violated.

Table 2. POR and LVD thresholds and reaction

Power Domain	Description	Threshold [V]	Reaction
Vpor	Rising and falling VDD POR detect voltage	1.1…2.0	Reset
Vlvr	LVR falling threshold (RUN, HSRUN, and STOP modes)	2.5….2.7	Reset
Vlvr_lp	LVR falling threshold (VLPS, VLPR modes)	1.97…2.44	Reset
Vlvd	Falling low-voltage detect threshold (not available in VLPS and VLPR)	2.8…3 V	Configurable: Reset or Interrupt
Vlvw	Falling low-voltage warning threshold (not available in VLPS and VLPR)	4.19…4.5	Configurable: Interrupt

2.5.2 S32K1xx family power modes

The Power Management Controller (PMC) provides multiple power options allowing users to optimize power consumption.

The following figure shows the power mode transitions. Any reset always brings the chip back to the Normal Run state. In run, stop modes active power regulation is enabled. The VLPR modes offer a lower power operating mode than normal modes. VLPR is limited in frequency.

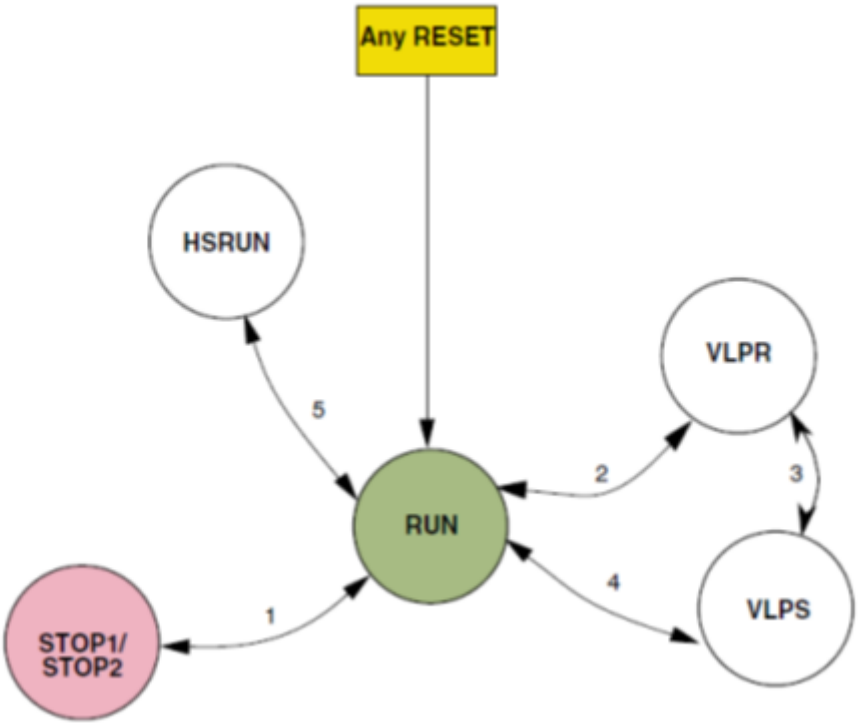

Figure 3. Power mode transitions

The following table compares the various power modes available on S32K1xx and provides current consumption indications which depend on device, frequency of operation and temperature. For detailed information on current consumption please refer to S32K1xx Datasheet chapter 4.7 Power consumption .

Table 3. Power modes available in S32K1xx

Chip Mode	Description	VREG Mode	LVD	M0/M4 Core Mode	Recovery Method	Current Consumption Indication
Normal RUN	Default mode out of reset	Normal	ON	Run	-	15 mA…70 mA
High Speed RUN	Maximum performance with restricted functionality	Normal	ON	Run	-	40 mA…100 mA
VLPR	Max 4 MHz system clock	Low Power	OFF	Run	-	1 mA…6 mA
STOP1	Static state All registers are retained.	Normal	ON	Deep Sleep	Interrupt	6 mA…23 mA
STOP2	Static state. Bus clock remains active. All registers are retained.	Normal	ON	Deep Sleep	Interrupt	7 mA…24 mA
VLPS	Lowest-power mode All registers are retained.	Low power	OFF	Deep Sleep	Interrupt	25 uA…3 mA

3 SBC UJA1169 / UJA113x / FS45 Feature overview

3.1 UJA1169 family

3.1.1 UJA1169 family and Functional Safety features

System Basis Chip (SBC) devices typically accompany a system Microcontroller such as S32K1xx family and provide various functions and features such as Voltage regulators, System management State machine, I/O functions, a Network communication interface such as CAN and/or Lin Transceivers as well as system - and safety relevant functions for example Watchdog, Event signaling, Protection schemes voltage monitoring and System Reset. The SBC configuration and diagnosis is done through SPI interface typically.

The UJA1169 SBC family offers 3V3 and 5V Regulator options, a Protected regulator for Off board supplies, system wakeup features, CAN FD Transceiver with Partial networking and CAN FD passive options as well as Limp home functionality and a

configurable Watchdog. An external PNP transistor can be applied to enhance system thermal performance avoiding Hotspots. Overall the device family provides entry and intermediate level of function/feature integration in a small housing (HVSON20 3.5 x 5.5 mm) and the table below lists available device and feature options of this SBC family.

Table 4. UJA1169 family feature overview

Product Type	Standby/ Sleep mode	Reset	VIO pin	V1: 5 V uC only	V1: 5 V uC and CAN	V1: 3V3 uC	V2: 5 V Can and on-board loads	Vext: 5 V protected	Watchdog	CAN FD,PN FD passive[1]
UJA1169 TK	Yes/Yes	Yes	No	up to 250 mA			up to 100 mA		yes	2Mbit/no/ no
UJA1169 TK/X	Yes/Yes	Yes	No		up to 250 mA			up to 100 mA	yes	2Mbit/no/ no
UJA1169 TK/F	Yes/Yes	Yes	No	up to 250 mA			up to 100 mA		yes	2Mbit/yes /yes
UJA1169 TK/X/F	Yes/Yes	Yes	No		up to 250 mA			up to 100 mA	yes	2Mbit/yes /yes
UJA1169 TK/L	Yes/Yes	Yes	Yes	up to 250 mA			up to 100 mA		yes	2Mbit/no/ no
UJA1169 TK/X/L	Yes/Yes	Yes	Yes		up to 250 mA			up to 100 mA	yes	2Mbit/no/ no
UJA1169 TK/F/L	Yes/Yes	Yes	Yes	up to 250 mA			up to 100 mA		yes	2Mbit/yes /yes
UJA1169 TK/X/F/L	Yes/Yes	Yes	Yes		up to 250 mA			up to 100 mA	yes	2Mbit/yes /yes
UJA1169 TK/3	Yes/Yes	Yes	No			up to 250 mA	up to 100 mA		yes	2Mbit/no/ no
UJA1169 TK/F/3	Yes/Yes	Yes	No			up to 250 mA	up to 100 mA		yes	2Mbit/yes /yes

1. CAN FD 5Mbit timing variant is planned

Functional safety is implemented on system level with specific safety goals for the desired application in mind. The SBC device may provide support for such goals through implemented functions. In this way, for example an ASIL A or B System Application might be implemented with a Quality Managed (QM) SBC if the functional safety goals can be achieved with the available feature set on system level.

SBC features in UJA1169 family, that can support functional safety goals in applications include:

- Under voltage monitoring for Regulators V1, V2 and for V1 with selectable threshold
- Supporting Microcontroller RAM Retention on V1 down to 2 V Vbat
- V1 & V2 regulators are current limiting regulators and short circuit proof to GND
- V_{ext} is current limiting regulator and protected against short to Vbat,GND and neg Voltages down to -18 V
- T_{xd} dominant time out detection on CAN interface
- CAN under voltage detection and listen only mode
- Over Temperature warning and shutdown

- Limp home mode with user selectable criteria
- On Chip Non Volatile Memory for storing configuration data

3.1.2 Voltage regulators and supervision

The UJA116x family is designed for Battery supply via Polarity protection and filter/buffering network and provides Gapless supply range on its Vbat bin. The device features two Linear Regulators with 2% tolerance and with integrated under voltage monitoring and current limiting. The V1 regulator is intended to supply the main Application Controller and is setting the reference voltage for its digital Interface pins. A typical application schematic is shown in Figure 1. on page 3.

The under voltage monitoring of the V1 regulator in its 5V variants is user selectable between 60%, 70% 80 % and 90% level relative to nominal V1 supply through configurable SPI register settings (Reg 74h) In the device option with V1 as 3V3 Regulator options only a 90% level is available. Triggering of the under-voltage Threshold will cause a reset on pin RSTN.

The V1 regulator has a special feature implemented that supports uC RAM data retention in case of under voltage events. If the Vbat drops far enough to trigger the under voltage reset, the load current of the regulator drops quickly as uC goes through reset state. A current source is switched in to buffer a minimal load current down to 2 Vbat to support RAM data retention process within the uC in its reset. A sudden overshoot of V1 during recovery at Vbat is prevented by a clamp structure until V1 regulator gets reactivated reaching its operating range.

An external PNP Transistor can be populated and configured with the SBC to prevent hotspot generation and overheating. An overvoltage warning threshold in the register set can be used to check if the application and the regulator is about to be overloaded or in recovery.

The V2 regulator does feature also overvoltage monitoring. A device option features this regulator called Vext protected against loss of Ground, short to Vbat and protected against negative Voltages. It is intended to supply "OFF Board" loads.

Status and Control of both Regulators can be done through Reg x10, x1B and x1C and further details are described in Application Note AH1306

3.1.3 Watchdog

The Software configurable Watchdog can operate in Window and timeout mode as well as Autonomous mode to enable for example a cyclic wakeup. Failure to trigger the watchdog correctly will result in a reset on Pin RSTN. During Software development mode fo the SBC the watchdog can be enabled and disabled to help during HW and SW development. Details of Watchdog configuration and triggering are in the datasheet and the Application note AN1306.

3.1.4 Limp home

The SBC features a Limp home pin that could be used to signal an Emergency situation through open drain, battery robust low side driver analog output. An Error counter is implemented and any Reset (including coming out of sleep mode) will increase the counter. The Limp output is asserted from floating to active low when LHC bit in Limp home register is set to “1”. LHC bit is set when:

- Reset counter RCC is overflowing (selectable through SPI, max RCC=3
- Overtemperature condition for longer than tdlimp
- SBC in Reset state (external or internal) for linger than tdlimp.

Limp conditions are stated in the table shown in the figure below and a Limp state diagram are described in section 6 of [Ref AH1306].

Condition	Comment
LHC set by SPI command	Setting (or resetting) of LHC via SPI is possible only, while the SBC is not in Reset Mode or Overtemp Mode
Reset Mode clamped	SBC is continuously in Reset mode due to a clamped RSTN pin or a permanent undervoltage on V1 e.g. due to overload condition. LIMP gets active, if Reset Mode lasts for longer than $t_{d(LIMP)}$ while RCC < 3 or Reset Mode is entered while RCC = 3
Overtemp Event	SBC is in Overtemp mode for more than $t_{d(LIMP)}$ while RCC <3 or Overtemp mode is entered while RCC = 3
RSTN LOW	RSTN was pulled LOW externally while RCC = 3
Watchdog Failure	Watchdog not triggered correctly causing Reset Mode Entry while RCC = 3
Illegal Sleep Mode Entry	Software tries to enter Sleep Mode with pending wake-up or no enabled wake-up source while RCC = 3
Wake-up from Sleep	Reset Mode entered out of Sleep Mode while RCC = 3

Figure 4. UJA1169 Limp home set conditions

3.1.5 CAN transceiver

The integrated CAN transceiver provides Gapless supply range (see Gapless specified CAN supply voltage range) and is monitored for under voltage independent from V1 and V2. This monitor can be enabled or disabled through CMC bits in CAN control Register x20h. Other CAN functions such as Partial networking is controlled through the same register. The CAN Status register x22h provides information about CAN Transceiver status (CTS), the CAN under voltage condition (VCS) and CAN TXD dominant timeout trigger (CFS). Partial networking related status bits can be also found in this register.

The Transceiver supports four different operation modes:

- CAN OFF
- CAN ACTIVE
- CAN OFFLINE
- CAN LISTEN ONLY

The CAN Transceivers Txd dominant timeout is supporting Fail Safe behavior. If Txd pin is forced low an integrated timer will release the bus pins to recessive state after a timeout is exceeded. The timer will reset upon Txd getting released to high. If the Txd is pulled low before CAN Active mode is selected the state machine will prevent it and selects automatically (or remains) in CAN Listen only mode to prevent further problems due to driving the bus and it remains there until Txd goes high again. During a bus failure the current provided by the CAN regulator is limited according to the datasheet conditions for short circuit current limits. If the under-voltage monitor is enabled and triggered, the CAN Transceiver moves to CAN OFFLINE mode. This would prevent communication but leaves the CAN ready for wakeup and recovery of supply. The CAN LISTEN ONLY mode could be used to prevent CAN communication and is selected through SPI Register access. For further details including the CAN state diagram please consult AH1306 and the Datasheet.

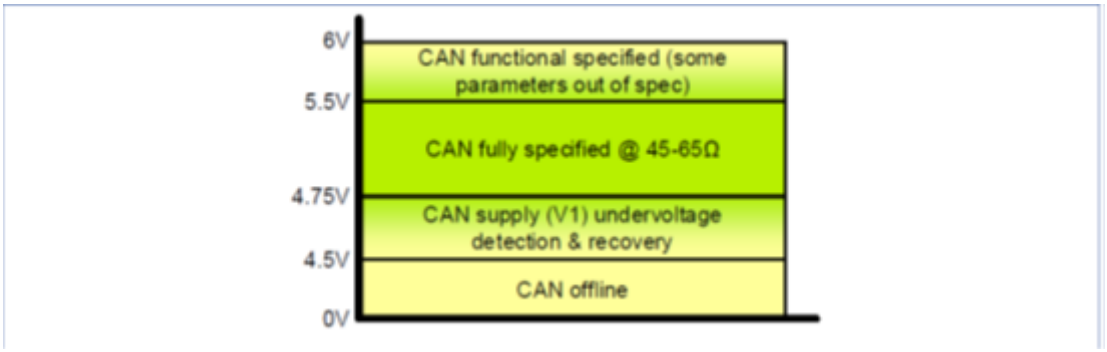

Figure 5. Gapless specified CAN supply voltage range

3.1.6 Low power features and MTP Memory configuration

The UJA1169 is supporting Sleep mode (typ 53 uA) with enabled CAN wakeup source. In sleep mode all regulators are off. A standby mode with enabled Regulator V1 and V2 (register configurable) is available with typically 71 uA without application load and CAN traffic. Additional wakeup through WAKE pin with selectable edge logic is implemented adding additionally typ 2 uA current. If Partial networking is enabled a higher sleep mode current needs to be planned as the device needs to Monitor the bus for Wakeup Frames (WUF). At least one wakeup source needs to be configured in the SBC before it is possible to enter sleep mode.

Multi Time Programmable Non Volatile Memory (MTPNV)is used for the Configuration Control Register to define desired behavior after initial cold start. The V1 under-voltage threshold, Forced normal or Software development mode as well as sleep mode enablement gets defined in this register and factory preset values are there to start up. This memory needs to be programmed initially and locked with a correct CRC code to proceed with application initialization after a reset cycle. The datasheet and application note provide detail information.

3.2 UJA113x system basis chip

3.2.1 Family overview and functional safety features

The UJA113x is a CAN/LIN SBC family providing an efficient buck and-pre-boost Switch mode converter architecture along with commonly used features in Automotive ECUs. The UJA113x SBC family can serve applications with higher load current requirements compared to UJA1169 family and supports boost functionality to cover Battery cranking scenarios. It provides additional LIN Transceivers, flexible Analog IO functions, four PWM Timers, two Battery Voltage ADCs and watchdog. It does support 3V3 and 5 V options, Protected regulator for Off board supplies, system wakeup features, CAN FD with Partial networking and CAN FD passive as well as Limp home functionality. A family-feature overview is shown in the figure below.

	Buck/high-current boost SMPS	Buck/low-current boost SMPS	V1 LDO 5 V, 500 mA	V1 LDO 3.3 V, 500 mA	V2/VEXT LDO 5 V 100 mA	CAN FD transceiver up to 2 Mbit/s	CAN partial networking; CAN FD passive	1 × LIN transceivers	2 × LIN transceiver	4 × HVIOs: HS/LS driver or WAKE input	8 × HVIOs: HS/LS driver or WAKE input	4 × timers for HVIO control	Battery monitoring	Watchdog	LIMP pin	Advanced LIMP function	SPI interface	Reset output	EN pin for controlling critical hardware	Mode control: Normal, Standby, Sleep	Overtemperature warning and shutdown	HTQFP48 package
UJA1131HW/5V0	•		•		•	•		•			•	•	•	•	•	•	•	•	•	•	•	•
UJA1131HW/3V3	•			•	•	•		•			•	•	•	•	•	•	•	•	•	•	•	•
UJA1132HW/5V0	•		•		•	•			•		•	•	•	•	•	•	•	•	•	•	•	•
UJA1132HW/3V3	•			•	•	•			•		•	•	•	•	•	•	•	•	•	•	•	•
UJA1135HW/5V0		•	•		•	•		•			•	•	•	•	•	•	•	•	•	•	•	•
UJA1135HW/3V3		•		•	•	•		•			•	•	•	•	•	•	•	•	•	•	•	•
UJA1136HW/5V0		•	•		•	•			•		•	•	•	•	•	•	•	•	•	•	•	•
UJA1136HW/3V3		•		•	•	•			•		•	•	•	•	•	•	•	•	•	•	•	•
UJA1131HW/FD/5V/4	•		•		•	•	•	•		•		•	•	•	•	•	•	•	•	•	•	•
UJA1131HW/FD/3V/4	•			•	•	•	•	•		•		•	•	•	•	•	•	•	•	•	•	•
UJA1131HW/FD/5V/0	•		•		•	•	•	•					•	•	•		•	•	•	•	•	•
UJA1131HW/FD/3V/0	•			•	•	•	•	•					•	•	•		•	•	•	•	•	•
UJA1132HW/FD/5V/4	•		•		•	•	•		•	•		•	•	•	•	•	•	•	•	•	•	•
UJA1132HW/FD/3V/4	•			•	•	•	•		•	•		•	•	•	•	•	•	•	•	•	•	•
UJA1132HW/FD/5V/0	•		•		•	•	•		•				•	•	•		•	•	•	•	•	•
UJA1132HW/FD/3V/0	•			•	•	•	•		•				•	•	•		•	•	•	•	•	•

Figure 6. UJA113x family-feature overview

The SBC family may support Functional Safety Goals on Application level with the following functions:

- Under voltage monitoring for Regulators V1, V2 and for V1 with selectable threshold
- Supporting Microcontroller RAM Retention on V1 down to 2V V_{bat}
- V1 & V2 regulators are current limiting regulators and short circuit proof to GND
- Vext is current limiting regulator and protected against short to Vbat, GND and neg Voltages down to -18 V
- Txd dominant time out detection on CAN interface
- CAN supply under voltage detection and Listen Only mode
- Over Temperature warning and shutdown
- Limp home mode with user selectable criteria
- HVIO pins that can be configured to support additional Limp home signaling
- En pin to control external and critical HW

- Two Interrupt pins with different priority and register based maskable source
- On Chip Non -Volatile Memory for storing configuration data

3.2.2 Voltage regulators

The SMPS operates in Buck mode, Boost mode or Auto mode which includes a SMPS bypass operation that is depending on configuration and actual operating conditions. The SMPS output voltage is configurable and can serve as the input for Linear Voltage Regulators and/or the HVIO supply pins or external additional Regulators or circuits. BATV2 and the BATHS supply pins might also be supplied by Vbat or additional Power supplies in the system.

The SMPS, V1 and V2 are current limited and the integrated Over Temperature warning could trigger the SMPS output voltage to go down to 5 V effectively reducing the output voltage and internal power dissipation of the 5 V LDO's. This might be still high enough to safe data and take appropriate emergency action. V1 and V2/V_{ext} are under voltage monitored and Vext is additionally over voltage monitored and can be configured for load shedding if Vbat ADC detects over/under voltage conditions. VCAN supplies the CAN transmitter and has also an independent under voltage monitor. This monitoring can also be disabled in a register to allow the CAN to transmit as long as possible during a undervoltage situation if desired.

3.2.3 Watchdog

The Watchdog is SW configurable in Window and Timeout mode as well as Autonomous mode and cyclic wakeup is supported. If watchdog is used a Failure to trigger the watchdog correctly will result in a reset on Pin RSTN. During Software development mode fo the SBC the watchdog can be enabled and disabled to help during HW and SW development. Details of Watchdog configuration and triggering are in the datasheet and the Application note AH1506.

3.2.4 Limp home, interrupt and EN pin

The SBC features a Limp home pin that could be used to signal an Emergency situation through is open drain, battery robust low side driver analog output. The implemented Error counter (RCC) will increase with any Reset (including coming out of sleep mode). At RCC = 3 (default setting) the device is asserting LHC register bit. The Limp output is asserted from floating to active low when LHC bit in Fail safe control register [02h] is set to "1." LHC bit is asserted when:

- SBC system controller enters Overload mode
- SBC system controller enters or Forced Sleep protection mode (multiple reset events)
- Host command is setting LHC bit to "1"

Multiple reset events can result from Overtemperature, watchdog service loss, short circuit of RSTN or V1 or external Reset. The Limp pin clears if System control is going through Off mode or Host command is overwriting LHC bit to 0.

In addition to the Limp pin, the HVIO2, HVIO3 and HVIO4 can be configured per Startup control register [73h] to support Limp home functionality. HVIO2 can be used as a high sider driver, HVIO3 and four as PWM drivers with different duty cycle and PWM frequency driven by Timers three and four of the device. The system controller state diagram is described in section 7.1 in the datasheet and the Limp, EN and HVIO Limp functions are described in AH1502.

The En pin is a Active low driver based on V1 voltage that can be controlled by Registers depending on Mode of the SBC, timer two or by the Battery Voltage ADC configured over and under voltage thresholds. This allows the EN pin to enable and disable critical HW functions in a very flexible way. Details can be found in AH1506 and Datasheet.

The INTN1 and INTN2 pins provide Interrupt information to the Host MCU. INTN1 provides all interrupts but could be possibly time delayed if pending Interrupts have been cleared shortly before a new one occurs. INtN2 signals a critical subset of Interrupts without delay. Most Interrupts are maskable except:

- Watchdog failure (WDI)
- Partial Network frame detect error (PNFDEI)
- Power on status (POSI)
- Over-voltage shutdown (OVSDI)

Interrupt status information is available in Registers x60 for global information and x61h to x67h for individual interrupts. An overview of available Interrupts and their Signaling pin is listed in the table displayed in the figure below.

Symbol	Description	Type	Pin	Source
CFI	CAN failure interrupt	diagnostic	INTN1	Status bit VCS and/or status bit CFS is set to 1.
CWI	CAN wake-up interrupt	regular	INTN1	A CAN wake-up event was detected while the transceiver was not in Active mode.
CBSI	CAN-bus silence interrupt	diagnostic	INTN1	The CAN-bus has been silent for $t > t_{to(silence)}$.
LWIn	LINn wake-up interrupt	regular	INTN1	A wake-up event was detected at LINn while the transceiver was not in Active mode.
WDI	watchdog failure interrupt	diagnostic	INTN1	The watchdog overflowed in Timeout mode. If the watchdog overflows while a WDI is pending, a reset is performed. Note that this interrupt cannot be deactivated.
OTWI	overtemperature warning interrupt	diagnostic	INTN1, INTN2	The global chip temperature has exceeded the over-temperature warning threshold.
PNFDEI	partial networking frame detect error interrupt	diagnostic	INTN1	A CAN error frame was detected by the partial networking receiver.
POSI	power-on status interrupt	diagnostic	INTN1	The SBC has left Off Mode; interrupt is always enabled.
SPIFI	SPI failure interrupt	diagnostic	INTN1	This interrupt is triggered by the following events: • illegal WMC code • illegal NWP code • illegal MC code • wrong SPI clock count (only 16-, 24- and 32-bit commands are supported) • write access to a locked register
V1UI	V1 undervoltage interrupt	diagnostic	INTN1, INTN2	V1 voltage dropped below the 90 % undervoltage threshold while V1 was active (no interrupt triggered in Sleep mode because V1 is off). This interrupt is independent of the V1RTC bit setting.
VEXTUI	V2 undervoltage interrupt	diagnostic	INTN1	V2/VEXT dropped below the 90 % undervoltage threshold.
VEXTOI	V2 overvoltage interrupt	diagnostic	INTN1	V2/VEXT above the 110 % overvoltage threshold.
BMUI	battery monitor undervoltage interrupt	diagnostic	INTN1, INTN2	The voltage measured at the active battery monitoring source (pin BAT or pin BATSENSE) dropped below the selected undervoltage threshold.
BMOI	battery monitor overvoltage interrupt	diagnostic	INTN1, INTN2	The voltage measured at the active battery monitoring source (pin BAT or pin BATSENSE) has risen above the selected overvoltage threshold.
OVSDI	overvoltage shut-down interrupt	diagnostic	INTN1, INTN2	A battery overvoltage will cause the SBC to enter Overload Mode; interrupt is always enabled.
SMPSSI	SMPS status interrupt	diagnostic	INTN1, INTN2	The state of bit SMPSS has changed (see Section 7.8.4.1)
IOnOLI	HVIOn open load interrupt	diagnostic	INTN1	An open load condition was detected at HVIOn while the high-side or low-side driver was active.
IOnSCI	HVIOn short circuit interrupt	diagnostic	INTN1	A short-circuit condition was detected at HVIOn while the high-side or low-side driver was active.
IOnREI	HVIOn rising edge interrupt	regular	INTN1	A rising edge wake-up signal was detected at pin HVIOn when configured as wake input.
IOnFEI	HVIOn falling edge interrupt	regular	INTN1	A falling edge wake-up signal was detected at pin HVIOn when configured as wake input.

Figure 7. UJA113x interrupt overview

3.2.5 CAN and LIN transceivers

The CAN Transceiver block provides gapless supply voltage definition similar to the UJA1169 (Gapless specified CAN supply voltage range) of its VCAN regulator. The receiver is supplied from Vbat or VSPMS whichever pin has higher voltage. Please note that the CAN Transmitter supplied through Vcan for example by V2 or by VSMPS or Vbat and as such is influenced on their voltage conditions. The Vbat ADC provides possibility to shut down the CAN Transceiver timely in case for example VSPMPS is expected

to overload temporarily on Vbat < VSMPS and avoiding secondary under voltage event of the CAN Transmitter regulator block. This will prevent Error Frames on the CAN bus in these situations.

The CAN State machine provides four modes:

- CAN OFF
- CAN ACTIVE
- CAN OFFLINE
- CAN LISTEN ONLY

The CAN Offline mode is triggered by Sleep, Reset or FSP (Forced Sleep mode Preparation) mode or if the CMC register (Can mode Control, x20h) values 00 in normal mode or unequal to 11 in Standby Mode.

The Listen only mode allows to monitor the bus.

The CAN Transceiver provides Txd dominant timeout in case the bus is hold dominant for longer than t to (dom)Txdc and CAN Active mode can only be entered if Txdc is high. These features might be helpful to realize Functional Safety goals in the applications.

The SBC family provides either one or two LIN Transceivers integrated. They are under voltage monitored and support four modes:

- OFF
- OFFLINE
- LISTEN ONLY
- ACTIVE

For details on CAN and LIN blocks check the datasheet and AH1507.

3.2.6 Low power features, ADC and MPT memory

Standby and a very low power sleep mode are supported by the device. The Voltage supply behavior, HVIO function and Watchdog can be configured in the low power standby mode low power modes depending on intended functionality. Wakeup sources are also configurable and can be the Transceivers, Host command, HVIO and watchdog (cyclic wake).

The integrated 10bit ADC features 2 channels (pin Bat and pin BATSENSE) that are continuously converting as soon as normal mode is reached. Their input range is from 2 to 20V and intend to read the Battery voltage before the polarity protection circuit (BATSENSE, with serial resistor) and after (BAT). Over- and Under-voltage-threshold registers can trigger Interrupt events that could deactivate the CAN Transceiver, V2, Vext, HVIO and the EN pin loads.

MTPNV Memory configuration for startup behavior of some critical functionality is implemented. The high and low side states of the HVIO, their Limp functionality, the Reset length at cold start, V2 availability on different modes and its On or OFF board supply configuration, Forced Normal and Software development mode, V1 under-voltage reset level and Sleep mode availability can be selected. The datasheet and AH1506 provide more information on this subject.

3.3 FS45 feature overview

The FS4500 device is a System Basis Chip from the second generation of NXP Safety SBCs. It includes both power management for S32K1 and other MCUs as well as several functional safety mechanisms.

3.3.1 Functional safety features

An independent Safety Monitoring block includes all the necessary functions to achieve ISO26262 safety level C or D of the system. The FS4500 safety concept is based on four safety main functions. The output voltages of the System Basis Chip are monitored for over voltage and under voltage. Reaction on such a severe event is configurable for each voltage rail.

The second safety function is the watchdog functionality. For the FS4500 it is a window challenger watchdog, means the MCU requests a question from the MCU and must send the correct answer back to the SBC in the open watchdog window.

In addition, the System Basis Chip has dedicated pairs of input, where the MCU or another IC can signalize a fault condition to the SBC. If the MCU is not able to handle the fault, the System Basis Chip brings the system to the safe state.

The last main functional safety feature are the fail-safe outputs for transition of the system in case of a fault. Latent faults in the Fail-safe state machine are covered by LBIST and ABIST after each wake-up from LPOFF mode.

3.3.2 Voltage regulators

The power management block of the FS4500 consist of a pre-regulator delivering a coarse regulated output voltage of 6.5 V out of the battery voltage. This pre-regulator can be configured as a simple buck regulator or as a buck-boost regulator. In latter configuration, the device supports the deep cranking pulse with minimum 3.2 V. The output of the pre-regulator serves as input for four linear post regulators. The first one is the Vcore regulator, normally used as VDD supply for the Microcontroller. Its output voltage is adjustable in the range of 0.8 V to 5.0 V with an output current of maximum 500 mA. A second regulator, Vcca, can deliver 3.3 V or 5.0 V with up to 100 mA. This output current can be extended to 300 mA by means of an external pnp transistor. The Vcca regulator can be used reference voltage for the A-to-D converter of the MCU because it has a tolerance of +/- 1 %. The third integrated LDO is the Vaux regulator, also configurable for an output voltage of 3.3 V or 5 V and a maximum output current of 400 mA. This regulator can also be configured as a tracking regulator, tracking the Vcca voltage. This feature and the short-circuit-to-battery and short-circuit-to-ground protection makes it ideal for supplying external sensors and loads, even it can also be used for loads on the board. The last LDO is intended for supplying the internal CAN transceiver, therefore the output voltage is fixed to 5.0 V and the current capability is maximum 100 mA. If the internal CAN transceiver is not used, this regulator can also supply other communication transceivers or loads. It is worth to mention that additional external voltage regulators can be attached to the Vpre as long as the current capability of this regulator is considered.

3.3.3 Voltage supervision

The following voltage rails are monitored for a monitored for an over voltage and under voltage event:

- Vcore
- Vcca
- Vaux

In case of such an event different fault reactions can be caused:

- event asserts both RSTB and FS0B
- event asserts FS0B only
- event asserts RSTB only
- event has no impact on RSTB nor FS0B

These different fault reactions are configurable according the system requirements by SPI for each rail and for over voltage and under voltage separately.

An overvoltage at Vpre causes an assertion of both RSTB and FS0B.

3.3.4 Watchdog

A windowed watchdog is implemented in the FS6500/FS4500 and is based on ’question/answer’ principle (challenger). The watchdog must be continuously triggered by the MCU in the open watchdog window, otherwise an error is generated. The error handling and watchdog operations are managed by the fail-safe state machine. For debugging purpose, this functionality can be inhibited by setting the right voltage on the DEBUG pin at start-up.The watchdog window duration is selectable through the SPI in the range from 1.0 ms to 1024 ms.

An 8-bit pseudo-random word is generated in the FS4500. The MCU retrieves the question word generated by the FS4500 by SPI and has to perform a pre-defined calculation. The result is sent through the SPI during the ’open’ watchdog window and verified by the FS4500. When the result is right, a new pseudo-random word is generated and the watchdog window is restarted. When the result is wrong, the watchdog error counter is incremented, the watchdog window is restarted, and the question word is not changed. Any access to the watchdog register during the ’closed’ watchdog window is considered a wrong watchdog refresh.

As soon as the watchdog error counter reaches its final value either one or both RSTB and FS0B pins are asserted. The final value and also RSTB and FS0B reaction can be programmed by SPI.

3.3.5 Fault indication

A safety critical error is indicated towards the system by assertion of the Fail Safe outputs FS0b and FS1b (depending on device version). Such an error can also reset the MCU by assertion of the RSTb output. For most of the critical faults the fault impact (assertion of the Fail Safe Outputs and / or the Reset output) can be configured by SPI.

The Fail Safe output FS0b is available in each version of the FS4500 SBC family and is the main Fail Safe output. Some versions of the family have a second Fail Safe output FS1b. This second output can be programmed for two different use cases. For the first one the FS1b is activated be a defined delay time after FS0b assertion. The delay time is configurable. The second variant is the assertion of FS1b at the same point in time as FS0b, but an automatic release after a configurable delay time.

3.3.6 Low power features

In the LPoff low power mode of the FS4500 all regulators are switched off, the typical current consumption is 32 µA only. The device can be woken-up from the LPoff mode by level change at the IOs, by CAN or LIN message (for device versions with integrated CAN transceiver respectively LIN transceiver). The possible wake-up sources are also configurable.

4 S32K1xx / SBC safety solutions

This chapter is intended to show application proposals based on S32K1xx family and NXP SBCs for different ISO26262 safety integrity levels.

The table below the following target metrics to each safety integrity goal as defined in the ISO26262 standard.

Table 5. Target metrics for safety integrity levels according to ISO26262

Targets/Results	ASIL B	ASIL C	ASIL D
Single Point Fault Metric	≥90%	≥97%	≥99%
Latent Fault Metric	≥60%	≥80%	≥90%
Probabilistic Metric for random Hardware Failures (MCU)	$\leq 10^{-8}$ /h	$\leq 10^{-8}$ /h	$\leq 10^{-9}$ /h

Table below summarized the different solutions for ASIL safety integrity levels It should be noted that in accordance to ISO26262 part five each device represent a safety element out of context and final safety integrity level for a defined safety function has to be proven by system supplier on system level.

Table 6. S32K1xx and SBC combinations for ISO26262 ASIL safety applications

System ISO26262Level	MCU 1	MCU1 ISO26262 Level	MCU 2	MCU2 ISO26262 Level	SBC	SBC ISO26262 Level	Max Current [A]
B	S32K1xx	B	not needed	NA	UJA1169	QM (incl. functional safety features)	0.25

Table continues on the next page...

Table 6. S32K1xx and SBC combinations for ISO26262 ASIL safety applications (continued)

System ISO26262Level	MCU 1	MCU1 ISO26262 Level	MCU 2	MCU2 ISO26262 Level	SBC	SBC ISO26262 Level	Max Current [A]
					UJA113x	QM (incl. functional safety features)	0.7
					FS45	D	1.5
C	S32K1xx	B	S32K1xx	B	FS45	D	1.5
			KEAxx	QM			
D	S32K1xx	B	S32K1xx	B	FS45	D	1.5

4.1 S32K1xx and SBC solutions for ISO26262 ASIL-B Safety applications

4.1.1 S32K1xx and UJA1169

Typical application that integrates the S32K1xx and UJA1169 is shown in the figure below. The UJA1169 devices provide power generation and voltage monitoring to the MCU and external watchdog supervision to detect failures of the MCU. The also monitors the error signal coming from the MCU and provide fail-safe mechanisms to maintain the system in a safe state, in case a failure occurs. The Limp output is a connection that could be used to signal emergency state depending on the SBC configuration to either the uC itself or an intendant HW Block or backup MCU. With the described features in the application note the support ASIL B on system level, depending on the safety goals in the application.

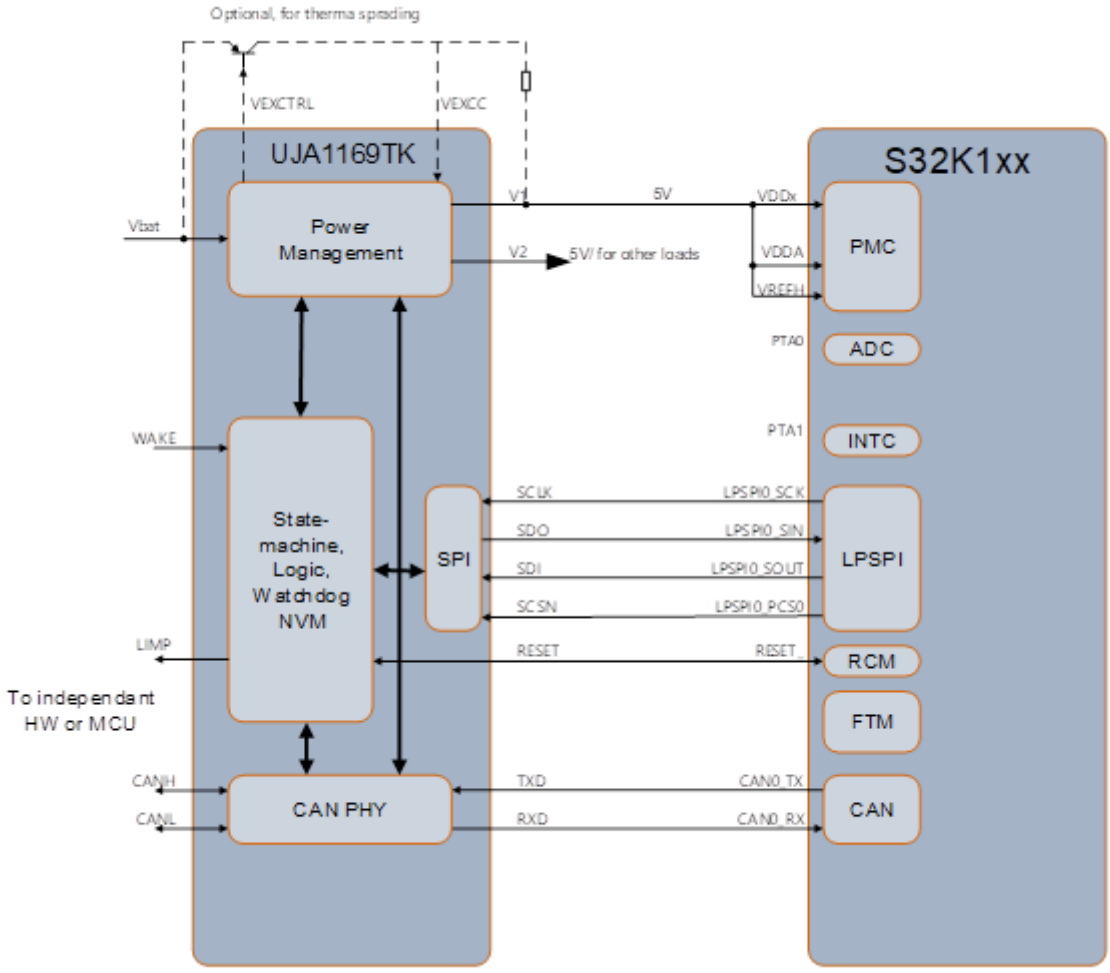

Figure 8. S32K1xx and UJA1169 typical application diagram

4.1.2 ASIL-B: S32K1xx and UJA1132x

A typical application that integrates the S32K1xx and UJA1131 is shown in the figure below. The UJA1131 devices provide power generation and voltage monitoring to the MCU and external watchdog supervision to detect failures of the MCU. The SBC to uC HW connection is not strictly depending on ASIL level but the features described in the application note might allow to fullfill ASIL-B requirements on system level.

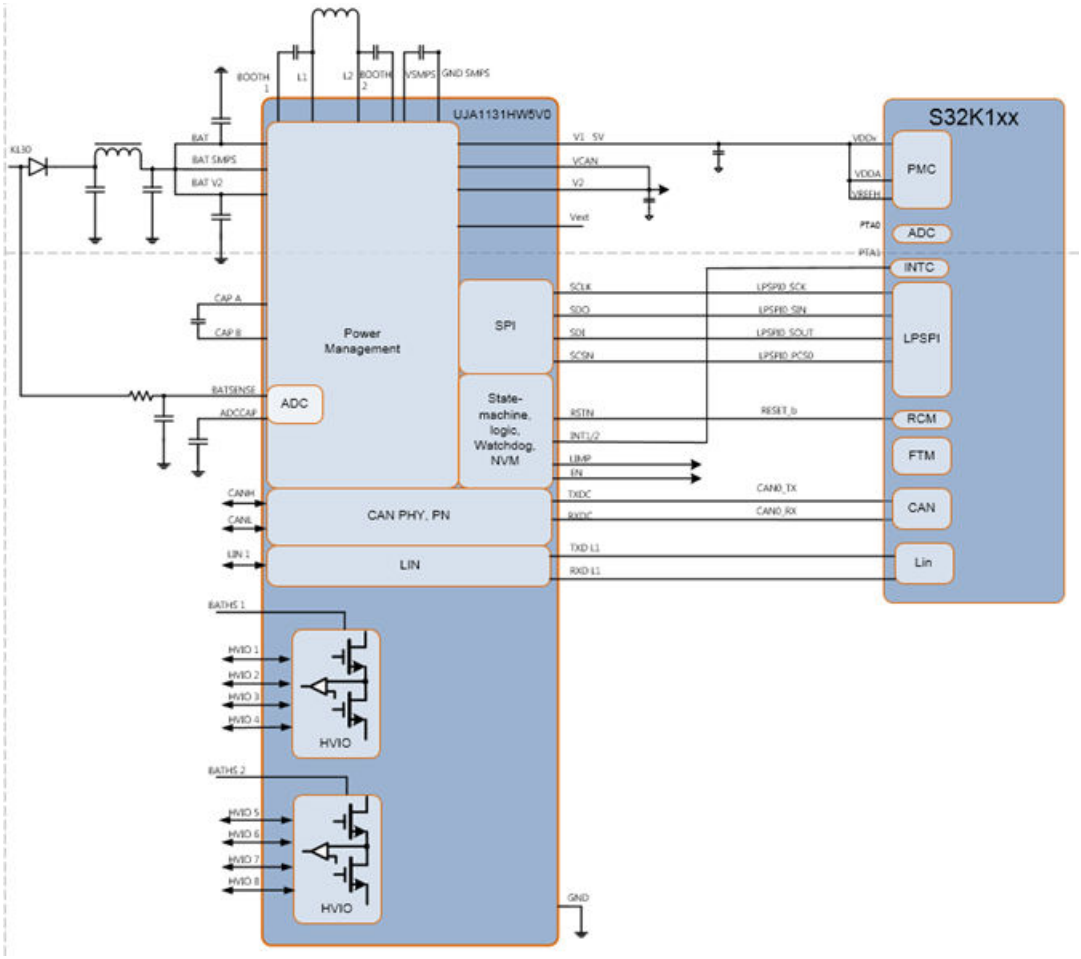

Figure 9. S32K1xx and UJA1131 typical application diagram

4.1.3 S32K1xx and FS45 SBC

Typical ASIL-B application that integrates the S32K1xx and FS45 is shown in the figure below. The FS45 devices provide power generation and voltage monitoring to the MCU and external watchdog supervision to detect failures of the MCU. The also monitors the error signal coming from the MCU and provide fail-safe mechanisms to maintain the system in a safe state, in case a failure occurs.

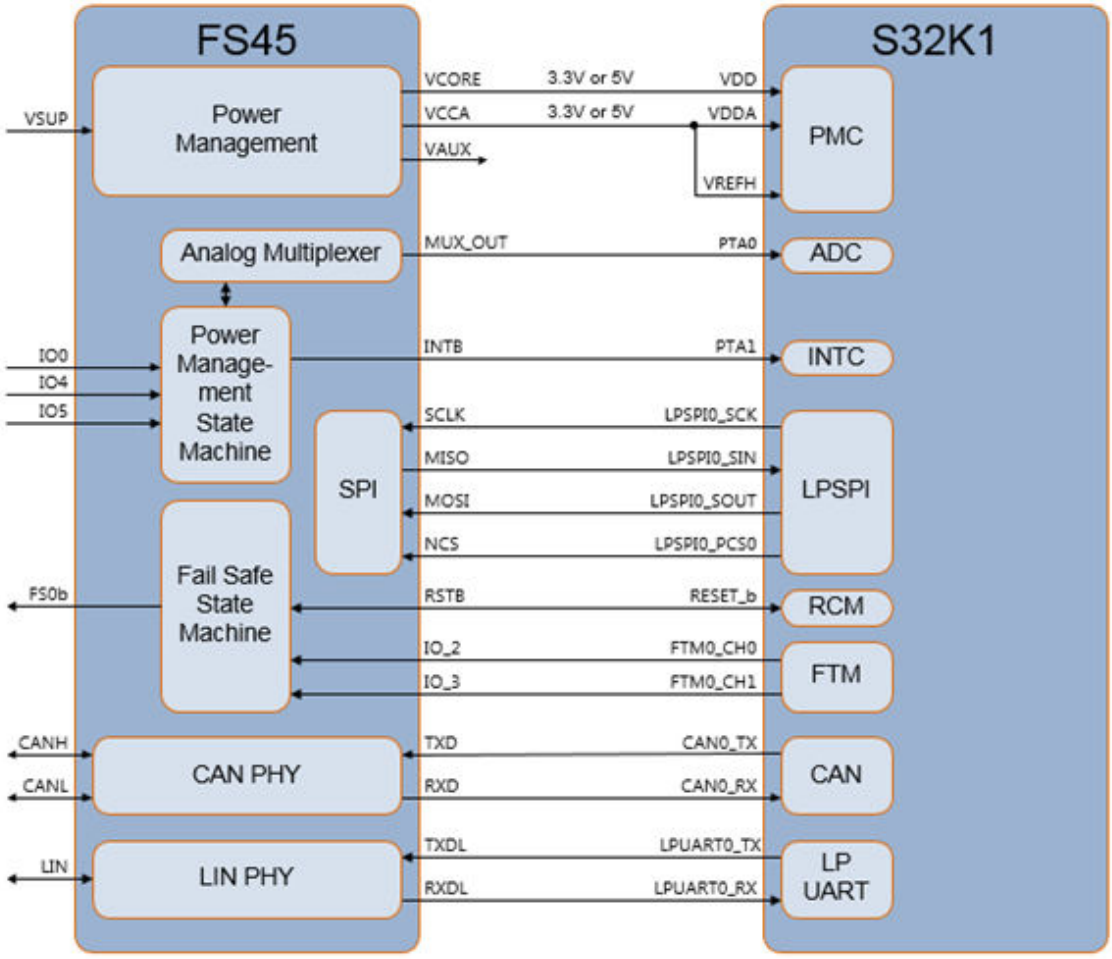

Figure 10. S32K1xx and FS45 typical application for ASIL-B

4.2 S32K1xx and SBC solutions for ISO26262 ASIL-C/D Safety applications

According to ISO26262 decomposition it is possible to achieve ASIL-C/D safety integrity level for certain safety function using two independent elements. According to ISO26262 the two components have to be independent - each must address the same safety goal and take the same safety state. The two components are used to achieve functional redundancy by using different design elements.

For ASIL-C/D safety functions one possible approach would be the use of ASIL-D SBC FS45 and 2x S32K1xx devices developed for ASIL-B applications. Typical application for this use case is shown in the below figure. The FS45 devices provide power generation and voltage monitoring for both MCUs. SBC and both MCUs are connected to the same bidirectional RESET line. Each MCU is using one FTM Timer output to monitor to the SBC a safety critical error leading to entering a fail safe state.

MCU1 is generating the watchdog SPI message to the SBC while MCU2 is reading the messages via an SPI based on different HW unit called FlexIO to ensure the correct and regular order of watchdog triggering events. MCU1 could also use this interface to send information to MCU2 and use another UART interface to provide send and receive safety critical system messages. An implementation of an SPI link to an external component utilized to achieve the safety function comprises LPURT link which is

used to send commands from MCU1 to MCU2. This commands are transferred to SPI and send to external component. MCU1 is also operating as a slave on this SPI interface and is able to check whether corresponding massages correlate to the one sent on the UART link.

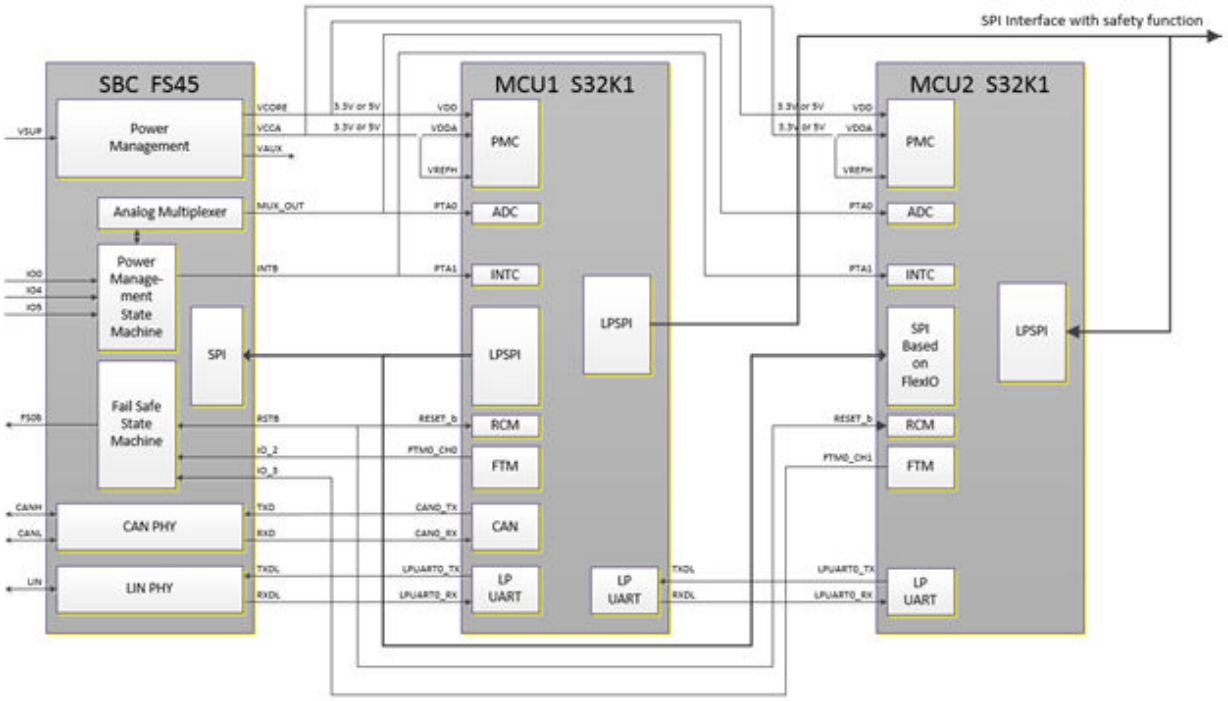

Figure 11. S32K1xx and FS45 typical application diagram for ASIL-C/D applications

5 Software support

5.1 S32 DS & SDK

UJA113x/UJA1169 software support - The source code for UJA113x/UJA1169 is available as part of the S32 SDK and can be obtained by downloading the S32 Design Studio provided by NXP free of charge. The libraries are developed following automotive standards and come with a quality package.The SDK delivery also contains ready to use examples for SBC configuration and communication when application is running.

UJA113x software package - The source code provides a set of low level functions allowing the user to quickly configure/evaluate the device. However, it doesn't contain any complex logic. As functionality may differ from application to application it's not possible to cover all use cases while keeping the code footprint small. Thus, required logic needs to be provided by the user. A set of examples demonstrating the use of library is included.For details, see the UJA113x documentation which is part of UJA1169 software package.

Porting to different platform - Although libraries are coupled to S32 SDK, it's easy to port them to another platform. The libraries rely on SPI communication only. Reimplementing the SPI interface by the user according to his needs without the need to change anything else in the library should be sufficient.

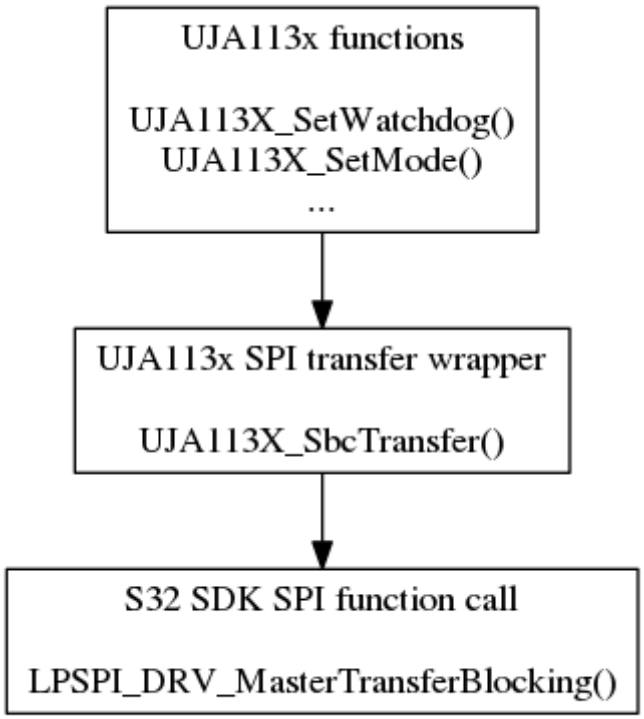

Figure 12. UJA113x layered architecture

FS45 software support : The FS45 driver source code provides a set of low level functions allowing the user to quickly configure/evaluate the FS45 device. The driver covers following functionality: SBC initialization, FSxb pins release, watchdog settings and refresh, register R/W with runtime register map, CAN/LIN settings, regulator outputs settings.A set of examples demonstrating the use of library is included into S32K1xx based Battery Management Reference Design. For details, see the FS45 documentation and NXP BMS reference design website.

6 Resources for safety applications

Table below summarizes the material available for each device discussed in this application note.

Table 7. Available material for the devices

	SBC ASIL Level	HW Design Guide	Safety Manual	FMEDA	Software support
S32K1	ASIL-B	yes	yes	yes	Safe MCAL / S32DS SDK drivers
KEA	QM	yes	no	partly	Safe MCAL / S32DS SDK drivers
UJA1169	QM	yes	no	no	Safe MCAL / S32DS SDK drivers
UJA113x	QM	yes	no	no	Safe MCAL / S32DS SDK drivers
FS45	ASIL-D	yes	yes	yes	Safe MCAL / S32DS SDK drivers

6.1 S32K1xx safety collateral

S32K14x Series Safety Manual - This document discusses requirements for the integration and use of the S32K14x Microcontroller Unit (MCU) in safety-related systems. The document is available on nxp,com webpage.

FMEDA - The Failure Modes, Effects and Diagnostic Analysis (FMEDA) carried out for the S32K1xx family is available on request and provides the Single Point Faults Metric (SPFM), the Latent Fault Metric (LFM), the Safe Failure Fraction (SFF), the Single Point and Residual failure rate, the dangerous undetected failure rate, and the multiple point failure rates.

Application Notes - Please find below a list of useful application notes which could further help you in your safety development process:

- AN5426, Hardware Design Guidelines for S32K1xx Microcontrollers
- AN5425, Power Management for S32K14x
- More application notes for S32K1xx family are available on nxp.com

Safety MCAL

S32 Design Studio - The S32 Design Studio IDE is an integrated development environment for S32K1xx family that enables editing, compiling and debugging of designs.

It is based open-source software including Eclipse IDE, GNU Compiler Collection (GCC) and GNU Debugger (GDB) and has no code-size limitations.

S32 Design Studio is available free of charge on nxp.com webpage.

Software Development Kit (SDK) - Automotive-grade software development kit (SDK) offers MISRA and SPICE Level 3 compliant low-level drivers (LLDs) for all S32K1xx peripherals It Optional application-specific middleware for communication with SBCs, LIN, NFC and touch sensing applications.SDK source code is well documented and offers out-of-the-box examples which eliminate the need for device documentation during application bring-up. The SDK is pre-installed in NXP's free S32 Design Studio (DS) and is available free of charge.

Evaluation Boards and Shield - S32K1xx evaluation boards are available for each derivative of S32k1xx family. The S32K1xx EVB is low cost evaluation platform and development system for quick application prototyping and demonstration for the S32Kxx. In addition to EVB NXP offers shields for m otor control, low power applications and touch sensing which can be used together with the evaluation board.

6.2 UJA11xx Collateral

The following collateral is available through Sales/Mktg:

- AH1306 UJA1169x HW application guide
- AH1403 Pin FMEA UJA113x
- AH1501 UJA113x SW appl note
- AH1502 UJA113x Application note HVIO
- AH1506 UJA113x Application Note
- AH1507 UJA113x Application Note CAN/Lin
- Thermal Calculators

For Standalone SBC Boards please contact Sales /FAE/ Mktg.

How To Reach Us

Home Page:

nxp.com

Web Support:

nxp.com/support

Information in this document is provided solely to enable system and software implementers to use NXP products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits based on the information in this document. NXP reserves the right to make changes without further notice to any products herein.

NXP makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does NXP assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters that may be provided in NXP data sheets and/or specifications can and do vary in different applications, and actual performance may vary over time. All operating parameters, including “typicals,” must be validated for each customer application by customer's technical experts. NXP does not convey any license under its patent rights nor the rights of others. NXP sells products pursuant to standard terms and conditions of sale, which can be found at the following address: nxp.com/SalesTermsandConditions.

While NXP has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer’s applications and products, and NXP accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP, the NXP logo, NXP SECURE CONNECTIONS FOR A SMARTER WORLD, COOLFLUX, EMBRACE, GREENCHIP, HITAG, I2C BUS, ICODE, JCOP, LIFE VIBES, MIFARE, MIFARE CLASSIC, MIFARE DESFire, MIFARE PLUS, MIFARE FLEX, MANTIS, MIFARE ULTRALIGHT, MIFARE4MOBILE, MIGLO, NTAG, ROADLINK, SMARTLX, SMARTMX, STARPLUG, TOPFET, TRENCHMOS, UCODE, Freescale, the Freescale logo, AltiVec, C-5, CodeTEST, CodeWarrior, ColdFire, ColdFire+, C-Ware, the Energy Efficient Solutions logo, Kinetis, Layerscape, MagniV, mobileGT, PEG, PowerQUICC, Processor Expert, QorIQ, QorIQ Qonverge, Ready Play, SafeAssure, the SafeAssure logo, StarCore, Symphony, VortiQa, Vybrid, Airfast, BeeKit, BeeStack, CoreNet, Flexis, MXC, Platform in a Package, QUICC Engine, SMARTMOS, Tower, TurboLink, and UMEMS are trademarks of NXP B.V. All other product or service names are the property of their respective owners. AMBA, Arm, Arm7, Arm7TDMI, Arm9, Arm11, Artisan, big.LITTLE, Cordio, CoreLink, CoreSight, Cortex, DesignStart, DynamIQ, Jazelle, Keil, Mali, Mbed, Mbed Enabled, NEON, POP, RealView, SecurCore, Socrates, Thumb, TrustZone, ULINK, ULINK2, ULINK-ME, ULINK-PLUS, ULINKpro, µVision, Versatile are trademarks or registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. The related technology may be protected by any or all of patents, copyrights, designs and trade secrets. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. The Power Architecture and Power.org word marks and the Power and Power.org logos and related marks are trademarks and service marks licensed by Power.org.

© NXP B.V. 2018. **All rights reserved.**

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: November 2018
Document identifier: AN12148

arm