Improving Gas Valve Safety Compliance with GreenPAK

Author: Mujammil Ali A S

Date: November 26, 2016

Introduction

Programmable Electronic based controls typically incorporate capability to accomplish safety functions. In the EU for example, compliance to IEC 60730 and IEC 61508 functional safety standards are mandatory. It even covers possible hazards caused by the malfunction of the safety mechanism itself.

Though many MCUs in the market have class B category software mandated by IEC 60730 (to monitor failure of the MCU), there is a need for some use cases to have a double check mechanism for more reliablility.

For instance, consider the opening and closing operation of the gas valve actuator in a boiler. If the MCU controlling it fails, things could be catastrophic.

This App note demonstrates the capability of the SLG46531V to safely drive five output pins on which critical actuators are connected. The SLG46531V monitors a "heartbeat" signal to decide the stability of the MCU.

The MCU sends commands via I2C to switch ON/OFF the output pins.

These Outputs run only during a stable state, and the actuator will always be OFF in any other state.

The advantages of employing this double check mechanism over class B software-only routine running in MCU are as follows:

- The software can crash due to coding oversights in the initial design phase, or software update phase (When adding the new device driver for a new component or existing component in this case).

- Re-certification is required for each software update (in the hardware layer). In contrast, this certification is needed only once if this critical actuator is interfaced directly by an ASIC.

- Though some MCU manufacturers provide digital IO peripheral test as recommended by Annex H of the IEC 60730-1 standard, the end application of a particular digital IO is usually customized, and then differs behaviorally compared to testing time.

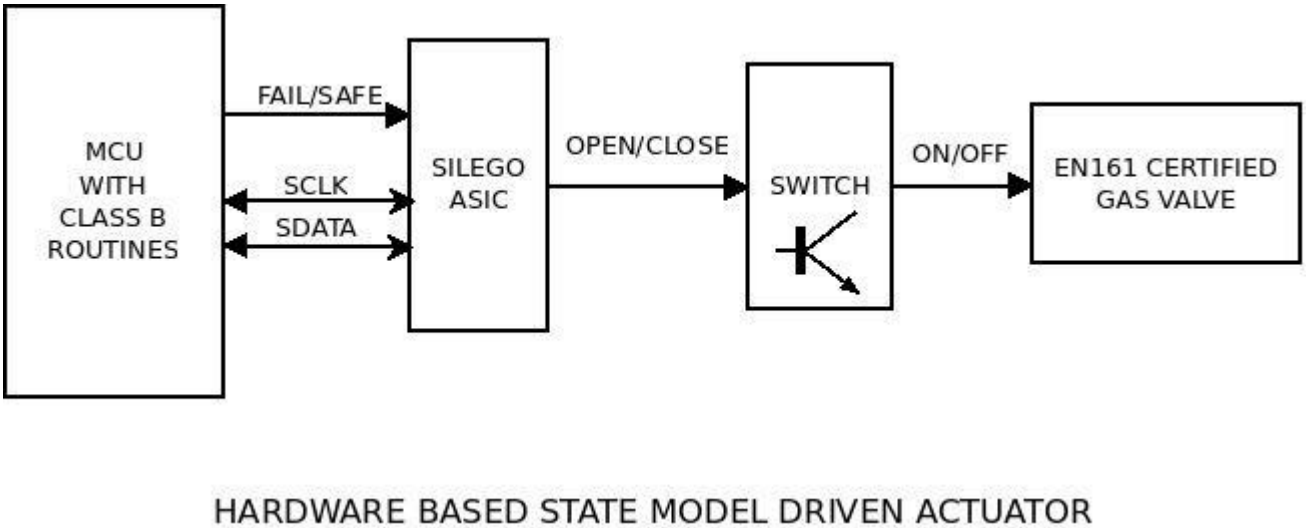

Figure 1. Typical Application

Application

In this system, the MCU and the Gas valve driving circuit are isolated by a GreenPAK.

The MCU sends a command to switch ON/OFF the particular IO pin through I2C commands. MCU runs class B self-test periodically to check its stable condition and sends a pulse of frequency (heartbeat signal) less than 23mSec. If Self-test is not OK, MCU stops sending the heartbeat signal.

GreenPAK monitors the heartbeat signal for any unexpected behavior such as no signal or fluctuating signal, and if detected it switches OFF all the output pins. It obeys the I2C command and the output pins allow an OK state only when GreenPAK receives good and stable heartbeat signal. All these operations are driven by the hardware-based ASM (asynchronous state machine) in GreenPAK.

Auto Lockout Output Driver with safe Reset

This ASM design drives all five output pins based on the stability indication of MCU. It utilizes four states to accomplish the task. Five ASM RAM bits are connected to D0_OUT, D1_OUT, D2_OUT, D3_OUT, and D4_OUT pins to out the commanded value corresponding to STABLE_OUT state by I2C. Upon start, ASM enters into STARTUP state in which it monitors for the steady pulse with the time period less than 23mSec.

When there is a good healthy pulse, it triggers the STABLE_LATCH state and then toggles between STABLE_LATCH and STABLE_OUT state. This toggling is necessary to reflect the internal ASM RAM table changes made by I2C command to the register address D1.

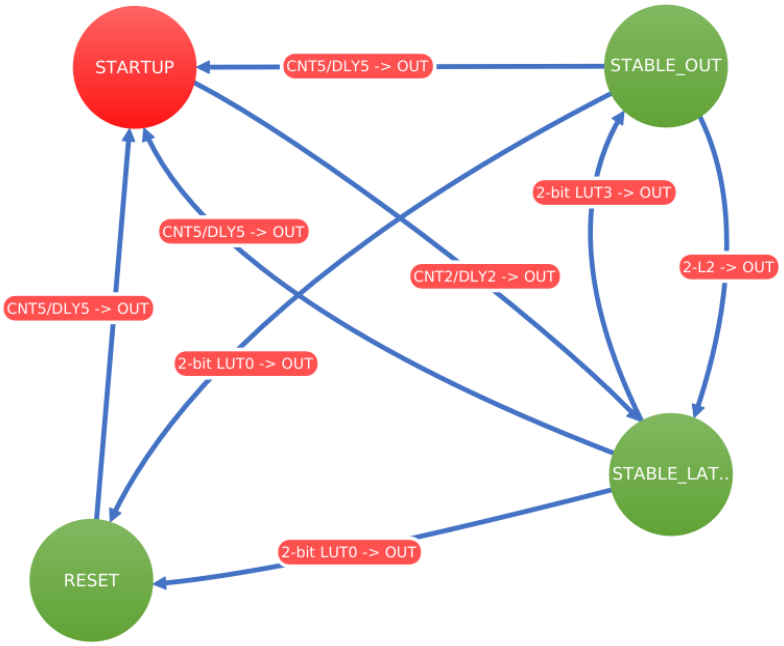

Figure 2. ASM State Machine

This Register is the only one among all that shall be modified by I2C command. All five output pins are latched using DFF3, DFF4 to DFF7 in STABLE_OUT and blocked in STABLE_LATCH state.

Once the ASM identifies about non-stability indication either by not receiving the pulse or fluctuation in pulse, it triggers the RESET state in which all output pins are OFF.

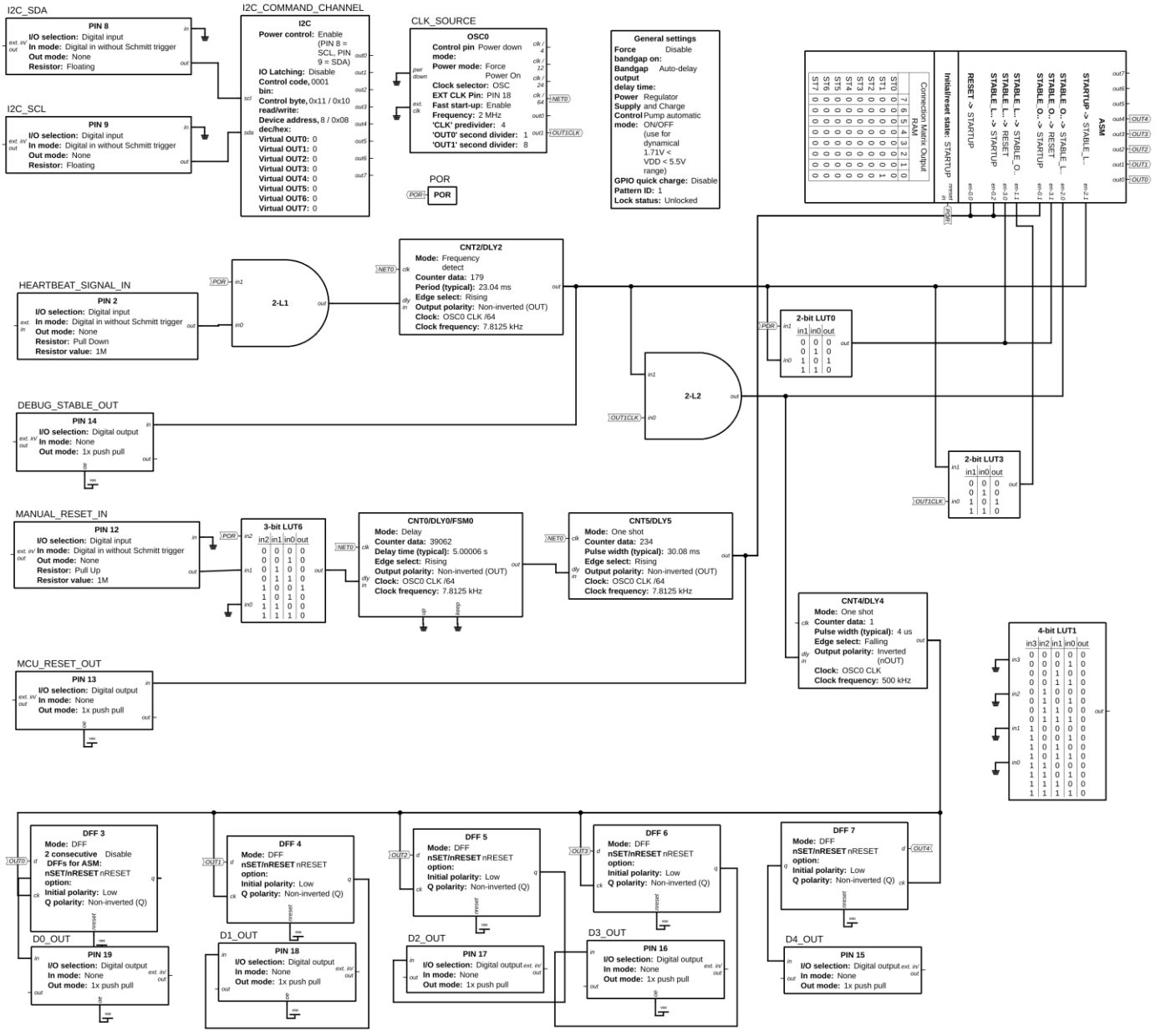

Figure 3. GreenPAK Schematic Overview

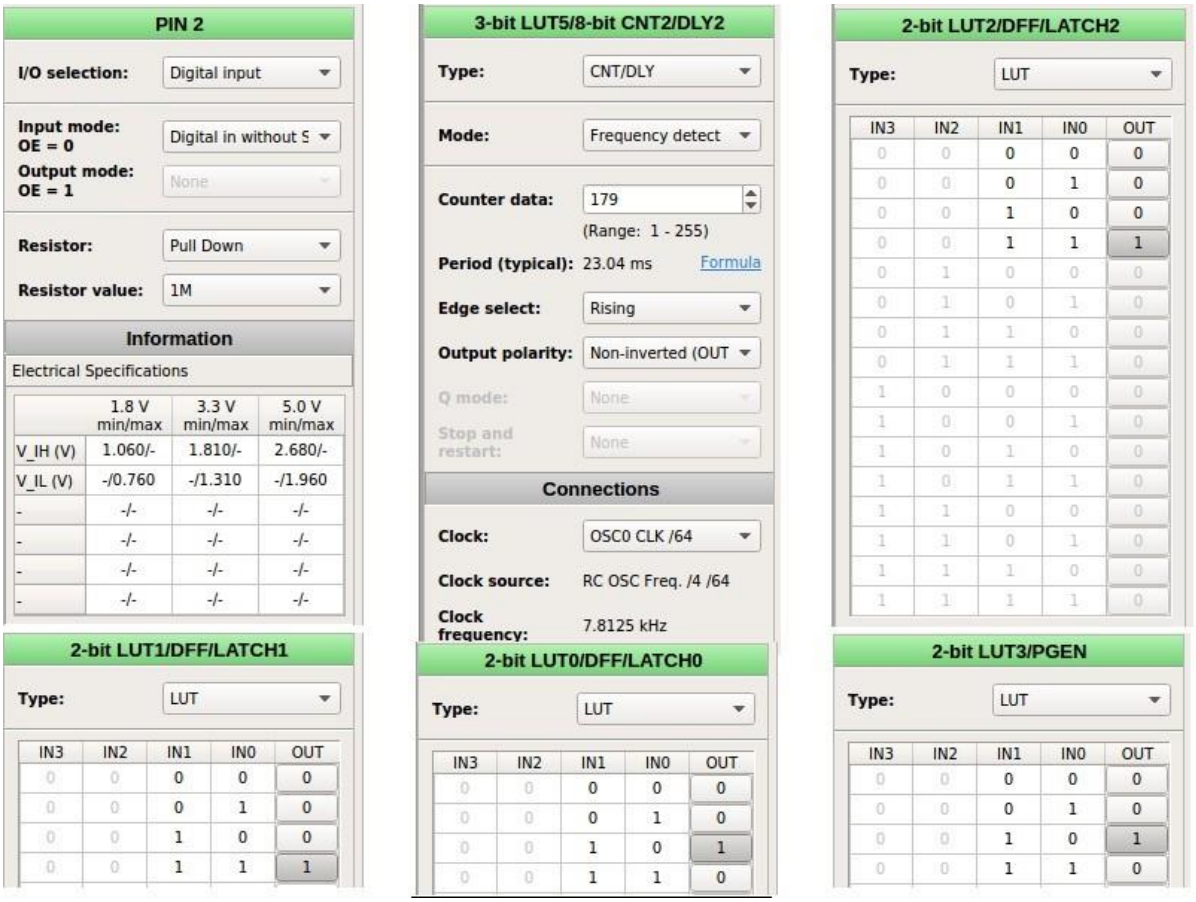

Figure 4. Configuration of Heartbeat signal monitoring circuit

It never returns to the (STARTUP) normal state until the manual reset operation is carried out by passing LOW signal (by pressing the manual reset button) to MANUAL_RESET_IN pin. The manual reset operation is functional as well in all states, and will immediately force the STARTUP state when enabled.

Heartbeat Signal Monitor

Stability of the heartbeat signal of MCU is inferred by measuring the period of the signal at PIN2 which is less than 23mSec. CNT2/DLY2 block is configured in frequency mode with rising edge.

The Counter value is set as 179 to capture the signal with the period of 23mSec or less.

The Output of this block is active high when the time period is less than or equal to the said period. It is then complemented with the help of programmed LUT0 block as a NOT gate, acting as a transition signal for RESET state.

The direct non-inverted output is carried to 2-L2 and LUT3 block which is responsible for creating toggling transition signal with the help of clock from STABLE_LATCH to STABLE_OUT and vice versa.

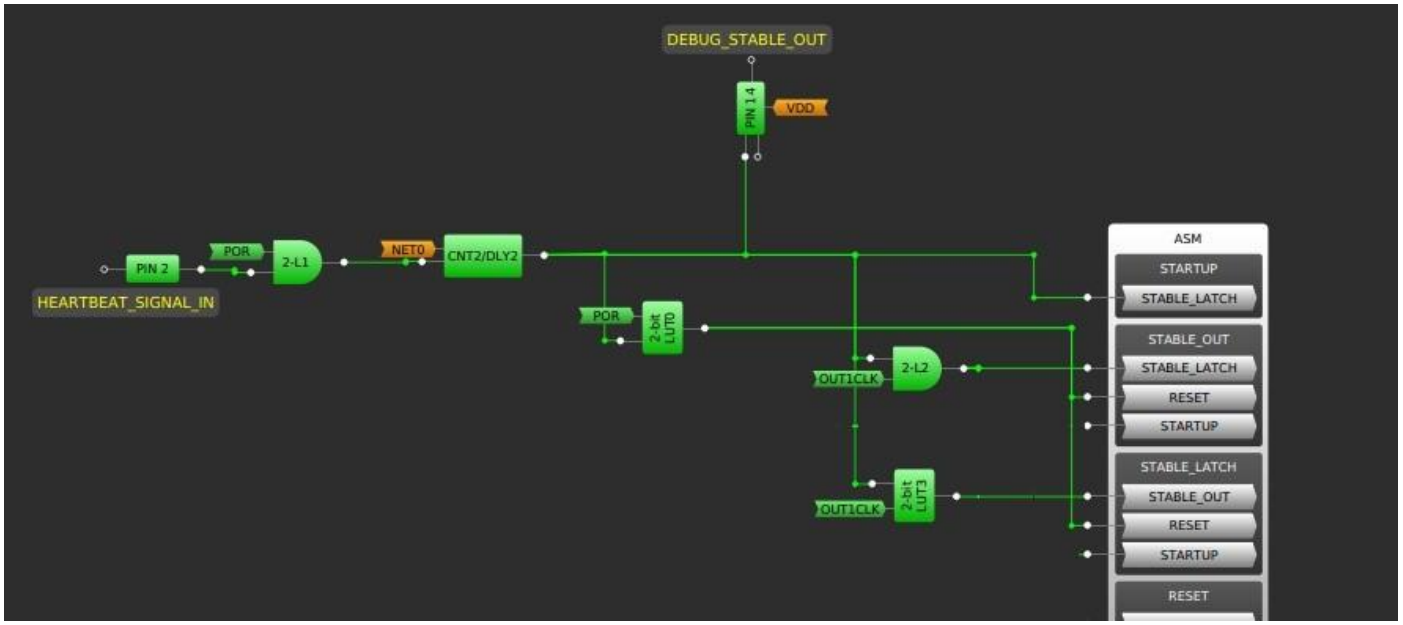

Figure 5. Heartbeat signal monitoring circuit

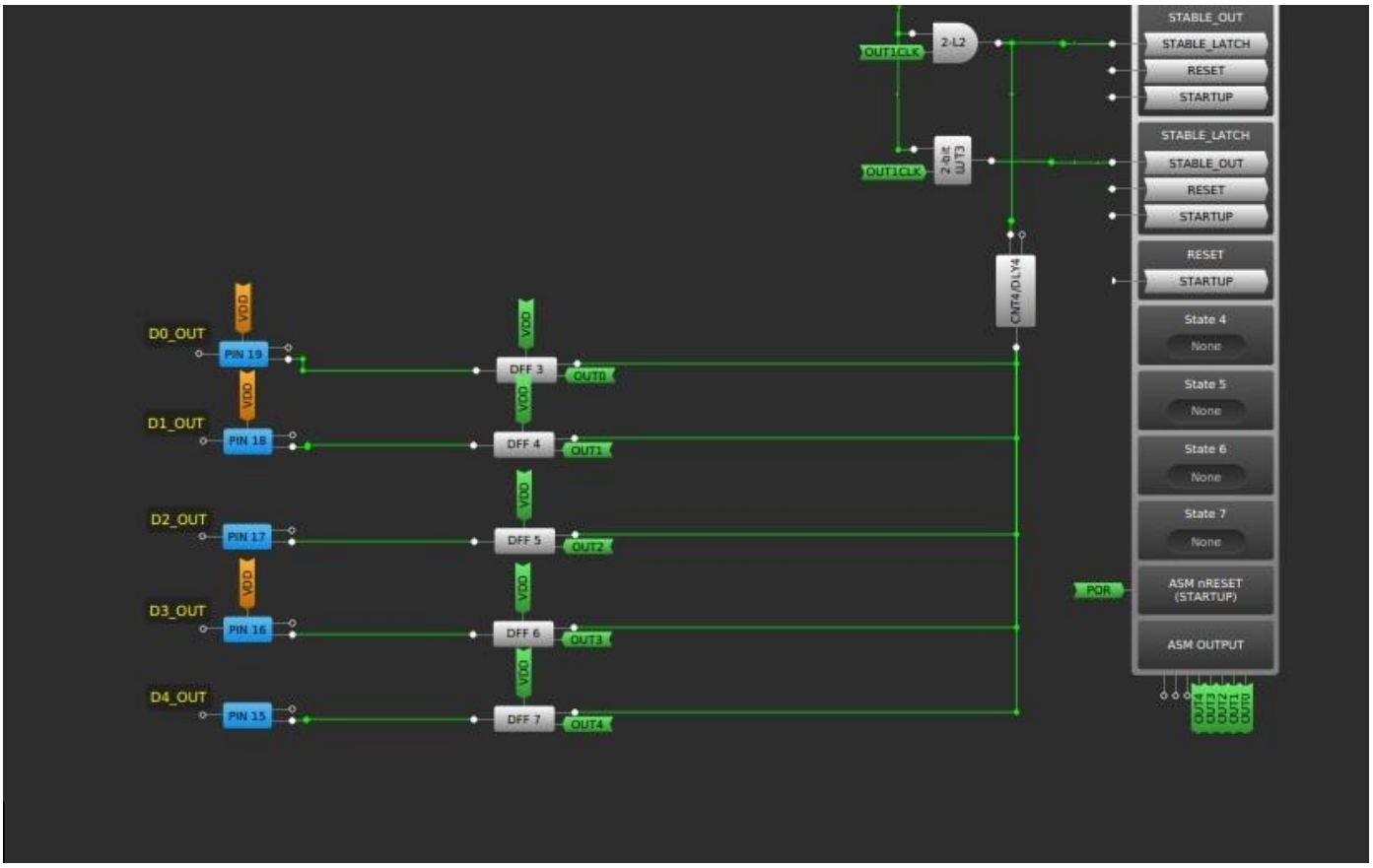

Figure 6. Output Latch

Extended IO Peripheral with Lockout using ASM

PIN15 to PIN19 are connected with Connection Matrix Output RAM of ASM using DFF7 to DFF3 respectively. Each DFF latches the data during STABLE_OUT state by the one-shot inverted pulse signal generated from CNT/DLY4. This CNT/DLY4 is configured as one-shot generator upon reception of falling edge from 2-L2.

Safe Manual Reset

In case an unstable condition arises due to no heartbeat or fluctuating pulse, GreenPAK shuts down the five output pins by making all the corresponding pins as LOW, and requires manual reset to unlock the Output interface and safe reset.

PIN12 is connected to pull down button and looks for pressing the button for more than or equal to 5 Seconds. CNT0/DLY0/FSM0 is configured in delay mode with detection of rising edge for 5 sec. Once the button is pressed, as the Pin is in pull-up mode and LUT6 is in inverted logic, the pin receives low to high transition. If the signal is at the high level for 5 seconds, it triggers the CNT5/DLY5 block that in turn activates the single pulse with a width of 30mSec. This Single pulse is used as a transition signal for STARTUP and routed to MCU through output pin 13.

Monitoring of Stable heartbeat signal at system startup

At System Startup, the heartbeat signal is received as if from the MCU which is emulated using GreenPAK Designer.

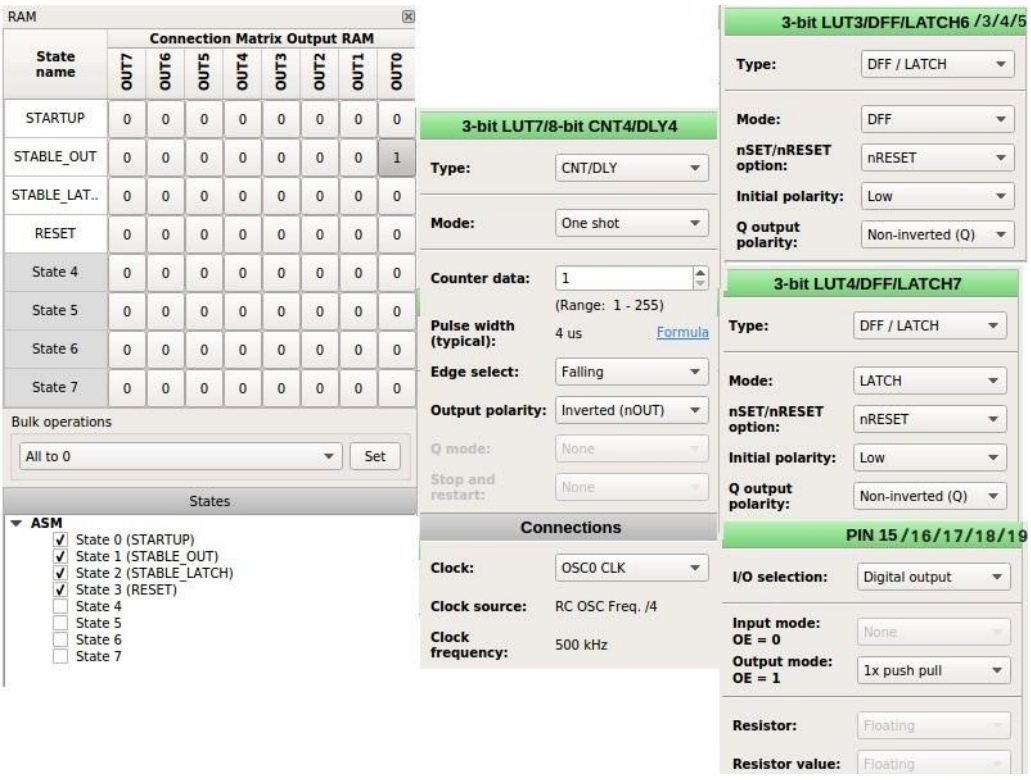

Figure 7. Output Pin and ASM Configuration

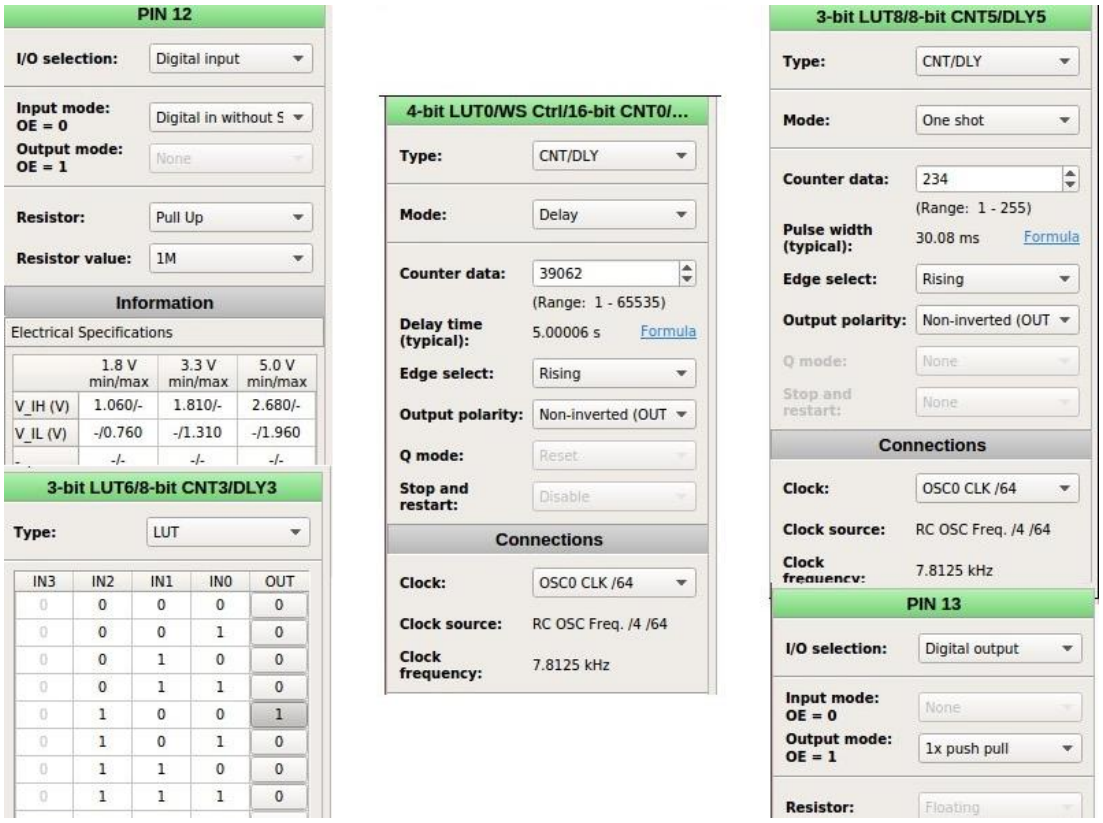

Figure 8. Manual Reset Circuit Configuration

SCL and SDA signals are for the I2C channel. HEARTBEAT_SIGNAL is a pulse signal that is stable upon start up. D0_OUT to D4_OUT refers to the output driver pins among which D0_OUT is ON. This ON status is due to the initial value present in the ASM output RAM matrix table.

The emulator is configured as follows: TP2 is acting as a signal generator that is used for creating stable and unstable heartbeat signal. TP15, TP16, TP17, TP18, and TP19 are used as output ON/OFF interface.

This design supports five output drivers. TP12 is set as pull down button.

TP13 is the one-shot reset signal for MCU, and unlocks the ASM.

I2C based Control of Output Interface

The Output matrix of ASM RAM table with address 0xD1 holds the value of all five output drivers from the 0th bit to 5th bit in this byte. I2C command to switch on all output pins is [0x08 0xD1 0x1F]. D0_OUT to D4_OUT are switched ON after the I2C command is received. [Device Address: 0x08 Register Address: 0xD1 Value: 0x1F].

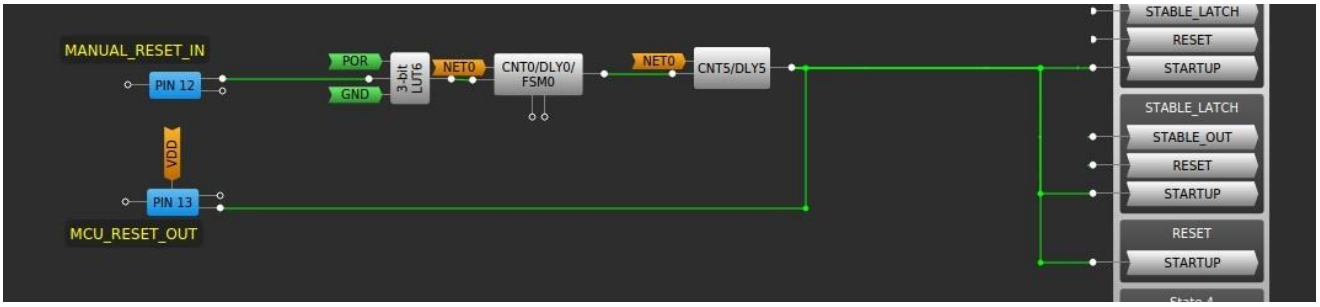

Figure 9. Manual Safe Reset

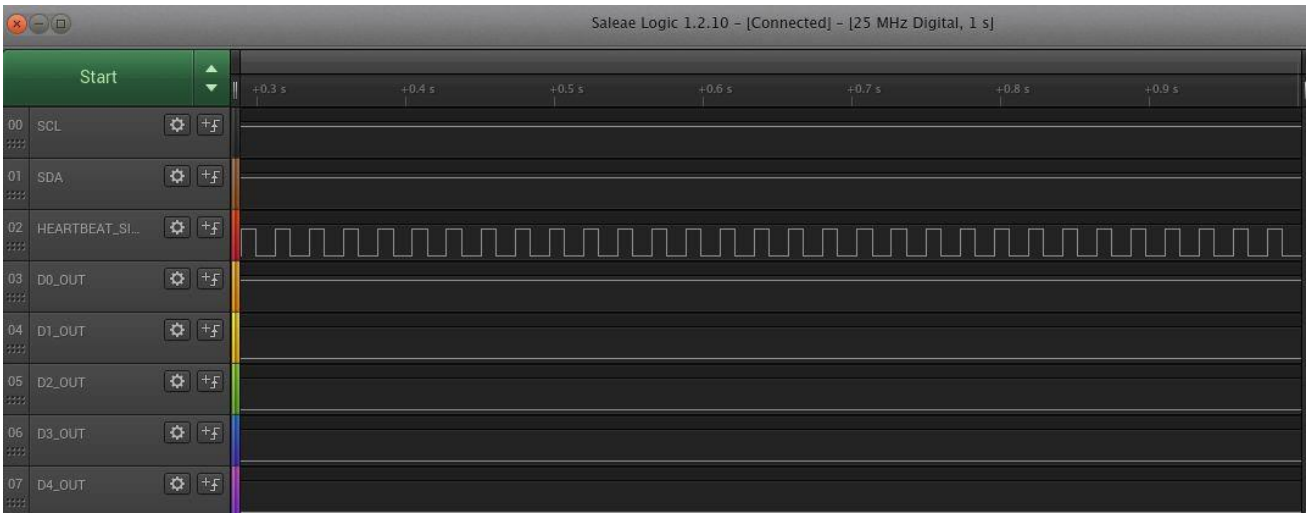

Figure 10. Waveform of Heartbeat and output signal at system startup

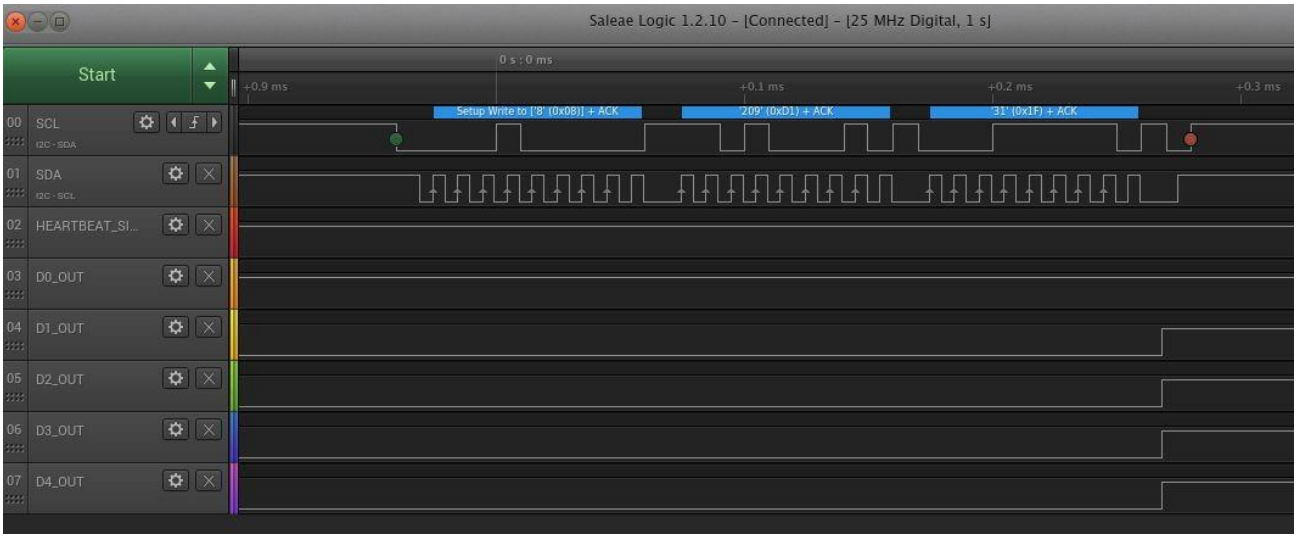

Figure 11. Controlling Output pins D0 to D4 via I2C

Auto Lockout

All Output pins are automatically switched to the OFF state when either there is no heartbeat signal or varying unstable heartbeat signal from MCU. The Following Figure 12.A shows that D0_OUT to D4_OUT are switched OFF when MCU stops sending the heartbeat signal.

It is understood that when there is a fluctuation in heartbeat signal (in Figure 12.B) shown by DEBUG_STABLE_OUT pin, ASM locks into RESET state upon first detection itself. DEBUG_STABLE_OUT is the output of frequency detection unit.

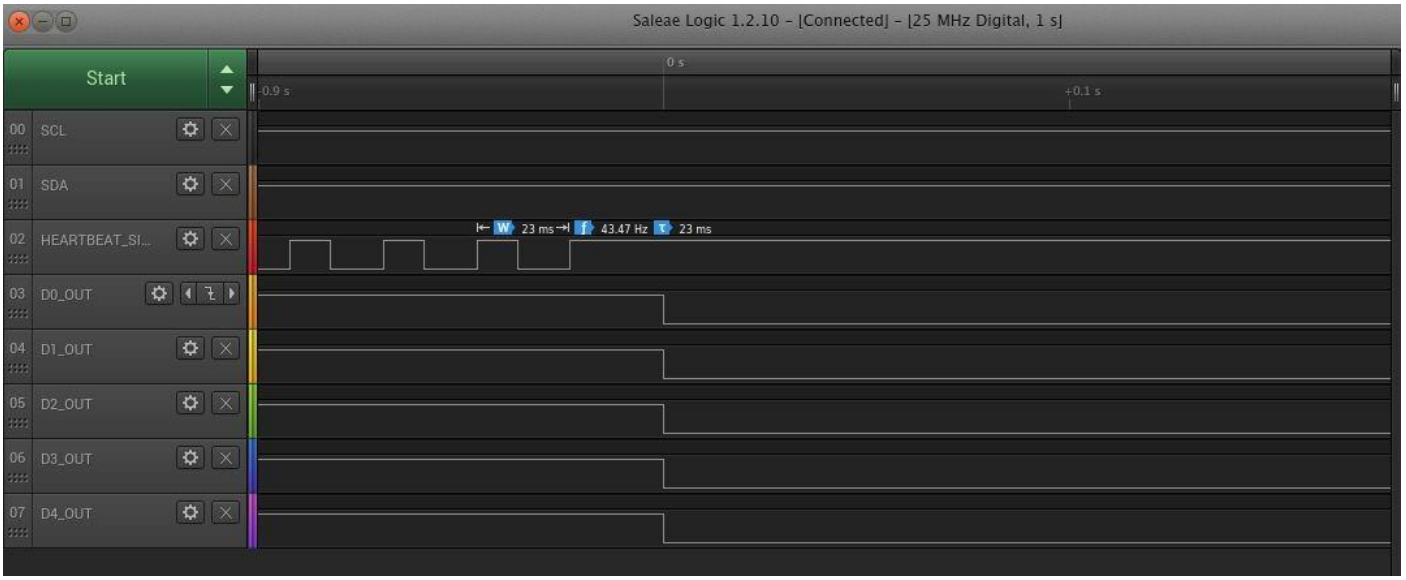

Figure 12(a). Auto lockout of Output pins when no or fluctuating heartbeat signal (No Signal)

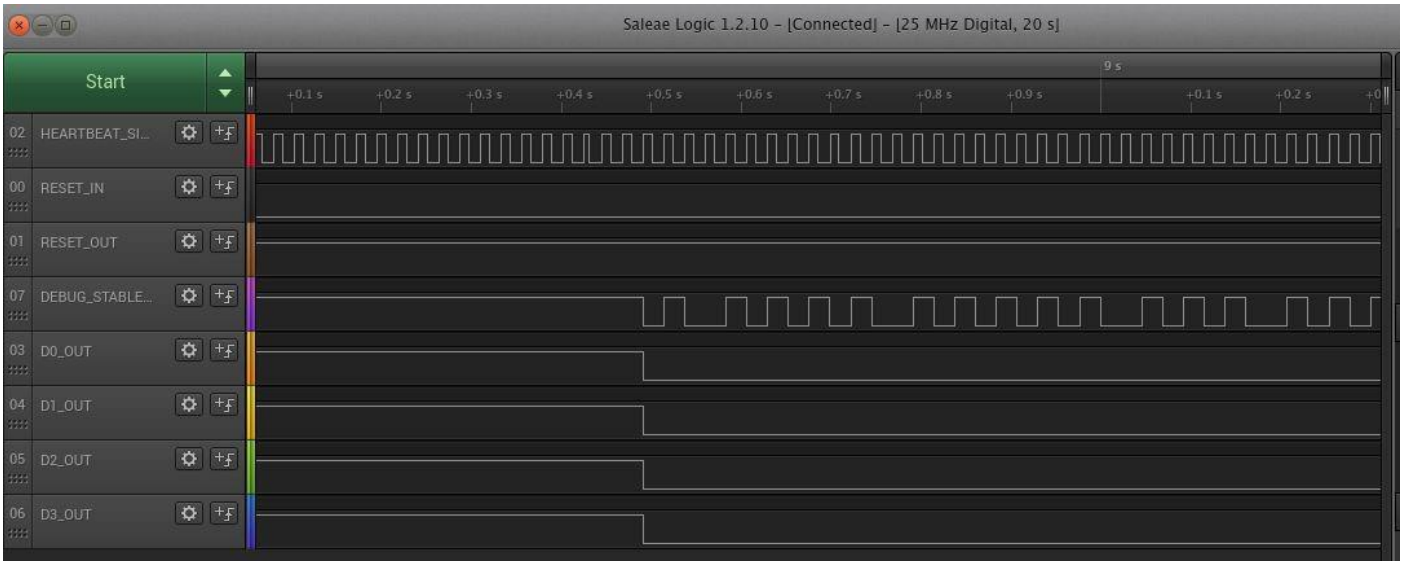

Figure 12(b). Fluctuating Signal

Unlocking the System safely using Manual Reset

Once the ASM is in RESET state, it requires manual reset by pressing the button connected in pull-down mode. RESET_OUT is the signal in the waveform that is generated by the switch; RESET_IN is the signal name for the signal going to MCU reset pin.

Manual reset is the safe operation and avoids automatic triggering of output drivers. Figure 13.A shows that the reset is triggered by a one-shot pulse in RESET_IN signal when there is a button press for more than 5 Seconds, indicated by RESET_OUT under the availability of unstable heartbeat signal.

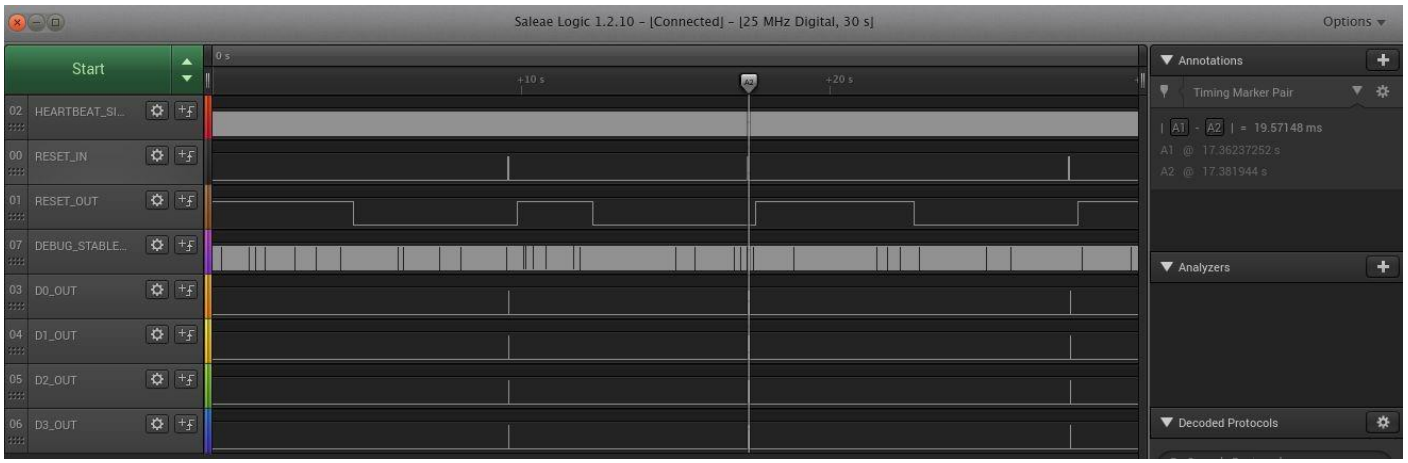

Figure 13(a). Manual Reset in case of unstable situation (During)

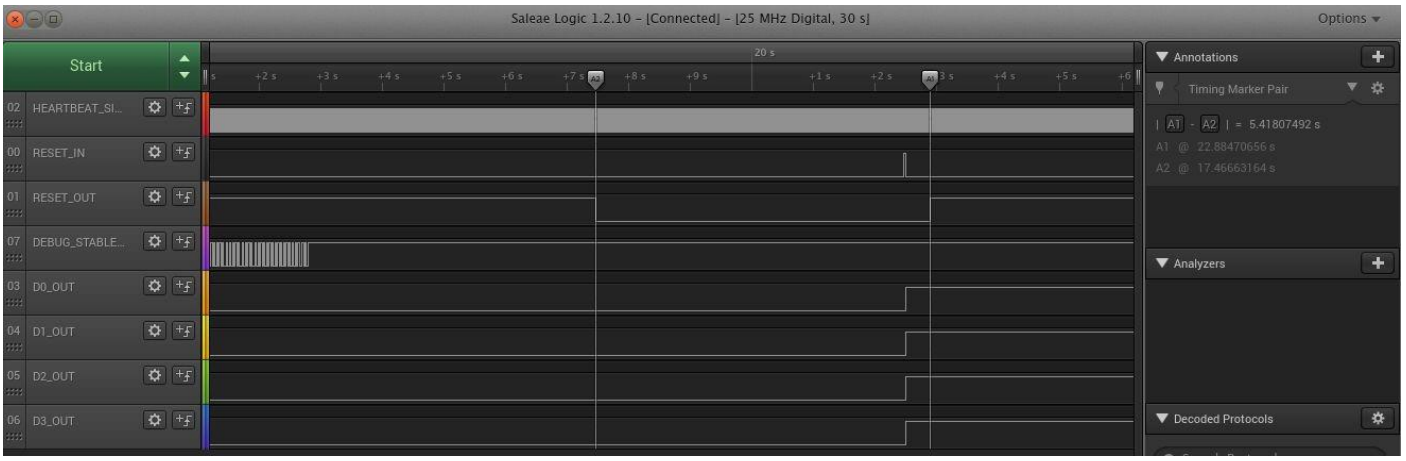

Figure 13(b). Manual Reset in case of unstable situation (After)

(D4_OUT waveform is not shown but it was expressly tested).

Figure 13.B shows the manual reset operation after receiving the stable heartbeat signal. In this case, all output pins will reflect the last value sent through I2C channel.

MCU Reset

Once the reset button is pressed more than 5 Seconds, it sends the One-shot pulse (Refer signal named RESET_IN in the below waveform) to unlock the ASM from RESET state. This same signal is used for host MCU reset. When there is a need to reset the MCU regardless of any lockout error, it is possible to use this signal to do so.

Conclusion

Functional safety is a primary concern in some of the use cases necessitated by the oil and gas industry, the machinery sector and so on. There is a safety advantage of hardware based GreenPAK ASM over a software approach. In this case, it is an ON/OFF driver driven by SLG46531V IC. The SLG46531V IC catches the undesired situation when pulse period approaches 23 mSec and safely lock out the output driver without fail. The GreenPAK IC helps in isolating the actuator, minimizes hazards, and occupies very little PCB board area.

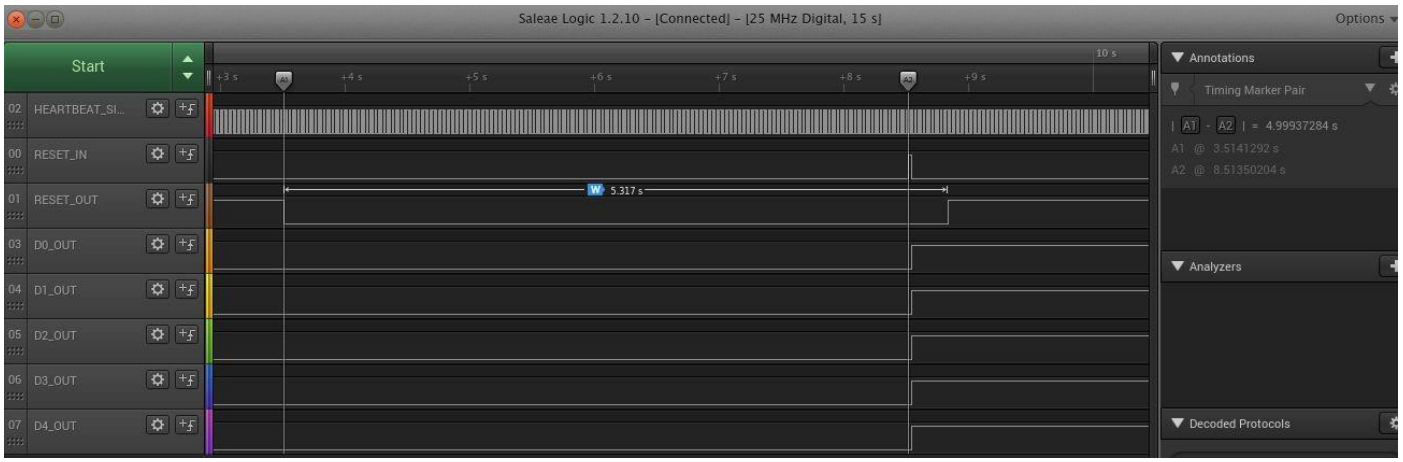

Figure 14. RESET signal for host MCU

IMPORTANT NOTICE AND DISCLAIMER

RENESAS ELECTRONICS CORPORATION AND ITS SUBSIDIARIES (“RENESAS”) PROVIDES TECHNICAL SPECIFICATIONS AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF THIRD-PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for developers who are designing with Renesas products. You are solely responsible for (1) selecting the appropriate products for your application, (2) designing, validating, and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. Renesas grants you permission to use these resources only to develop an application that uses Renesas products. Other reproduction or use of these resources is strictly prohibited. No license is granted to any other Renesas intellectual property or to any third-party intellectual property. Renesas disclaims responsibility for, and you will fully indemnify Renesas and its representatives against, any claims, damages, costs, losses, or liabilities arising from your use of these resources. Renesas' products are provided only subject to Renesas' Terms and Conditions of Sale or other applicable terms agreed to in writing. No use of any Renesas resources expands or otherwise alters any applicable warranties or warranty disclaimers for these products.

(Disclaimer Rev.1.01 Jan 2024)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan
www.renesas.com

Contact Information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit www.renesas.com/contact-us/.

Trademarks

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.