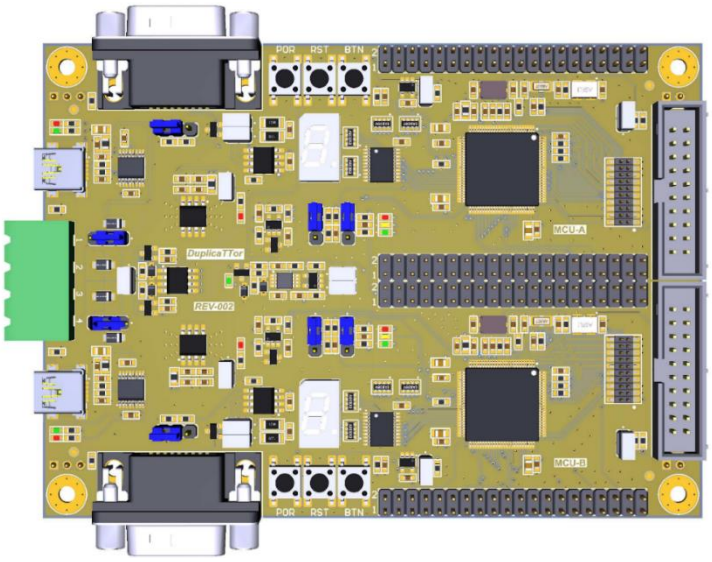
DuplicaTTor® Evaluation Board 0405

User Guide

Document ID:	**DEB-0405-R002-UG-V01F**
Product ID to which document applies:	**DEB-0405-R002**
Target microcontroller(s):	**STM32F405**
Document release date:	**29 June 2018**



SafeTTy Systems™

www.SafeTTy.net

Restrictions on the use of the DEB-0405

DuplicaTTor Evaluation Boards (DEBs) are available only to business customers.

DEBs are intended to support 'benchtop' software evaluations, as part of internal research and development (R&D) activities in the company that purchases the board(s). No warranty is provided as to their suitability for any other purpose.

In keeping with their intended use, DEBs: [1] are not intended to be complete in terms of either product safety or environmental measures; and [ii] are not designed for (and are not suitable for) use in a product that is released to consumers in any form.

As they are intended solely for business R&D purposes, DEBs do not fall within the scope of the European Union directives regarding electromagnetic compatibility (EMC), restricted substances (RoHS), recycling (WEEE), FCC, CE or UL, and therefore may not meet the technical requirements of these directives or related directives in other parts of the world.

Use of a DEB implies acceptance of these usage restrictions.

Trademarks

Acknowledgements

The schematics presented in this document were prepared by Attila Gönczi: please refer to D2 for details.

Contents

Document revisions

DEB-0405-R002-UG-V01A (2017-09-13)	Original document release
DEB-0405-R002-UG-V01B (2017-10-08)	General tidying up.
DEB-0405-R002-UG-V01C (2017-10-21)	Restructured to improve readability. Additional guidance on fault-injection included. Added links to DDS-0405.
DEB-0405-R002-UG-V01D (2017-11-06)	Minor updates (for consistency) following publication of Indian edition of 'ERES2'.
DEB-0405-R002-UG-V01E (2018-02-28)	Improved description of jumper settings. Minor updates to reference 'RTL TTRDs'.
DEB-0405-R002-UG-V01F (2018-06-29)	Updated 'RTL TTRD' material. Minor tidying up throughout for consistency with related documentation.

Related documents

This document should be read in conjunction with:

[D1] Pont, M.J. (2016) "The Engineering of Reliable Embedded Systems (Second Edition)", ISBN: 978-0-9930355-3-1 ('International Hardback Edition 2.3' or later); or,
Pont, M.J. (2017) "The Engineering of Reliable Embedded Systems (Second Edition)", ISBN: 978-0-9930355-4-8 ('International Paperback Edition 2.3' or later); or,
Pont, M.J. (2017) "The Engineering of Reliable Embedded Systems (Second Edition)", ISBN: 978-0-9930355-5-5 ('Indian Paperback Edition 2.3' or later).

[D2] The DuplicaTTor Evaluation Board 0405 Hardware Guide
(Document ID 'DEB-0405-R002-HG-V01A', or a later version of this document)

1. Introduction

This document describes how to use a 'DuplicaTTor® Evaluation Board' (DEB) that incorporates two STM32F405 microcontrollers (MCUs).

The full Product ID for the board that is discussed here is 'DEB-0405-R002': the abbreviated identifier 'DEB-0405' will be used throughout the remainder of this document.

It is expected that most organisations that purchase a DEB-0405 will be interested in exploring the use of 'Time Triggered' (TT) software architectures as a means of meeting the requirements of IEC 61508, IEC 60730 / IEC 60335, ISO 13849, ISO 26262, IEC 62304, DO-178C or a related international safety standard.

2. Information about TT software architectures

Please refer to 'D1' for detailed information about TT software architectures.[1]

3. Using the DEB-0405 with public TTRDs

The DEB-0405 can serve as a general-purpose evaluation platform for developers of TT systems.

For example, some of our public 'Time-Triggered Reference Designs' (TTRDs) can be used with DEB-0405: https://www.safetty.net/ttrds

4. Using the DEB-0405 with RTL TTRDs

In addition to our public TTRDs, we provide a range of more advanced code examples – RTL TTRDs – to organisations that hold a ReliabiliTTy Technology Licence.

Please refer to our website for further details:
https://www.safetty.net/rtl-ttrds

5. What else will you need to use your DEB-0405?

To make full use of your DEB-0405, you will require:

- A suitable Keil[2] compiler (e.g. 'Keil MDK-ARM Essential').
- A debugger / programmer interface: for example, an 'ST Link v2' is a cost-effective option.
- One or two USB cables (USB-A to USB-Mini-B) to support UART/USB reporting (if required).
- A 6V desktop / laboratory power supply.

[1] Full references to 'D1' and other related documents are given on p.4.

[2] Other compilers that target the STM32F405 can be used with this board (but at present the code examples that are are available from SafeTTy Systems are written for the Keil compiler).

6. Typical application of the DEB-0405 in 'IEC 61508' designs

International safety standard IEC 61508 is concerned with functional safety, achieved by means of systems that are implemented primarily in electrical and/or electronic and/or programmable electronic technologies (for example, using microcontrollers – MCUs – and appropriate software).

Hardware Fault Tolerance (HFT) is a key consideration in many IEC 61508 designs.

- When we have an HFT of 0, this means that we have only a single processing path available. If this path fails, it may be challenging to: [i] detect this failure; and [ii] ensure that the system can enter an appropriate 'Fail-Safe State'.
- When we have an HFT of 1, this means that we have a second (independent) processing path available: if one processing path fails, the second processing path is intended to be able to both detect this failure and act appropriately.

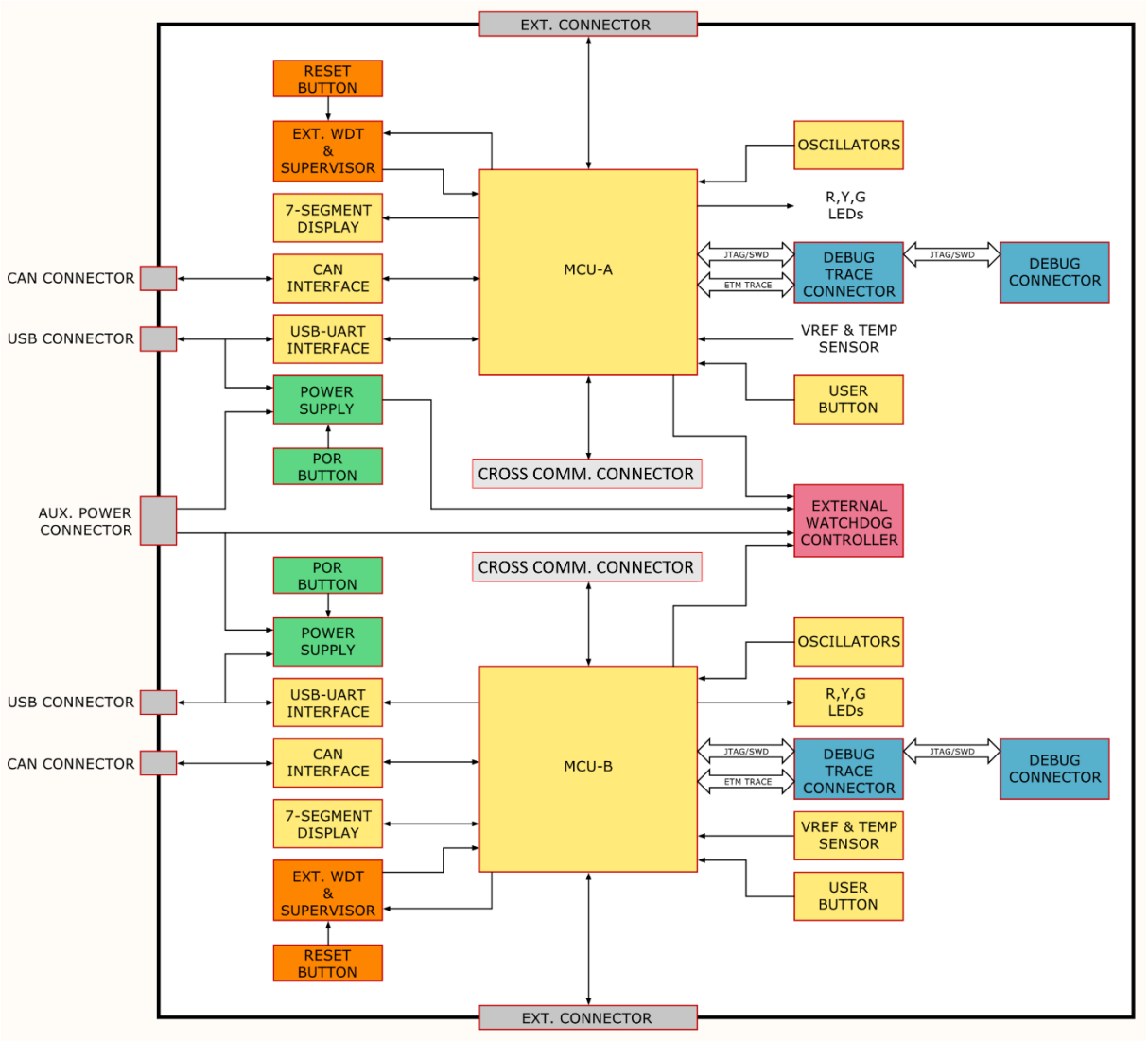
In order to provide a hardware framework that can meet the requirements of IEC 61508 and related international safety standards, the DEB-0405 incorporates two independent hardware channels (Channel-A, Channel-B). Each channel contains the following:

- an STM32F405VG microcontroller with debug (JTAG/SWD) and trace (ETM) interfaces;
- a 16MHz crystal-based oscillator module;
- a voltage supervisor with watchdog and manual reset functions;
- a linear power supply (3.3VDC / 400mA);
- a UART3-USB Interface (typically used for reporting to a laptop and / or for fault injection);
- a CAN Interface with protection and on-board termination;
- a reference voltage source (3.0V) for analogue measurements;
- a PTC-based temperature sensor;
- a 7-segment LED display with driver circuitry;
- three LEDs (red, yellow, green) for general use;
- a Power-On Reset (POR) button;
- a reset button;
- a user button;
- a 40-pin port extension connector;
- a 40-pin cross-communications connector (to facilitate data transfers between the boards).

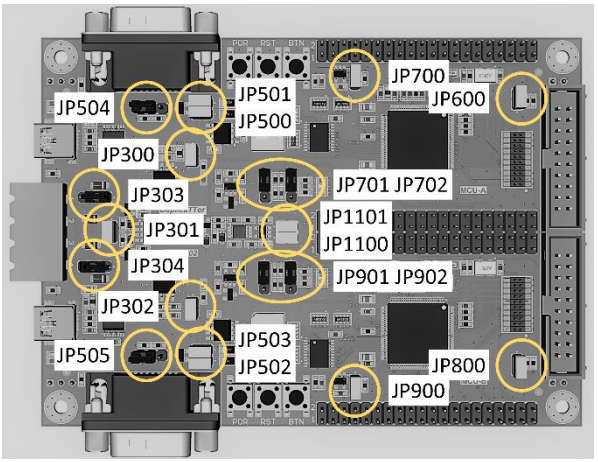
The DEB-0405 also incorporates a single high-voltage 'external watchdog controller' (eWDC) module, based on a MAX16997A IC. Such an eWDC is designed to provide a further 'safety net' (for situations when neither MCU is operational). For evaluation purposes, the eWDC unit on the DEB-0405 may be controlled by either Channel-A or Channel-B (or by both): see Section 14f for further details.

7. Hardware block diagram

An overview of the components that make up the DEB-0405 is shown below.



8. Jumpers



The DEB-0405 can be configured using various jumpers.

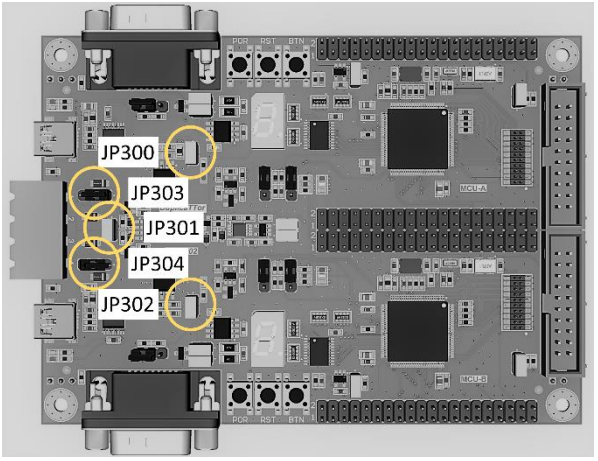
A summary of the jumper functions is given in the table below: further information about individual jumper settings is provided in the remainder of this document.

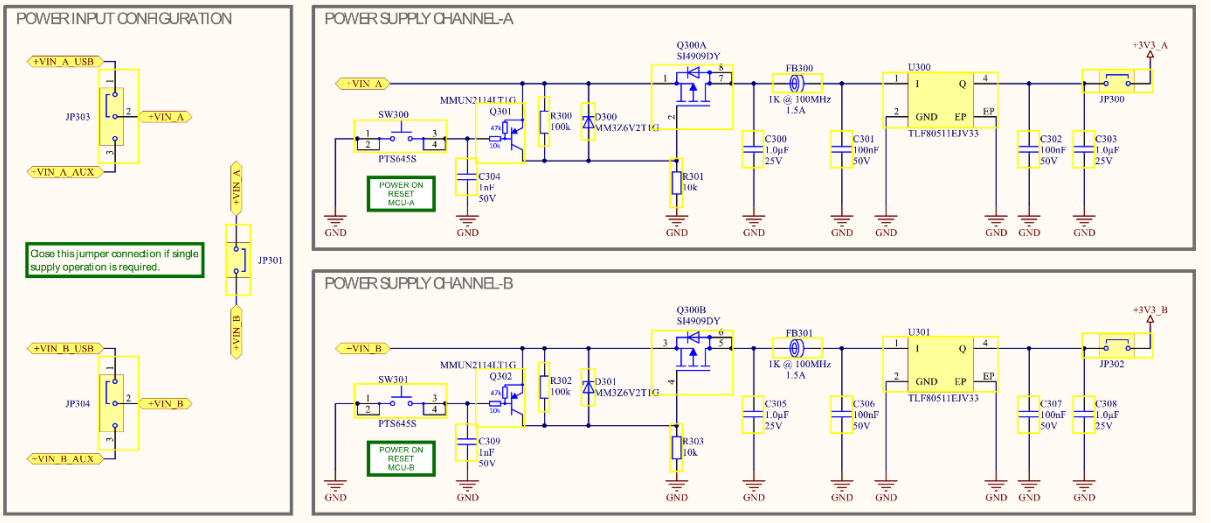
Jumper(s)	Functionality	Further information
JP3xx	Power supply configuration.	See Section 9.
JP5xx	CAN configuration.	See Section 11.
JP600	Main oscillator (fault-injection test).	See Section 14e.
JP700	External supervisor - WDT (fault-injection test).	See Section 14d.
JP701	Supply voltage monitoring (fault-injection test).	See Section 14b.
JP702	ADC (fault injection test)	See Section 14c.
JP800	Main oscillator (fault-injection test).	See Section 14e.
JP900	External supervisor - WDT (fault-injection test).	See Section 14d.
JP901	Supply voltage monitoring (fault-injection test).	See Section 14b.
JP902	ADC (fault injection test)	See Section 14c.
JP1100	eWDC configuration and fault-injection test.	See Section 14f.
JP1101	eWDC configuration and fault-injection test.	See Section 14f.

9. Power supply options

The DEB-0405 can be powered via a USB connector or by means of an external 6V power supply.

The JP3xxx jumpers can be used to configure the power-supply configuration as required.



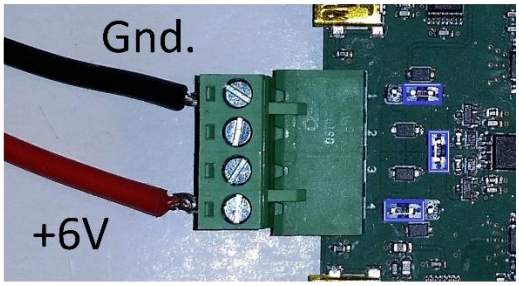


NOTES:

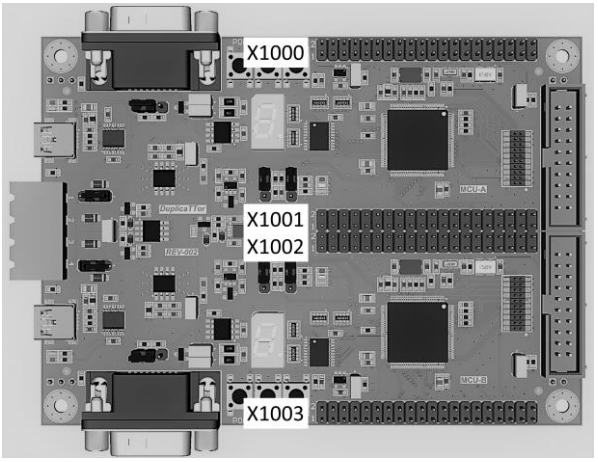
The use of the external watchdog controller (eWDC) requires +VIN_B to be higher or equal to 5V. Due to the rectifier diodes and the voltage drop over the USB cabling, the eWDC will not operate correctly if the DEB-0405 is powered by a USB port.

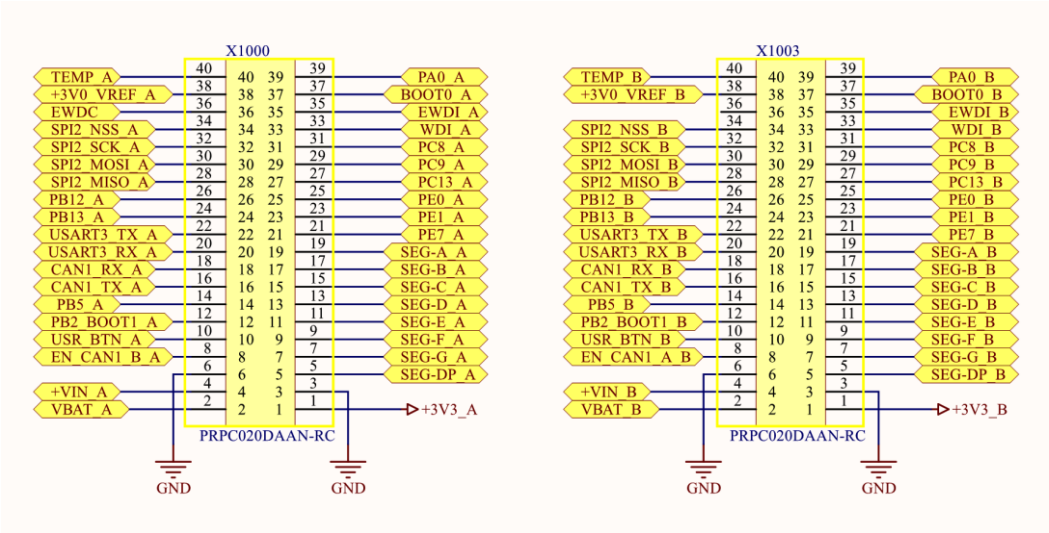
To ensure correct operation, the DEB-0405 should be powered by an external 6V power supply when the eWDC is used. Please note that this applies to the DDS-0405-EC software configuration.

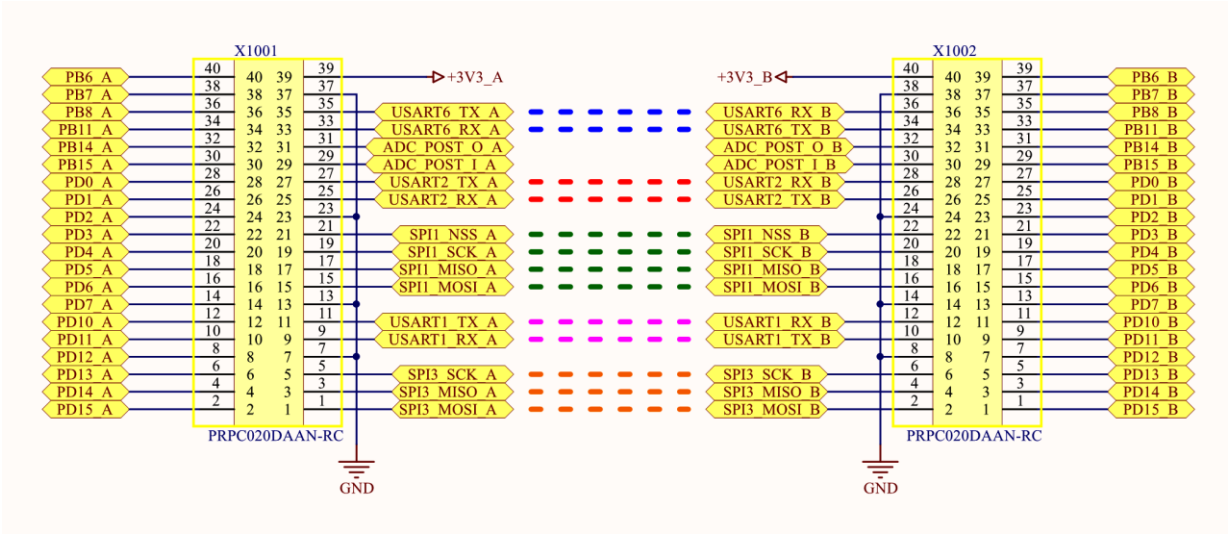
If (for example) a single 6V source is used, the connections and jumper settings shown below will ensure that power is supplied correctly to both boards.



10. External and cross-communication connectors





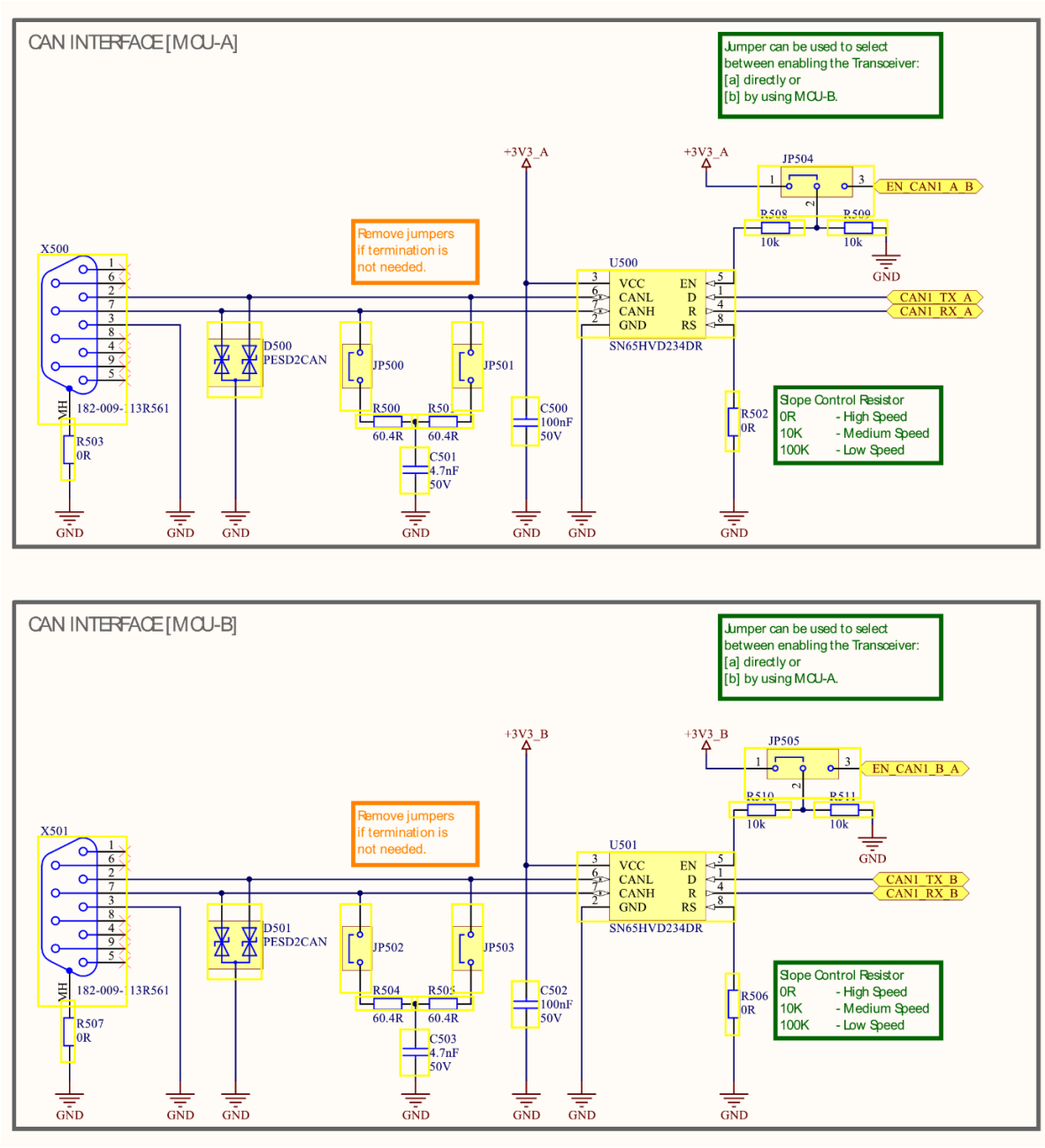


NOTES:

The DEB-0405 provides external access to various pins on the MCUs via connectors X1000, X1001, X1002 and X1003.

X1001 and X1002 are positioned on the PCB in a manner that makes it easy to set up communication links between the two MCUs very easily by means of jumpers. USART1, USART2, USART6 plus SPI1 and SPI3 are available in this way. Please see Section 12 for an example of a typical configuration.

11. Configuring the CAN interfaces



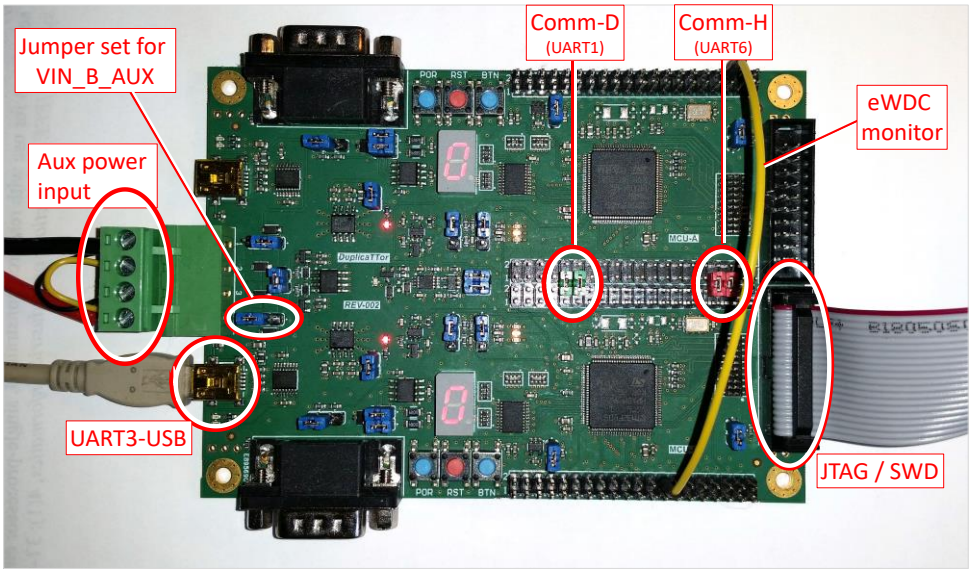
NOTES:

JP500, JP501, JP502 and JP503 provide control of the termination resistors on the CAN bus.

JP504 and JP505 are used to control how the CAN transceivers are enabled: the options are ‘always enabled’ or ‘controlled by the other MCU’ (that is, MCU-A controls the transceiver on MCU-B and vice versa). Such an arrangement might be used (for example) to implement a form of ‘bus guardian’ (reducing the probability of ‘babbling-idiot’ failures).

12. Typical hardware configuration

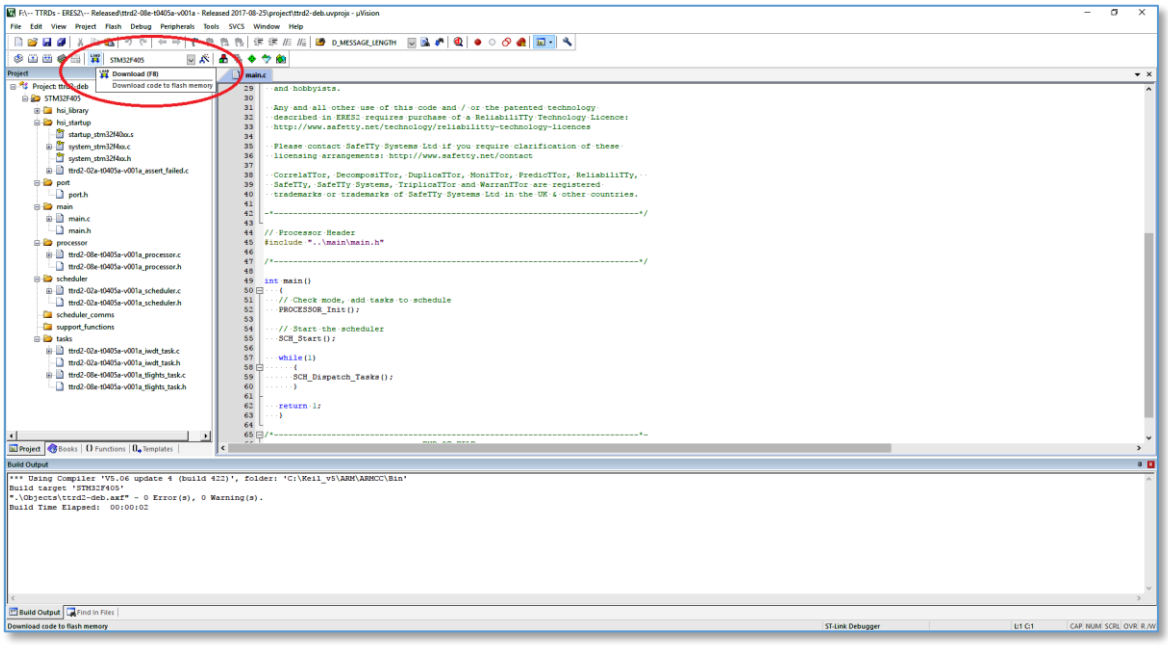
The figure below shows a DEB-0405 configured to run the DuplicaTTor Design Suite (DDS-0405).



13. Loading code on the board (Keil® example)

Where the Keil® compiler is used to generate executable code for use with the DEB-0405, the ST Link V2 provides a cost-effective means of programming the board and controlling the debugging process.


[STLink V2. Photo adapted from ST brochure]



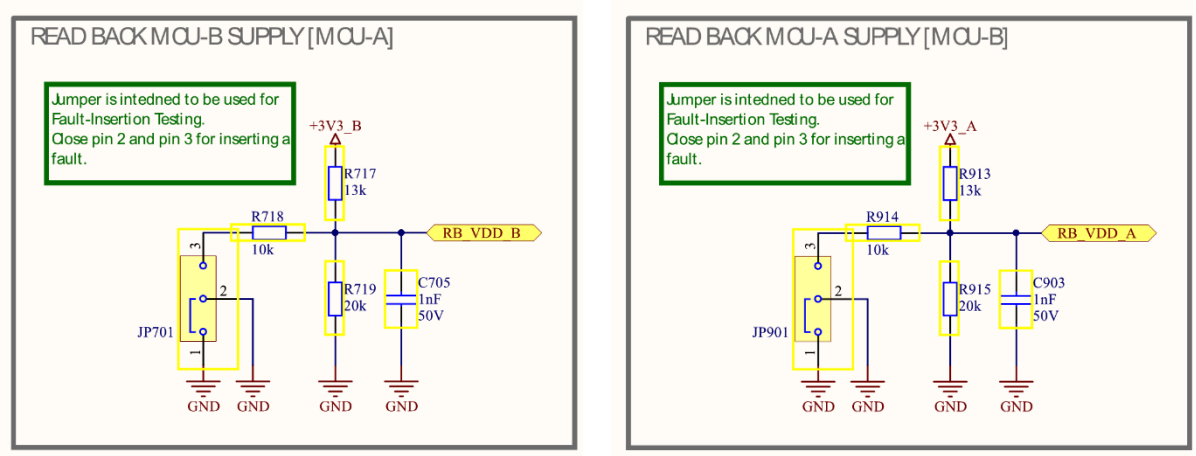
14. Performing fault-injection tests

a. Overview

DEB-0405 has various jumpers that can be used to support fault-injection tests.

An overview of these capabilities is provided in this section.

b. Supply voltage cross-monitoring jumpers (JP701 and JP901)

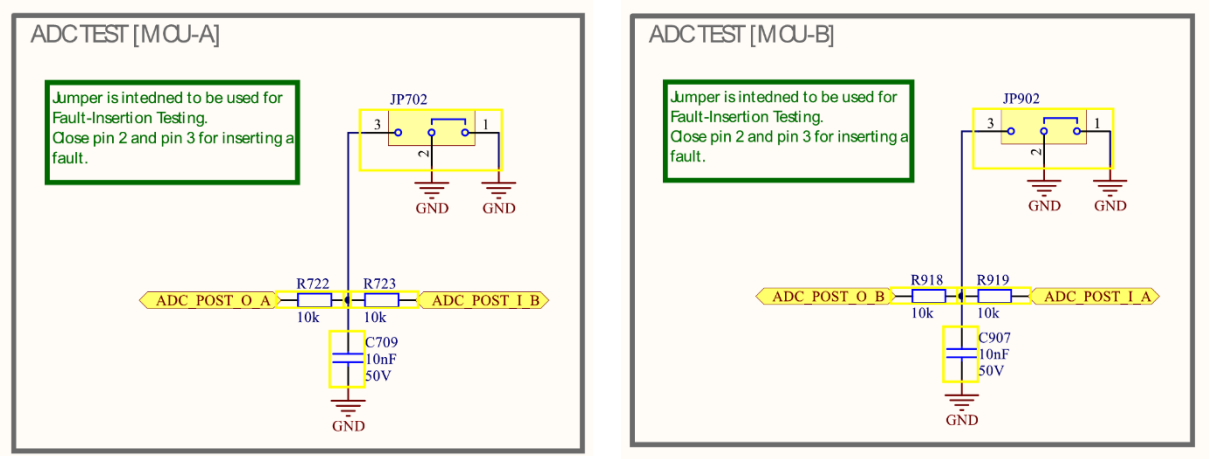


NOTES:

The DEB-0405 provides the ability for each MCU to monitor the power-supply voltage on the other MCU.

When this facility is used, JP701 / JP901 can be used to simulate a power-supply fault.

c. ADC test serial jumpers (JP702 and JP902)

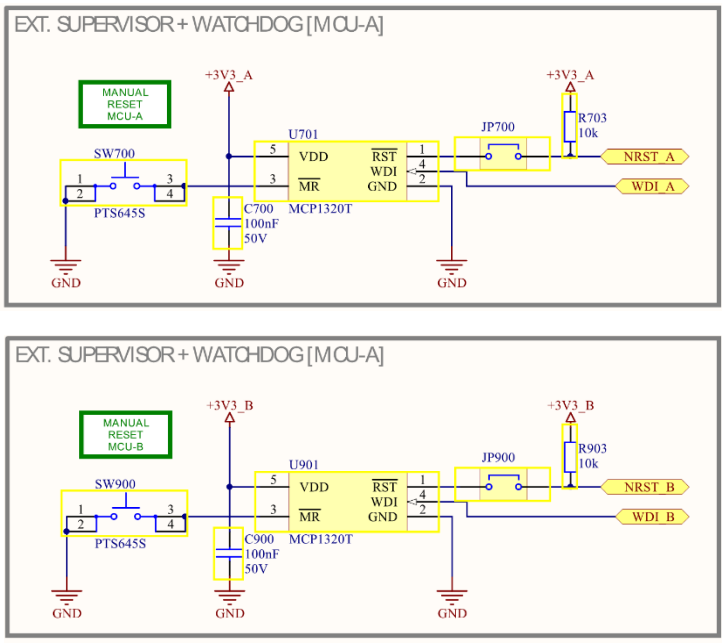


NOTES:

The DEB-0405 provides the ability for each MCU to generate signals that can be used to test the ADC unit on the other MCU.

When such a facility is used, JP702 / JP902 can be employed to inject faults into this test system.

d. External supervisor and watchdog timer jumpers (JP700 and JP900)



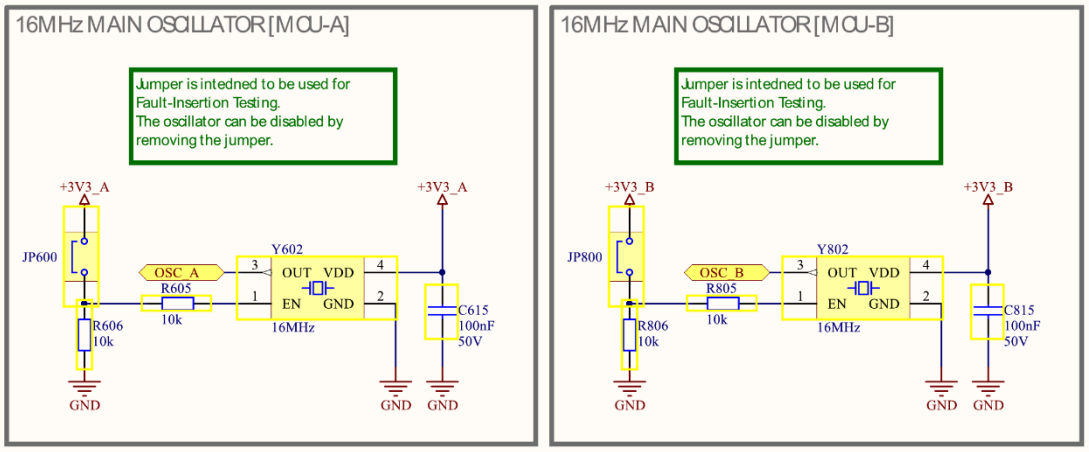
NOTES:

The MCP1320T provides both a voltage supervisor and an external watchdog.

The watchdog behaviour is optional: it is started with a falling edge on the WDI pin.

The MCP1320T can be removed from the circuit (for each MCU independently) by means of JP700 / JP900. This facility is provided to support code testing.

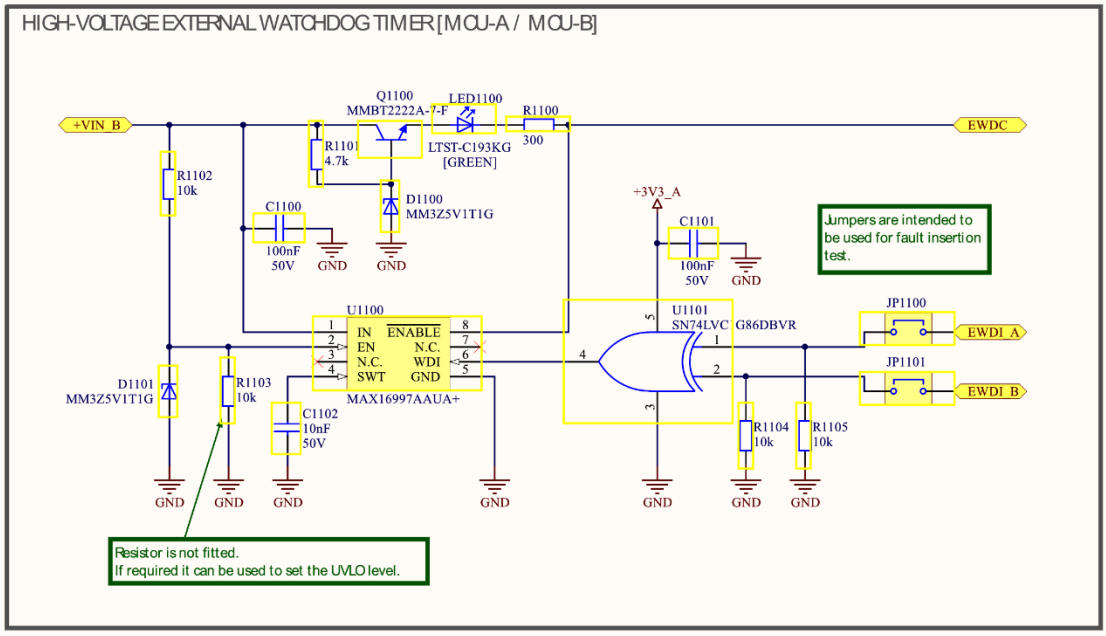
e. Main oscillator jumpers (JP600 and JP800)



NOTES:

JP600 and JP800 are included to support fault-injection tests (oscillator failure).

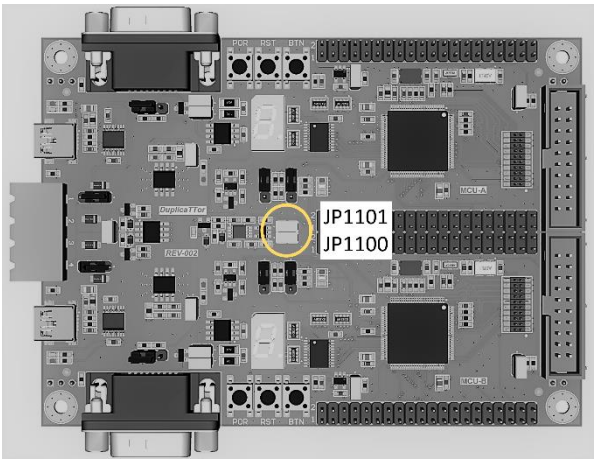
f. eWDC jumpers (JP1100 and JP1101)



NOTES:

JP1100 and JP1101 can be used to disconnect MCU-A and MCU-B (respectively) from the eWDC: these jumpers are primarily intended to support fault-injection testing on the board.

Please note that the jumpers are 'swapped' on Revision 002 of the board: that is, JP1100 (that controls MCU-A) is positioned next to MCU-B (and vice versa).



www.SafeTTy.net