TEST REPORT

Evaluation of safety critical functions

Report Reference No.........................:	6108070.51QS
Date of issue.......................................:	2021-11-17
Total number of pages......................	25 pages
Applicant's name...............................: Address... :	LEE YEONG INDUSTRIAL CO., LTD. No.2, Kejia Rd., Douliu City, Yunlin County 64057, Taiwan
Testing Laboratory............................:	DEKRA Testing and Certification (Shanghai) Ltd. 3F, #250 Jiangchangsan Road, Building 16, Headquarter Economy Park Shibei Hi-Tech Park, Jing'an District, Shanghai, 200436, China
Test Specification: Applied standards................................ :	Cl. K.18.8 of the below standards: IEC 62841-1:2014; EN 62841-1:2015; IEC 62841-2-1:2017; EN 62841-2-1:2018+A11:2019;
Test procedure................................... :	-
Test item description..........................:	Safety critical functions of battery powered Diamond core drill See chapter 2 for details
Trade Mark...:	AGP
Manufacturer...:	LEE YEONG INDUSTRIAL CO., LTD. No.2, Kejia Rd., Douliu City, Yunlin County 64057, Taiwan
Model/Type reference.........................:	DMC160; D6; DD6; D160; D63; DD63; DMC63; PRO CD 182; 20116078; CDR3HWV-220; DMC262; DD262; DD62 DD160; DD262; D160; DM6; DM160; DM63; CM160; CM6; CM63; CM262; C6; C160; C63; C262; CD6; CD160; CD63; CD262; PM6; PM160; PM63; PM262; PD6; PD160; PD63; PDM6; PDM160; PDM63; PDM262
Ratings..:	DD160; DD262; D160; DM6; DM160; DM63; CM160; CM6; CM63; CM262; C6; C160; C63; C262; CD6; CD160; CD63; CD262; PM6; PM160; PM63; PM262; PD6; PD160; PD63; PDM6; PDM160; PDM63; PDM262: 110-120 Vac; 50-60 Hz; 1700 W; n_0=1250/2500 min^{-1}; 230-240 Vac; 50-60 Hz; 2200 W; n_0=1250/2500 min-1; max. 80 mm; Class II 220 Vac; 50-60 Hz; 2000 W; n0=1250/2500 min^{-1}; DMC160; D6; DD6; D160; D63; DD63; DMC63;

	PRO CD 182; 20116078; CDR3HWV-220; DMC262; DD262; DD62: 110-120 Vac; 50-60 Hz; 1700 W; n_0=1000/1600/4450 min^{-1}; 230-240 Vac; 50-60 Hz; 2200 W; n_0=1000/1600/4450 min^{-1}; 220 Vac; 50-60 Hz; 2000 W; n_0=1000/1600/4450 min^{-1};
Hardware version(PCB)……………..:	DMC160-V01
Software version……………………..:	DMC160AMPV1_V01

Testing procedure and testing location:		
☒ **Testing Laboratory:**	DEKRA Testing and Certification (Shanghai) Ltd.	
Testing location/ address................................:	3F, #250 Jiangchangsan Road Building 16,Headquarter Economy Park Shibei Hi-Tech Park, Jing'an District Shanghai 200436 CHINA	
☐ ~~**Associated CB Testing Laboratory:**~~		
~~**Testing location/ address................................:**~~		
Tested by (name + signature)..........................:	Chris Feng	
Approved by (name + signature)...................:	Allan Chen	
☐ ~~**Testing procedure: TMP/CTF Stage 1:**~~		
~~**Testing location/ address................................:**~~		
~~**Tested by (name + signature)..........................:**~~		
~~**Approved by (name + signature)...................:**~~		
☐ ~~**Testing procedure: WMT/CTF Stage 2:**~~		
~~**Testing location/ address................................:**~~		
~~**Tested by (name + signature)..........................:**~~		
~~**Witnessed by (name + signature)..................:**~~		
~~**Approved by (name + signature)...................:**~~		
☐ ~~**Testing procedure: SMT/CTF Stage 3 or 4:**~~		
~~**Testing location/ address................................:**~~		
~~**Tested by (name + signature)..........................:**~~		
~~**Witnessed by (name + signature)..................:**~~		
~~**Approved by (name + signature)...................:**~~		
~~**Supervised by (name + signature)................:**~~		

Table of content

1. Test Program

Safety Critical Functions (SCFs) shall either be single fault tolerant or meet the applicable Performance Level (PL) requirements.

DEKRA evaluated the structure, the functions and where necessary the achieved performance level(s) of safety critical functions of the above listed power tools.

Where necessary, for evaluation of the achieved performance level(s), the IEC/EN ISO 13849-1 is applied. For evaluating the software, Cl. H.11.12.3 of IEC 60730-1 is applied, where necessary.

According to the end-product standard IEC/EN/BS EN 62841-2-1, the required performance level (PLr) of the safety critical functions of diamond drills is:

Table 1: Required Performance Level of Safety Critical Functions

Potential Safety Critical Function (SCF)	Minimum Performance Level (PL)	Verdict
Power switch – prevent unwanted switch-on for tools with MR, max ≤ 25 Nm measured in accordance with 19.102	a	N/A
Power switch – prevent unwanted switch-on for tools with MR, max > 25 Nm measured in accordance with 19.102	b	P
Power switch – provide desired switch-off for tools with MR, max ≤ 25 Nm measured in accordance with 19.102	a	N/A
Power switch – provide desired switch-off for tools with MR, max > 25 Nm measured in accordance with 19.102	c	P
Power switch – provide desired switch-off for tools that require bracing in accordance with 8.14.1.101	c	N/A
Provide desired direction of rotation for tools that do not require bracing in accordance with 8.14.1.101	Not an SCF	N/A
Provide desired direction of rotation for tools that require bracing in accordance with 8.14.1.101	b	N/A
Prevent output speed from exceeding 130 % of rated no-load speed without accessories mounted	a	N/A
Prevent self-resetting as required in 23.3 for tools with MR, max ≤ 25 Nm measured in accordance with 19.102	a	N/A
Prevent self-resetting as required in 23.3 for tools with MR, max > 25 Nm measured in accordance with 19.102	b	P
Limit the torque to comply with 19.102	c	N/A
Prevent unwanted lock-on of the power switch function for tools with MR, max ≤ 25 Nm measured in accordance with 19.102	a	N/A
Prevent unwanted lock-on of the power switch function for tools with MR, max > 25 Nm measured in accordance with 19.102	c	N/A
Prevent exceeding thermal limits	a	P

1.1 Document history:

Report No.	Date	Description
6108070.51QS	2021-11-17	First release.

2. Description of Test Object

The products under evaluation are the safety critical functions of the diamond drill models manufactured by Lee Yeong Industrial Co., Ltd.

Only the following safety critical functions are evaluated in this report.

SCF1. Power switch-prevent unwanted switch-on

The diamond drill uses a power switch. According to above table 1, PLr = b.

SCF2. Power switch-provide desired switch-off

The diamond drill uses a power switch. According to above table 1, PLr = c.

SCF3: Prevent self-resetting as required in 23.3

The diamond drill has protective circuits that switch off the tool and Monitoring switch status. So, a protective circuit is provided to meet this requirement. According to above table 1, PLr = b.

SCF4. Prevent exceeding thermal limits

Protective electronic circuit is developed to provide battery over peak current protection (OCP) to pass the test of Clause b) “The terminals of each motor are shorted one at a time.” and c) “The rotor of each motor is locked one at a time.” of 18.1 of IEC/EN 62841-1. According to 18.1, PLr = a.

Below are the schematics of the diamond drill models:

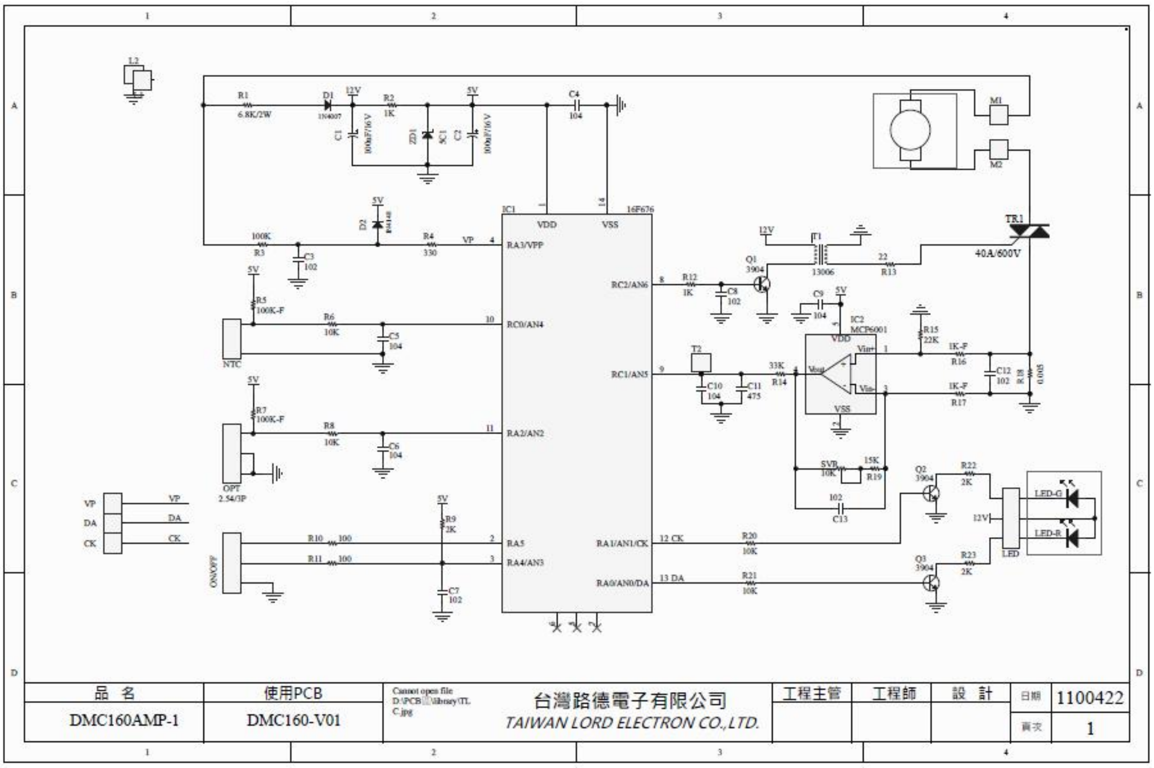


Figure 1: Circuit diagram of DMC160-1

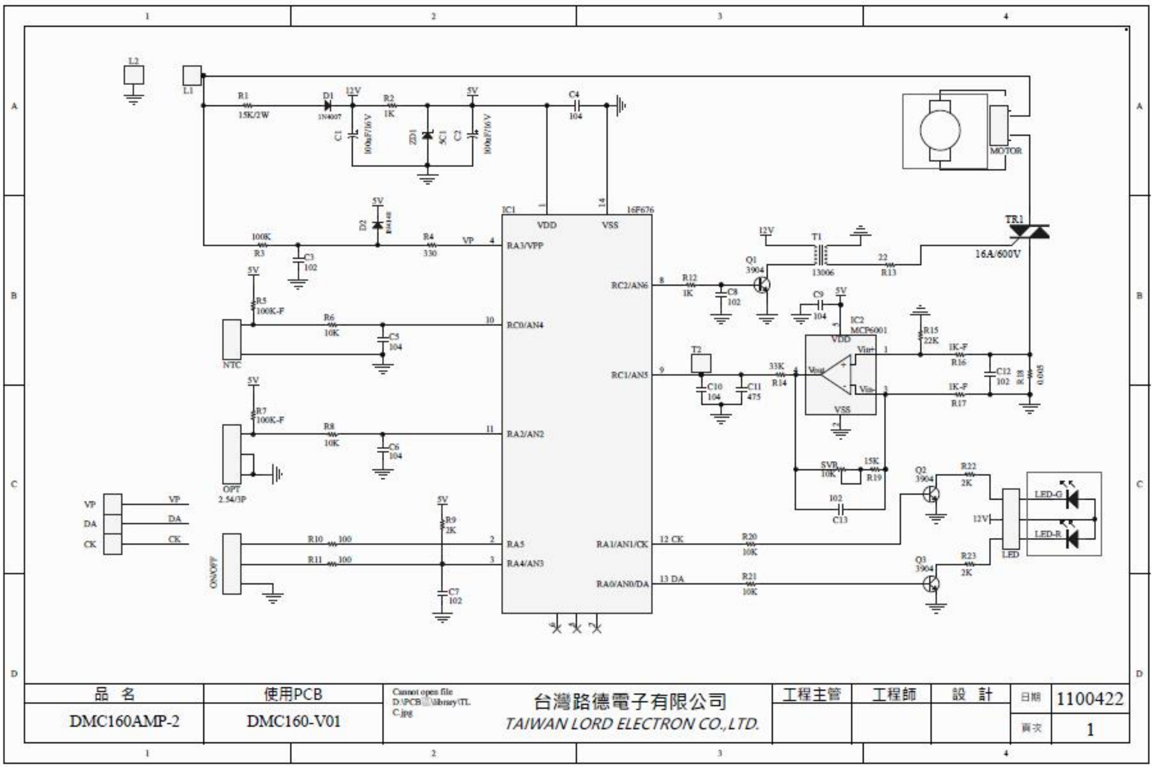


Figure 2: Circuit diagram of DMC160-2

3. Ability to perform a SCF under expected electromagnetic environmental stresses

Below are the test records.

Some instructions in the following table:

“Performance criterion” means: the minimum product requirements:

A: The product has no reaction or abnormality and the original state remains unchanged.

B: Errors but they can be recovered.

C: There are abnormalities that cannot be recovered, requiring manual intervention.

D: Damage.

“Test Result criterion” means: Actual results.

According to 18.8.1 of IEC/EN, electronic circuits that provide safety critical functions shall not susceptible to loss of safety critical function due to exposure to electromagnetic environmental stresses encountered in anticipated environments.

The circuits providing the SCFs have been evaluated by exposing the diamond drill to the electromagnetic environment as specified in Clause 18.8.2 and 18.8.7 of IEC/EN. Below is the test record.

For the SCF1-power switch-prevent unwanted switch-on, the diamond drill was switched off during the EMC test. The test result was satisfactory as during and after the EMC test, the diamond drill not operated.

For the SCF2-power switch-provide desired switch-off, the diamond drill under no-load operation during the EMC test. The test result was satisfactory as after the EMC test, the tool can be switch off.

For the SCF3- Prevent self-resetting, the motor of the tool was blocked which caused the tool stopped during operation. The tool cannot restart until the trigger switch was released and then retriggered. The test results were satisfactory.

For the SCF4- Prevent exceeding thermal limits, the motor of the diamond drill was locked during normal operation. The test result was satisfactory as there was no charring or burning or explosion during or after the EMC test.

Below is the test data.

Conductive Susceptibility Measurement Results

Project No.:

Application:		**Date of Measurement**	2021/08/28
Test Site		**Temperature**	25°C
EUT:	DMC160AMP-1	**Humidity**	
M/N:		**Barometric Pressure**	
S/N:		**Input Voltage**	120V, 60Hz
Test Mode:	待機、正常運轉、電流跳脫、過溫跳脫		
Standard:	IEC 61000-4-6:2008		
Measurement Equipment:			

Conducted Signal	AM 80% Modulated with 1kHz @ 1% Frequency Step Size
Test Dwell Time	☒ 3 Seconds ☐ 5 Seconds ☐ Seconds

Input a.c. power ports

Frequency (MHz)	Inject Voltage (V)	Inject Ports	Inject Method	Performance criterion	Test Result criterion	Result	Observation
0.15-230	3	AC Mains	CDN (M016-M2)			Pass	Note 1

Note 1: There was no change operated with initial operating during the test.

Voltage Dips and Interruptions Test Result

Application:		**Date of Measurement**	2021/08/28
Test Site		**Temperature**	25°C
EUT:	DMC160AMP-1	**Humidity**	
M/N:		**Barometric Pressure**	
S/N:		**Input Voltage**	120V, 60Hz
Test Mode:	待機、正常運轉、電流跳脫、過溫跳脫		
Standard:	IEC 61000-4-11:2004		
Measurement Equipment:			

Input a.c. power ports

Item	Voltage % Reduction	Test Duration (periods)	Performance criterion	Test Result criterion	Result	Observation
Voltage Dips	>95	0.5			Pass	Note 1
	>95	1			Pass	Note 1
	60	10			Pass	Note 1
	30	25			Pass	Note 1
	20	250			Pass	Note 1
Voltage Interruption	>95	250			Pass	Note 1

Note 1: There was no change operated with initial operating during the test.

Note 2: The system shut down during the test, but can recover itself.

Electrical Fast Transient/Burst Measurement Results

Application:		**Date of Measurement**	2021/08/28
Test Site		**Temperature**	25°C
EUT:	DMC160AMP-1	**Humidity**	
M/N:		**Barometric Pressure**	
S/N:		**Input Voltage**	120V, 60Hz
Test Mode:	待機、正常運轉、電流跳脫、過溫跳脫		
Standard:	IEC 61000-4-4:2012		
Measurement Equipment:			

Input a.c. power ports (Tr/Th: 5/50ns, Repetition Frequency: 5kHz)

Inject Line	Polarity	Test Level (kV)	Test Duration (second)	Inject Method	Performance criterion	Test Result criterion	Result	Observation
L	+	2	120	Direct			Pass	Note 1
L	-	2	120	Direct			Pass	Note 1
N	+	2	120	Direct			Pass	Note 1
N	-	2	120	Direct			Pass	Note 1
L+N	+	2	120	Direct			Pass	Note 1
L+N	-	2	120	Direct			Pass	Note 1

Note 1: There was no change operated with initial operating during the test.

Electrostatic Discharge Measurement Results

Application		**Date of Measurement**	2021/08/28
Test Site		**Temperature**	25°C
EUT	DMC160AMP-1	**Humidity**	
M/N		**Barometric Pressure**	
S/N		**Input Voltage**	120V, 60Hz
Test Mode	待機、正常運轉、電流跳脫、過溫跳脫		
Standard	EN 55014-2: 2015; EN 61000-4-2:2008		
Measurement Equipment			

Air Discharge (10 Discharges @ Per Test Point)

Test Location	Test Level (kV) & Test Result criterion												Performance criterion	Result	Observation
	+2	-2	+4	-4	+8	-8	+15	-15							
1-10	OK	OK	OK	OK	OK	OK	OK	OK						Pass	Note

Contact Discharge (25 Discharges @ Per Test Point)

Test Location	Test Level (kV) & Test Result criterion												Performance criterion	Result	Observation
	+2	-2	+4	-4	+6	-6	+8	-8							
11-20	OK	OK	OK	OK	OK	OK	OK	OK						Pass	Note

Horizontal Coupling (25 Discharges @ Per Test Point)

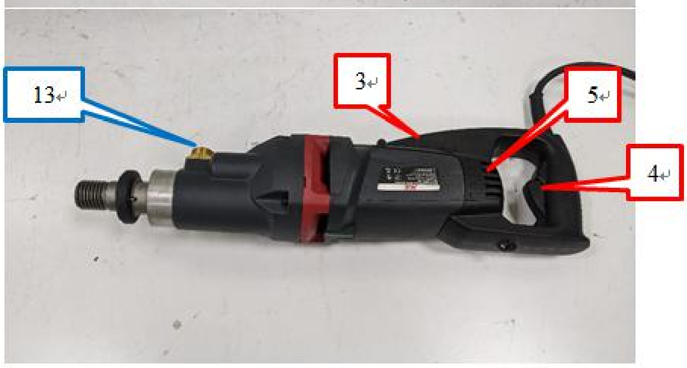
Test Location	Test Level (kV) & Test Result criterion												Performance criterion	Result	Observation
	+2	-2	+4	-4	+6	-6	+8	-8							
Front	OK	OK	OK	OK	OK	OK	OK	OK						Pass	Note
Rear	OK	OK	OK	OK	OK	OK	OK	OK						Pass	Note
Left	OK	OK	OK	OK	OK	OK	OK	OK						Pass	Note
Right	OK	OK	OK	OK	OK	OK	OK	OK						Pass	Note

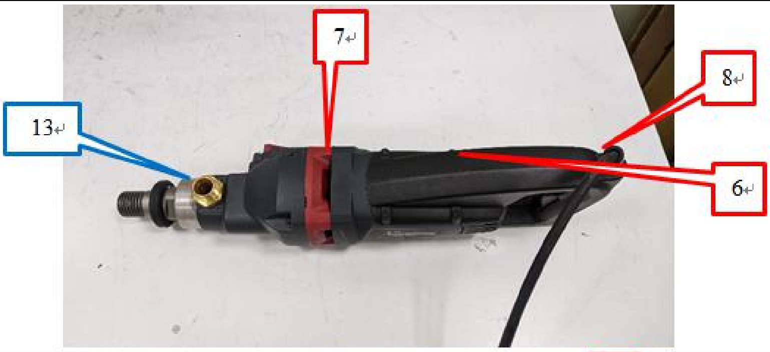
Vertical Coupling (25 Discharges @ Per Test Point)

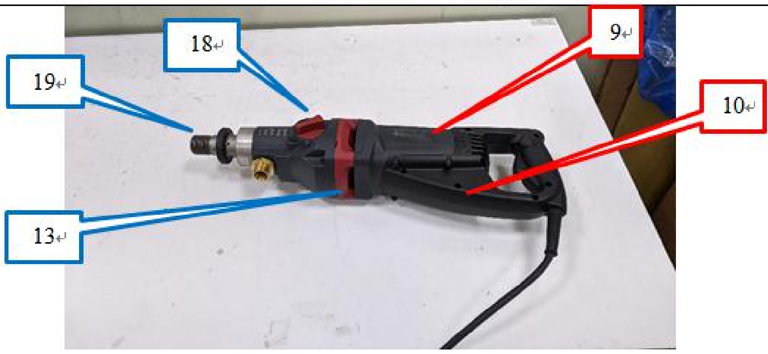
Test Location	Test Level (kV) & Test Result criterion												Performance criterion	Result	Observation
	+2	-2	+4	-4	+6	-6	+8	-8							
Front	OK	OK	OK	OK	OK	OK	OK	OK						Pass	Note
Rear	OK	OK	OK	OK	OK	OK	OK	OK						Pass	Note
Left	OK	OK	OK	OK	OK	OK	OK	OK						Pass	Note
Right	OK	OK	OK	OK	OK	OK	OK	OK						Pass	Note

Test Location Photos

分节符(下一页)







Note : There was no change operated with initial operating during the test.

Note : There was no change operated with initial operating during the test.

4. Achieved Performance Level

4.1 Calculation of MTTFd for SCFs

For SCF3, the achieved performance level (PL) is based on the simplified procedure of Cl. 4.6 of EN ISO 13849-1.

MTTFd of channel in years according IEC/EN 62841-1:

Table 3: Achieved Performance Level according MTTFd

MTTFd	
Range of each channel	**PL**
5 years ≤ MTTFd < 20 years	a
20 years ≤ MTTFd < 50 years	b
50 years ≤ MTTFd	c

Note: SW requirements are covered by IEC/EN 62841-1, cl. 18.8.

To skip a detailed FMEA, LEE YEONG INDUSTRIAL CO., LTD. decided to sum all MTTFd of the electrical components.

According to EN ISO 13849-1, the MTTFd of the single components can be based on:

- worst case values as stated in Annex C
- MTTFd values declared by the component manufacturer
- Calculations using the B10 values
- MTTFd values determined by using TR 62380
- SN29500

Due to the fact that the calculation was done with the sum of all existing electronic components, the MTTFd of the SCF is the same as the overall MTTFd calculated. Below is the calculation of MTTFd provided by the manufacturer.

MTTFd					
Component	Reliability Reference	No.	Units n	MTTFd Typical years	n/MTTFd Typical 1/year
Resistor-Carbon Film	ISO 13849	R1	2	114155	0.0000175
Capacitor-Ceramics	ISO 13849	C3、C4、C5、C6、C7、C8、C9、C10、C11、C12、C13	11	45662	0.0002409
Aluminium electrolytic	ISO 13849	C1 、C2	2	45662	0.0000438
Rectifier diodes	ISO 13849	D1、D2	2	228311	0.0000088
Zener diode Ptot < 1 W	ISO 13849	ZD1	1	228311	0.0000044
Low frequency inductors	ISO 13849	T1	1	45662	0.0000219
Transistor-Bipolar, universal	ISO 13849	Q1、Q2、Q3	3	76104	0.0000394
MCU	supplier	IC1	1	10435	0.0000958
Triac	ISO 13849	TR1	1	3044	0.0003285
					0.0008010
MTTFd (years)Total：1248					

Table 4: Calculation of MTTFd

The calculated overall $MTTF_d$ value is **1248 years (> 50 years)**. According to above table 3, the circuitry design can meet this requirement.

Software embedded in the microcontroller used in the circuitry is involved in providing the SCF3. Therefore, software shall be evaluated its compliance with the requirements for software class B in accordance with Subclause H.11.12.3 of IEC 60730-1:2010. Software evaluation will be described in the following chapter.

5. Software Evaluation

According to IEC/EN 62841-1, the software was assessed. The result was satisfactory, see below table:

IEC 60730-1:2013 Subclause H.11.12.3			
H.11.12.3	Measures to avoid errors		P
H.11.12.3.1	For controls with software class B or C the measures shown in Figure H.1 to avoid systematic faults are applied		P
	Other methods utilized that incorporate disciplined and structured processes including design and test phases		N/A
H.11.12.3.2	Specification		P
H.11.12.3.2.1	Software safety requirements		P
H.11.12.3.2.1.1	The specification of the software safety requirements includes:		P
	• A description of each safety related function to be implemented, including its response time(s): - functions related to the application including their related software classes - functions related to the detection, annunciation and management of software or hardware faults		P
	• A description of interfaces between software and hardware		P
	• A description of interfaces between any safety and non-safety related functions		P
H.11.12.3.2.2	Software architecture		P
H.11.12.3.2.2.1	The description of software architecture include the following aspects:		P
	• Techniques and measures to control software faults/errors (refer to H.11.12.2)		P

	• Interactions between hardware and software		P
	• Partitioning into modules and their allocation to the specified safety functions		P
	• Hierarchy and call structure of the modules (control flow)		P
	• Interrupt handling		P
	• Data flow and restrictions on data access		P
	• Architecture and storage of data		P
	• Time based dependencies of sequences and data		P
H.11.12.3.2.2.2	The architecture specification is verified against the specification of the software safety requirements by static analysis		P
H.11.12.3.2.3	Module design and coding		P
H.11.12.3.2.3.1	Software is suitably refined into modules. Software module design and coding are implemented in a way that is traceable to the software architecture and requirements. The module design specified:		P
	– function(s)		P
	– interfaces to other modules		P
	– data		P
H.11.12.3.2.3.2	Software code is structured		P
H.11.12.3.2.3.3	Coded software is verified against the module specification, and the module specification is verified against the architecture specification by static analysis		P
H.11.12.3.2.4	Design and coding standards		P
	Program design and coding standards is used during software design and maintenance		P

	Coding standards ....:		—
	– specified programming practice		P
	– proscribed unsafe language features		P
	– specify procedures for source code documentation		P
	– specify data naming conventions		P
H.11.12.3.3	Testing		P
H.11.12.3.3.1	Module design (software system design, software module design and coding)		P
H.11.12.3.3.1.1	A test concept with suitable test cases is defined based on the module design specification.		P
H.11.12.3.3.1.2	Each software module is tested as specified within the test concept		P
H.11.12.3.3.1.3	Test cases, test data and test results are documented		P
H.11.12.3.3.1.4	Code verification of a software module by static means includes such techniques as software inspections, walk-throughs, static analysis and formal proof		P
	Code verification of a software module by dynamic means includes functional testing, white-box testing and statistical testing		P
H.11.12.3.3.2	Software integration testing		P
H.11.12.3.3.2.1	A test concept with suitable test cases is defined based on the architecture design specification		P
H.11.12.3.3.2.2	The software is tested as specified within the test concept		P
H.11.12.3.3.2.3	Test cases, test data and test results are documented		P
H.11.12.3.3.3	Software validation		P

H.11.12.3.3.3.1	A validation concept with suitable test cases is defined based on the software safety requirements specification		P
H.11.12.3.3.3.2	The software is validated with reference to the requirements of the software safety requirements specification as specified within the validation concept		P
	The software is exercised by simulation or stimulation of:		P
	• input signals present during normal operation		P
	• anticipated occurrences		P
	• undesired conditions requiring system action		P
H.11.12.3.3.3.4	Test cases, test data and test results are documented		P
H.11.12.3.4	Other Items		P
H.11.12.3.4.1	Equipment used for software design, verification and maintenance was qualified appropriately and demonstrated to be suitable for purpose in manifold applications		P
H.11.12.3.4.2	Management of software versions: All versions are uniquely identified for traceability		P
H.11.12.3.4.3	Software modification		N/A
H.11.12.3.4.3.1	Software modifications are based on a modification request which details the following:		N/A
	• the hazards which may be affected		N/A
	• the proposed change		N/A
	• the reasons for change		N/A
H.11.12.3.4.3.2	An analysis is carried out to determine the impact of the proposed modification on functional safety.		N/A

H.11.12.3.4.3.3	A detailed specification for the modification is generated including the necessary activities for verification and validation, such as a definition of suitable test cases		N/A
H.11.12.3.4.3.4	The modification is carried out as planned		N/A
H.11.12.3.4.3.5	The assessment of the modification is carried out based on the specified verification and validation activities.		N/A
H.11.12.3.4.3.6	All details of modification activities are documented		N/A
H.11.12.3.5	For class C control functions: One of the combinations (a–p) of analytical measures given in the columns of table H.9 is used during hardware development...:		N/A

5.1 Safety Software Requirements

System Description

General product description is given above in Chapter 2.

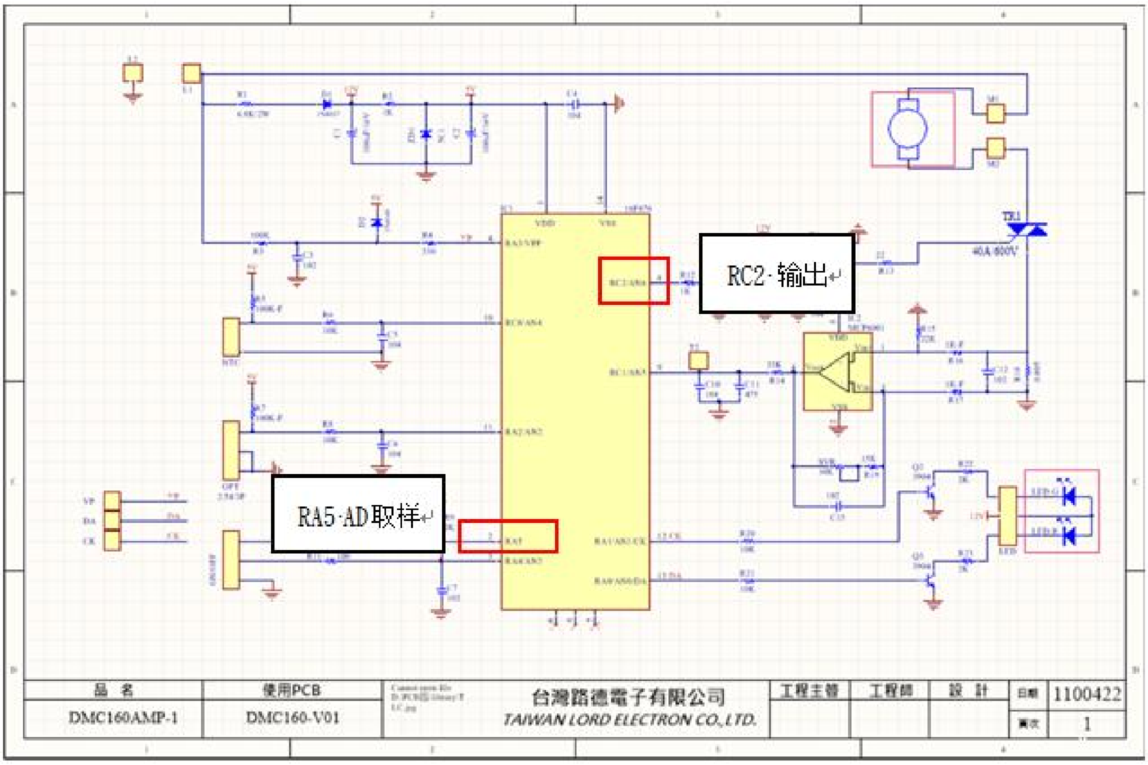
The normal operation of the system is as follows:
The diamond drill does not work with power switch open. Only when the switch is pressed on, it starts to operate.

During normal operation of the diamond drill, in the case that the rotor of the motor of it is locked or the terminals of the motor are shorted, it is stopped operating immediately.

When the switch is released during normal operation of it, it is stopped immediately.

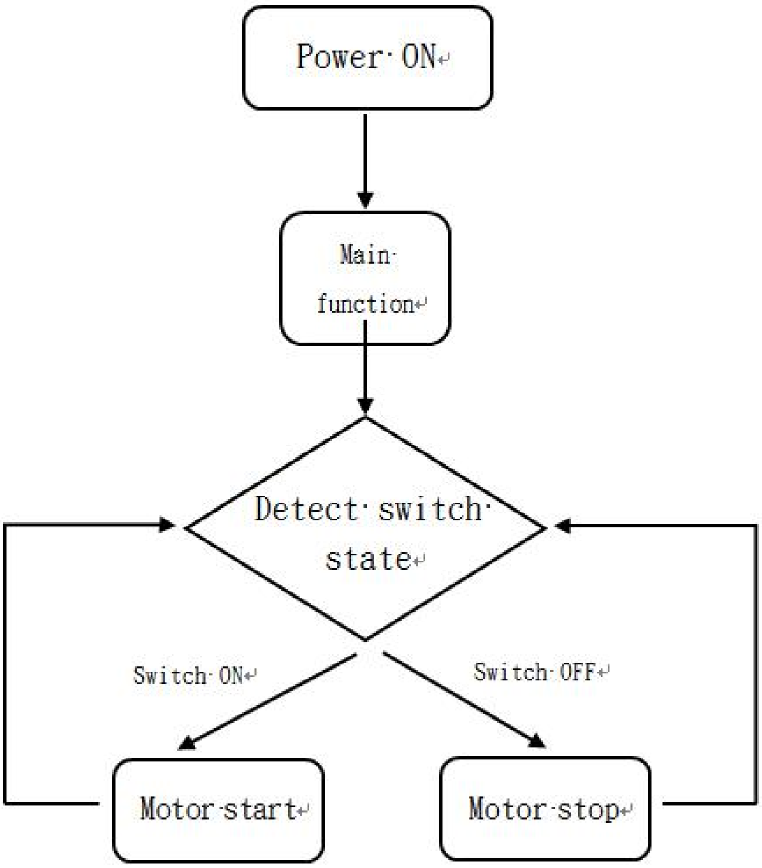
5.1.1 Description of SCF- Power switch-prevent unwanted switch-on

MCU pin configuration:



Sampling pin2: RA5
Output pin8: RC2

Flowchart:



Execute instructions:

ON/OFF Switch action:

First, when the drill is powered on, the main function will load, and MCU will detect the switch state, If switch on, MCU will output signal to drive the Motor. If switch off, the motor stop.

When the power supply and switch in lock-on state, the motor does not run, it can be switched to OFF to enter standby state and then switched to ON to start the motor running.

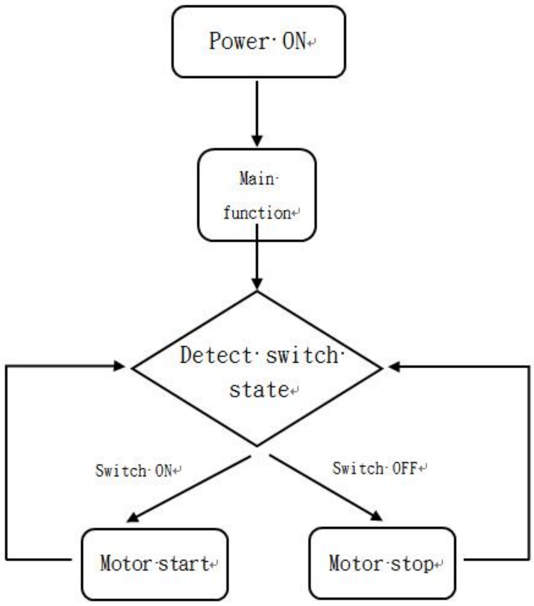
When the motor is running, the switch is turn to OFF and the motor stops running.

When the motor is running, over-temperature or over-current protection occurs, it can be cleared when the switch turn to OFF state.

5.1.2 Description of SCF- Power switch-provide desired switch-off

This item's implementation principle and execution mode are the same as above. MCU will detect the switch state, If switch on, MCU will output signal to drive the Motor. If switch off, the motor stop.

5.1.3 Description of SCF- Prevent self-resetting



The tool has hall switch action detection function, when the tool in lock-on state and power supply, the motor does not run, it can be switched to OFF to enter standby, and then switched to ON to start the motor running.

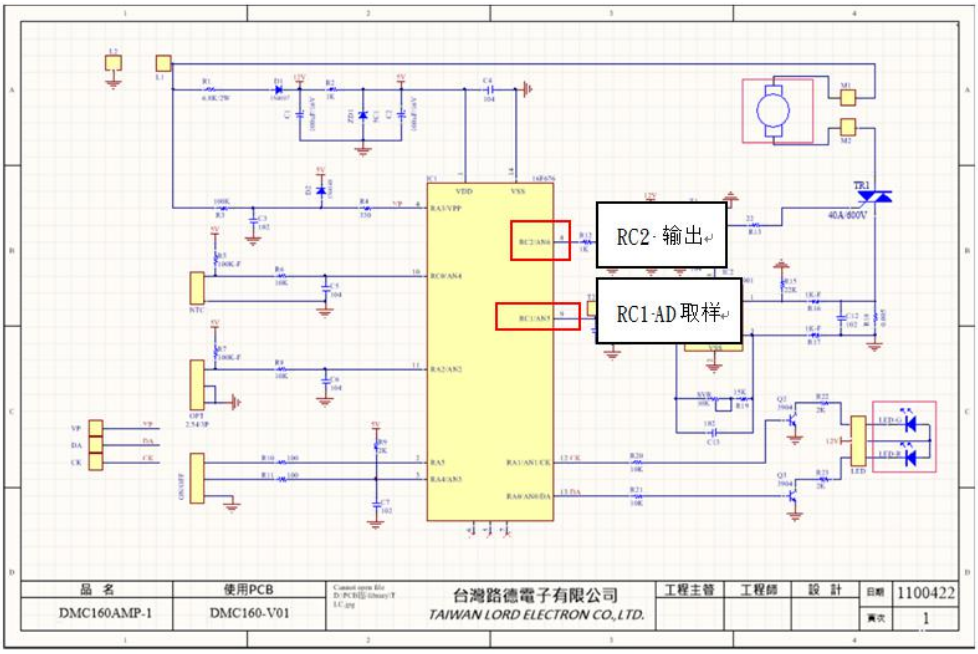
In standby mode, the motor is started when ON is turned ON.

When the motor is running, switch cut to OFF and the motor stops running.

In operation, when over-temperature or over-current occurs, the switch can be cleared to OFF.

5.1.4 Description of SCF- Prevent exceeding thermal limits

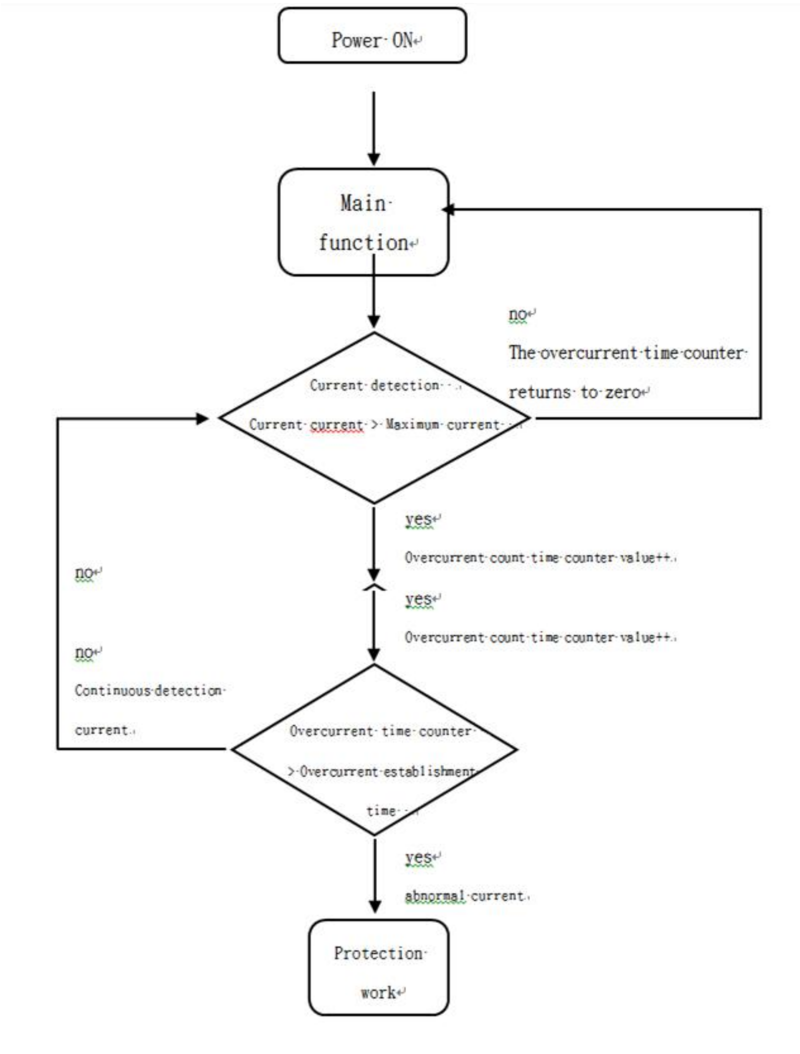
MCU pin configuration:



Sampling pin2: RC1

Output pin8: RC2

Flowchart:



Protection mechanism:

If TRIAC is not triggered, the motor stops running.

Execute instructions:

Motor current detection:

Motor start within 2 seconds (85% output), after which motor running current is less than (load judgment point -0.1A)(85% output) greater than or equal to load judgment point (100% output)

Load judgment point:

Dmc160AMP-1: set 13A.

No current detection within 2 seconds of motor operation.

DMC160AMP-1 current set point:

Current warning point, 22A.

Current overload point 1, 23A is established for 3 consecutive seconds.

Current overload point 2, 25A is established for 0.3 consecutive seconds.

5.2 Software Architecture Design

5.2.1 Software Architecture

The software flow is as follows:

Firstly, MCU initialization is performed, including initializing MCU peripheral, clear watchdog, etc. Then, sampling is enabled. The tool starts working only when the switch is determined pressed on, otherwise, it is kept not working. When the system works in the normal working state, the battery pack current is periodically checked. If over current is judged, OCP is executed, the tool is stopped working within 1 second. If the switch is determined released during normal operation of the tool, the tool is stopped within 1 second. Figure 9, as shown below, is the flowchart of the software.

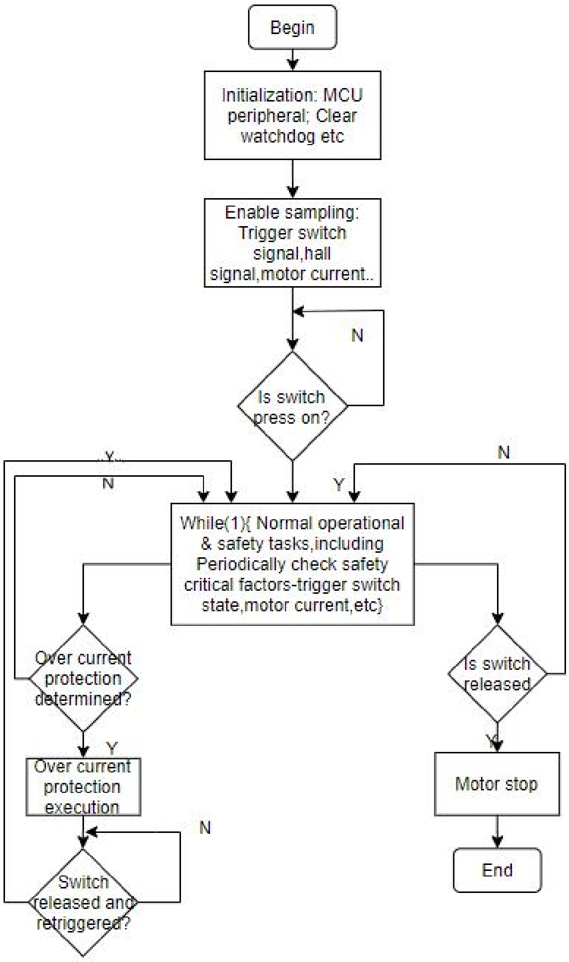


Figure 9: Main Flowchart

5.3 Architecture Verification

A control flow analysis is used as the static analysis approach to verify the architecture against the software safety requirements.

The following aspects of the drop prevention function have been taken into account:

- Proper flow of the code
- Code structure analysis
- Data processing

The code must meet the following criteria:

1. For the control flow of the code:
   - Meet the predefined design in terms of code sequence
   - No uncontrolled loops
   - No unused code and variables/objects
   - No unexpected code (paths/flow)

2. For code structure:
   - No unexpected/unintended outputs
   - No unexpected actions/responses
3. For data processing:
   - All safety related variables must be in a certain range
   - All safety related variables must be initialized before using
   - All safety related variables must be correctly used after definition (to avoid variables unused or improperly used)

After verification, all the code meets these criteria. The software developed has the same architecture design as the software specification, see manufacturer's document "DMC160AMP-1_動作測試(一般)-1100827".

The control flow of the main loop is shown above as Figure 9.

5.4 Module Design and Coding

5.4.1 Module Design and Coding Techniques

Following techniques are used to assure the modular design and coding of the software:

- Size of functional module is limited to be as small as possible
- Each software module refers to a single object
- Values get from ADC out of a certain range is illegal
- Divide by zero situations is handled individually for each division
- During initialization, RAM memory is erased (0 value) to assure a known value before executing of any code

Following techniques are used to keep the code structured:

- An internal coding standard is used
- No dynamic variables used and no dynamic memory allocation involved
- Interrupts are fixed at design level
- Recursion is not used
- No unconditional jump are used

5.4.2 Module Verification

A control flow analysis is used as the static analysis approach to verify the module against the module techniques specification. After verification, all the code meets these criteria. The software module developed has the same architecture design as the software module specification, see manufacturer's document "DMC160AMP-1_動作測試(一般)-1100827".

5.5 Validation

The diamond drill was used during verification and validation testing. The test results were satisfactory. Validation test performed are described as below.

5.5.1 Validation of Power switch-prevent unwanted switch-on

The tool was connected to power supply. When the switch was not pressed on, under no circumstance, the tool started working. It started working only when the switch was pressed on. See manufacturer's document "DMC160AMP-1_動作測試(一般)-1100827".

5.5.2 Validation of Power switch-provide desired switch-off

During normal operation of the tool, when the switch was released, the tool stopped working. See manufacturer's document "DMC160AMP-1_動作測試(一般)-1100827".

5.5.3 Validation of Prevent self-resetting

The motor of the tool was blocked which caused the tool stopped during operation. The tool cannot restart until the trigger switch was release
d and then retriggered. See manufacturer's document "DMC160AMP-1_動作測試(一般)-1100827".

5.5.4 Validation of Prevent exceeding thermal limits

When the terminals of motor are shorted or the rotor of motor is locked, the tool non-hazardous like no charring, burning, or explosion and the tool was protected. See manufacturer's document "DMC160AMP-1_動作測試(一般)-1100827".

6. Conclusion

Achieved PL:
SCF1- Power switch-prevent unwanted switch-on: c;
SCF2-Power switch-provide desired switch-off: c;
SCF3- Prevent self-resetting: PL = c;
SCF4- Prevent exceeding thermal limits: PL = c;

--END--