

	SARA SAE ENGINEERING SPECIFICATION	
	Section: SES 26 – 853	
	Issue: “A”	Rev No: “0”
	Eff. Date: 17.01.2019	Page: 1 of 24

Control of System Software as per clause 5.18 of API16D edition 3rd

Rev	Reason of Change	Date	Prepared by	Reviewed by	Approved by	Status
0	Initial release	17.01.2019	SKG	USR	AS	Released



	SARA SAE ENGINEERING SPECIFICATION	
	Section: SES 26 – 853	
	Issue: “A”	Rev No: “0”
	Eff. Date: 17.01.2019	Page: 2 of 24

Control of System Software as per clause 5.18 of API 16D edition 3rd.

1. Purpose

- 1.1. The scope of this procedure for BOP control system software design verification, installation and validation procedure. It also includes software FMEA and its maintenance.

2. Reference documents

- 2.1. API 16D

3. General requirement as per clause 5.18.1 of API16D

- 3.1. The control system software requirement per customer should be fulfilled. The proof of fulfilment should be verified , documented and provided to customer. The Proof of fulfilment is to be covered through **Factory Acceptance Test (FAT) procedure for individual control unit.**
- 3.2. The reference standards and process involved in the design and development of the system software is to be followed properly.
- 3.3. The processes involved in Design and Development beside upgradation of software is to be documented with tracibility records and revision no. (eg: The PLC input and Output addressing to be preseved with identification no.)
- 3.4. The software is passoward protected to prevent its use by the person do not have in proper knowledge of design and deveoploment of software.
- 3.5. Software used- 10.0 PAC Machine Edition Professional Development Suite
programming language - Ladder Diagram OR LD
Standard used- IEC 61131-3
programmable logic controller (PLC) used – EMERSON

4. Classification of Software Life Cycle Process as per clause 5.18.2 of API 16D

Software life cycle is process by which software is developed , deployed and sucessfully installed on the control unit.

The software life cycle process shall include the following:

- 4.1. Software functional specification



	SARA SAE ENGINEERING SPECIFICATION	
	Section: SES 26 – 853	
	Issue: “A”	Rev No: “0”
	Eff. Date: 17.01.2019	Page: 3 of 24

- 4.2. Software Design and Development
- 4.3. Software Verification and Validation
- 4.4. Software Production and Maintenance



5. Software functional Specification per clause 5.18.3 of API16D

- 5.1. All the functional specification is documented per clause 5.18.3.1 of API16D in **Annexure 'A'**.
- 5.2. All the additional functional specification is documented per clause 5.18.3.2 of API16D in **Annexure 'A'**
- 5.3. Technical requirment of system capabilities represent in checklist and documented per clause 5.18.3.3 of API 16D in **Annexure 'A'**
- 5.4. Software functional specification review format documented per clause 5.18.3.4 of **API16D** in **Annexure 'B'**

6. Software Design and Development as per clause 5.18.4 of API 16D

- 6.1 Software design review should be conducted and tested at different stages as per clause **5.18.4.1 of API 16D**. All panel should be tested individually at preliminary , critical and final design stages and documented in **Annexure 'B'**
- 6.2 The system design architecture drawing includes system topology,logic flow diagram as per clause **5.18.4.2of API16D** and documented in **Annexure 'C'**
- 6.3 Failure modes effect analysis (FMEA) per clause **5.18.4.3 of API16D** is tobe carried out and documented in **Annexure 'G'**.
- 6.4 The design and development of software code should follwed per IEC standard.
- 6.5 The software code includes the design and devoplement of programming software that it could be understood and implemented by other relevant software engineer. as per clause **5.18.4.5 of API16D**
- 6.6 Softcopy of installation and **devoplement tools guide** should be documented as per clause **5.18.4.6 of API16D** (manufacturer, software platform and version) .
- 6.7 Software itself enables developer to provide the possible solution if some error occured. Generally,this is possible by using PLC software inbuilt.

7. Software Validation and Verification as per clause 5.18.5 of API 16D

- 7.1 Software verification and validation for BOP control system enable user to provide local,

	SARA SAE ENGINEERING SPECIFICATION	
	Section: SES 26 – 853	
	Issue: “A”	Rev No: “0”
	Eff. Date: 17.01.2019	Page: 4 of 24

system and global effect per Annexure 'G'

- 7.2 PLC Software enable and validate all the operational logic , instructions and communication parameter
- 7.3 The Individual software component testing is to be documented in Annexure 'B'
- 7.4 Assembled panel testing performance is to be documented in Annexure 'B'
- 7.5 Every line of code and corresponding logic path having statement true/false is to be executed at least once. This facility is available in plc software itself.
- 7.6 The Software integration level test is to be done to test the complete integrated Modules beside testing individually before integrating the components. Once all the module are tested, software integration testing is done by integrating all the modules and the system as a whole is tested. and the result is to be documented in Annexure 'B'
- 7.7 The testing shall be performed with BOP control unit per **Factory Acceptance Test procedure (FAT)**.
- 7.8 In case of failure of the communication between the panels provision of communication fail alarm is to be incorporated through software.
- 7.9 Every line of code and logic path shall be tested as part of white box testing as per Annexure 'E'
- 7.10 Single Unit functionality which provides input v/s output shall be treated as black box testing as per Annexure 'B', Annexure 'F' & Annexure 'A'

8. Software Production and Maintenance as per clause 5.18.6 of API 16D

- 8.1. The modification to existing software shall be reviewed and documented in softcopy (retain old program and modify program)
- 8.2. The PLC software is developed ,deployed and installed under software development life cycle (SDLC) with traceability records.
- 8.3. The Updated software if amended is to be reviewed and documented in softcopy.
- 8.4. The software shall be recorded with its current revision having all the details i.e.date, time, reason, unique identification and name of person conducting change. Software Back-up is to be stored in safe location separately. in Annexure 'H'
- 8.5. Risk assessment is not to be carried out for software security being no external access and internet accessibility to software.
- 8.6. The latest version of manufacturer supplied software platform is to be used to create PLC Programme for control unit. Date of incorporation of latest software platform is to be recorded.



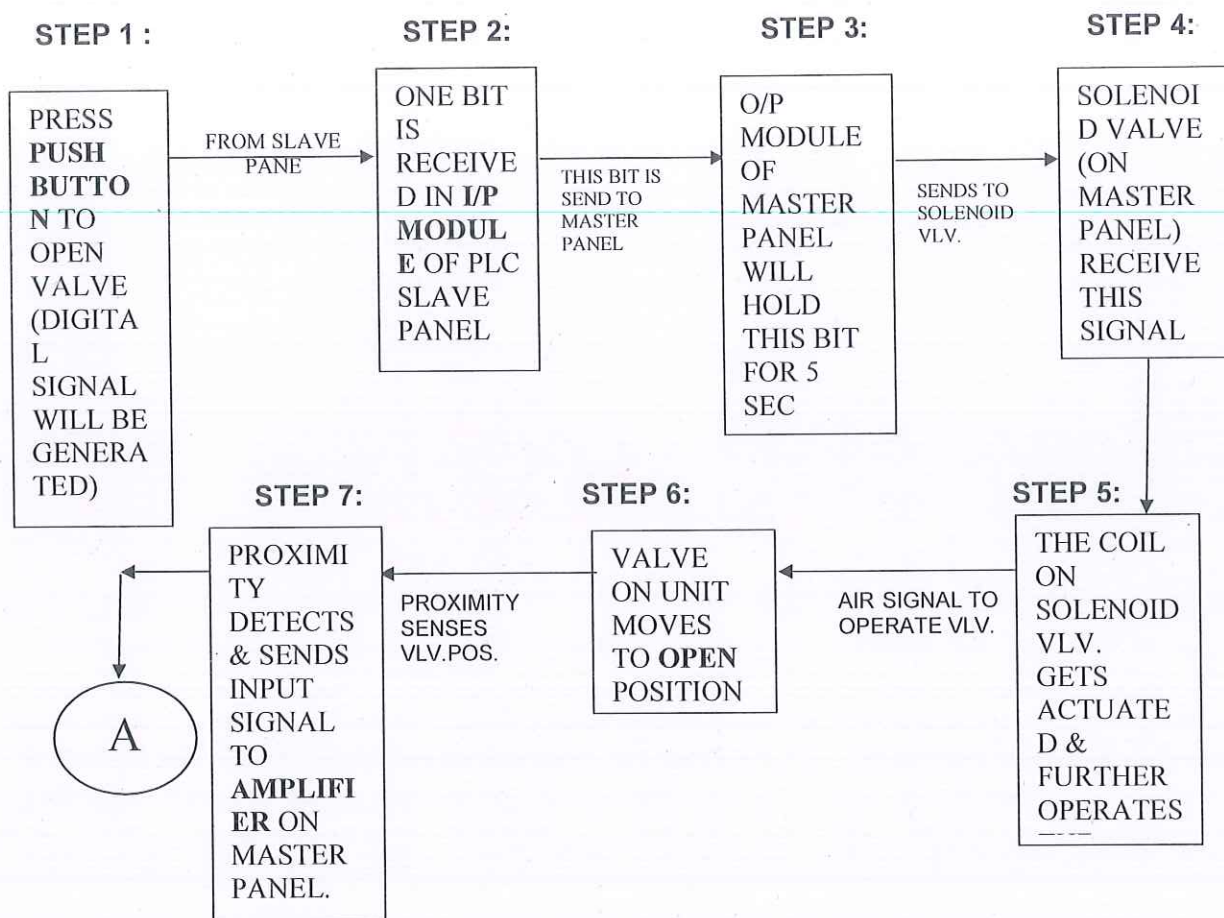
	SARA SAE ENGINEERING SPECIFICATION	
	Section: SES 26 – 853	
	Issue: "A"	Rev No: "0"
	Eff. Date: 17.01.2019	Page: 5 of 24

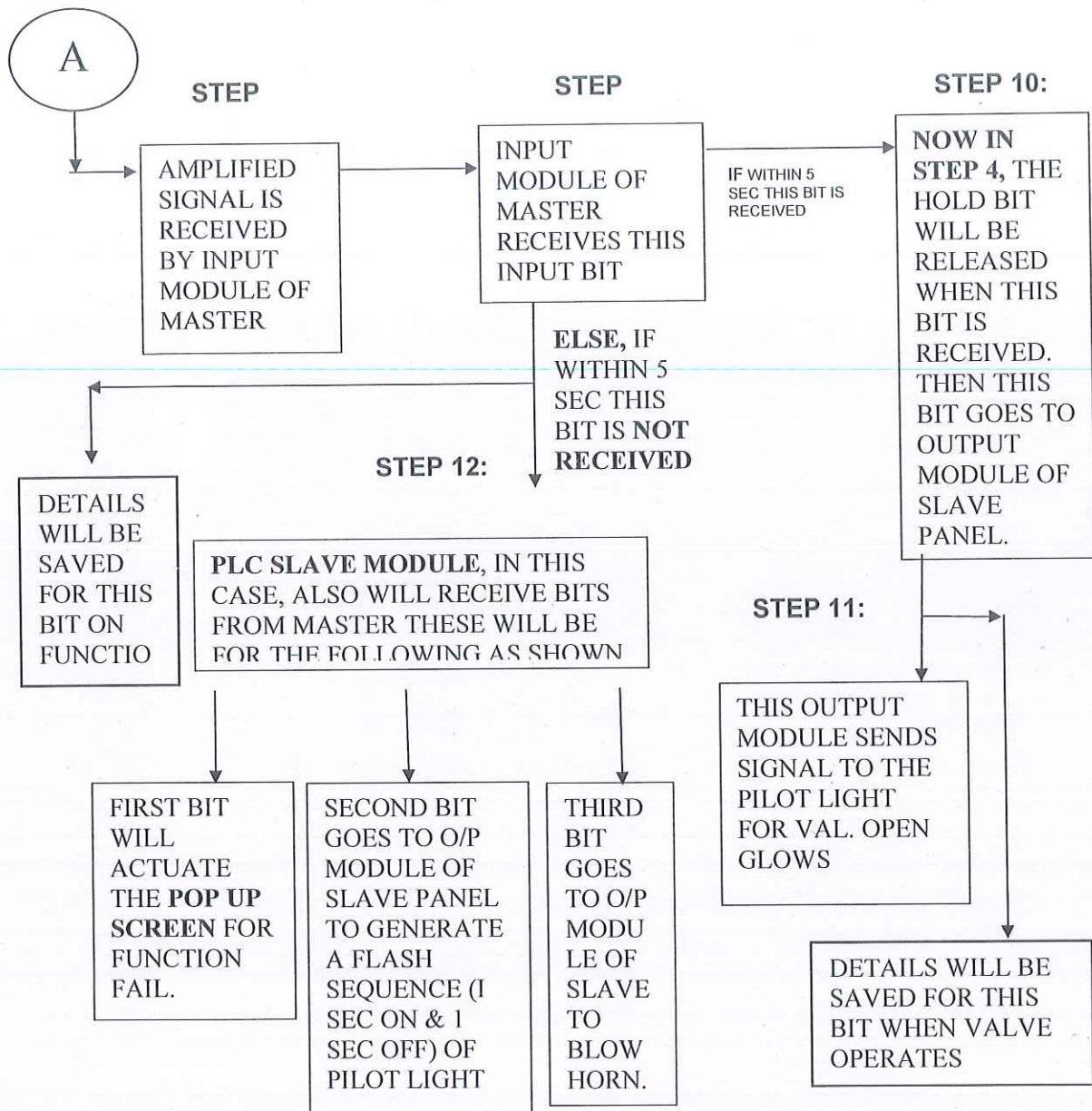
Annexure 'C'

SOFTWARE FUNCTION PROCEDURE FOR PLC SLAVE PANEL

OBJECTIVE: TO CREATE A BLOCK DIAGRAM WHICH WILL SHOW HOW A VALVE CAN BE OPERATED FOR OPEN & CLOSE FUNCTIONS

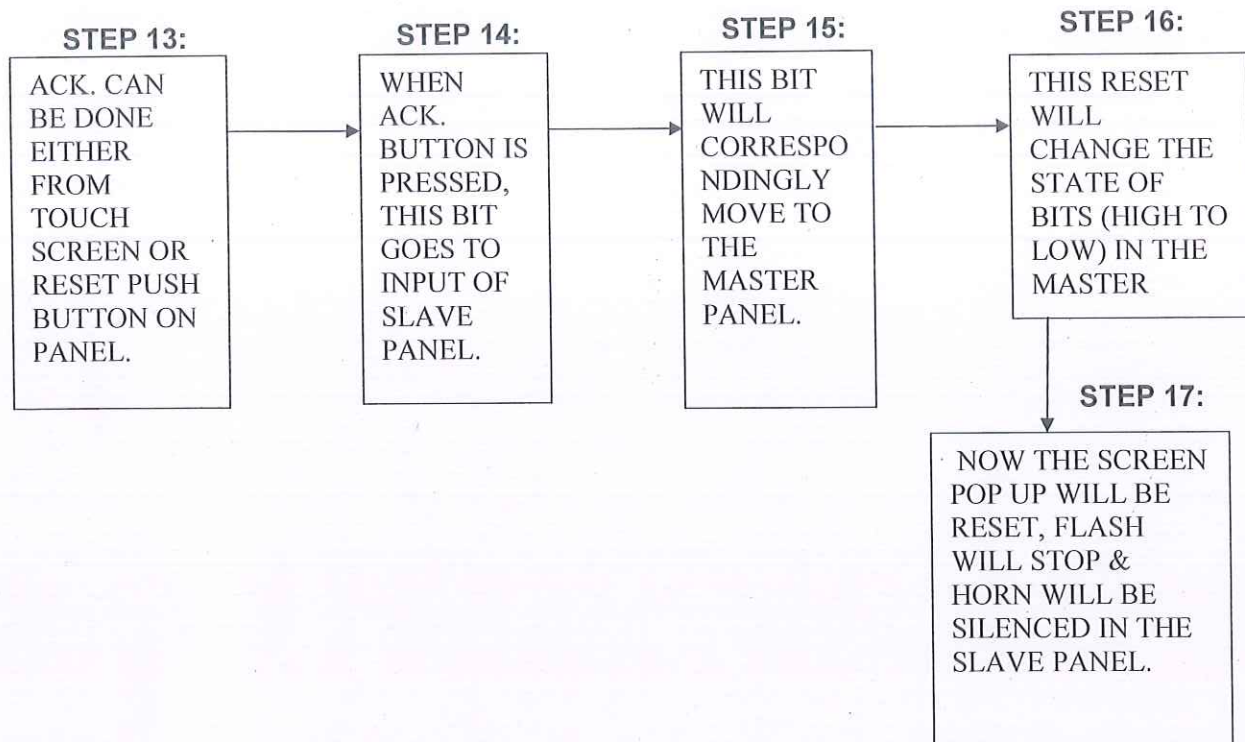
BASIC LAYOUT: (A) FOR OPEN FUNCTION





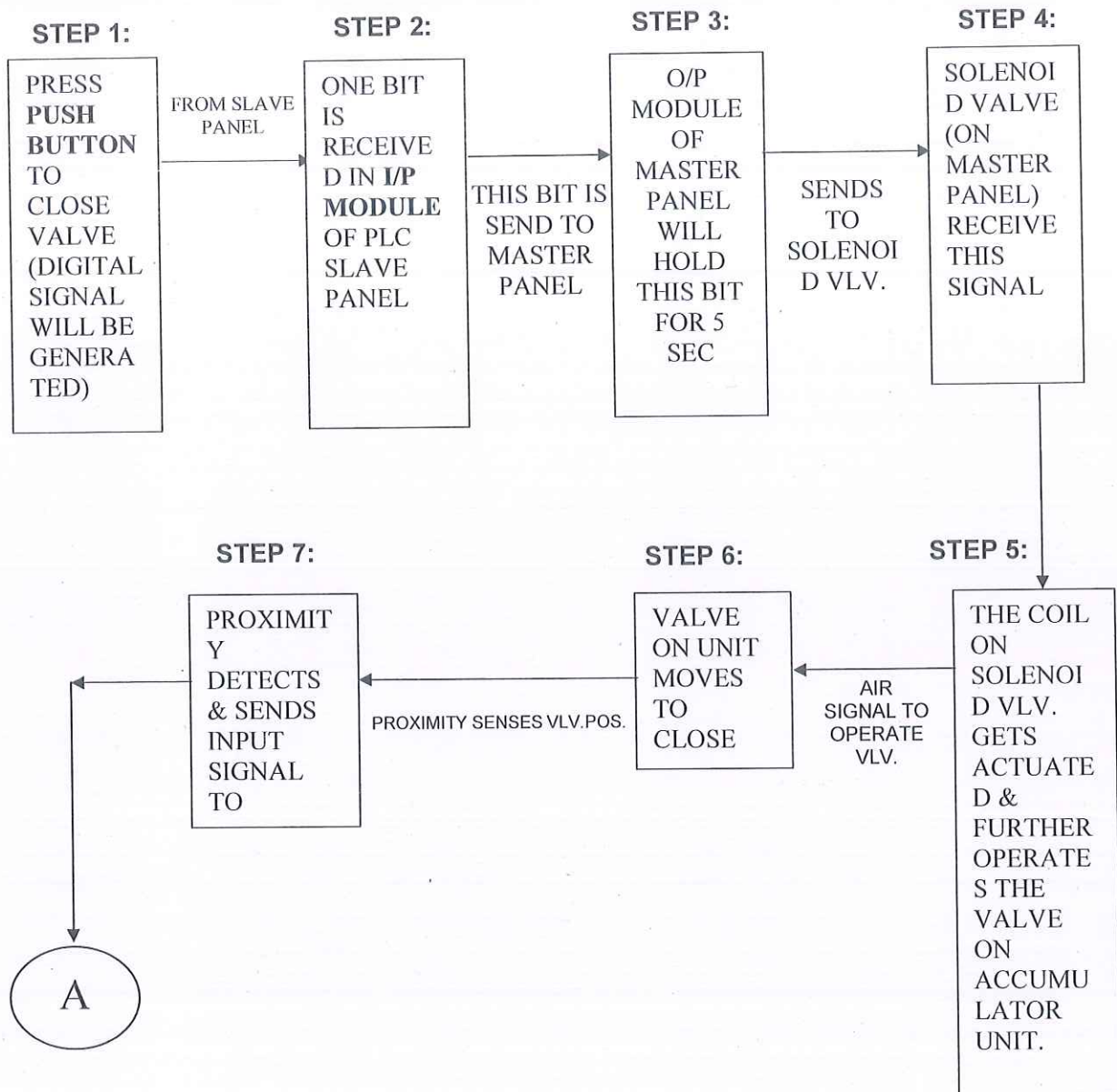
	SARA SAE ENGINEERING SPECIFICATION	
	Section: SES 26 – 853	
	Issue: “A”	Rev No: “0”
	Eff. Date: 17.01.2019	Page: 7 of 24

NOW THESE THREE BITS WILL HAVE TO RESET BY ACKNOWLEDGE (ACK.) BUTTON ON THE SLAVE MODULE.

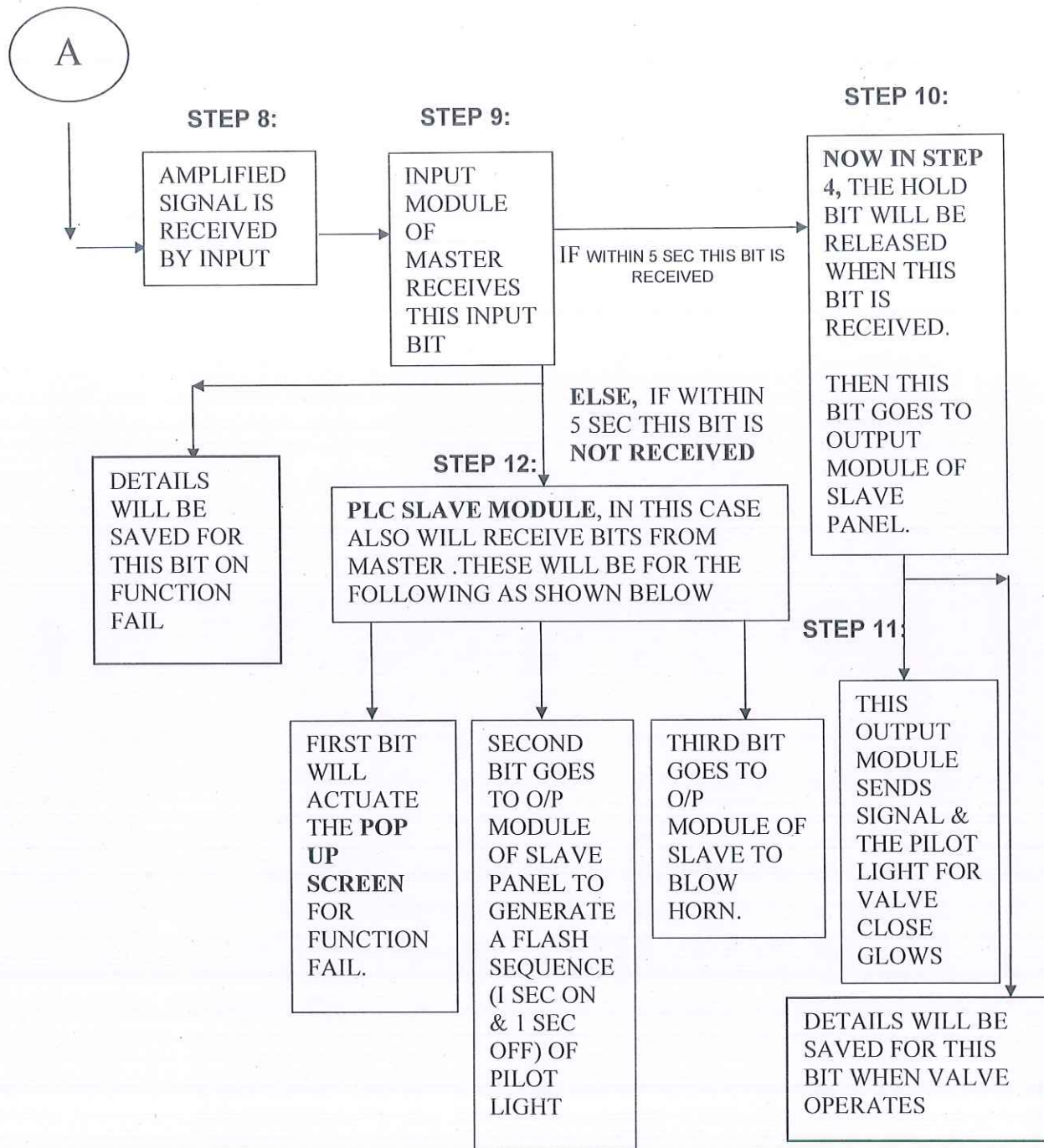


(THIS WILL BE BECAUSE THERE WILL BE NO SIGNAL FROM MASTER PANEL FURTHER)



BASIC LAYOUT: (B) FOR CLOSE FUNCTION


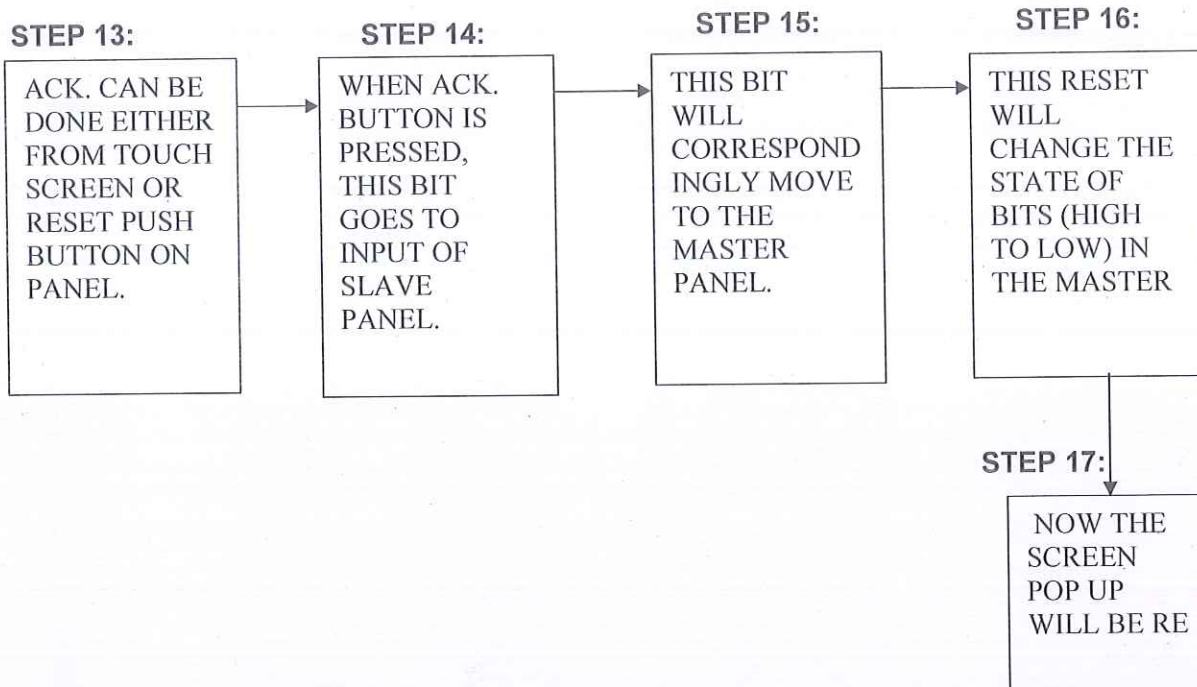
	SARA SAE ENGINEERING SPECIFICATION	
	Section: SES 26 – 853	
	Issue: “A”	Rev No: “0”
	Eff. Date: 17.01.2019	Page: 9 of 24



NOW THESE THREE BITS WILL HAVE TO RESET BY ACKNOWLEDGE (ACK.) BUTTON ON THE SLAVE MODULE.



	SARA SAE ENGINEERING SPECIFICATION	
	Section: SES 26 – 853	
	Issue: “A”	Rev No: “0”
	Eff. Date: 17.01.2019	Page: 10 of 24

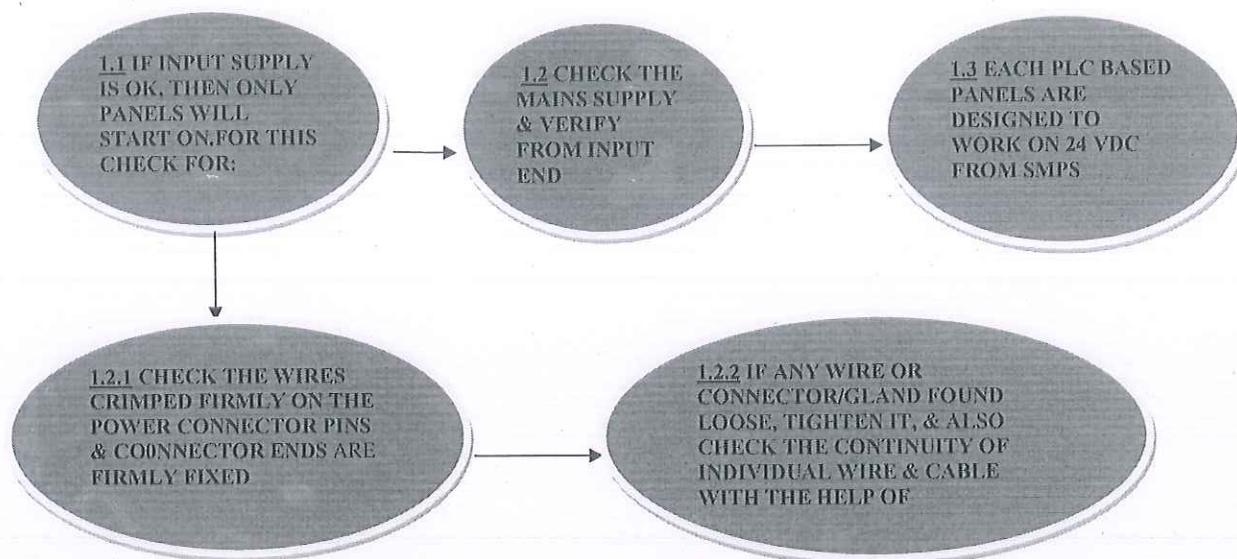


(THIS WILL BE BECAUSE THERE WILL BE NO SIGNAL FROM MASTER PANEL FURTHER)

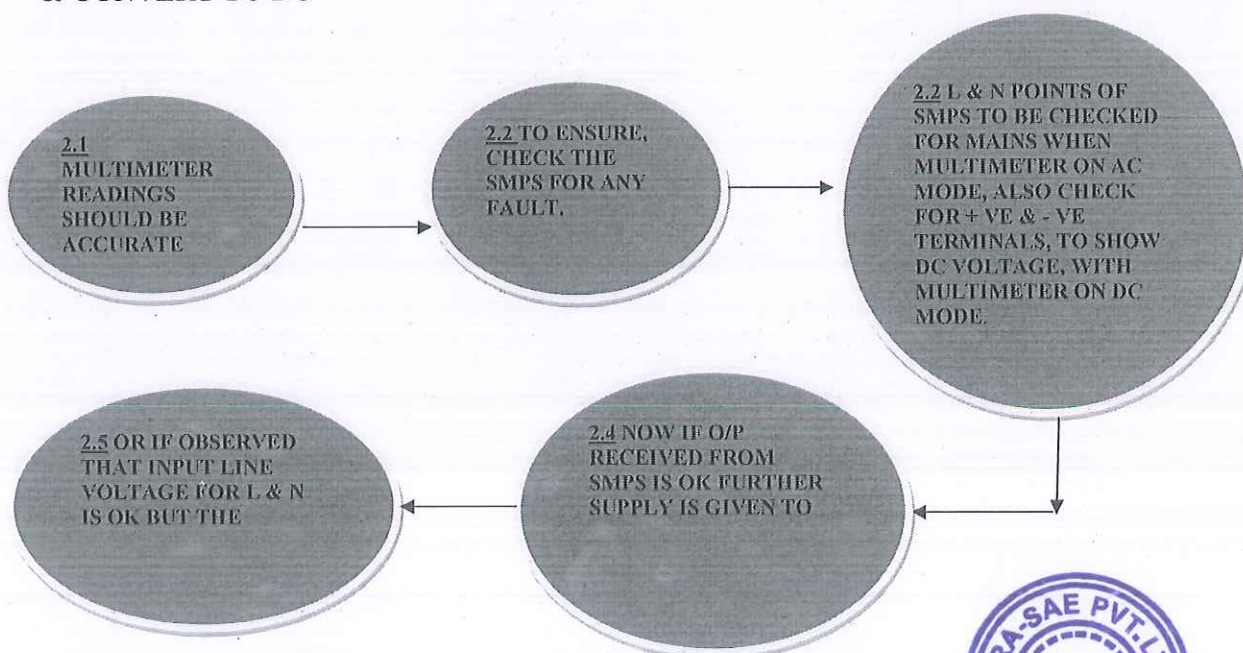


	SARA SAE ENGINEERING SPECIFICATION	
	Section: SES 26 – 853	
	Issue: “A”	Rev No: “0”
	Eff. Date: 17.01.2019	Page: 11 of 24

TROUBLESHOOTING GUIDE FOR SMART CONTROL PLC PANEL
FAULT - 1: ON TURNING ON THE PANEL, NOTHING COMES UP



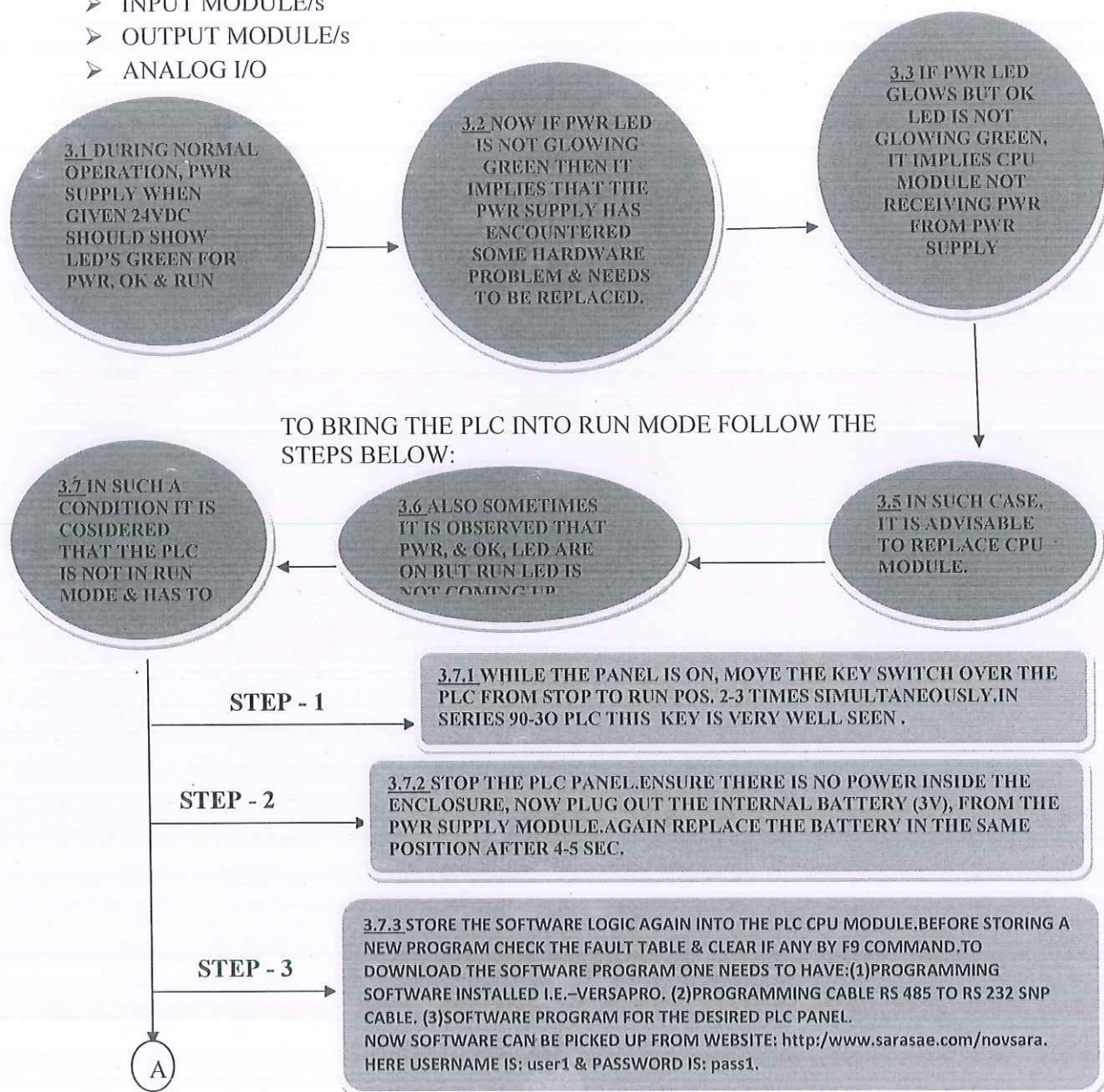
FAULT - 2: AC –DC CONVERTER (SMPS) IS SUSPECTED TO RECEIVE MAINS SUPPLY & CONVERT TO DC

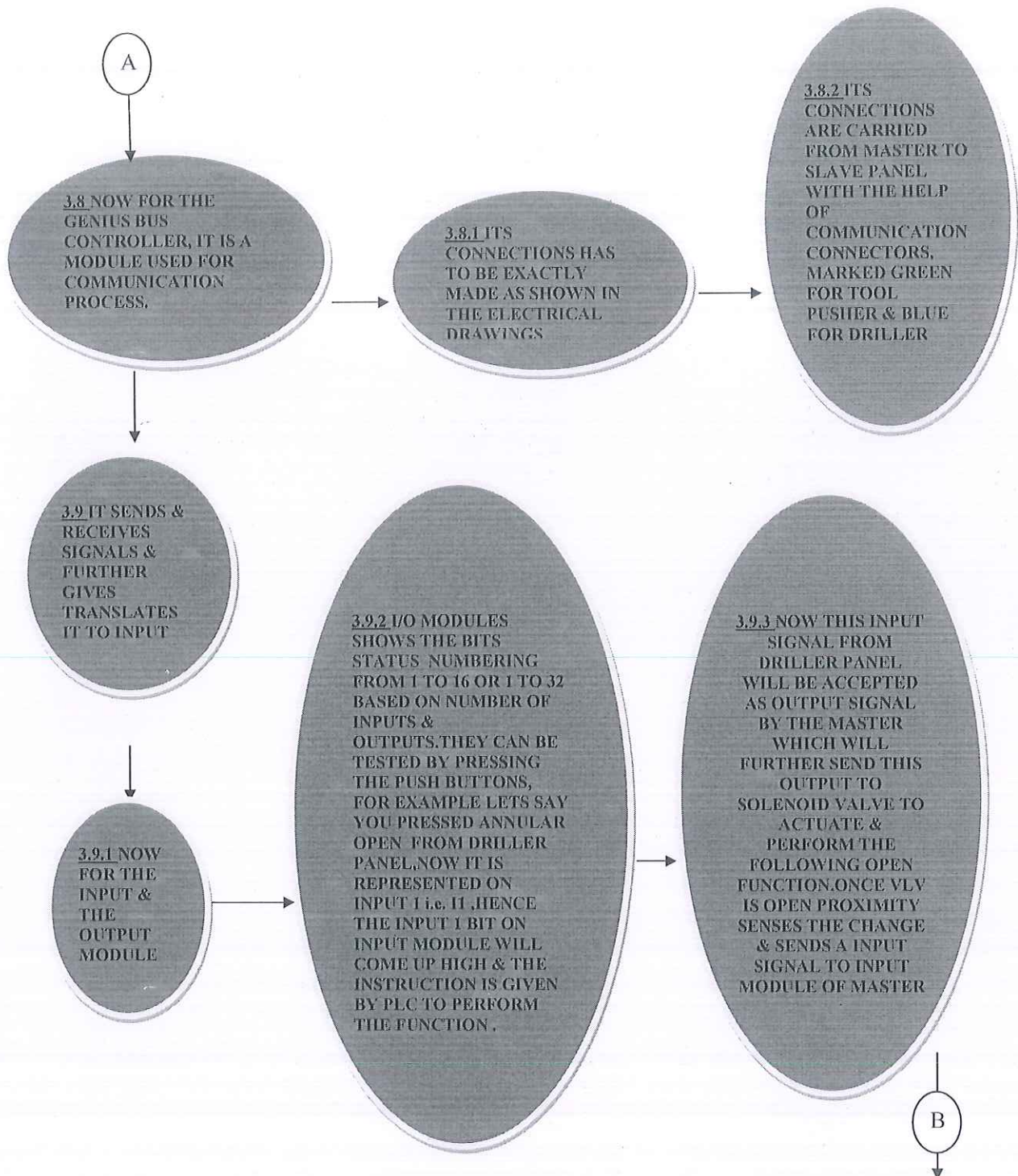


	SARA SAE ENGINEERING SPECIFICATION	
	Section: SES 26 – 853	
	Issue: “A”	Rev No: “0”
	Eff. Date: 17.01.2019	Page: 12 of 24

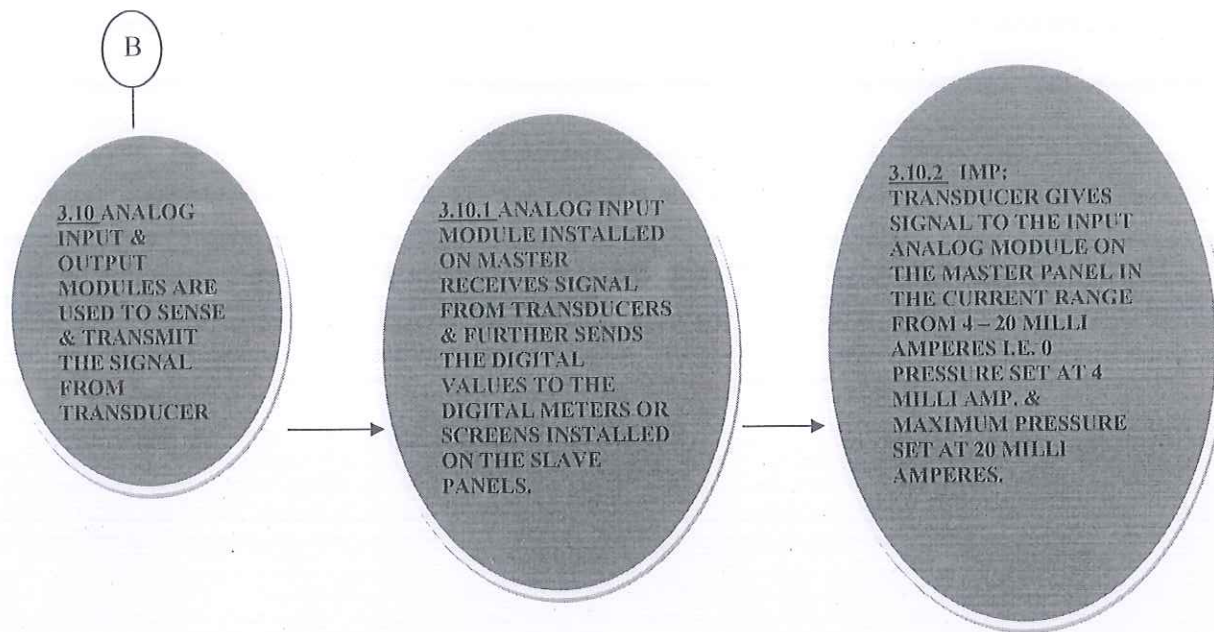
FAULT - 3: PROBLEMS OBSERVED ON PLC MODULES

- POWER SUPPLY
- CPU MODULE
- GENIUS BUS CONTROLLER
- INPUT MODULE/s
- OUTPUT MODULE/s
- ANALOG I/O

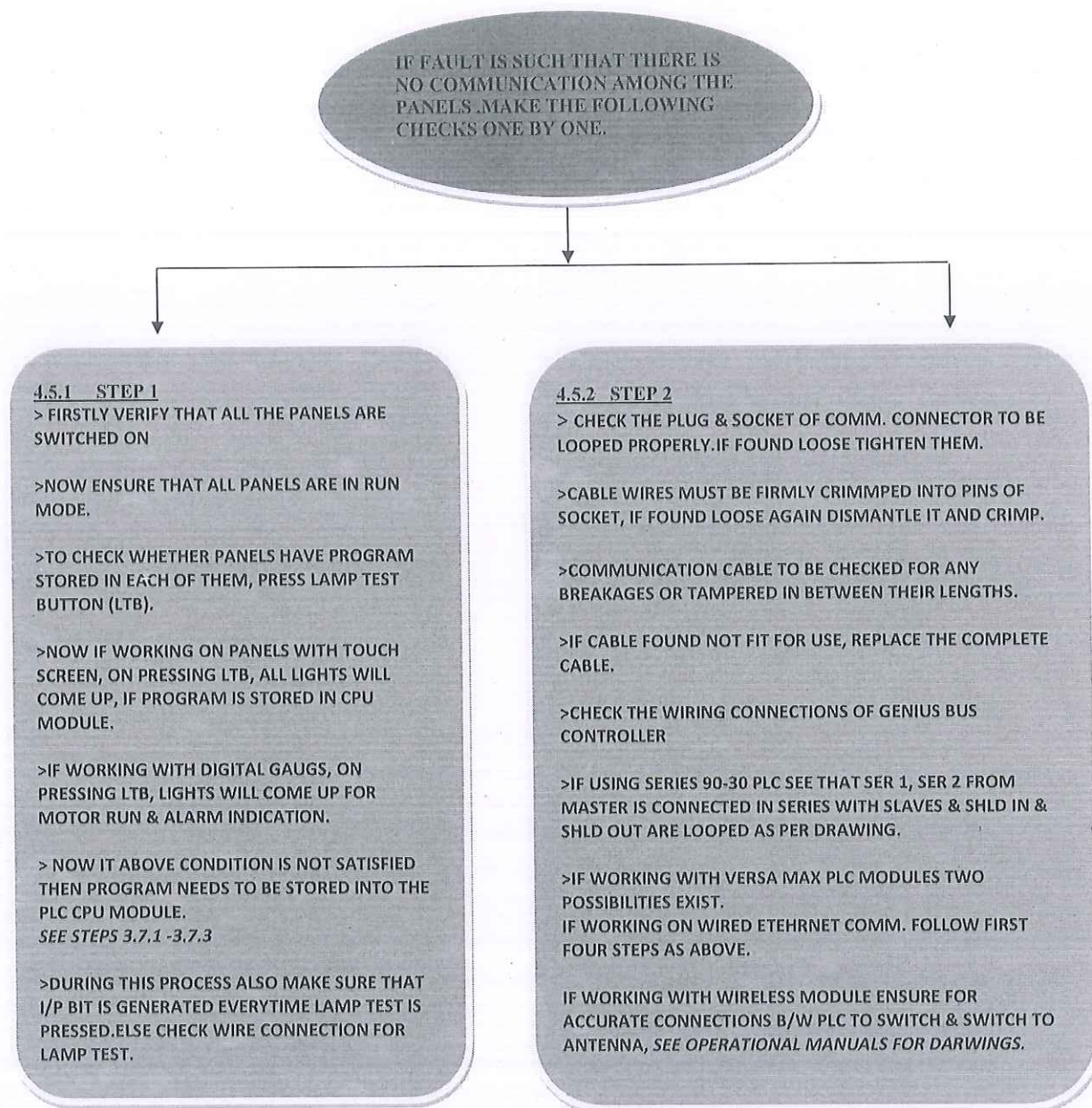




	SARA SAE ENGINEERING SPECIFICATION	
	Section: SES 26 – 853	
	Issue: “A”	Rev No: “0”
	Eff. Date: 17.01.2019	Page: 14 of 24

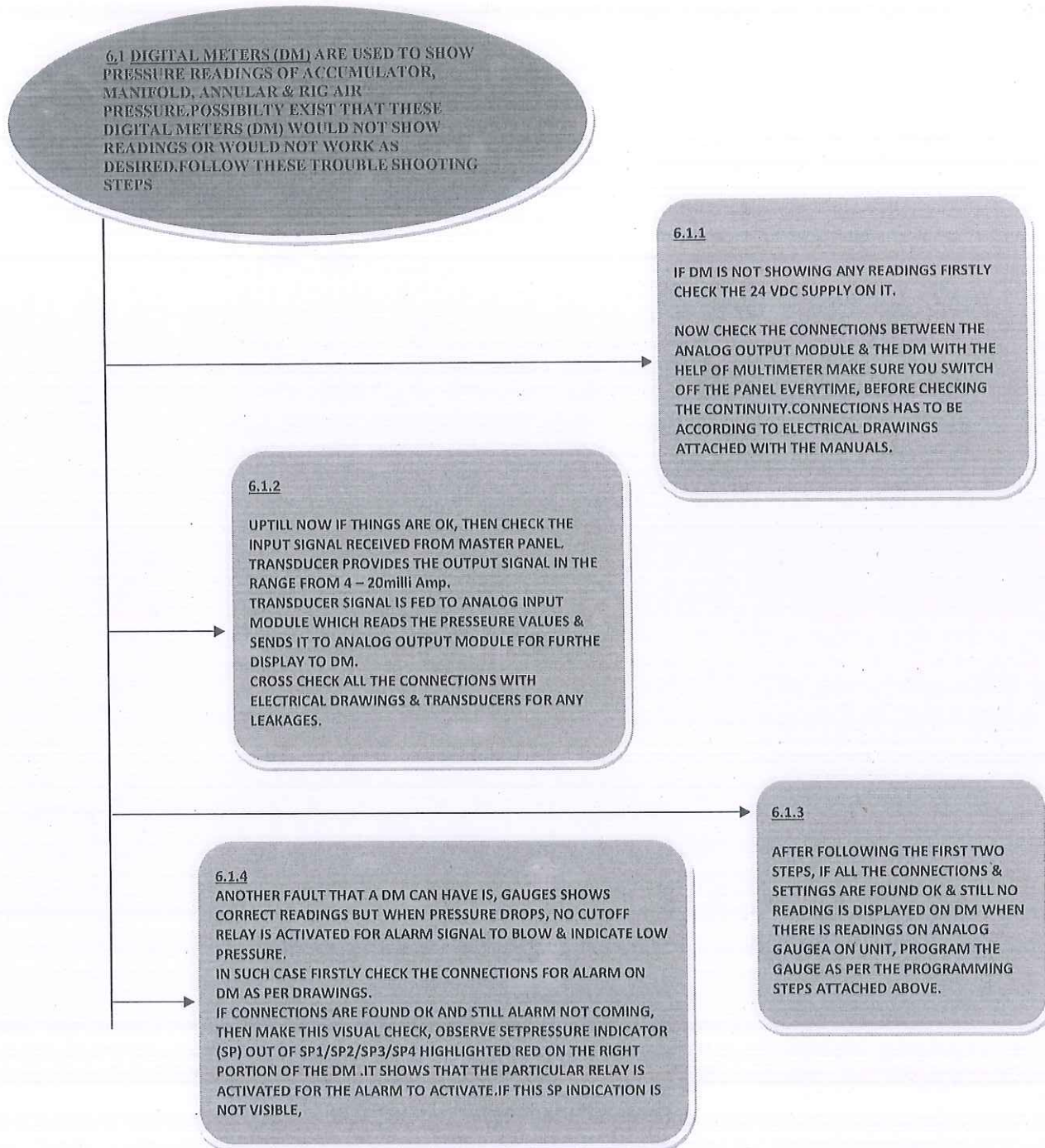


FAULT- 5: NO COMMUNICATION BETWEEN MASTER PANEL & SLAVE PANELS.



	SARA SAE ENGINEERING SPECIFICATION	
	Section: SES 26 – 853	
	Issue: “A”	Rev No: “0”
	Eff. Date: 17.01.2019	Page: 16 of 24

FAULT- 6: NO READINGS IS OBSERVED ON DIGITAL GAUGES



	SARA SAE ENGINEERING SPECIFICATION	
	Section: SES 26 – 853	
	Issue: “A”	Rev No: “0”
	Eff. Date: 17.01.2019	Page: 17 of 24

License -

Order Number: EM00439594

Purchase Order #: 824817U

Software	Qty	Description	Serial Number	Legacy Serial Number	Contract Level	Contract End	Activation Code	Action
PAC Machine Edition	1	Machine Edition v10.0 Professional Development Suite 700 Points	7-43959401-003-001	7-43915201-003-001, 7-43915201-003-002	None		6be0106c-db65-446a-ae0e-b2a4d4d12a9e	Updated
PAC Machine Edition	1	Machine Edition v10.0 Professional Development Suite 700 Points	7-43959401-003-002	7-43915201-003-001, 7-43915201-003-002	None		a4e0ba2a-28bc-4ab0-bdd4-cd167320a73b	Updated

Objectives

Programming Languages are LD, SFC, FBD, CFC and ST.

Ladder Diagram remains popular and easier because of its graphical nature so we used LD (Ladder Diagram).

As with lawn power tools, it is most efficient to use the best programming language for the application, to avoid the complexity of driving the square application peg into the round tool hole. With IEC 61131-

3 programming languages, PLC programming and maintenance are enhanced when the strengths of all the languages are used.

Programming languages: LD, SFC, FBD, CFC and ST

the strengths and best applications Ladder Diagram (LD) and Sequential Function Chart (SFC).

“Which IEC 61131-3 Programming Language is best? Part 2” will discuss Function Block Diagram (FBD), Continuous Function Chart (CFC), Structured Text (ST), and how they can be mixed and matched for optimal results.

What is Ladder diagram (LD) programming?

Ladder diagram programming or LD, traces its history back some 100 years to relay ladder logic (RLL), which was created to describe systems of electrical components such as relays, timers and motors. In the early days of automation, when PLCs were replacing relays and timers, it made perfect sense to create a programming language familiar to the user base and similar to the tool it was replacing. Unfortunately, as controllers became more capable and evolved past relays and timers, the original LD language was pressed into services it was never intended for and was poorly suited.



	SARA SAE ENGINEERING SPECIFICATION	
	Section: SES 26 – 853	
	Issue: “A”	Rev No: “0”
	Eff. Date: 17.01.2019	Page: 18 of 24

This situation was exacerbated by the slow pace at which PLC vendors provided new languages better suited to PLC and programmable automation controllers (PAC) applications. This was particularly true with controllers originating in North America, which explains the global differences in the enduring popularity of LD.

Strengths of LD programming

The strength of LD and the key to its enduring popularity is its graphical nature. Of all the generalizations one can say about engineers, it is safe to say engineers tend to be graphically oriented. (Who among us can effectively communicate without paper and pencil, or a white board?) Early on, most LD programming alternatives were text-based languages that did not resonate with engineers’ graphical nature. This led to further reluctance to move on from LD. Fortunately, that situation is changing.

LD remains a great language for which it was originally intended – complex Boolean logic. Staying within this realm, LD logic is simple to design and simple to debug. Figure 3 illustrates this point by showing the same Boolean logic in several IEC 61131-3 languages. Say we are expecting “Inspect” to be TRUE. How easy is it to determine why the result is not as expected? In LD, the answer is quickly determined by observing where the path of solid blue contacts is interrupted.

Use the right language for control system programming

To communicate effectively in the English language, it’s important to have the right vocabulary and know how to use that vocabulary effectively. To create effective industrial controls programs, it is important to have the right languages and know how to use those languages effectively. IEC 61131-3 provides the languages, and this article has provided guidance on effective use of LD





SARA SAE ENGINEERING SPECIFICATION		
Section: SES 26 – 853	Rev No: "0"	
Issue: "A"	Page: 19 of 24	
Eff. Date: 17.01.2019		

SOFTWARE (REMOTE PANEL)													
Before Corrective Action							After Corrective Action						
S.No.	Items/function	Block Type Subroutine	Design Intentions	Failure Mode	Cause	Local Effects	System Effects	Global Effects	Corrective / Recommended Action	Severity	Detection	Probability Of Occurrence	Risk Priority Number (RPN)
1	Master	Hardware configuration	Remote Operation	Program execution fails to start.	CPU and Modules failure; RAM data corruption; hardware configuration errors at boot not compensated for with diagnostic	PLC goes into STOP mode. Applicable status indicator is lit on CPU module.	loss of ability to operate the BOP RAM/diverter (via remote interface) sequencing timing or interlock function; loss of alarm capability; loss of logging capability.	BOP Ram/Diverter will not operate for open/close	diagnose the problem in PLC program fault table/hardware and rectify	5	6	2	60
									Operate manually selector valve from BOP control unit to operate Ram for open/close	5	2	1	10
									PLC programmer	Completed			
2	Master	Press	Remote Operation	Prepressure Program execution stops.	PLC program may be not correct; hardware configuration errors: Analog input module may be faulted or loose	PLC goes into STOP mode. Applicable status indicator is lit on CPU module.	loss of ability to see all the pressure of the BOP /diverter; loss of alarm capability for pressure; loss of logging capability of pressure.	Could not see all the pressures of BOP control unit.	diagnose the problem in PLC program/hardware and rectify	6	7	2	84
									Operate manually selector valve from BOP control unit to operate Ram for open/close	6	2	2	24
									PLC programmer	Completed			
3	Master	FAULT	Remote Operation	In the event alarm in program execution will stop.	PLC program may be not correct;	Any alarm will not come	loss of ability to come and reset the alarm of the BOP /diverter ;	Could not received the alarm then horn will not blow	diagnose the problem in PLC program and rectify	4	6	2	48
									check the PLC program in FAULT block	4	2	1	8
									PLC programmer	Completed			
4	Master	IP_OP	Remote Operation	operation and feedback of four way valve execution will stop.	Low level hardware failure; Input/output module may be faulty; data corruption.PLC program may be not correct;	4-way valve will not operate and feedback of valve position will also not execute	Loss of operation capability of 4-way valve.	BOP Ram will not operate for open/close	diagnose the problem and rectify	5	4	3	60
									check the PLC program in IP_OP block; also check input and output module	5	2	1	10
									PLC programmer	Completed			



Section: SES 26 - 853

Issue: "A"

Rev No: "0"

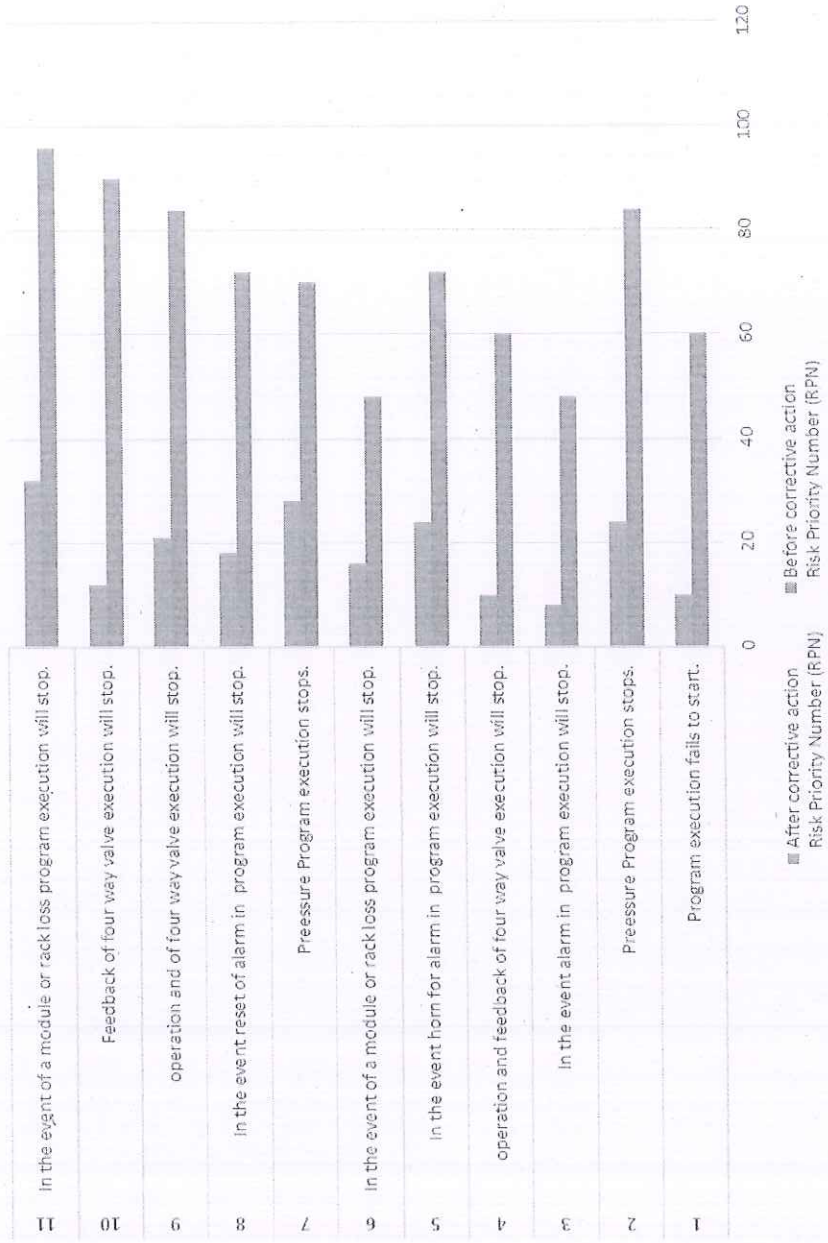
Page: 20 of 24

[illegible]





Risk Priority Number (RPN) Control System For Software (Remote panel)





SARA SAE ENGINEERING SPECIFICATION		
Section: SES 26 – 853		Rev No: "0"
Issue: "A"		Page: 23 of 24
Eff. Date: 17.01.2019		

HARDWARE (REMOTE PANEL)																			
Before Corrective Action										After Corrective Action									
S.No.	Items/ function	Design Intentions	Failure Mode	Cause	Local Effects	System Effects	Global Effects	Corrective / Recommended Action	Severity	Detection	Probability Of Occurrence	Risk Priority Number (RPN)	Current Control	Responsibility	Action Taken and Completion Date	Severity	Detection	Occurrence	Risk Priority Number (RPN)
1	proximity	Feedback of four way valve position.	Feedback of four way valve execution will stop.	Proximity may be faulty;connection loose between proximity to amplifier	Feedback of 4-way valve position will also not execute	Loss of capability to see the position of 4-way valve.	BOP Ram position for open/close could not see	diagnose the problem and rectify	5	3	3	45	check the proximity valve	Assembly department.	Completed	5	2	1	10
2	Solenoid valve	operation and of four way valve execution.	operation and of four way valve execution will stop.	solenoid may be faulty	4-way valve will not execute	Loss of operation capability of 4-way valve.	BOP Ram will not operate for open/close	diagnose the problem and rectify	6	4	3	72	check the solenoid valve	Assembly department.	Completed	6	2	2	24
3	Pushbutton	To operate four way valve.	operation of four way valve execution will stop.	Pushbutton may be faulty	4-way valve will not execute	Loss of operation capability of 4-way valve.	BOP Ram will not operate for open/close	diagnose the problem and rectify	5	3	3	45	check the pushbutton	Assembly department.	Completed	5	2	1	10
4	Pilot light	To see the valve position	Could not see valve position	LED/pilot light may be faulty	No effect	No effect	No effect	diagnose the problem and rectify	5	3	2	30	check the pilot light and LED	Assembly department.	Completed	5	1	2	10
5	Digital Gauge	To see the Pressure Value	could not see the different pressure	Digital Gauge may be faulty	No effect	No effect	No effect	diagnose the problem and rectify	6	4	2	48	check the digital gauge	Assembly department.	Completed	6	1	2	12
6	Amplifier	For Amplify the signal.	Feedback of four way valve execution will stop.	Proximity may be faulty;connection loose between proximity to amplifier	Feedback of 4-way valve position will also not execute	Loss of capability to see the position of 4-way valve.	BOP Ram position for open/close could not see	diagnose the problem and rectify	5	4	3	60	check the proximity	Assembly department.	Completed	5	2	1	10
7	PLC CPU and it's module	For Process the complete cycle	Pressure Program execution stops.	PLC program may be not correct; hardware configuration errors; Analog input module may be faulted or loose	PLC goes into STOP mode. Applicable status indicator is lit on CPU module.	loss of ability to see all the pressure of the BOP /diverter ; loss of alarm capability for pressure ; loss of logging capability of pressure.	Could not see all the pressures of BOP control unct.	diagnose the problem in PLC program/hardware and rectify	8	5	2	80	Operate manually selector valve from BOP control unit to operate Ram for open/close	PLC programmer	Completed	8	2	2	32



Risk Priority Number (RPN) Control System For Hardware (Remote panel)

