VFD RELIABILITY ASSESSMENT AND TRIPPING CIRCUIT SIL EQUIVALENT DESIGN

Paper No. PCIC Europe EUR25_13

Ilya Nariyev
Fluor
Engineering
Farnborough
United Kingdom

Nirav N Chokshi
Fluor
Engineering
Farnborough
United Kingdom

Frieder Endrejat
Fluor
Engineering
Farnborough
United Kingdom

Axel Rauber
ABB
Engineering
Zurich
Switzerland

Jess Galang
ABB
Engineering
Zurich
Switzerland

Abstract – Variable Frequency Drives (VFDs) are used in running important processes like Mixed Refrigerant, Pre-cool Mixed Refrigerant (PMR), Injection Compressors etc. When used in safety applications, it is imperative that VFDs meet their reliability targets as determined by hazard analysis processes such as Hazard and Operability Studies (HAZOP) and Layers of Protection Analysis (LOPA) to trip the electrical equipment when demanded. This issue applies not only to VFDs, but also to the whole electrical chain including upstream High Voltage (HV) switchgear and other disconnecting devices. The key requirement is to make sure that the entire trip circuit meets the Safety Integrity Level (SIL) requirement, e.g. SIL2 or SIL3, according to Functional Safety Standards such as IEC 61511-1 [1] and IEC 61508 [2].

Performing reliability assessment of electrical trip circuits can be a complex task as it may involve numerous components. Often such components may not have the reliability data available in the form of a safety manual or a SIL certificate. In such cases, it may be necessary to justify the design based on the data available. The Functional Safety Standards also demand a level of redundancy in the design for higher SIL levels to achieve a level of Hardware Fault Tolerance (HFT). It may be difficult to achieve HFT electrically in some cases. Some circuits may involve energize-to-trip arrangements, e.g. for HV switchgear. This would require assessment of the failure modes of associated motive force such as power supplies, to make sure a common cause failure of power supply does not degrade the trip functionality.

The purpose of this paper is to provide an overview of reliability assessment of VFD system design and the challenges that may be faced when performing their reliability assessments. Examples of typical trip circuits encountered will be given together with solutions that can be considered. The examples in this paper may not be suitable for all applications as the intention of the paper is to provide educational aspects of the Safety Instrumented System (SIS) and VFD system design complexities.

Index Terms – VFDs, trip circuits, SIL, SIS, reliability.

I. INTRODUCTION

Many industrial facilities are increasingly moving toward complete electrification with minimal or no use of local gas turbines. This trend will in future only be increasing with the global shift to zero carbon emissions.

For gas or steam driven compressors, there may be requirements when a delayed shutdown is not acceptable, as it possesses the risk to human lives and/or may cause expensive equipment damage, leading to significant operational constrains and/or revenue loss. One of the Significant consequences may lead to the release of a large number of hydrocarbons especially, when immediate shutdown is not guaranteed.

Traditionally, high power compressors are driven by turbines where safety loops are designed for reliable fault detection and fast response to prevent mechanical failure and catastrophic damage. SIL loops with high reliable sensors, robust voting logic and certified fuel valves or pneumatic trip system ensures reliable and fast shutdown. This obviously differs when the compressors are driven by the VFDs, where the final tripping element is either HV Circuit Breakers (CBs) or VFD itself.

Some critical processes require reliable equipment to operate. However, what is even more important is that this equipment or systems can trip reliably on demand. This requirement may result in the equipment or system being safety-related with an appropriate SIL rating specified for them by a reliability assessment study e.g. HAZOP and LOPA. TABLE I below provides the Probability of Failure (PFDAvg) and Risk Reduction Factor (RRF) requirements for individual SIL levels as specified in [2].

TABLE I
SIL RELIABILITY DATA

SIL	PFDavg	RRF
1	$10^{-1} – 10^{-2}$	10 – 100
2	$10^{-2} – 10^{-3}$	100 – 1000
3	$10^{-3} – 10^{-4}$	1,000 – 10,000
4	$10^{-4} – 10^{-5}$	10,000 – 100,000

Complexities of the tripping circuits, especially within HV CBs show the importance of the design consideration while specifying requirements for how CB(s) can be tripped.

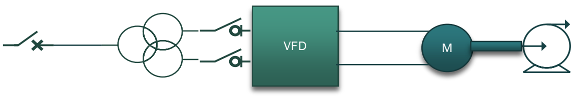

Fig. 1. Large VFD Typical Configuration.

The complete tripping circuit may include the VFD itself and the upstream switchgear. To guarantee successful tripping, at least the switchgear CB(s) or the VFD must isolate the power. The trip can be done as “energized-to-trip” or “de-energized-to-trip” in both VFD and switchgear CB(s) depending on the selected equipment and design considerations. Therefore, both VFD and CB(s) may act as final elements for power isolation.

Within the VFD and switchgear there may be multiple redundancies built-in such as redundant auxiliary power supply, trip coils (shunt and undervoltage), and auxiliary relays and therefore one or more SIS trip signals can be routed to switchgear and/or the VFD to enhance reliability design.

With the VFD, in contrast to switchgear, normally there will not be any physical power isolation due to absence of switching devices, however torque and power to the motor can be removed electronically.

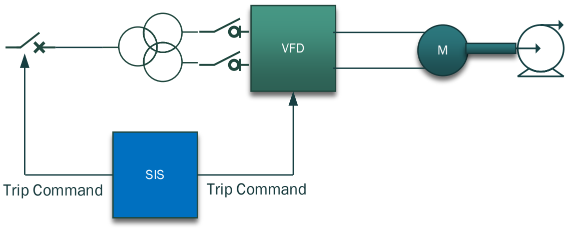

Fig. 2. Large VFD SIS Trip Arrangement.

There may be optional disconnectors on both line input and output to allow the motor sides to open on no-load for maintenance purposes, but those are not considered for power isolation on demand.

Design of the complete high power VFD system, which includes HV CB, Transformer and VFD, may not be SIL certified, which leads to the importance of the design evaluation of the complete VFD system equipment in terms of reliability.

Some requirements for VFDs in relation to functional safety:

TABLE II
FUNCTIONAL SAFETY REQUIREMENTS

Customer Requirements	Customers may demand functional safety evaluation before purchasing equipment Customers may use it as a Technical Quality Specification (a single statement in their specification results in several requirements for the supplier)
Regulations	Some regulatory bodies require or encourage functional safety evaluation
Internal Requirements	Legal protection / Product Liability Internal organization Safety and Reliability requirements
Market Acceptance	Having a functional safety certification maintains a product’s competitiveness in the marketplace
Legislation	Legislative requirements, such as some European Directives, require a functional safety evaluation
Insurance Companies	Insurers may require a FS evaluation before equipment is installed in the workplace, or may provide discounted premiums for using products evaluated for functional safety

For the applications focused on in this paper, the "low demand mode" is usually applied, where the frequency of demands is not greater than once per year, considering the target of uninterrupted operation for several years. In this context, a quick restart is not required, and it is acceptable or even desirable to trip the CBs in case of an emergency.

II. VFD SIL AND RELIABILITY DESIGN

A. General

The applications considered require a shaft power rating exceeding 5,000 kW, often reaching several tens of megawatts. For instance, Mixed Refrigerant (MR) compressors in large-scale Liquefied Natural Gas (LNG) liquefaction plants can exceed 50 MW. Consequently, Medium Voltage (MV) VFD systems are utilized, with output voltages of 3.3 kV and higher. Additionally, speed control of the compressors is a fundamental requirement, meaning that only full VFD systems are considered. Soft-starting and direct-online operation are not within the scope of this discussion.

B. Semiconductors and VFD Topologies

Unlike Low Voltage (LV) VFDs, high power MV VFDs utilize different semiconductors. As discussed in [3], key selection criteria for high power VFD technology include safety, reliability, availability, and maintainability at a low cost. The optimization of these criteria depends on the VFD vendor's philosophy. Notably, functional safety has not been the primary focus when selecting semiconductors and topologies for different power ranges.

Semiconductors can be categorized into two groups:

1. Off-State Semiconductors: These semiconductors remain in an off-state if the gate driver is disconnected or without power. Examples include Insulated Gate Bipolar Transistors (IGBT) and Phase-Controlled Thyristors (PCT).
2. Undefined-State Semiconductors: These semiconductors do not have a defined state if the gate driver is disconnected or without power. An example is the Integrated Gate-Commutated Thyristor (IGCT).

Various topologies are chosen by manufacturers, including Cascaded H-Bridge (CHB), 3-level Neutral Point Clamped (NPC), Modular Multilevel Converter (MMC or M2C), and Load Commutated Inverter (LCI). From a functional safety perspective, the choice of topology is of minor relevance.

C. Functional Safety relevant for large VFDs

According to [4] following categories of stop functions are distinguished:

1. Stop Category 0
   This is stopping by immediate removal of power to the machine actuators, i.e. an uncontrolled stop.

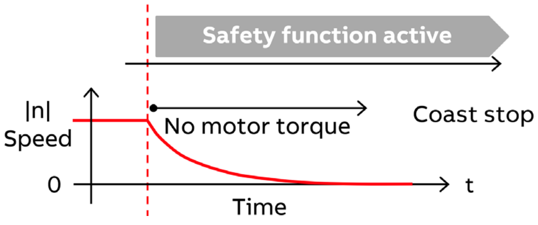

Fig. 3. Stop Category 0

This safety sub-function corresponds to a “Safe Torque Off” (STO) in accordance with [5].

2. Stop Category 1
   This is a controlled stop with power available to the machine actuators to achieve the stop and then removal of power when the stop is achieved.

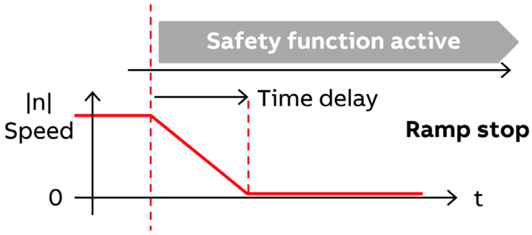

Fig. 4. Stop Category 1

This safety sub-function corresponds to a "Safe stop 1" (SS1) in accordance with [5]. [5] gives three options, to initiate and control the motor deceleration (-d), to initiate and monitor it (-r) or to initiate deceleration and remove power after a fix delay (-t) as indicated in the Figure above.

3. Stop Category 2
   This is a controlled stop comparable with Stop Category 1 but with power remaining available to the machine actuators.
   This safety sub-function corresponds to a "Safe stop 2" (SS2) in accordance with [5]. Also, here there are the same options as mentioned for SS1: (-d), (-r) and (-t).

D. Implementation of Functional Safety

Stop Category 2 is not typically offered by large drive suppliers. This is because certifying the firmware for motor control and other core functionalities would require significant effort. Given that such certification is not mandated for most applications, the effort to achieve and maintain it is not justified.

Stop Category 0 and 1 can be handled with two base concepts:

1. Depending on a Circuit Breaker (CB)
   When initiated by a "Safety Function Input" (SFI), a Safety Logic (SL) acts on a circuit breaker of the VFD and not on the signal from the semiconductor gate driver (GD).

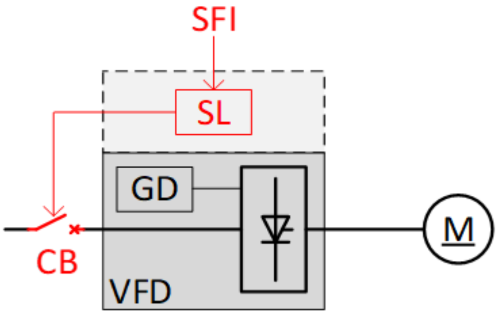

Fig. 5. Functional safety depending on CB

SFI can originate from a safety Programmable Logic controller (PLC) or push button for example. The SL could be a dedicated safety relay or an integrated control safety device. The SL may or may not be part of the VFD. Particularly if it acts on the CB, which is external to the VFD, there is no clear advantage to integrating it within the VFD.

2. Preventing semiconductor gate firing
   Here, the SL output is used to prevent the firing/gating of semiconductors.

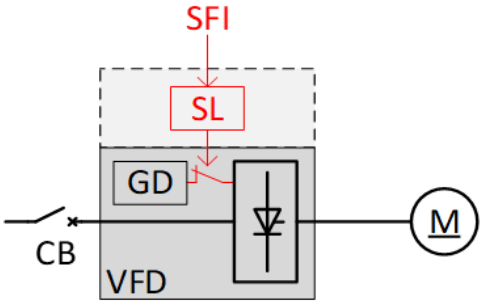

Fig. 6. Functional safety output prevents gate firing

For the approach based on "preventing semiconductor gate firing" the SL is integrated into the VFD. These safety function modules provide a straightforward method to enhance the safety features of VFDs and are designed and offered by some VFD manufacturer, especially in LV applications. LV VSD solutions are widely used where machine safety is essential to safely increase the level of automation in factories (e.g. conveyor systems). For these applications the "high demand mode" is applied, where, as per [8], the Safety Instrumented Function (SIF) is performed with a frequency of demands greater than once per year. Additionally, it is advantageous that the CB can remain closed to enable a quick restart. The available LV solution can often not be implemented one-to-one in MV VSDs due to the more complex topology and/or the use of "Undefined-State" semiconductors, although there are other means such as blocking the optical firing impulse to the semiconductor. Furthermore, especially for high power applications like large compressors "high demand mode" solutions are not required, and the tripping of the CB is acceptable or even desirable as mentioned above.

E. Achievable SIL

For higher SIL applications (e.g. SIL3), there is a requirement in [2] to provide redundancy in the final element subsystem design. This can be achieved by combining the approaches discussed in Sections II.D above as shown in Figure 7.

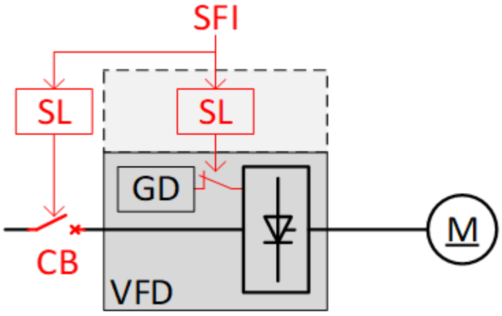

Fig. 7. Functional safety output prevents gate firing and trips the CB for high SIL

It is also possible to add an output CB to achieve the same result, avoiding the dependency on the input CB, which might be high voltage (e.g. 132 or 150 kV) and also saving inrush energization stress on the feeding transformer.

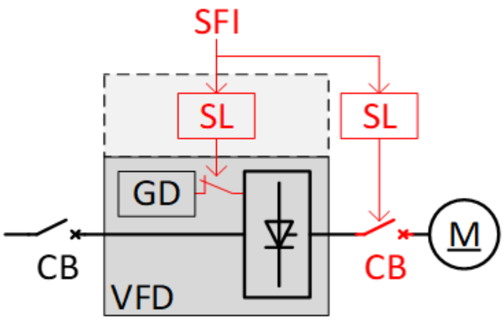

Fig. 8. Functional safety output prevents gate firing and trips the output CB for high SIL

The flexibility can also help to accommodate "brownfield" projects where part of the equipment already exists, thereby avoiding costly replacements.

Most Common relevant Functional Safety Standards and key takeaways for MV VFDs on demand is presented in Table III.

TABLE III
FUNCTIONAL SAFETY REQUIREMENTS

IEC 61508 Parts 1-7 Core Functional Safety Standard for electrical safety-related systems	**ISO 13849-1** Safety of machinery – Safety-related parts of control systems	**IEC 60204-1** Safety of Machinery – Electrical equipment of machines	**IEC 61800-5-2** Adjustable speed electrical power drive systems: Safety requirements – Functional
Definition of Safety Integration Levels (SIL) and their requirements.	Definition of Performance Level (PL) and their requirements.	Categories of Emergency Stopping Functions (e.g.): Stop Category 0 Stop Category 1 Stop Category 2 These functions are typically used for emergency situations such as electrical or mechanical/process emergency. **Note** "Emergency Switching Off" is another functional category.	18 Safety sub-functions are listed in the standard. Among all, "Stopping functions" are listed below: Safe Torque Off (STO) Safe Stop 1 (SS1) Safe Stop 2 (SS2) These functions are typically used for routine processes of daily operation, as well as a part of emergency procedures.

III. HV DISTRIBUTION SCHEMES CONFIGURATION

Regardless of the MV VFD development, and consideration for electronic power isolation, the primary isolating device for MV VFD systems is upstream switchgear. The important aspect for consideration is to evaluate the configuration of this switchgear.

Multi-MWs driven loads are critical for successful process operation and any nuisance tripping or/and loss of power may result in significant downtime with revenue and reputational losses. Therefore, selection of the distribution system design in many instances is not driven by the SIS requirements but for electrical reasons, including providing reliable power supply to the VFD driven loads. Consequently, distribution arrangements where two HV CBs feeding the same load are often met in the industry.

Number of possible configurations available like Double Bus and Single Breaker, Breaker and a Half, Breaker and a Third, Double Bus, and Double Breaker etc.

Normally, there are no isolation devices between VFD and their respective converter transformers. As for example a 24-pulse transformer would lead to four devices. Disconnectors are very rarely added as part of the VFD anyway. When they are included, it is not for functional safety purposes but to provide a visible disconnection and maybe grounding, allowing safe maintenance work on the equipment. However, even in these cases, they do not offer benefits since the upstream part still depends on de-energizing the CB.

Therefore, upstream switchgear reliability has an important role to play in making sure of isolation of the process of VFD driven loads.

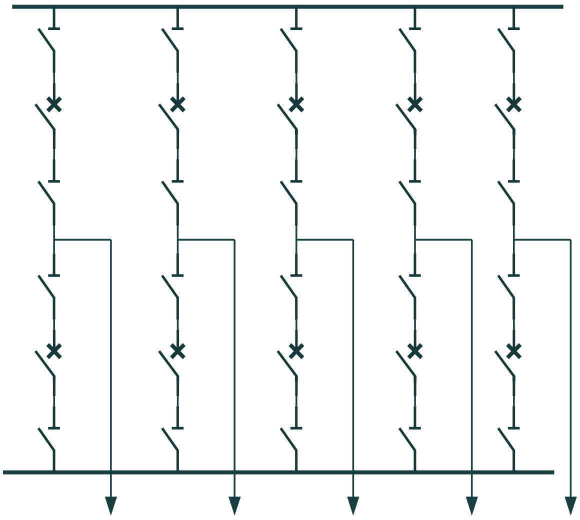

Fig. 9. Double Bus Double Breaker HV Scheme Configuration.

Equally, for important industrial processes, availability of power supply also plays an important factor. Here, highly reliable switchgear configuration schemes are required, where upon the nuisance trip of a single CB, power supply to the load is not compromised.

For the cases where the distribution schemes may incorporate multiple CBs that serve the same load (Double Bus and Double Breaker or Breaker and a Half), it would be necessary that two or more CBs are isolated to interrupt the power successfully.

To achieve this level of confidence in design, certain redundancies need to be introduced in the tripping circuit of the CBs.

One of the benefits of the switchgear configurations is that due to redundant CBs, a certain level of diagnostics and testing can be done in addition to normal testing of some tripping circuits like relay monitoring and trip circuit supervision. An example is a complete trip of one of two CBs servicing the same VFD driven load. This will allow testing of complete CB tripping circuits on a regular basis without impact on the VFD driven load operation. Obviously, such considerations should be addressed in the design stage and a required control scheme to be introduced. In addition, this may be considered for regular plant turnaround timing.

IV. HV SWITCHGEAR CIRCUIT DETAILS

High power VFD driven loads in a range from a few ten MWs to approximately hundred MWs are normally connected to HV switchgears (e.g. 110 – 132kV), which as a standard incorporate some level of redundant design. This may include two independent trip circuit power supplies (UPS1 and UPS 2) and redundant trip coils (TC). In addition, relay protections are also redundant and moreover for very critical applications, it is common to use relays from different manufacturers or as a minimum, different models.

Protection considerations for high power VFDs, with a breaker and a half feeder scheme, are provided in [6]. The SIS inputs are addressed in [6] as well, however the impact of this topology on the SIL assessment is not described. As discussed in [6], details of the VFD protection, other schemes like Double Bus and Double Breaker will have identical considerations as two CBs are servicing a single load.

There are multiple tripping circuits arrangements available, and they are heavily customized depending on the project requirements.

One of the key constraints for HV switchgear configurations is that it is not always possible to use “de-energized” to trip configuration, as undervoltage TC cannot always be used for HV switchgears. HV switchgears are equipped with shunt TC by default, which are “energized” to trip by nature. This will lead to introducing interposing relays for converting “energized” SIS signal to “de-energized” signal within CB tripping circuit. As discussed in [7], the traditional shunt trip coil is normally specified, and their use is chosen for operational and electrical reasons and not associated with safety instrumented function. A primary function of circuit breakers is to clear faults. However, if the circuit breaker fails to trip, there are various mechanisms to still clear the fault, e.g co-ordinated upstream tripping, breaker failure detection etc. This is another reason why “de-energized to trip” is normally not used from an electrical protection perspective.

V. DESIGN CONSIDERATIONS

This section presents a design consideration of reliability assessment of an HV switchgear trip circuit based on a Double Bus and Double Breaker topology for a VFD driven motor. This can also be applied as a reference for switchgear design where two CBs serve the same load.

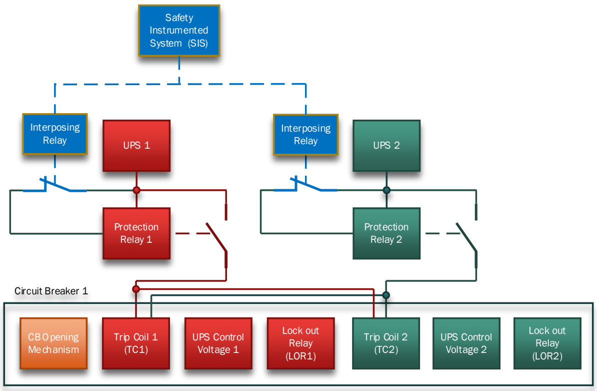

Fig. 10. High Level Tripping circuit of individual CB.

Such HV switchgear topologies are often used where high availability of power supply is required. Typical tripping circuit of the single CB is shown in the Fig. 10.

For the design consideration, it is assumed that a HAZOP analysis followed by SIL determination using a risk matrix method is completed which has identified a SIL2 SIF to trip a compressor motor on detecting the trip signal. Figure 11 shows the overall SIF architecture. The sensors, which are configured as 2oo3 can be applicable for many processes such as pressure, level etc. depending on the driven load application.

The SIF is modeled in a SIL verification tool where the reliability data of the sensors, logic solver, and the final elements are provided as input together with the details such as proof test intervals, diagnostic coverage etc., to verify that the achieved PFDAvg is within the requirements defined in TABLE I and [2]. While the reliability data for sensors and logic solvers are readily available, for electrical circuit associated with the VFD driven load, a detailed analysis needs to be carried out as below to calculate the overall failure rate of the circuit.

1. Analyze schematic diagram of the trip circuit to identify the components that are associated with the safety function of the trip circuit, i.e. the components that may impact the operation of both CBs from opening on demand
2. Obtain the failure rates data for all such components participating in the tripping on demand
3. Develop a fault tree model of the trip circuit to calculate the overall Probability of Failure (PFDAvg) for the trip circuit. Use such PFDAvg value to then obtain the dangerous failure rate of the trip circuit for use in a SIL verification tool.

The section below illustrates the analysis carried out for each of the three steps above. Step 1: Analysis of Trip Circuit Design

Figure 12 shows an overview schematic of the components involved in the trip circuit for the compressor motor. For high reliable switchgear topologies, the VFD driven motor will be supplied from two HV Circuit Breakers, whereby if any of the CB supplies are lost and tripped, the feeder will remain energized from the other CB. This means that to trip the compressor motor, both CBs need to be isolated, i.e. a 2oo2 trip requirement.

Many manufacturers publish typical Mean Time Between Failure (MTBF) data and other reliability data for equipment. There are also some standards which show a MTBF like standard [8].

In this design, the following components were assumed and considered:

- Relays IR1/IR2 are used in the CB tripping circuit for the scenario where there are no undervoltage trip coils available. Therefore, an intermediate relay is required to convert SIS “de-energized-to-trip” signal to “energized-to-trip signal” to act on a CB shunt trip coil. This should introduce more pessimistic and more complexity with an expected lower reliability data scenario.
- For simplicity, two identical protection relays are used for these applications, where both relays have 100% redundant function.
- Circuit Breaker reliability data varies significantly across manufacturers and therefore some typical value is considered to this paper, whereas detailed calculation is recommended for each case.
- Redundant power supply is also assumed for this application where each DC UPS power supply is 100% redundant. UPS1 and UPS2 are provided for this application.

The trip command from SIS to the breaker is received via two redundant, “de-energize-to-trip” digital output contacts. These contacts drive two interposing relays IR1 and IR2. The Normally Closed (CO) contacts from IR1 and IR2 are then wired to protection relays REL1 and REL2. These protection relays provide additional protection functions associated with the circuit breaker, which themselves also lead to a trip of the motor. Relays REL1 and REL2 convert ‘de-energize-to-trip’ outputs from SIS to ‘energize-to-trip’ outputs that are then interfaced to the shunt tripping coils of the CBs. Two separate power supplies, UPS1 and UPS2, are used to provide redundancy in the case of loss of a single power supply. The relays REL1 and REL2 can also be chosen to be of different makes or models to reduce common cause failures between them.

Each circuit breaker comprises two shunt trip coils as a minimum, TC1 and TC2, both can trip the breaker. The control voltage of the TC is also supplied from UPS1 and UPS2. Loss of a single UPS control voltage for a trip would not prevent CB from opening as it is fully redundant configuration.

As shown in Figure 12, both CBs share the same trip arrangements, i.e. the trips from REL1 and REL2 relays are sent to both CBs, such that any of the relays can trip both breakers.

It is noted that the VFD itself was not considered as a final element that can be used to isolate the supply. VFD manufacturers do however have the capability to receive a SIS input, and this practice is also described in [6]. The VFD SIS input and its associated SIL certification should be considered as part of the overall safety scheme. This integration may reduce the requirements for the switchgear tripping scheme (e.g., to achieve SIL 2) or enhance the system where higher integrity levels (e.g., SIL 3) are needed. Some VFD vendors offer a “Preventing Semiconductor Gate Firing” feature, as outlined in Chapter II–D, which can for example, already be SIL 2 certified. Incorporating this functionality can improve the probability numbers for the overall safety scheme. In contrast, other VFD vendors rely on the CB-based functional safety features, which typically provide limited added value, as the CB is usually already included in the safety architecture.

VI. STEP 2: ANALYSIS OF FAILURE RATES

Failure rates for all components in the trip circuit were identified from relevant manufacturer’s documents, standards or certificates. These are listed in [8] or publicly available. It is noted that apart from IR1/IR2 relays none of the other components were SIL certified as such. It was considered that the failures listed in Table IV be used conservatively to analyze failure rates. In doing so it was assumed that all failures obtained from MTBF are dangerous undetected and that there are no online diagnostics involved in any of these components.

The task of making correct assumptions and failure rates may lead to significant differences in the results, therefore this step requires careful analysis to be carried out of failure rate data.

VII. STEP 3: FAULT TREE ANALYSIS.

A fault tree can be constructed to calculate the probability of failure of the VFD driven load to trip on demand from SIS. Figure 13 shows the resulting fault tree diagram.

TABLE IV
COMPONENT FAILURE RATES IN THE TRIP CIRCUIT

Component	MTBF (Years)	Failures and Hour	Failure Rates (Per 109 Hours (FITs))				
			λDU	λDD	λSU	λSD	λNE/RE
Interposing Relays (IR1/IR2)	130	8.78E-7	3.60	0	-	0	-
Protection Relay (REL1)	29	3.936E-6	3,936	0	-	0	-
Protection Relay (REL2)	29	3.936E-6	3,936	0	-	0	-
Circuit Breaker	1,000	1.14E-7	114	0	-	0	-
Trip Coils	27	4.228E-6	4,228	0	-	0	-
Power Supplies (UPS1/UPS2)	114.16	1E-6	1,000	0	-	0	-

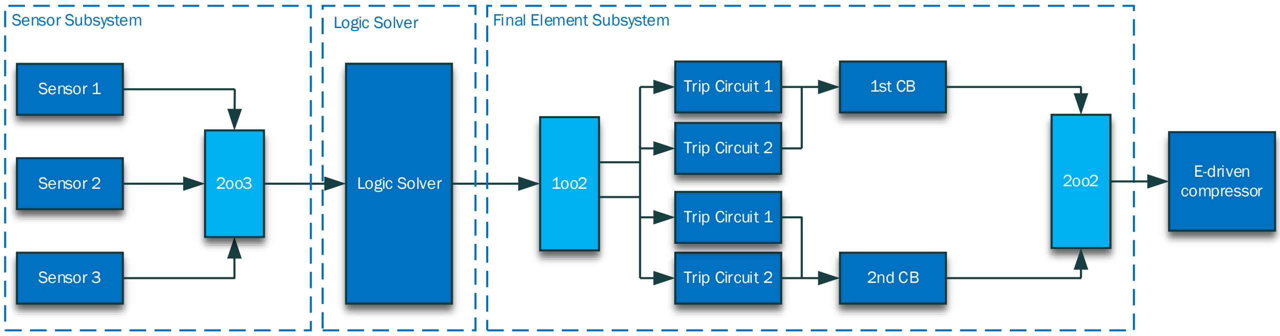

Fig. 11. Overview SIF Architecture for High-High (HH) Trip Signal.

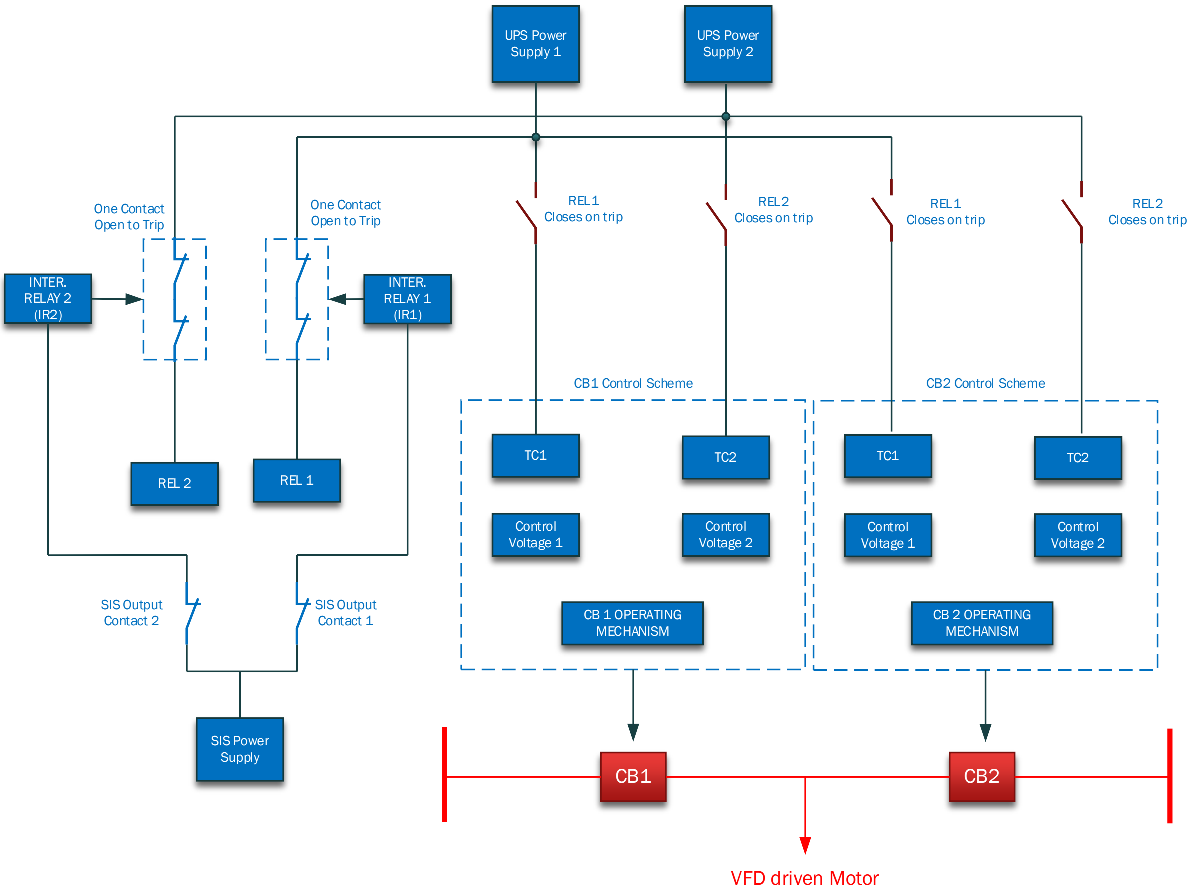

Fig. 12. Overview Schematic Diagram of Trip Circuit.

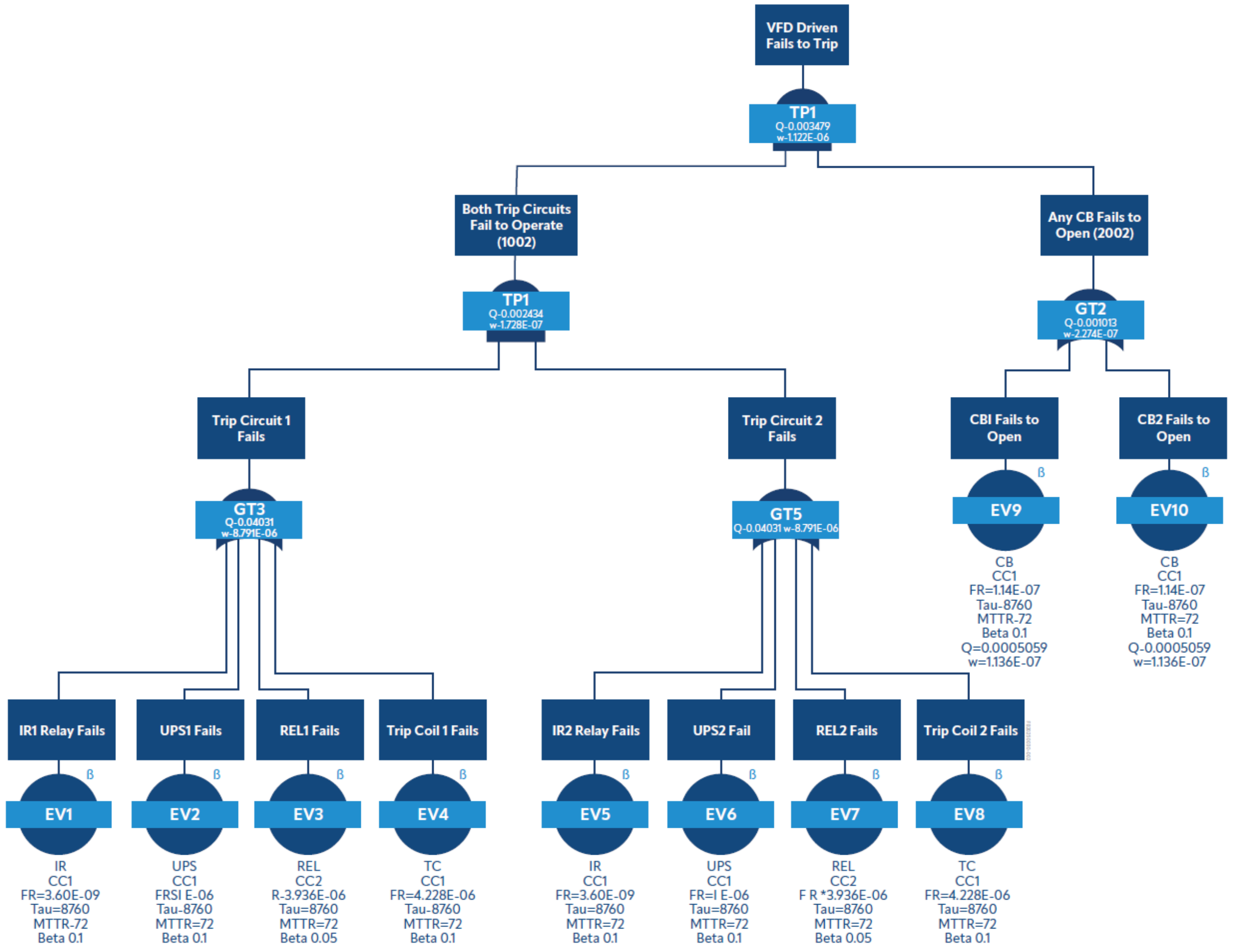

Fig. 13. Fault Tree Analysis (10 Years Proof Test Interval).

The top event “VFD driven load failed to trip” can occur if at least one of two CBs fail to open on demand. Each CB may fail to open if there is a fault within the breaker or if there is a fault with both trip circuits and associated devices. It may be possible to use the component failure rates of the CB to derive the overall failure rates as is done in [9], however for the purposes of this paper a single failure rate representing the whole breaker is used according to TABLE V below. The two trip circuits are considered redundant, and both must fail on demand to result in the breakers not opening. Important to note is that for HV switchgear, BF – Breaker Failure – protection is provided and if CB commanded to trip on demand fails, then BF protection of the next CB upstream may be activated and this may enhance the protection of the VFD, but a complete failure of the trip circuits is considered, which includes BF protection. BF protection introduces a time delay in tripping the VFD system, which may not always be acceptable as discussed in Chapter I.

The fault tree is developed using [2] failure model for the base events. TABLE V shows parameters used in modelling the base events and the associated common cause events. The parameters are selected according to criteria below:

- Dangerous Failure (%): This represents the % of total failures that are dangerous. This is assumed as 100% for all components.
- Dangerous Coverage (%): This represents the % of dangerous failures that can be detected by internal diagnostics within the component. This is assumed to be 0% for all components.
- Safe Coverage (%): This represents the % of safe failures that can be detected by internal diagnostics within the component. This is assumed to be 0% for all components.
- Proof Test Coverage (%): This represents the % of failures that can be detected by proof test coverage. A single number of 90% is used for all components as a conservative number.
- Test Interval: This represents the proof test interval for the trip circuit and is taken as one year or 8,760 hours.
- Overhaul Interval: This represents the ‘mission time’ or overhaul period for refurbishing or replacement of the components. This is retained as 20 years for typical HV CB and is assumed to be 10 years as the mission time for all other components.
- MTTR: This is taken as 72 hours for all major components.

TABLE V
BASE EVENT PARAMETERS IN FAULT TREE ANALYSIS

Component	Dangerous Failure (%)	Dangerous Coverage (%)	Safe Coverage (%)	Proof Test Coverage (%)	Test Interval	Overhaul Interval	MTTR (Hours)	Beta Factor (%)
Interposing Relays (IR1/IR2)	100	0	0	90	1 year	10 years	72	10
Protection Relay (REL1)	100	0	0	90	1 year	10 years	72	5
Protection Relay (REL2)	100	0	0	90	1 year	10 years	72	5
Circuit Breaker	100	0	0	90	1 year	10 years	72	10
Trip Coils	100	0	0	90	1 year	10 years	72	10
Power Supplies (UPS1 & UPS2)	100	0	0	90	1 year	10 years	72	10

Beta Factor: This represents the common cause factor for individual components. This is taken as 10% (or 0.1) for all components apart from redundant relays. While these two components are diverse, they are considered to have a smaller common cause based on the similar internal components, therefore a common cause factor of 5% or 0.05 is used and is common to both relays.

For the purposes of simplicity, no common cause failures were modeled for individual components.

VIII. RESULTS INTERPRETATION

Evaluation of the fault tree provides the overall unavailability of the final element subsystem including trip circuits and the CBs to isolate the power supplies from the motor. For the overhaul interval of 20 years, the results entail a PFDAvg of 3.479E-03. This value is then used to calculate the composite failure rate of the final element sub-system based on a simple formula of PFDAvg = (lambda * TI)/2 where lambda is the failure rate to be calculated, and TI is the test interval. With test interval of 1 year or 8,760 hours, this gives the failure rate of 7.94E-7 failures per hour. This failure rate was then used in the SIL verification tool to calculate the overall PFDAvg for the entire SIF. For a given set of failure rate data for sensors and logic solver (not included here for brevity), this results in a PFDAvg of 7.32E-03 or the RRF of 137, i.e. the SIF achieves SIL2 level from a PFDAvg perspective.

It is noted that SIL verification according to [1] also requires additional consideration of architectural constraints and systematic capability of the SIF design to achieve the overall SIL level of the SIF. Architectural constraints demand a level of redundancy or so-called Hardware Fault Tolerance (HFT) built into the trip circuit design. According to [8], an HFT of 0 (no redundancy) is acceptable for SIL1 and SIL2 applications, however for SIL3 an HFT of 1 is required, which entails at least two independent channels of trip circuit design is required. The systematic capability aspect investigates the aspects of design and development of trip circuit design and associated components to eliminate systematic errors in the design and manufacturing process. More details on this can be found in [2] standards.

IX. CONCLUSION

This paper showed that based on reasonable design considerations, SIL2 level of reliability may be achieved for VFD system related power isolation. However, the detailed calculation is heavily dependent of the input data such as CB or its associated components safety numbers. One of the important aspects to note is that SIL 2 was achieved with 1-year test interval, and this is not always possible. For many industries, 5-year or even 6-year uninterrupted operation is required. This may be mitigated by providing redundant VFD system or for switchgear configuration with redundant parallel breakers, one breaker may be tested at a time without interrupting VFD driven load operation. The paper also illustrates the merit in developing MV VFDs further that utilize SIS inputs reliably, in conjunction with breaker trip schemes to increase the required test interval.

Further work for CB design and VFD technology may lead to even a higher level i.e. SIL3, which may be possible for two parallel means of isolation meeting certain SIL criteria.

X. ACKNOWLEDGEMENT

The authors acknowledge Jon Bradshaw (Chief Electrical Engineer at Fluor Limited UK) for performing an internal review of the paper and his associated contributions.

XI. REFERENCES

[1] IEC 61511-1 (Edition 2.1) Functional safety – Safety instrumented systems for the process industry sector Part 1: Framework, definitions, system, hardware and application programming requirements

[2] IEC 61508-1 (Edition 2.0) Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements

[3] A. Rauber, Peter den Bakker, “Adjustable Speed Drive System Comparison VSI and LCI for High Power Applications,” PCIC United States 2018.

[4] IEC 60204-1 (Edition 6) Safety of machinery – Electrical equipment of machines – Part 1: General requirements

[5] IEC 61800-5-2 (Edition 2.0) Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional

[6] B. Pandya, D. Haas, A. Pandya, I. Constantin, “Considerations for the Protection of Adjustable Speed Drive Installations,” proceedings of the IEEE Petroleum and Chemical Industry Technical Conference, 2022.

[7] SIL Verification of Safety Instrumented Functions, Technical Report, ISA-TR84.00.02-2022. 1 January 2022.

[8] IEEE 493-1997 – IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems (Gold Book)

[9] ISO 13849-1:2023 (Edition 4.0) Safety of machinery – Safety-related parts of control systems

XII. VITA

Ilya Nariyev is a Chartered (UK) Electrical Director, at Fluor Corporation, who graduated with a BSc (Hons) from Karaganda State Technical University in Kazakhstan in 2004 and started his career with one of the Fluor's joint ventures in the same year. In 2008 he joined Fluor Corporation in the United Kingdom and in 2013 obtained his MSc degree from the University of Manchester, United Kingdom. He is a Subject Matter Expert in Variable Speed Drives, Motors, and Power System Studies. ilya.nariyev@fluor.com

Nirav N Chokshi is a Senior Design Engineer at Fluor Corporation. He holds a B.Eng degree in Instrumentation and Control from Gujarat University, India in 1995 and a PhD degree in Process Control and Automation from University of Cambridge, UK in 2003. He is a Subject Matter Expert in Safety Instrumented Systems at Fluor and is affiliated to IEC 61508 [2], IEC 61511 [1] and IEC 61512 maintenance committees as the UK expert in functional safety for process applications.
nirav.n.chokshi@fluor.com

Frieder Endrejat is a Chartered (UK) Electrical Director, at Fluor Corporation, who graduated with a B.Eng and M.Eng from the University of Pretoria, South Africa in 1997 and 1999, respectively. He received a Ph.D. in electrical engineering from University of Cape Town South Africa, in the field of MV Adjustable Speed Drives in 2010. He was with Sasol from 1999 to February 2020 which included electrical leadership on complex and mega projects. He was employed at Air Products from March 2020 to December 2023. Since January 2024 he has been with Fluor UK, Farnborough. He has worked on energy transition projects/proposals in the fields of Carbon Capture, Hydrogen and Green Hydrogen from March 2020 to present. He is a Senior Member of IEEE.
frieder.endrejat@fluor.com.

Axel Rauber graduated from the Staatliche Studienakademie Baden-Württemberg, Mannheim, Germany in 2001 with a degree in electrical engineering – Diplom-Ingenieur (BA). In 2001 he started his professional career at ABB System Drives and is currently employed as a global product manager. He is responsible for VSI and LCI based products for high power applications. He has authored three previous papers.
axel.rauber@ch.abb.com

Jess Galang graduated from the University of Alabama, Tuscaloosa (USA) with a BScEE degree. He is the Head of Product Management and is Global Product Manager for the ACS6000 and ACS6080 converters at ABB System Drives in Switzerland. He has been working for ABB in the power electronic and converters industry for 15 years with various application experience.
jess.galang@ch.abb.com

This paper was developed with the permission of Fluor as part of Fluor's P4 Program. Note that the views expressed in this paper may be directed to a large audience and may not be suitable for any particular client, project or situation. Fluor does not provide any warranties relating to the content of this paper, and your use or reliance on it is at your own risk.