SPRING21
+17TH GCPS
A Joint AIChE and CCPS Meeting

"Is Your SIF Trying to Do Too Much?"

Arthur M. (Art) Dowell, III, PE
Process Improvement Institute, Inc.
2437 Bay Area Blvd, PMB 260
Houston, TX 77058-1519
Adowell@piii.com

PROCESS IMPROVEMENT INSTITUTE

©2021 Process Improvement Institute, Inc., all rights reserved

Prepared for Presentation at
American Institute of Chemical Engineers
2021 Spring Meeting and 17th Global Congress on Process Safety
Virtual
April 18 - 22, 2021

AIChE shall not be responsible for statements or opinions contained
in papers or printed in its publications

"Is Your SIF Trying to Do Too Much?"

Arthur M. (Art) Dowell, III, PE
Process Improvement Institute, Inc.
2437 Bay Area Blvd, PMB 260
Houston, TX 77058-1519
Adowell@piii.com

Keywords: SIF, SIS, SIL, safety instrumented function, LOPA

Abstract

The number of inputs and outputs to a SIF (safety instrumented function) -- as well as how they vote -- affects the probability of failure on demand (PFD) and the SIL (safety integrity level), assuming the test interval remains the same. The larger the number of inputs and outputs, the higher the PFD and potentially the lower the SIL.

What if the SIF includes all the sensors and final elements that are involved in any trip of a large processing unit like a heater, a reformer, or a distillation column? What if the SIF includes the actions to shutdown upstream units that feed the unit being tripped? What if the SIF includes the actions to shutdown downstream units fed by the unit being tripped? When SIL verification is done for a SIF as described here, the result may be that the target PFD and SIL cannot be achieved. The temptation may be to add redundancy in sensors and final elements or to reduce the proof test interval in an attempt to reduce the calculated PFD. Frustration may abound as capital and operating costs rise steeply.

This paper shows how to use the principles of LOPA (layer of protection analysis) and the information in the PHA (process hazard analysis) to split up the massive SIF into smaller SIFs that are more manageable. The smaller SIFs need include only the sensors, logic solver(s), and final elements that detect and prevent a specific scenario (one cause leading to one consequence). The approach makes sure all the smaller SIFs can protect against all the scenarios that the massive SIF was intended to prevent. Trips of upstream and downstream units are considered as

orderly shut-down actions. If needed, trips of upstream and downstream units are analyzed as small SIFs, as well.

Depending on the voting, the SIL verification calculation for the massive SIF may estimate a lower overall PFD than what can be achieved with the smaller SIFs for each scenario. This situation gives a higher actual risk than what was estimated.

With reasonable size SIFs, there is an opportunity to design each SIF with a reasonable number of sensors and final elements, and a reasonably long proof test interval.

An example is included.

1 Introduction – A Massive SIF Example

As a legacy from practices before IEC 61511 [1, 2] and before layer of protection analysis (LOPA), today we still see SIFs that include all the sensors and final elements to shut down a major process unit such as a reformer. An example of such a configuration is shown in Table 1. The target PFD for the reformer shut-down SIF-01 was specified to be ≤0.01, which corresponds to SIL 2.

Table 1. Example Reformer Shutdown SIF-01, Sensors and Final Elements

Reformer SIF-01 Sensors		Reformer SIF Final Elements	Target PFD	Target SIL
Combustion air fan K-201 stopped MSAL-10 Flue gas fan K-202 stopped MSAL-11 1oo1 Fuel Gas 02-PT-37A/B/C (2oo3) Furnace Box PSAH-13 02-PT-13ABC 2oo3 NG 02-FT-01A/B/C (2oo3) NG Comp Trip IS-21 Reformed Gas 02-TI-37A/B/C (2oo3) STM 02-FT-03A/B/C (2oo3) STM DRUM 02-LT-18 A/B/C (2oo3)		Flue Gas Fan K-202 & Comb Air Fan K-201 (2oo2) Fuel Gas 02-USV-15, 02-USV-16 (1oo2) NG 02-FV-01 & 02-FV-02 & 02-USV-01	≤0.01	2
Note: this example SIF is not intended to be representative of any particular installation, nor is it intended to be a recommendation or a suggestion for any design. It is shown here only to illustrate the concept of an SIF with too much to do.				

In Table 1, we have combined several sensors into voting groups, such as 2oo3 (two out of three). Likewise, we combined several final elements into voting groups such as 1oo2 or 2oo2 based on logic that was included in this example SIF design. The selected SIL verification software supports these combinations for many configurations of sensors and final elements; it is helpful if the devices in a voting group are the same type of sensor or the same type of valve. The software we used for the sample evaluation was exSILentia version 3.7.2.1122 provided by exida LLC.

Depending on the sensor group that triggers the SIF, different combinations of the sensor voting groups in Table 1 are required to vote 1oo2 or 2oo2. Similarly, different combinations of the final element voting groups in Table 1 are required to vote 2oo2 or 2oo3.

The first issue we notice is that the software can accept only four voting groups for sensors and four voting groups for final elements. Table 1 has nine sensor voting groups. While there are three final element voting groups, other SIFs are known to have more than four final element voting groups.

For simplicity, Table 1 does not show additional actions to trip downstream units. If they were included in the SIL verification, the capability of the software would be exceeded.

If we attempted to model Table 1 with fault tree analysis (FTA), we might be tempted to assume that the sensor voting groups would vote as 1oo9. However, voting 1oo9 gives a lower PFD for the sensor part of the SIF than voting 2oo3 or 2oo2. We also might be tempted to assume that the final element voting groups would vote as 1oo3, but for some sensor combinations, the final elements vote 1oo2 or 2oo2. It becomes apparent that the various combinations of sensors and final elements are too complicated to model in FTA or with the SIL verification software.

2 Application of LOPA Concepts to the Massive SIF

The problem is that there are eight different scenarios that the components of SIF-01 are trying to detect and to prevent. To resolve this problem, we need to recall the principles of layer of protection analysis (LOPA) where we evaluate one scenario at a time and determine what IPLs protect against that scenario [3]. A scenario is one cause-consequence pair; that is, one cause leads to one consequence.

Table 2 shows the same sensors and final elements as shown in Table 1, but they have been arranged into eight groups corresponding to the different scenarios that need to be detected and prevented. For example, the scenarios are low flow of natural gas to the reformer, low steam flow to the reformer, low air flow to the reformer, low steam to carbon ratio in the reformer feed, high furnace box pressure, low reformer steam drum level, high temperature of the reformed gas, and low pressure of the fuel gas. Abbreviations in Table 2 are shown in the Glossary.

It may be possible to identify the scenarios from a LOPA (or PHA).

Now that Table 2 has eight SIFs with a reasonable number of sensor groups and final element groups, each one can be verified with the SIL verification software to determine the PFD and SIL.

The sensor groups are designated for each of the eight SIFs as **all** of the sensor groups that can detect that specific scenario, and **only** those sensor groups. For example, there are two sensor groups that can detect low natural gas flow, 1) the 2oo3 voting on the natural gas flow transmitters 02-FT-01A/B/C, and 2) the signal that the natural gas compressor has tripped.

The final element groups are designated for each of the eight SIFs as the **minimum** final element groups that can prevent the specific scenario, and **only** those final elements. For example, for low natural gas flow, the consequence for the scenario is damage to the reformer exchanger tubes; to prevent damage, the heat flow into the exchanger must be stopped. The final elements that can prevent the consequence are 1) closing the fuel gas valves 02-USV-15 and 02-USV-16 (1oo2), and 2) tripping the flue gas fan K-202 and tripping the combustion air fan K-201 (2oo2). Both actions 1) and 2) are required (2oo2).

SIF-01-1 Low Natural Gas Flow Trip of the Reformer takes the immediate action required to avoid the scenario. The other shutdown actions of the SIF shown in Table 1 are taken for orderly shutdown, recognizing that the reformer cannot run correctly without natural gas.

Table 2. Example Reformer Shutdown SIF, split into single scenario SIFs, including Sensors and Final Elements

Reformer Single Scenario SIFs	Reformer SIF Sensors		Reformer SIF Final Elements	PFD$_{avg}$	SIL
SIF-01-1 Trip of Reformer H-201 NG FALL	NG 02-FT-01A/B/C (2oo3) NG Comp Trip IS-21 1oo2		Fuel Gas 02-USV-15, 02-USV-16 Flue Gas Fan K-202 & Comb Air Fan K-201 2oo2	7.34E-3	2
SIF-01-2 Trip of Reformer Steam FALL	NG 02-FT-01A/B/C (2oo3)		Fuel Gas 02-USV-15, 02-USV-16 NG 02-FV-01 & 02-FV-02 & 02-USV-01 Flue Gas Fan K-202 & Comb Air Fan K-201 3oo3	9.26E-3	2
SIF-01-3 Trip of Reformer Low Air	Combustion air fan K-201 stopped MSAL-10 Flue gas fan K-202 stopped MSAL-11 1oo2		Fuel Gas 02-USV-15, 02-USV-16 1oo2	1.55e-3	2
SIF-01-4 Trip of Reformer Steam/carbon low ratio	NG 02-FT-01A/B/C (2oo3) STM 02-FT-03A/B/C (2oo3) 2oo2		Fuel Gas 02-USV-15, 02-USV-16 1oo2 Flue Gas Fan K-202 & Comb Air Fan K-201 2oo2 NG 02-FV-01 & 02-FV-02 & 02-USV-01 3oo3	9.31E-3	2
SIF-01-5 Trip of Reformer High Furnace Box Pressure	Furnace Box PSAH-13 02-PT-13ABC 2oo3 Flue gas fan K-202 stopped MSAL-11 1oo1 1oo2		Fuel Gas 02-USV-15, 02-USV-16 1oo2 Comb Air Fan K-201 2oo2	7.66E-3	2
SIF-01-6 Trip of Reformer Low Level Steam Drum	STM DRUM 02-LT-18 A/B/C 2oo3 Flue gas fan K-202 stopped MSAL-11 1oo1 1oo2		Fuel Gas 02-USV-15, 02-USV-16 1oo2 NG 02-FV-01 & 02-FV-02 & 02-USV-01 2oo2	3.38E-3	2
SIF-01-7 Trip of Reformer Reformed Gas TAHH	Reformed Gas 02-TI-37A/B/C 2oo3		Fuel Gas 02-USV-15, 02-USV-16 1oo2 NG 02-FV-01 & 02-FV-02 & 02-USV-01 2oo2	3.65E-3	2
SIF-01-8 Trip of Reformer H-201 Fuel Gas PALL	Fuel Gas 02-PT-37A/B/C (2oo3)		Fuel Gas 02-USV-15, 02-USV-16 1oo2	1.63E-3	2
Note: these example SIFs are not intended to be representative of any particular installation, nor are they intended to be a recommendation or a suggestion for any design. They are shown here only to illustrate the concept of dividing up an SIF with too much to do.					

3 Protocol to Identify and Correct SIFs That Are Trying to Do Too Much

Here is an outline of a protocol to identify and correct SIFs that are trying to do too much.

1. Triggers to identify SIFs that are trying to do too much
    a. The SIF includes all the sensors and final elements that are involved in any trip of a large processing unit.
    b. The SIF includes actions to shutdown upstream units that feed the unit being tripped.
    c. The SIF includes actions to shutdown downstream units fed by the unit being tripped.
    d. The SIF has more than three process variables as inputs (Redundant sensors that measure the same process variables on the same stream do not contribute to this trigger.).
    e. The SIF has more than two final element actions (Redundant final elements that take the same actions on the same stream do not contribute to this trigger.).
2. Determine if the sensors and final elements of the SIF are protecting against multiple scenarios. Consult the PHA (process hazard analysis) or the LOPA for the facility for additional information.
3. Separate the sensors and final elements of the SIF into sub-SIFs such that each sub-SIF is detecting and preventing one scenario.
    a. Select **all** of the sensors that can detect that specific scenario, and **only** those sensor groups.
    b. Select the **minimum** final elements that can prevent the specific scenario, and **only** those final elements.
    c. Do not select sensors or final elements that do not detect or prevent the specific scenario, but that are for orderly shutdown.
    d. Perform the SIL verification calculations for each sub-SIFs.
    e. Check to confirm that all of the sensors and final elements for the massive SIF have been included in the sub-SIFs.

4 Conclusion

This paper shows the difficulty presented by an SIF that attempts to protect against too many scenarios and lumps too many sensors and final elements together into one SIF. An example was presented showing how to split up a massive reformer SIF into reasonably-sized sub-SIFs. A protocol was outlined for the work process.

With reasonably-sized SIFs, there is an opportunity to design the SIF with a reasonable number of sensors and final elements, and a reasonably long proof test interval.

5 Glossary

Table 3 has definitions for acronyms.

Table 3. Glossary

1oo1	One out of one voting
1oo2	One out of two voting
1oo3	One out of three voting
1oo9	One out nine voting

2oo2	Two out of two voting
2oo3	Two out of three voting
Comb	Combustion
FT	Flow transmitter
FV	Flow valve
IPLs	Independent protection layers
LT	Level transmitter
LOPA	Layer of protection analysis
MSAL	Motor stop alarm
NG	Natural gas
PFD	Probability of failure on demand
PHA	Process hazard analysis
PSAH	Pressure switch alarm high
PT	Pressure transmitter
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
STM	Steam
USV	Open/closed shutdown valve

6 References

[1] IEC 61511-1:2016+AMD1:2017 CSV, Consolidated version: Functional safety - Safety instrumented systems for the process industry sector -- Part 1: Framework, definitions, system, hardware and application programming requirements, International Electrotechnical Commission (IEC), Geneva, Switzerland, 2017.

[2] ANSI/ISA-61511-1-2018 / IEC 61511-1:2016+AMD1:2017 CSV, Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, definitions, system, hardware and application programming requirements (IEC 61511-1:2016+AMD1:2017 CSV, IDT), International Society of Automation, Research Triangle Park, North Carolina, 2018.

[3] CCPS, *Layer of Protection Analysis, Simplified Process Risk Assessment*, American Institute of Chemical Engineers, New York, New York, 2001.