

## **A New Software-based HAZOP Study Development Methodology**

**György Baradits**

SIL4S  
Baláca u. 54, H-8200 Veszprém, Hungary  
bgs@controrg.hu

**János Abonyi**

Department of Process Engineering, University of Pannonia  
Egyetem u. 10, H-8200 Veszprém, Hungary  
e-mail: abonyij@fmt.uni-pannon.hu

*Abstract: HAZOP study is the basic tool for assessing of hazards and risks in the Process Industry. In our article we are investigating possibilities of amending the HAZOP study. A novel HAZOP software has been developed called 'Tool4SIL' to support the development and analysis of HAZOP studies and SIL evaluation projects. In this article we discuss the challenging questions and our answer related to the development of this new software and the related methodology.*

*Keywords: HAZOP, Process Risk, Risk Matrix, LOPA, SIL, SIL evaluation*

### **1 Introduction**

In May of 2001 there was published a European Standard CEI IEC 61882 which has the following main goals:

- *'Identifying potential hazards in the system. The hazards involved may include both those essentially relevant only to the immediate area of the system and those with a much wider sphere of influence, e.g. some environmental hazards;*
- *Identifying potential operability problems with the system and in particular identifying causes of operational disturbances and production deviations likely to lead to nonconforming products.'*

The HAZOP (Hazard and Operability Study) Study (CIA, 1992; Kletz, 1992; Freeman, 1991; Freeman et al. 1992) is a process analysis procedure which seeks to identify systematically the risks, faults and operational problems which may compromise personal or environmental safety, or plant operation. Moreover, it can also assess the consequences of deviation from standard function and propose corrective actions. The procedure is based on the generation of a series of questions for submission to a multi-disciplinary team with expertise in the process under examination. To this end, a combination of parameters and guide words is applied to all parts of the plant considered potentially dangerous. In addition to being particularly demanding from the point of view of the man-hours required, HAZOP studies have strong systemic and multi-disciplinary features typical of plant projects, and can thus be seen as small projects in themselves.

The traditional HAZOP study is a team work with a team leader and other participant like operators, plant managers, instrumental engineers, safety specialist requiring the knowledge of both technology and instrumentation. It should also be noted that of the deliverables generated by safety engineering, HAZOP studies are of greatest interest to the client, and the latter often participates directly in the meetings at which the analysis is carried out. The traditional HAZOP study is finished when the team have found the causes of Hazards, the consequences, protection layers and other protective actions and no dealing with how to allocate the Safety Instrumented Functions and protection Layers, calculate the SIL value and realizes the Safety system.

The development of HAZOP studies is a difficult, complex problem that requires supporting tools. Software products, like the proposed Tool4SIL, stand out from generic solutions, such as accounting spreadsheets and word processors, which were never specifically designed for risk analysis studies. A tailored software lets you immediately begin conducting a Process Hazards Analysis much more quickly, efficiently and cost-effectively. With the application of a good supporting tool the studies can be completed up to 50%+ faster than by any other means. Plus, a good tool could help the users to identify more risks than ever before – ultimately creating a safer workplace.

Such software provides expert guidance for studying a full range of facilities to help companies identify hazards in order to eliminate them, and simplifies Process Safety Management (PSM) with a series of templates and a preformatted worksheet. When the user finished the PHA or HAZOP study, he or she can produce consistent, auditable documentation in seconds in HTML, Microsoft® Word and other formats.

The market is full with such solutions. A detailed list of these can be found in:

[http://www.plant-maintenance.com/maintenance\\_software\\_RCM.shtml](http://www.plant-maintenance.com/maintenance_software_RCM.shtml)

Most of these solutions (like Hazop Studies or Hazop+) incorporate features and facilities that:

- Serve as a framework within which preparation for the review can be structured.
- Ease the task of recording the meeting minutes, and help to maintain the team's focus of attention and interest.
- Give speedy access to material useful to the study team, such as previously identified problems, failure rate data and other such historical information.
- Allow professionally formatted reports to be produced with the minimum of effort.
- Permit additional management information to be extracted from the study records.
- Provide a comprehensive and easy to use system for effective action follow-up and close-out, without the significant administrative burden that this usually entails.

As these items illustrate the major advantage of these tools is that it provides a very convenient way to enter and store the study information. The information is stored in a database from where it can be filtered sorted and displayed. Hence, a good HAZOP support software speeds up the process of recording and managing the potentially large amounts of information. The second major advantage is that such software also offers a powerful report generator for the creation and printing of professional quality reports, and also offers a project wizard to simplify creation of new projects.

In this article we discuss a novel methodology optimized for the development HAZOP studies and our new XML based software designed for its support. Compared to the other solutions the proposed tool is also amended with Risk matrix possibilities, matching the IEC 61511 Life Cycle Philosophy.

In the following the basics of the development of HAZOP studies are presented, that is followed by the detailed discussion of the motivation of the development of our new solution is given. Finally the developed Tool4SIL software is presented, and some conclusions are also given related to its application experience.

## **2 HAZOP Study**

There are many different tools and techniques available for the identification of potential hazards and operability problems, ranging from Checklists, Fault Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA) to HAZOP. Some techniques, such as Checklists and What-If/analysis, can be used early in the system life cycle when little information is available, or in later phases if a less

detailed analysis is needed. HAZOP studies require more details regarding the systems under consideration, but produce more comprehensive information on hazards and errors in the system design.

HAZOP is particularly useful for identifying weaknesses in systems (existing or proposed) involving the flow of materials, people or data, or a number of events or activities in a planned sequence or the procedures controlling such a sequence. As well as being a valuable tool in the design and development of new systems, HAZOP may also be profitably employed to examine hazards and potential problems associated with different operating states of a given system, e.g. start-up, standby, normal operation, normal shutdown, emergency shutdown. It can also be employed for batch and unsteady-state processes and sequences as well as for continuous ones. HAZOP may be viewed as an integral part of the overall process of value engineering and risk management.

Here we do not want to deal with limitation of HAZOP study as this mainly depends on the the expertize of team leader and team member involved in the HAZOP study work. The better is the documentation available and the bigger practice having the participant the less is the limitation. It is important that the HAZOP Study is not a static one it shall be repeated in all case of modification which may influence the safety of the part or total of the Plant (see Management of Change, IEC 61508 and IEC 61511).

## 2.1 Definitions

For the purposes of this International Standard, definitions contained in IEC 60050(191) as well as the following terms and definitions apply:

**Characteristic** : qualitative or quantitative property of an element

*NOTE Examples of characteristics are pressure, temperature, voltage.*

**Design intent** : designer's desired, or specified range of behaviour for elements and characteristics

**Deviation** : departure from the design intent

**Node** : subsystem of technology under hazard investigation

**Element** : constituent of a part which serves to identify the part's essential features

*NOTE: The choice of elements may depend upon the particular application, but elements can include features such as the material involved, the activity being carried out, the equipment employed, etc. Material should be considered in a general sense and includes data, software, etc.*

**Guide word** : word or phrase which expresses and defines a specific type of deviation from an element's design intent

- Harm** : physical injury or damage to the health of people or damage to property or the environment
- Hazard** : potential source of harm, any happening with inherent risk
- Part** : section of the system which is the subject of immediate study
- NOTE A part may be physical (e.g. hardware) or logical (e.g. step in an operational sequence).*
- Risk** : combination of the probability of occurrence of harm and the severity of that harm

## 2.2 The HAZOP Study Procedure

The HAZOP study typically consist of typically sunsequent steps. This steps have to be designed in advance by the HAZOP project leader and agreed upon the client. Here is a short summary of these steps.

### 1 Definition

- Define scope and objectives
- Define responsibility
- Select team

### 2 Preparation

- Plan the study
- Collect data
- Agree style of recording
- Estimate the time
- Arrange a schedule

### 3 Examination

- Divide system into parts
- Select a part and define design intent
- Identify deviation by using guide words on each element
- Identify consequences and causes
- Identify whether a significant problem exists
- Identify protection, detection, and indicating mechanisms
- Identify possible remedial/mitigating measures (optional)
- Agree actions
- Repeat for each element and then each part of the system

### 4 Documentation and follow-up

- Record the examination
- Sign off the documentation

- Produce the report of the study
- Follow up that actions are implemented
- Re-study any parts of system if necessary
- Produce final output report

### 2.3 Principles of Examination

The basis of HAZOP is a 'guide word examination' which is a deliberate search for deviations from the design intent and thus the design intent will contain the following elements: materials, activities, sources and destinations which can be viewed as elements of the part.

The Hazard and the design intent connected to the given Hazard may have a parameter, like pressure, temperature, flow etc. The 'trip' point where the Hazard may be released called 'guide word'. The guide words and definition without completeness are in Figure 1.

In the HAZOP meeting the technology is divided into Nodes, the Nodes are divided parts and based on parameter and guidewords the HAZOP team try to find all the cause why the selected parameter does not match the design intent. The HAZOP team also looking for safety guards and action taking into consideration reducing the risk.

Guide words	Description
High	Higher than the design intent
Low	Lower than the design intent
More	Quantitative increase
Less	Quantitative decrease
Reverse	Logical opposite of the design intent
As well as	Qualitative modification/increase
Part of	Qualitative modification/decrease
Other than	Complete substitution

Figure 1  
Example of guide words

### 3 The Proposed HAZOP Development Methodology

#### 3.1 Example of HAZOP Study

In our simple example (see Figure 2) we show all the feature of our ‘Tool4SIL’ SW. Our simple example is the Natural Gas supply of a Process Furnace. We divided the Burner unit three different ‘Nodes’: Technology, Gas burner, and Radiation and Convection Zone. Our example refers to the ‘Gas Burner Node’ only. Within this node the HAZOP team is dealing with four different ‘Parts’: Main gas supply, Ignition gas supply, Combustion air supply, Ignition of the burner. In our example we focused onto the pressure (parameter), taking into consideration when this pressure deviate from the design intent (High trip point).

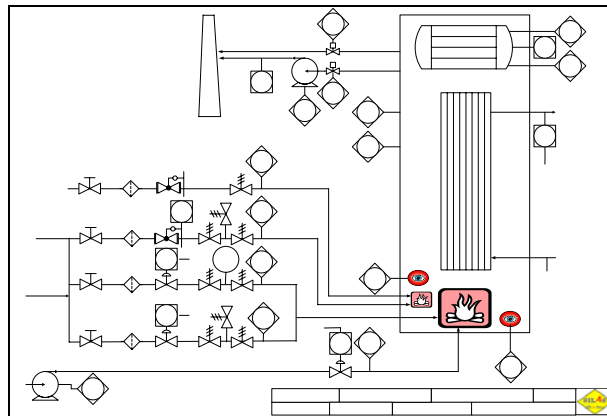


Figure 2  
Example of Natural gas burner

When all cause is found and the consequences are evaluated together with the safeguards and action taking into consideration. The Figure 3 shows the result of this activity (HAZOP Report). In this figure the Display is splitted into three parts:

- The upper narrow part is the traditional web communication panel.
- The middle narrow part includes information about the plant, node, part of the node, parameter, guide word and deviation.
- The lower part documents the causes, consequences, safeguard/actions (including the Safety Instrumented Functions in blue colour).

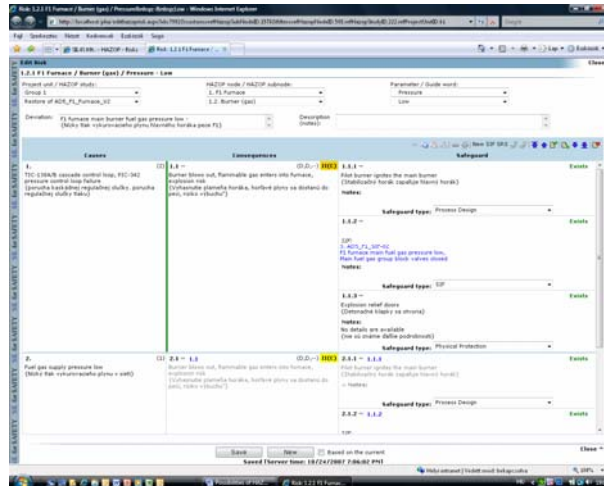


Figure 3  
 Example of Traditional HAZOP study

### 3.2 Motivation of ‘Tool4S’ SW Development

We have got a work preparing tens of HAZOP studies and we are looking for a SW in the market. After evaluating the existing ones none of them match our demand and we decided to develop a new SW. Meanwhile working on our HAZOP and SIL calculation project got a lot of experience which was integrated into our SW taking into consideration the idea and request of our partners. The basic philosophy using in the new ‘Tool4S’ SW was the followings:

- Using new development tools of Microsoft and
- Using the web techniques and running on a web server.
- Insisting on the Process Safety Standard Safety Life Cycle philosophy.

We used Microsoft Visual Studio as a development environment, the main technologies are ASP .NET, ASP .NET AJAX and Sql server. A good question why we prefer web techniques? No one answer only. The first issue is building up a Corporate Safety Knowledge Data Base within the Company, which is open for everybody. The second issue is giving the possibility of common work even from other country where the server was installed. As we were working according IEC 61508 and IEC 61511 our SW device also have to follow this standards.



### **3.3 Scope of Development-based on Evaluating the Existing HAZOP Study and Programs**

We mentioned above that the HAZOP study is the first step assessing the risks of the technology. Based on our practice we have found the problems with the basic HAZOP study. There was different SW on the market but neither of them was able to solve all of our task. We shall have to buy minimum two SW without any compatibility and communication between them. The result would have been a non consistent documentation and a lot of extra manual work uploading information from one SW to another.

In principle the HAZOP team has all knowledge and experience make them able to perform the complete risk evaluation process consisting of the following steps.

- Decision about the frequency of causes
- Decision of the severity of the consequences for Health of people (injury and fatality), Environment and Business.
- Allocate safety function(s) to protection layers (IEC 61511/3 p. 39)
- Identify safety function(s) needed (IEC 61511/3 p. 39)

Final idea of us was to match the Life Cycle principle of Process Safety Standards:

- Hazard and Risk assessment (Life Cycle 1)
- Allocation of safety Function to Protection Layers (Life Cycle 2)
- Safety Requirement Specification (Life Cycle 3)
- Basic design (Life Cycle 4)
- Validation (Life Cycle 6)

In practice the HAZOP study is giving the possibility of calculating the SIL value of the Safety Instrumented Functions. That is why our basic HAZOPO SW program is to be amended with LOPA and SIL calculation features.

## **4 Approaching the Novel HAZOP SW**

Based on our experience the traditional HAZOP SW shall have to be amended with the following features:

### **4.1 HAZOP Study of Existing Plants**

The problems are based on the practical request of the clients: evaluating the existing plants giving suggestions for the modification. This task is more complex than dealing with a 'green field' application. The program shall give the

possibility of this type of evaluation. The Figure 4 shows an example about this feature of our Tool4SIL program.

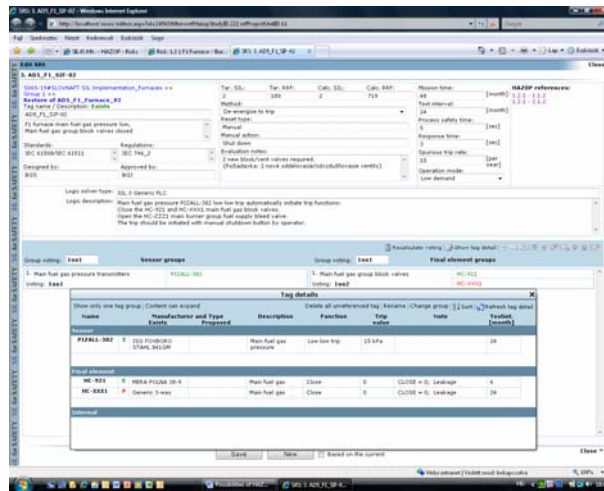


Figure 4  
 Existing Plant evaluation

The HAZOP team evaluates the existing control and safety loops safety point of view giving the possibility of documenting the results and suggestions with the P@ID tags even concrete type of instruments (like manufacturer, type code etc...). In this case one part of HAZOP documentation gives additional information about the problems of an existing system and suggestions what the Client shall have to done to fit the Company Safety Policy. The HAZOP team has the possibilities of suggesting new control of safety loops increasing the Integrated Level of Safety. E means existing while P means proposal.

## 4.2 Narratives and Logic Integrated Into the HAZOP Study

The HAZOP study is prepared either before the realisation of the Plant or before any kind of modification of the Plant according the Management of Change Policy of the Company. That means that the instrument designer needs safety information from the licensor or technological designer. The best way of doing it of using HAZOP study. The HAZOP team members are familiar with the technology and able to decide about the Safety Instrumented Functions. Best way doing it of using both 'narratives' and 'SIF Realibility Block Diagram'. Our Tool4S SW gives the possibility of documenting both 'narratives' and 'logics' of all Safety Instrumented Function. This part of HAZOP study documentation will be a basic design for the instrument ingeneer preparing the 'Detailed Engineering'. Our SW gives the possibilities of different voting systems also. Figure 4 shows and example

about this feature of our Tool4SIL program. The upper part of the Display gives the following information (without completeness) about one Safety Instrumented Function (in our case 'AD5\_FI\_SIF-02'):

- Task of the Safety Function
- Target Risk Reduction factor and SIL value
- Calculated Risk Reduction factor and SIL value
- Evaluation notes
- Logic description (narratives)
- Maintenance and operational information
- Type of voting both for sensors and actuators and RBD

In a separate box one can see the tag details including the trip value of the SIF (see also 4.1 paragraph).

### **4.3 Company Safety Policy Integrated into the HAZOP Study**

The calculation of target risk reduction factor and target SIL needs information about the Company Safety Policy telling us what is the tolerable frequency of happening a harm or fatality with the workers, the damages and losses in environment and business. This requirement focus on the necessity of integration of Company Safety matrix into our HAZOP program giving the possibilities of the HAZOP team members to calculate the frequency of Hazardous event and severity of consequence for the people, environmental and business. Based on this matrix the HAZOP team member was able to calculate the Risk Reduction Factors of the Safety Instrumented Functions. Figure 5 shows an example about this feature of our Tool4SIL program.

In the box of 'Cause' there is a number in bracket '(2)'. That refers how often the unwanted event may happen. In the box of 'Consequence' there are letters in bracket '(D,D,-)'. These letters refer to the severity of the consequences for people, business and environment. This is called 'Risk Ranking' and refers to the Company Safety Policy (Company Risk matrix). See also 4.3 paragraphs. In Figure 3 one can see a Risk Matrix for environment as part of a Company Safety Policy. This Risk Matrix is ranked from A to E, and based on this matrix, the HAZOP team is able to evaluate the severity of the consequences.

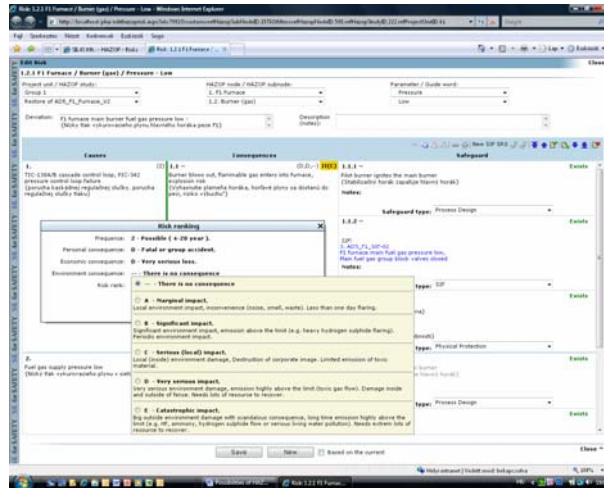


Figure 5  
Risk ranking within the HAZOP Study

#### 4.4 Safety Requirement Specification Integrated into HAZOP Study

According to the IEC 61508 and IEC 61511 the Basic Safety Documentation must include the Safety Requirement Specification as a guidance for the detailed design, installation, commissioning and maintenance. We also integrated this feature in our program. The Figure 4 shows an example about this feature of our Tool4SIL program.

#### 4.5 LOPA Integrated into the HAZOP Study

LOPA (Layer of Protection Analysis) is the best semi-quantitative method to calculate the SIL value and Risk Reduction Value of the Safety Instrumented Functions. This feature is under development and will be finished till the end of this year.

#### 4.6 SIL Validation Integrated into the HAZOP Study

All systems including the Safety System must be validated. In the case of a Safety System, the validation is mandatory and based on SIL calculation of the Safety Instrumented Loop. Minimum requirements for validation include having a database including the PFD value and other figures of the component according to the Process Safety Standards. Other measures include the mathematics of different voting systems

which is public. That is why this feature is in 'looking for co-operation partner' phase and will be finished till end of next year.

## 4.7 Reports

The Tool4SIL program generates reports, see Figures 6.

### Conclusions

The development of a new HAZOP software was a 'Real Time' development, since we continuously modified the development to support our HAZOP studies. The result at that moment a lot of extra feature which makes the design of the Safety system faster and cheaper and more understandable not only the instrument people but the process people also increasing the safety culture of the people within a company.

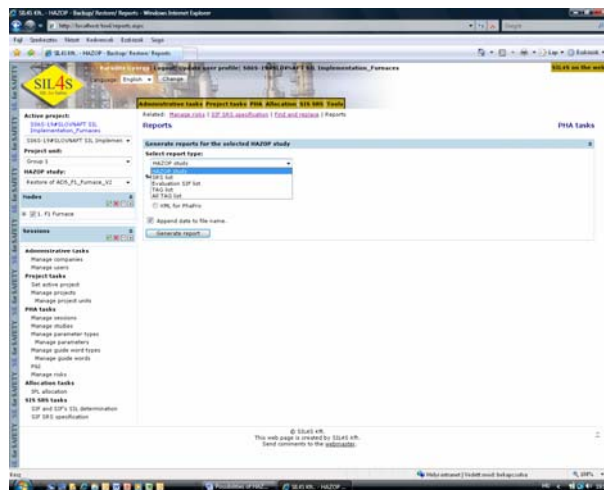


Figure 6  
Report generator

### Acknowledgement

Here we would like to express our acknowledgement to our colleges at SIL4S Ltd. for their continuous contribution to this development and the Department of Process Engineering of Pannon University, Veszprém taking part the test of our SW and giving some idea to us. Janos Abonyi acknowledge the financial support of the Cooperative Research Centre (VIKKK, project 2004-I), the Hungarian Research Found (OTKA 49534), the Bolyai János fellowship of the Hungarian Academy of Science, and the Öveges fellowship.

## References

- [1] IEC 61508 1 – 7: Functional safety of electrical / electronic/programmable electronic safety - related systems
- [2] IEC 61511 1 – 3: Functional Safety: Safety Instrumented Systems for the Process Industry Sector
- [3] SafetyLine Institute: Occupational Health & Safety Practitioner, MANAGEMENT OF MAJOR HAZARD FACILITIES
- [4] Hazard and Operability (HAZOP) Studies
- [5] Morten Lind: Functional Approach to HAZOP Studies
- [6] James W. Vinson, 1998: Putting the 'OP' Back in 'HAZOP'
- [7] Ken Bingham, 2004: Integrating HAZOP and SIL/LOPA Analysis: Best practice Recommendations
- [8] Foster Wheeler Energy Ltd., 2000: Safer Safety
- [9] P Fenelon, 2000: Applying HAZOP to Software Engineering Models