A SOFTWARE SYSTEM TO CHECK DESIGNS AUTOMATICALLY AGAINST PROCESS SAFETY AND BEST PRACTICE

Joe McDonald[1], Brendan Rieley[1], Jim Madden[1], John de Brugha[1] and Paul W.H. Chung[2]
[1]Hazid Technologies, Suite 14b-c, Beeston Business Park, Beeston, Nottingham NG9 2ND
[2]Department of Computer Science, Loughborough University, Leicestershire LE11 3TU, UK

It is well known that the cost of change escalates as the design progresses. Early design safety reviews will catch fundamental process safety issues. But if detailed changes dictated by regulator, client or engineering contractor best practices are not detected until Hazop studies, materials may already be on order, driving up the cost of change and the project schedule may be delayed. Project managers will debate how to apportion the cost between contractor and client.

The rise of so-called "intelligent" CAD systems (where the information represented on PFDs and P&IDs is stored in an underlying database) means that it is now feasible to build a complementary system to automatically check the design at any stage against relevant design or best practice guides to ensure a certain design quality is achieved and well tested component configurations for safe operation and maintenance are used.

This paper describes a Design Checker which can work with any of the leading intelligent P&ID systems. The Design Checker reads the P&IDs and applies a set of design rules to the design, providing detailed or 'by exception' reports. Action management facilities enable changes to be followed up and actioned before costs escalate.

Examples are used to illustrate the effectiveness of this approach. Easy to use tools for editing and managing existing rules and adding new ones are described in the paper.

INTRODUCTION

Safety studies rely on the plant P&IDs giving the best and most detailed picture of the process, the plant configuration and plant systems. The P&IDs enable information needed from other disciplines to be placed in context to provide a full understanding of the plant and the potential hazards. It is, therefore, vital that the P&I records the best company engineering practice, and approved company safety practices. Otherwise, much time will be wasted in safety study meetings and potential problems may not be apparent to the team.

The production of P&IDs requires the coordination of a large volume of information from many disciplines, some of which may be expressed visually on the diagram and some held as information with the diagram, It can be a lengthy process and may often be held up awaiting information. The stop-start nature of the process increases the difficulty of representing all the information accurately and completely. Some of the concerns are that pressure relief values are not present and vessels are not sized correctly for capacity. Design Checker is developed specifically to check that the emerging P&IDs conform to best engineering and safety practices and that information has not been omitted.

DESIGN CHECKER

The Design Checker takes as input the symbolic description of the design of a plant from the database of an intelligent CAD system. An example of this is Intergraph's SmartPlant® P&ID. Typically the description contains the items of equipment, their connectivities and any process data.

Another input that the Design Checker takes is a set of rules that represents best practices in safety and design. The system contains a set of predefined design rules. One such rule set represents the domain knowledge contained in ISO 10418 (ISO, 2003). For example, Figure 1 is a PSH tank, taken from the ISO document, showing the recommended safety devices connected to it. It also has an associated safety analysis description "input from a pump or compressor that cannot develop pressure greater than the maximum allowable working pressure of the vessel." From the figure one can extract a list of safety devices as shown in Figure 2 and from the description a rule for safety analysis check. Therefore, there are two types of checks – safety device check and safety analysis check.

The Design Checker provides a Rule Builder for users to input their own rules. A user can expand on an existing rule set or create new rule sets. The following provides an explanation of the different parts of the Rule Builder by referring to the numbers and labels shown on Figure 3:

1. The equipment model tree (minimised in the figure) allows the user to select a specific equipment type or group of equipments to apply the rule to.
2. The equipment state allows the user to select a particular state or states the equipment must be in for the rule to be applicable.
3. The rule type allows the user to select which rule types to apply to the equipment or group.
   a. Configuration rules for use with the other parts of the Hazid system
   b. Recommended safety devices as detailed from the standard
   c. SAFE charts used to create Cause & Effect charts

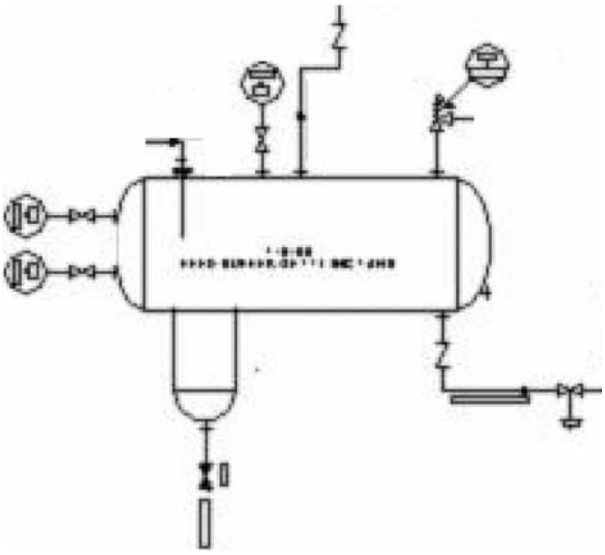
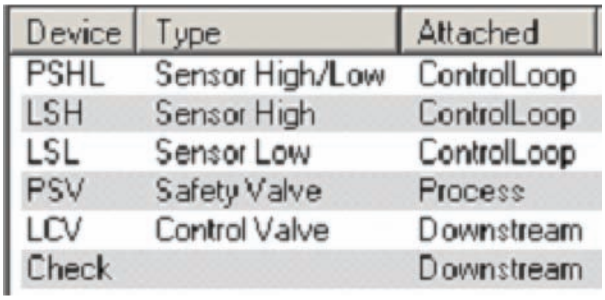


Figure 1. Recommended safety devices for PSH from ISO 10418



Device	Type	Attached
PSHL	Sensor High/Low	ControlLoop
LSH	Sensor High	ControlLoop
LSL	Sensor Low	ControlLoop
PSV	Safety Valve	Process
LCV	Control Valve	Downstream
Check		Downstream

Figure 2. Extracted list of recommended safety devices for PSH

d. Safety analysis checklist as detailed from the standard

4. The name of equipment or group of equipment the current rule set is valid for is shown.
5. The rule display panel shows the current rules which will be applied to the equipment.
6. The rule entry panel is used to enter the trigger for a rule:

a. Include branching lines or only search along the main flow line.

b. Where is the trigger item attached in relation to the equipment?
- Upstream – Anywhere upstream of the equipment.
- Downstream – Anywhere downstream of the equipment.
- Process – Anywhere surrounding the item in a process line.
- Self – The item itself.
- Control loop – On a control loop associated with the item.
- Attached – Directly attached to the item.

c. What type of device the trigger is
- G – A group of item types
- M – A specific equipment type
- I – An item code, PSV for example

d. The type of Item group or equipment type if G or M is selected.

e. Whether only to check for the presence of the trigger item.

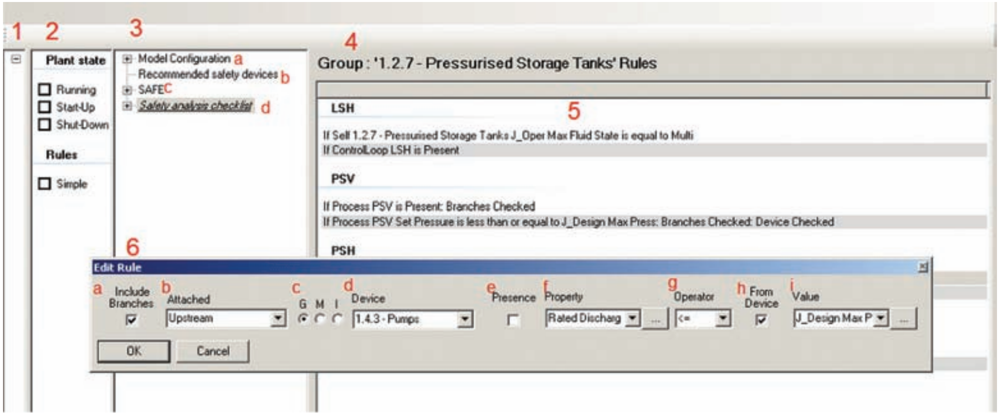
f. The property of the trigger item on which to evaluate; Pressure, Temperature etc.

g. Operator; Less than, Greater than etc.

h. Whether comparison is to be done against an attribute on the item or a specific value.

i. Where to enter the specific value or the attribute of the equipment item to compare against.

When the system is activated it will apply the specified set of rules to the plant design to identify any problems



Group : '1.2.7 - Pressurised Storage Tanks' Rules

LSH

If Self 1.2.7 - Pressurised Storage Tanks J_Oper Max Fluid State is equal to Multi
If ControlLoop LSH is Present

PSV

If Process PSV is Present: Branches Checked
If Process PSV Set Pressure is less than or equal to J_Design Max Press: Branches Checked: Device Checked

PSH

a Include Branches ☑ b Attached: Upstream c G ● M ○ I ○ d Device: 1.4.3 - Pumps e Presence □ f Property: Rated Discharg g Operator: <= h From Device ☑ i Value: J_Design Max P

Figure 3. Rule Builder user interface

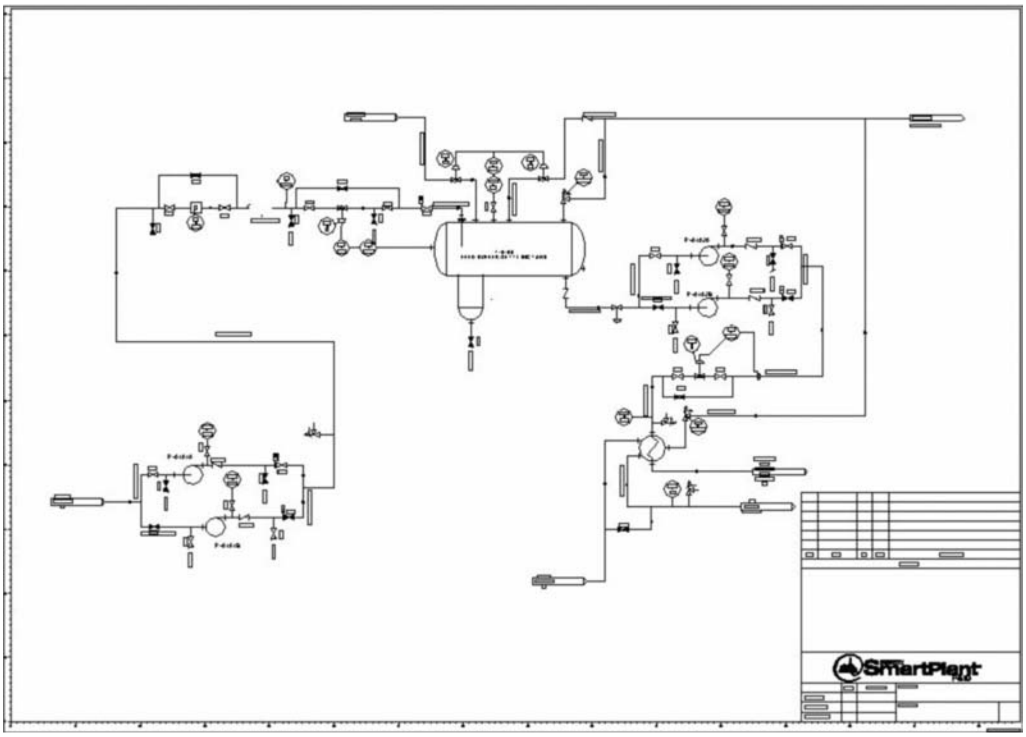


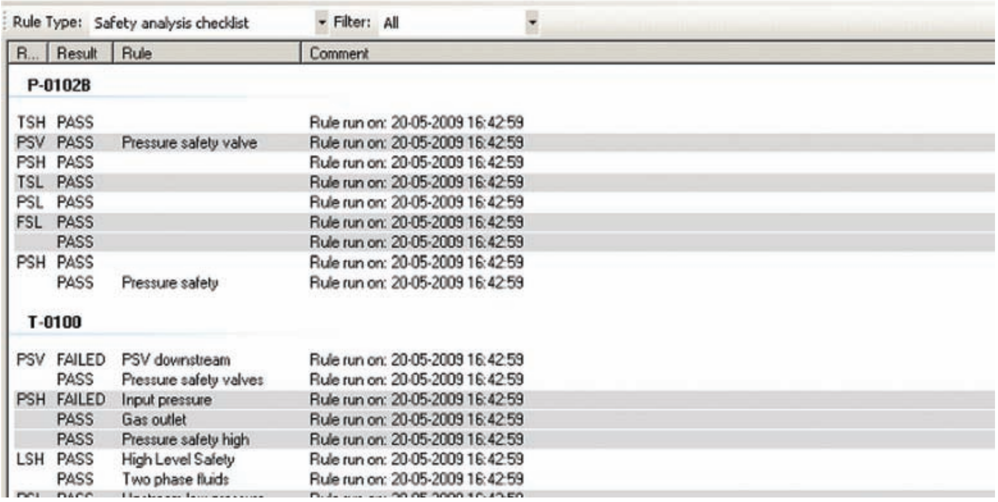
Figure 4. An example P&ID

and then provide detailed or 'by exception' report, depending on the user's preference.

EXAMPLE CASE AND RESULTS

To illustrate the working of the system, the P&ID shown in Figure 4 is used as input together with the default ISO 10418 rule set. The P&ID is a modified version of the one described in Lawley (1974) with a small number of design faults deliberately introduced for illustration purposes.

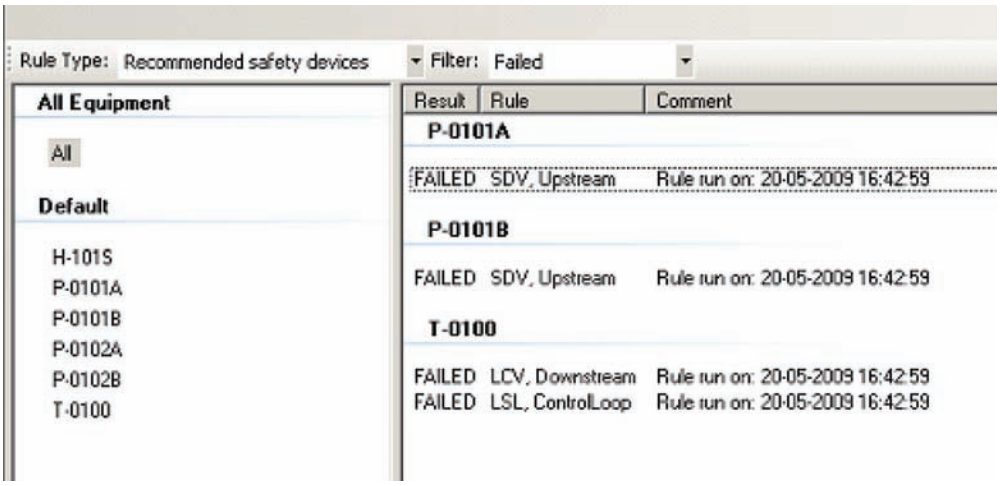
After running the system with the detailed reporting option selected the results generated for apply the safety analysis rules are shown in Figure 5. The detailed report shows both the checks that have passed and failed. Figures 6 and 7 show the exception reporting option for failed cases for safety device check and safety analysis check respectively.



Rule Type: Safety analysis checklist ▾ Filter: All ▾

R...	Result	Rule	Comment
P-0102B			
TSH	PASS		Rule run on: 20-05-2009 16:42:59
PSV	PASS	Pressure safety valve	Rule run on: 20-05-2009 16:42:59
PSH	PASS		Rule run on: 20-05-2009 16:42:59
TSL	PASS		Rule run on: 20-05-2009 16:42:59
PSL	PASS		Rule run on: 20-05-2009 16:42:59
FSL	PASS		Rule run on: 20-05-2009 16:42:59
	PASS		Rule run on: 20-05-2009 16:42:59
PSH	PASS		Rule run on: 20-05-2009 16:42:59
	PASS	Pressure safety	Rule run on: 20-05-2009 16:42:59
T-0100			
PSV	FAILED	PSV downstream	Rule run on: 20-05-2009 16:42:59
	PASS	Pressure safety valves	Rule run on: 20-05-2009 16:42:59
PSH	FAILED	Input pressure	Rule run on: 20-05-2009 16:42:59
	PASS	Gas outlet	Rule run on: 20-05-2009 16:42:59
	PASS	Pressure safety high	Rule run on: 20-05-2009 16:42:59
LSH	PASS	High Level Safety	Rule run on: 20-05-2009 16:42:59
	PASS	Two phase fluids	Rule run on: 20-05-2009 16:42:59

Figure 5. Detailed report for safety analysis checks

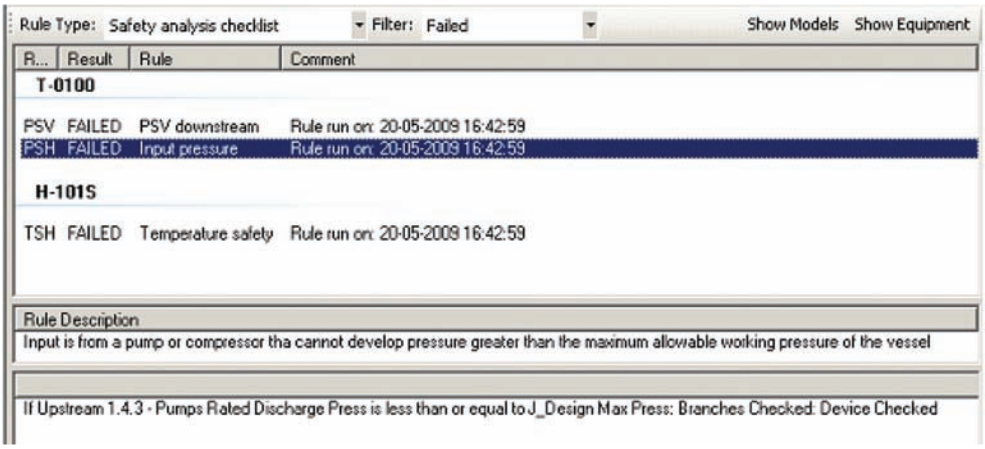


```
Rule Type: Recommended safety devices      Filter: Failed

All Equipment                 Result  Rule              Comment
                              P-0101A
  All                         FAILED  SDV, Upstream     Rule run on: 20-05-2009 16:42:59

Default                       P-0101B
                              FAILED  SDV, Upstream     Rule run on: 20-05-2009 16:42:59
  H-101S
  P-0101A                     T-0100
  P-0101B                     FAILED  LCV, Downstream   Rule run on: 20-05-2009 16:42:59
  P-0102A                     FAILED  LSL, ControlLoop  Rule run on: 20-05-2009 16:42:59
  P-0102B
  T-0100
```

Figure 6. Report of failed checks for safety devices



```
Rule Type: Safety analysis checklist   Filter: Failed        Show Models  Show Equipment

R...  Result  Rule                Comment
T-0100
PSV   FAILED  PSV downstream      Rule run on: 20-05-2009 16:42:59
PSH   FAILED  Input pressure      Rule run on: 20-05-2009 16:42:59

H-101S
TSH   FAILED  Temperature safety  Rule run on: 20-05-2009 16:42:59

Rule Description
Input is from a pump or compressor tha cannot develop pressure greater than the maximum allowable working pressure of the vessel

If Upstream 1.4.3 - Pumps Rated Discharge Press is less than or equal to J_Design Max Press: Branches Checked: Device Checked
```

Figure 7. Report of failed checks for safety analysis

As can be seen from figure 6 the failed results the inlet Pumps P-1010A and P-1010B have failed their recommended safety device rules for the SDV on the upstream as it is not present. If the SDV was present on the adjoining P&ID the Design Checker would pick this up and pass the rule. Tank T-0100 also failed recommended safety device rules as it has only a LSH whereas the standard asks for both LSH and LSL and also as the control valve LCV is on the upstream side and not the downstream as the standard specifies.

Tank T-0100 has also failed two of the safety analysis rules as shown in figure 7. One checks whether all of the downstream pressure relief valves are set at the correct pressure to relieve the vessel before it over pressurises. The other rule as described previously which determines whether the input of the vessel can over pressurise it. These rules are determined from the data stored within the intelligent P&ID. For this illustration the set pressure of the relief valve PSV-PRV01 situated on the tank is set at 3 barg, the rated discharge pressure of the inlet pumps P-0101A/B is also 3 barg, and the maximum design pressure of the tank is 2 barg.

REVISED EXAMPLE CASE AND RESULTS

In response to the analysis results reported by the Design Checker, a change is made to the plant design by adding the relevant recommended safety devices in the correct configuration to the tank T-0100 and also changing its maximum design pressure to 3 barg (see Figure 8).

Running the revised example through the Design Checker a new set of results is produced (see Figures 9 and 10). It can be seen that the problem related to T-0100 is now removed. However, further changes are required to remove the remaining problems.

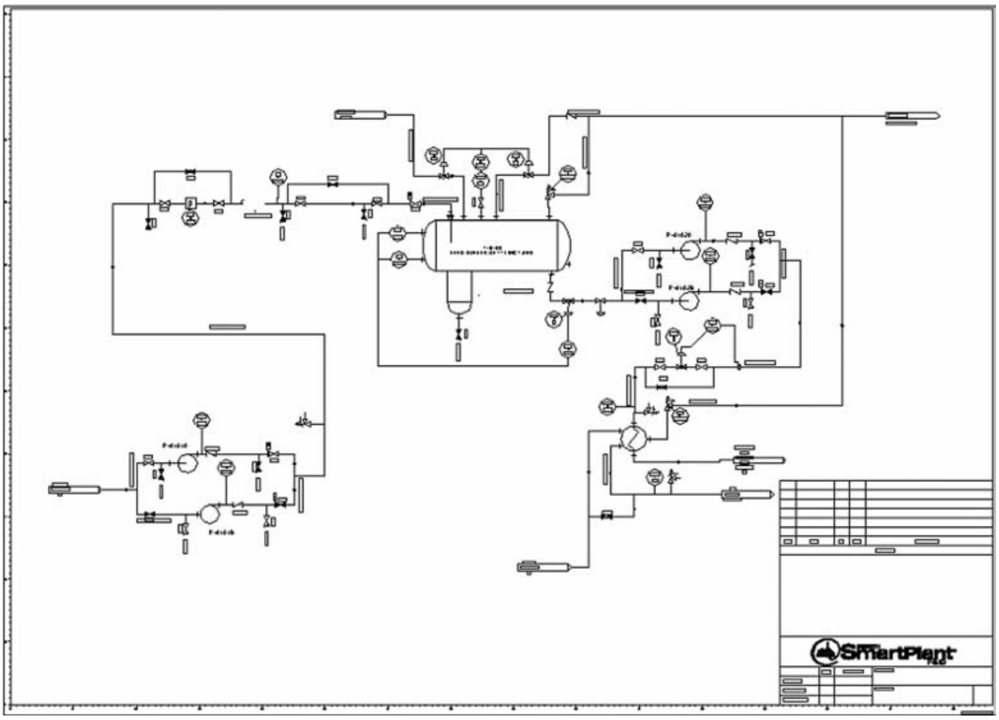
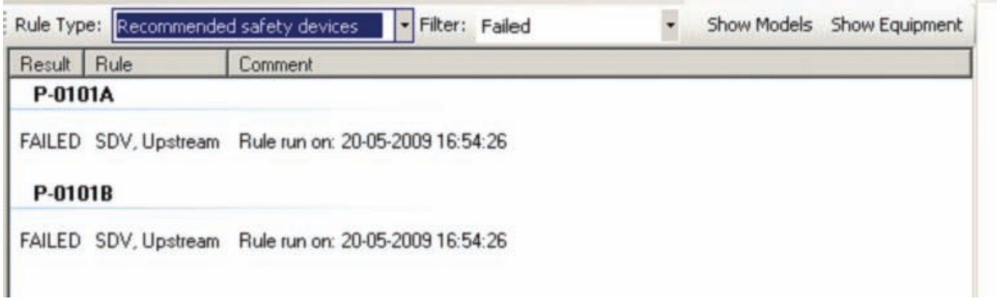


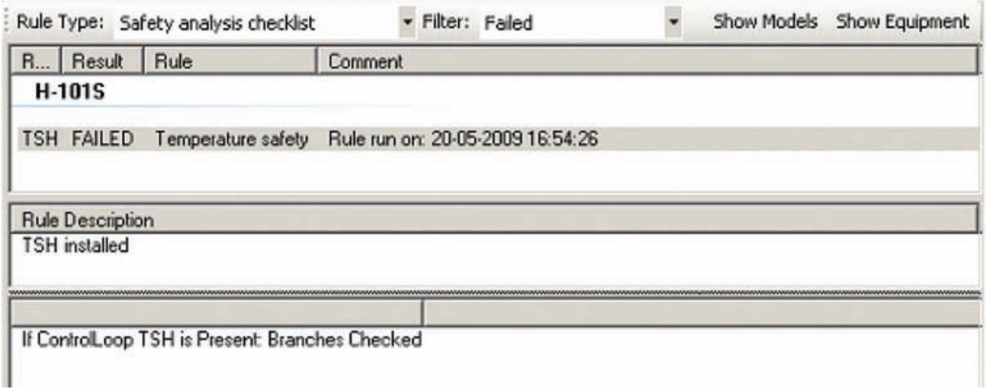
Figure 8. Modified P&ID



Rule Type: Recommended safety devices
Filter: Failed

Result	Rule	Comment
P-0101A		
FAILED	SDV, Upstream	Rule run on: 20-05-2009 16:54:26
P-0101B		
FAILED	SDV, Upstream	Rule run on: 20-05-2009 16:54:26

Figure 9. Result of revised case for safety device checks



Rule Type: Safety analysis checklist
Filter: Failed

R...	Result	Rule	Comment
H-101S			
TSH	FAILED	Temperature safety	Rule run on: 20-05-2009 16:54:26

Rule Description

TSH installed

If ControlLoop TSH is Present: Branches Checked

Figure 10. Result of revised case for safety analysis checks

CONCLUSIONS

Design Checker is intended to capture best practice knowledge related to safety and design in rule form and to help the production of P&IDs that embody best practice. With the direct integration of the Design Checker with intelligent CAD systems, P&IDs can be easily checked at any stage of the design process. This will avoid the necessities for rework and late changes to the P&IDs and to the plant, and will minimise time spent in safety study meetings on checking whether the P&IDs conforms to best practices.

Design Checker is developed to accommodate a number of rule sets representing different guidelines or standards so that a plant design can be checked against any of the rule set as appropriate. The paper illustrated an example using ISO 10418.

REFERENCES

ISO, 2003, ISO 10418 Petroleum and Natural Gas Industries – Offshore Production Installations – Basic Surface Process Safety Systems, HIS, Switzerland.

Lawley, H.G., 1974, 'Operability studies and hazard analysis', Chemical Engineering Progress, Vol. 70, pp.105–116.