IMPACT OF EMERGENCY SHUTDOWN DEVICES ON RELIEF SYSTEM SIZING AND DESIGN

R. K. Goyal and E. G. Al-Ansari
Bahrain Petroleum Company, Bahrain Refinery, The Kingdom of Bahrain

In the sizing of individual relief valves protecting equipment or process or system, it is a common practice not to take cognizance of any immediate operator action or the action of any mitigating devices. However, an increasing number of consultants and practitioners are recommending not applying the same philosophy when it comes to designing an overall refinery flare system to cope with common mode failures (e.g., loss of power, cooling water supply failure). They propose taking credit for the action of devices such as unit emergency shutdown (ESD) systems, trips (for example, fired heater fuel supply cut-offs), or auto-starts of pumps whose actions reduce the potential load on the overall refinery flare system. Savings can thus be realized in the sizing of flare headers and other ancillary equipment. While there is no objection, in principle, to taking credit for ESDs in the design of relief systems, its application in practice deserves careful scrutiny. There are still many related issues that have not been adequately addressed by the proponents of the credit-taking approach. This paper highlights these concerns and offers practical advice to those facing relief system design decisions.

1. TAKING CREDIT FOR SHUTDOWN DEVICES

In a modern refinery, the practice of atmospheric discharge of gaseous hydrocarbons from pressure relief valve (PRV) tail pipes, irrespective of whether on-plot or off-plot, is neither permissible under environmental guidelines nor desirable from a safety standpoint. The common approach, therefore, is to tie all (or most) pressure relief discharges from a unit into a manifold or unit header, which is then routed to a refinery relief header connected to a suitably sized flare system. Two systems are sometimes preferred – a low-pressure system and a high-pressure system.

The key parameters in the design and sizing of such a relief/flare header or manifold are the flow rate, the driving pressure and the type of material expected to enter the header from the discharge pipes of various relief valves connected to it. This in turn depends upon assumptions made as to the concurrence of relieving from several sources.

If it is assumed the header is required to handle the numerical sum of the *rated* capacities of all the relief devices in all the units discharging to it, then its calculated design size will truly be of enormous proportions – and require an equally enormous flare stack to match! Clearly, such an approach is wasteful and unjustifiable, especially where it can be demonstrated that an event culminating in simultaneous relief from all the valves at their

Contents of this paper are based upon views and opinions of the authors, and do not necessarily represent BAPCO's present or past policy, codes, standards and/or practices.

respective rated capacities is impossible to occur (except, perhaps, as an extremely elaborate act of sabotage).

A certain degree of realism can be injected into the header design process by assuming that the maximum relief load will be equal to the sum of the actual expected maximum relief flows from those valves which could lift under a given emergency situation. For example, consider utility failure (power, cooling water, instrument air, steam, fuel oil/fuel gas, inert gas, or a combination based upon inter-relationship or common cause) or unit/plant fire. The header size derived will be smaller than that resulting from the total rated relieving-capacity assumption discussed previously. It will, however, be large enough to handle the relief load from all foreseeable emergency situations.

Hence, in sizing a header/flare system, there can really be no serious objection to utilizing a conservative time-line analysis approach or a dynamic analysis based on process parameter levels expected under "upset" conditions to calculate the required relief load, provided individual peak relieving rates get adequately addressed in the analysis.

Further economy in the header and flare system size can be realized by assuming that, in practice, several of the relief valves will not be required to lift in an emergency. Pressure in the vessels or equipment protected by them will not rise above the PRV set pressures due to the action of any "automatic instrumentation" installed that tends to pacify the source of pressure build-up. Automatic instrumentation here does not refer to the normally operating control systems and instruments used to operate the refinery [sometimes referred to as the Basic Process Control systems (BPCS) – *see* CCPS (1993) automation guidelines]. It refers to non-normal instrumentation such as emergency shutdown devices (ESDs), trips, safety interlock systems, auto-lockouts or auto-starts (all termed "ESD" for the purpose of this paper).

Size reduction sought on the basis of ESDs (i.e., taking credit for ESDs in relief and flare system design) – though it appears to have a "prima facie" justification – is nonetheless fraught with controversy and a source of genuine concern, especially among operations managements. The key question, therefore, is: **should we or should we not take credit for ESDs in the relief/flare system design?**

Before delving into the pros and cons of the practice of taking credit for ESDs, some clarifications and comments regarding the applicable standards and other related topics need to be made in order to better define the scope of the concerns and the real, underlying issues.

Take process vessels designed in accordance with ASME "Boiler and Pressure Vessel Code" Section VIII, Division 1. The need for pressure relief devices is included in Parts UG-125 to UG-136 of the code. Similarly, British standard BS-5500 "Unfired fusion welded pressure vessels," specifies the need for PRVs. In terms of relief header sizing, no distinction is made between PRVs installed for code compliance purposes and those installed for other reasons.

Once a decision is made to install a PRV at a given location in a refinery unit, its inlet piping needs to be designed per API RP-520, Part II, Section 4. Similarly, design of other parts of the relief system – such as PRV sizing, individual discharge piping and the header piping – can be carried out on the basis of the various API recommended practices. Applicable sections of the API RPs are illustrated in Figure 1.

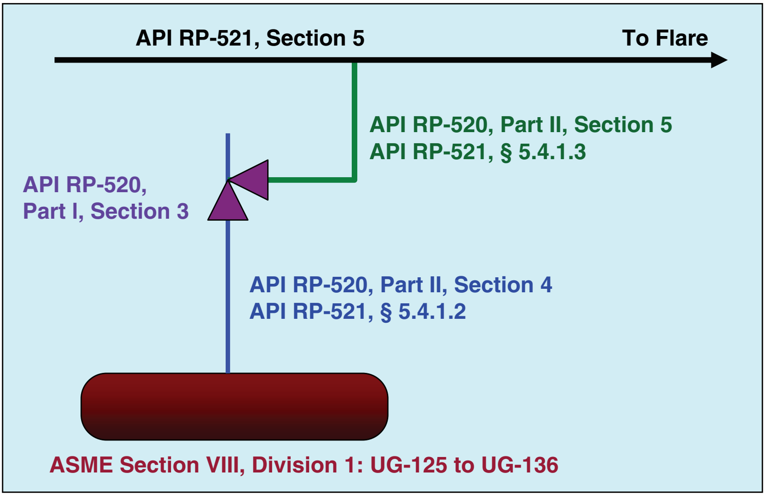
API RP-521, Section 5
To Flare
API RP-520, Part II, Section 5
API RP-521, § 5.4.1.3
API RP-520,
Part I, Section 3
API RP-520, Part II, Section 4
API RP-521, § 5.4.1.2
ASME Section VIII, Division 1: UG-125 to UG-136

Figure 1. Applicable standards

Some designers in this field will argue that the API RP-520 Part I (January 2000), Part II (August 2003) and RP-521 (March 1997) are merely "recommended practices," implying that these need not be adhered to as meticulously as warranted by codes of practice or standards. It should be noted that these two RPs are extensively used by designers worldwide in order to identify the minimum requirements necessary for an acceptable design. For all practical purposes, the status of these two RPs is on a par with that of any other internationally recognized standard or code.

In addition to being connected to various PRV discharges, the unit manifold may also be connected to piping carrying excess gas which needs to be directed to the flare header from time to time as part of the normal operation in the refinery or as part of a controlled flaring activity following a minor plant upset. A utility failure scenario at a time when such flaring is taking place has not been considered in this paper.

2. ADVANTAGES OF TAKING CREDIT

Clearly, the biggest advantage of taking credit for ESDs is minimizing the size of the relief system required to handle the PRV discharges from a unit or the entire refinery. Relief and flare headers are typical of other safety-related equipment in a refinery – they cost a great deal of money to design and install to begin with, and then take up a significant portion of the regular maintenance effort.

Consider the flare system shown in Figure 2. The main flare is designed to take discharges from four crude distillation units, a crude gas recovery unit, a visbreaker, a kerosene rerun unit, a hydrodesulfurization unit, a LPG treater, a naphtha rerun complex,

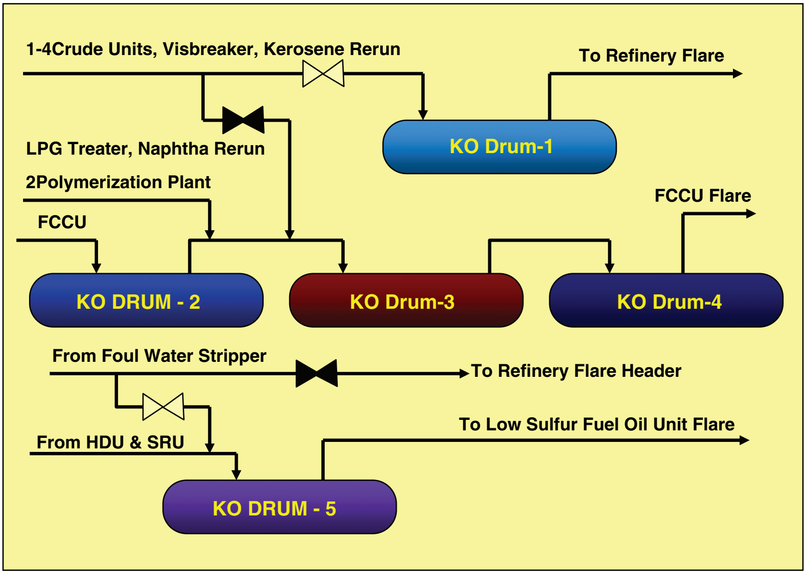

Figure 2. A typical refinery flare system

and several drip drums in the refinery gas circuit. The second flare (the FCCU Flare) is connected to the FCC unit, a crude unit associated with the FCCU, a polymerization plant, and a gas compression unit. During FCCU shutdowns for maintenance, the main refinery flare can also be taken out of service for maintenance by diverting its flare load to the FCCU flare.

The third, independent flare system – the LSFO (low sulfur fuel oil) Flare – serves the requirements of a hydrogen plant, a hydrodesulfurization unit, and a sulfur recovery unit. The foul water stripping unit is normally routed to the LSFO, but can be directed to the main refinery flare header if need be (this is to enable other units in the refinery to remain on-stream when the LSFO complex is down for maintenance). The presence of a Platformer/Unifiner unit brings into question the requirement of a fourth flare.

Header sizes of 36″, 42″, and larger are needed to handle the maximum possible flows from the units. In a large, well-spaced refinery requiring flare stacks to be located at a safe distance away, costs of installing large headers and associated equipment can be substantial. Furthermore, if some sections of the header system call for special metallurgy, then the costs escalate further.

If credit is taken for the unit/equipment ESDs in the belief that these will tend to reduce the expected flare load, then considerable savings in the investment costs can be realized by installing smaller size headers and ancillary equipment (valves, knockout drums, seal drums, etc.). Space required for the system would be smaller as would the civil/structural work. In some cases, a smaller system will result in lower regular maintenance costs (cleaning, inspection, etc.).

A major advantage of ESD credit taking is the use of existing relief/flare system for the purpose of permitting additional discharges into it. In the example illustrated in Figure 2, if ESD credit taking is not allowed then a fourth, new flare system will have to be engineered and installed to accommodate the relief load from the Platformer/Unifiner Unit.

If, on the other hand, credit is taken for the existing ESDs in various units of the refinery, then the existing flare headers can be modified to take in the relief load from the Platformer/Unifiner Unit at a fraction of the costs associated with a new flare system. The need to accommodate additional relief load is not just a hypothetical case. Many refineries have faced this problem – the need arising from a variety of reasons such as:

- Changes in product slate requiring alterations in process parameters
- Revamping or debottlenecking of existing units
- Technology upgrade
- Addition of new units
- Seeking compliance with more stringent environmental regulations
- Capacity increment.

Invariably, economic considerations must, and do enter into decision making on issues such as those illustrated in the example above. Consider a scenario in which ESDs are installed in the Platformer/Unifiner Unit and credit is taken for these ESDs in terms of reduction in the expected relief load, then it may be possible to accommodate this reduced load into one of the existing flare systems. If the life-cycle cost estimated for the installation and maintenance of the ESDs turns out to be greater than that associated with a new flare system, then the question of ESD credit taking is only of academic interest to the decision at hand.

It can be argued that there may be other reasons for the installation of ESDs to be considered. It could be due to the need to meet existing (or foreseeable, future) environmental regulations or part of an overall safety enhancement recommended by a HAZOP (hazard and operability) study team. Under these conditions, it might not be possible to maintain independence between these reasons and that related to the flare system.

Reduction in relief load means reduced flare stack diameter and length, reduced header and sub-header sizes, and hence lower investment. In addition to the effect on installation costs, and perhaps of greater significance, is the impact of relief load reduction on the following key parameters associated with the performance and siting of a flare stack:

- In-plant thermal radiation at grade
- Radiation received at adjacent equipment
- Radiation level at refinery fence-line
- Combined radiation from more than one flare
- Dispersion of combustion products
- Dispersion on flame failure
- Compliance with environmental regulations

- Health impact on immediate area
- Health impact on surrounding communities
- Quantity of product sent to flare.

3. TYPES OF ESDS

As mentioned earlier, the term "ESD" has been used in a generic mode in this paper. However, before discussing various ways in which credit could be taken for ESDs, there is a need to briefly describe the type of ESDs under question and the different terms being used in literature to refer to these. The emphasis is on *brief* descriptions rather than providing an elaborate set of definitions. A few noteworthy efforts in clearing up some of the confusion from safety system performance terms have been Gruhn (1993) and Beckman (1992 & 1993).

Safety Interlock System (SIS) is a term favored by the CCPS Safe Automation Guideline (1993). It consists of a dedicated controller (PLC) taking input from instrumentation installed for normal operating process control and/or sensors installed exclusively for the SIS. The output is in the form of dedicated alarms, event logger, and field actuation (automatic valve, motor starter or motor trip, etc.).

Three integrity levels can be considered for SIS design:

- Level 1 (low level) is a single path design with no redundant components
- Level 2 (medium level) consists of some redundancy (especially of components with known low reliability)
- Level 3 (high level) is a fully redundant system in which a high degree of reliability is achieved by means of redundant components, enhanced self-diagnostics, and avoidance of common mode failures (by selecting different types of sensors, etc.).

In addition to these, the term "**triple-modular-redundant** (TMR)" has been used to describe systems in which the objective is to achieve both high reliability and high availability (these are more popularly known as "two out of three voting" systems or simply as "2oo3").

Auto-lockout device refers to non-normal automatic instrumentation that trips or shuts a power or heat source. It is actuated by an abnormal condition and results in the stoppage of a process stream, a utility stream, and/or a piece of equipment that adds to a relief load. Examples are:

- Automatic steam supply shut off (valve closed) to a tower reboiler on high tower pressure
- Fuel gas supply shut off to the burners in a fired heater on high pass flow temperature, etc.

Auto-start devices, on the other hand, are those that attempt to reduce the flare load by *starting* some equipment. Examples are:

- An automatic start-up of a spare reflux pump (steam turbine driven) on electric power failure
- Automatic start-up of a cooling water circulation pump.

Shutdown systems for fired-heaters can consist of several levels; for example, individual main fuel trips, total "heat-off" and emergency shut down of the entire unit or a complex within the refinery. Process parameters that need to be brought into the ESD design logic can be determined by carrying out a quantitative risk analysis (QRA) of the costs in relation to the degree of desired availability and/or reliability of the installation. For further information on QRA methodology, *see* Goyal (1986 & 1993) and CCPS Guidelines (1989). Typical process parameters commonly considered in a QRA study for fired-heater shutdown systems are shown in Table 1.

The number of parameters from this list, which can be cost-effectively brought into the ESD design logic, depends entirely on the particular circumstances of a furnace installation. Hence, results from a QRA study identifying these parameters for one furnace installation cannot be directly used for a different furnace.

It should be noted that not all ESDs necessarily reduce the expected flare load. There can be situations in which an automatic trip can actually *increase* the expected flare load. An example of this is a steam-turbine-driven reflux pump which is expected to continue to work in the event of an electric power failure but gets cut out by a steam-load-shedding system acting to prevent failure of the overall plant steam supply system.

4. VARIOUS METHODS OF CREDIT TAKING

Either a time-line analysis or a dynamic analysis (sometimes referred to as "transient analysis") is generally performed to determine relief volumes under various emergency situations and on the basis of assumptions made about the impact of ESDs. It should be

Table 1. Parameters for furnace shutdown systems

#	Process parameter
1	High tube skin temperature
2	High individual pass outlet temperature
3	Low total heater pass flow
4	Low fuel gas pressure
5	Low pilot gas pressure
6	Low fuel oil pressure
7	Low atomizing steam pressure
8	High and low combustion air pressure (for forced draft)
9	Low combustion air flow (for forced draft)
10	High pressure in firebox
11	Low percentage of oxygen in flue gas
12	High percentage of combustibles in flue gas
13	High smoke density in flue gas
14	Low flue gas temperature (for air preheaters)

noted that the adequacy and applicability of methods currently available for sizing relief valves and a relief header to handle a *given*, predetermined relief load are beyond the scope of this paper. For more information on these topics, reference is made to several excellent articles by Cassata et al (1993), Coker (1992), Hall (1993), Leung (1992), Niemeyer and Livingston (1993), and Papa (1991).

The most popular method of taking credit for ESDs appears to be the "largest-load-failure" method. This can be illustrated through the example shown in Figure 3. The relief lateral for a given processing unit can be sized for the largest single relief valve within that unit under this method. For example, in Figure 3, if the Relief Valve "A" represents the largest load (i.e. it is greater than either "B" or "C"), then the Unit relief header could be sized to match the requirement of "A".

Consider a processing complex (say, part of a refinery) consisting of three units. Refer to Figure 4. The equipment in Unit-1 is protected by PRVs *A*, *B*, and *C*; in Unit-2 by *D*, *E*, and *F*; in Unit-3 by *G*, *H*, and *I*. The PRVs discharge into their respective unit relief headers, which in turn are connected to a common header for the whole complex. Additionally, assume that all equipment is protected with ESDs of reasonably high integrity, which act to prevent lifting of the PRVs under a specific contingency.

The sizing of inlet and discharge piping associated with each PRV is governed by rules given in API RP-520. If no credit is taken for the presence of ESDs, then Unit-1 relief header needs to be sized to accommodate the combined load from $A + B + C$. In the

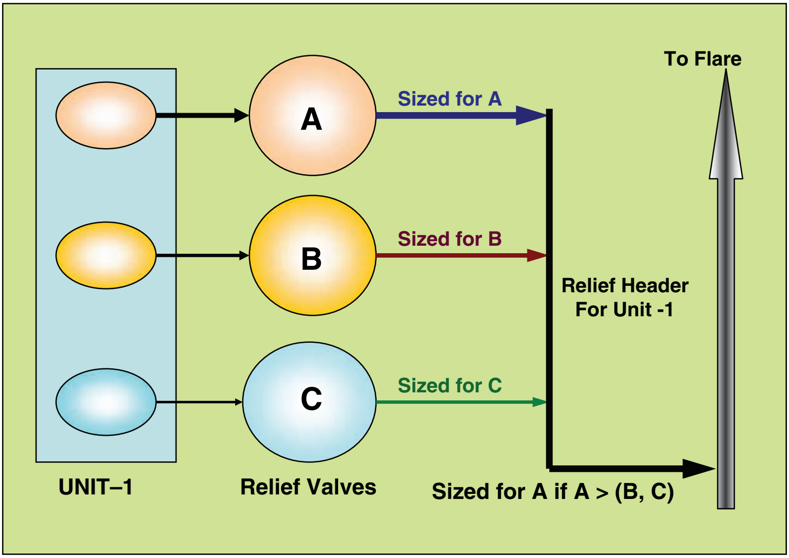

Figure 3. "Largest load failure" method

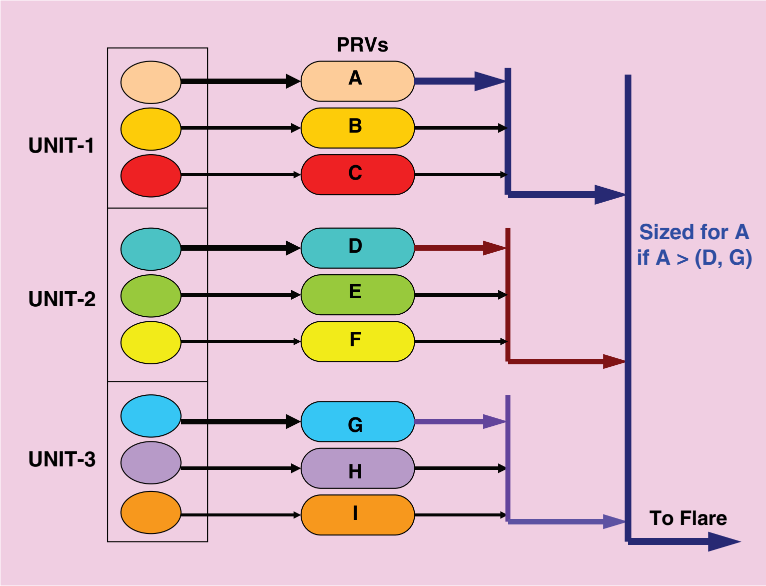

Figure 4. Further illustration of the largest-load-failure method

"largest-load-failure" method, it is assumed that the ESD corresponding to the largest individual load could fail under the stipulated emergency situation (i.e., fail to prevent the lifting of the PRV).

It should be noted that for the purposes of this discussion, the largest or maximum load is not necessarily the largest number of pounds per hour; it is the flow that results in the greatest friction loss through the header or pipe segment in question. Thus Unit-1 relief header need only be sized to take load from relief valve *A*, if *A* is largest among *A*, *B*, and *C*. Similarly, Unit-2 header can be sized for the load from *D* and Unit-3 for load from *G*; *D* and *G* being the largest among their respective unit loads.

This "largest-load-failure" concept is further utilized in sizing the common header for the complex. If the load corresponding to *A* is the largest among *A*, *D*, and *G*, then the common header can also be sized to accommodate load from *A* alone. The method can be extended and repeated to cover the entire refinery. Several variations on the basic theme of the largest-load-failure method have been proposed by engineering consultants and corporate engineering departments of operating companies.

An example of such a variation is inclusion of a caveat to ensure that the size of any relief manifold is not smaller than that corresponding to at least 25% of the total rated capacities of all relief valves connected to it. Another variation, closely related to the 25%-rated-capacity type, incorporates the requirement that the manifold size should be at least large enough to handle 25% of the total load expected in case of all associated ESDs failing to act. In the example illustrated in Figure 3, this requirement can be expressed as:

Size for Unit-1 Header = A, if $A > B$, and $A > C$, and $A > [0.25\ (A + B + C)]$
Otherwise,
Size for Unit-1 Header = $0.25\ (A + B + C)$

Some consultants recommend a more conservative "largest-pair-of-loads-failure" approach. This assumes that the ESDs corresponding to the two largest relief loads connected to the header will fail to act (i.e., fail to prevent lifting of the PRVs). Under this method, for the example in Figure 3:

Size for Unit-1 Header = $(A + B)$, if $(A, B) > C$.

Again, caveats such as the 25% rule, can be incorporated into the largest-pair-failure method. Since the methods listed above are all based on assumptions related to "failures" of ESDs, it is inevitable that selection of a particular method will be governed largely by the reliability (perceived as well as actual) of the ESDs under question.

5. OBJECTIONS TO CREDIT TAKING

There is no objection in principle, to the concept of taking credit for ESDs or any other shutdown devices/trips in evaluating relief system capacities. It is no different from any other cost versus risk-reduction benefit decisions faced by managements every day. In the highly competitive environment, which currently prevails in the refining business, the potential for savings associated with a smaller flare system cannot be dismissed lightly.

Nonetheless, before lending unequivocal support to the concept, a few concerns need to be aired and resolved. From the standpoint of operations and engineering managements these are considered to be extremely significant – in fact so much so as to disfavor the practice of ESD credit taking. Past incidents on record involving flare systems further add to a plant owner's anxiety in what is perceived as "cutting corners" in the system design. One example is the Grangemouth (U.K.) Refinery incident, *see* HSE (1989). Although not related to flare line sizing, it was, nonetheless, a major incident involving a flare system.

5.1 WHAT DO THE CODES RECOMMEND?

API RP-521 (March 1997) is considered the most widely used "guideline" in the design of relief and depressuring systems. An extract from paragraph 5.4.1.3.1 is worth reproducing here:

> *"... The discharge piping system should be designed so that the built-up back pressure caused by the flow through the valve under consideration does not reduce the capacity below that required of any pressure relief valve that may be relieving simultaneously."*

The above-mentioned statement is extremely clear and specific in terms of its content and guiding intent. It can be argued that ESD credit-taking violates the requirement quoted above in that if a smaller header size is selected it may permit the build-up of back pressure to such a level as to reduce the capacity of another PRV connected to the system *if the ESDs fail to act in the assumed manner*.

Nonetheless, the same source (i.e., API RP-521, paragraph 5.4.1.3.1) then goes on to state:

> *"...Common header systems and manifolds in multiple-device installations are generally sized based on the worst-case cumulative* required *capacities of all devices that may reasonably be expected to discharge simultaneously in a single overpressure event."*

The inclusion of "reasonably" in the above paragraph can be interpreted as providing justified support for the practice of ESD credit taking!

Apart from references of the type mentioned above, the latest publications of API RP-520 and RP-521 do not specifically sanction it nor do they oppose it. Furthermore, to our knowledge, there are no other internationally recognized standards, codes of practice or guidelines, which specifically permit or deny ESD credit-taking in relief system design.

5.2 LEGAL CONCERNS

The hydrocarbon processing and the chemical industries are sometimes portrayed in the media as being those causing many major incidents resulting in loss of life and property. Setting aside the validity of such claims, there is no denying that most reputable companies have been acutely aware of their responsibilities in terms of safety of the communities and the environmental issues since well before the onset of recent legislation on clean air and process safety management.

In the U.K., many companies embarked on a systematic search and evaluation of hazards in their plants in the mid 1970s. The driving force behind this effort was mostly self-imposed criteria by the industry rather than the force of law, *see* Al-Ansari (1990).

In Canada, the Canadian Chemical Producers Association (CCPA) published a policy on "Responsible Care" in 1983 and promulgated the "responsible care code of practice," CCPA (1989). In the U.S.A., the Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers picked up the challenge, and has admirably served the industry through the "guidelines" series of books. This "voluntary" effort by the industry culminated in API RP-750 (1990), which subsequently formed the basis for OSHA's proposed rule-making (July 1990) and regulation (February 1992).

A significant characteristic of the pre-OSHA era was that targets for risk reduction and/or risk acceptability began to appear in numerical, quantitative terms. CPQRA (Chemical Process Quantitative Risk Assessment) thus became an effective tool in the armory of the decision-makers – *see* CCPS (1989). Owner or operations management were readily willing to back decisions based on calculated risk. If a CPQRA analyst could demonstrate that the risk associated was negligibly small, then operating managements were willing to support a relief header sized by taking credit for ESDs.

In the post-OSHA period, the situation seems to have changed markedly. The punitive element, invariably associated with the law, has forced a major modification in the outlook of many operations managers. CPQRA no longer rules supreme. The first question management wants answered is: "Does this decision conform to existing international standards, codes of practice, or guidelines or best-known/approved practices?" Or, conversely: "Will we be in violation of, or interpreted to be in violation of any international code?" In the past, the fact that the API has been silent on the subject of ESD credit taking would have been just one factor in the overall decision-making process. Nowadays, this silence will get noticed with added alarm.

API must revise RP-521 to specifically permit ESD credit taking. Only then can operations management be expected to consider this a viable option in relief system design.

Acceptance of the ESD credit-taking practice despite the absence of a recognized standard backing the concept can lead to potential violation of the intent of OSHA 1910.119 (U.S. Federal Register, February 1992) "Process Safety Management ...." paragraph (d)(3)(H)(ii) which states that the employer shall document that equipment complies with *recognized* and generally accepted good engineering practices; the statement being applicable to relief system design and design basis as per paragraph (d)(3)(D) of the OSHA regulation.

Lack of a recognized standard leaves engineers and managers, who permit the design and installation of a relief system taking credit for ESDs, vulnerable to the possibility of unfavorable comment from official investigations of any loss or injury incidents involving relief system sizing. This concern should not be considered a mere speculation. Past experience of refinery management on incidents elsewhere, in which established industry practices were set aside in favor of calculated low-risk options, forces us to a closer scrutiny of this issue.

OSHA should be presented with the current situation related to the two paragraphs referenced earlier as a test case for interpretation of their mandate. They should be requested to state specifically that ESD credit taking does not constitute a violation of their intent. Only then will the practice be considered legally acceptable.

5.3 COMPROMISING A KEY SAFETY FEATURE

Even if the law permits taking credit for ESDs, a carte blanche approval can not be granted for this practice. Each application must be thoroughly analyzed on the basis of its particular situation.

In the field of loss prevention in the process industry, there are a few key features related to layout and design, which tend to enhance the intrinsic safety of a plant. For example:

proper ***spacing*** *(between equipment/units)*
proper ***size*** *(pipe/vessel size/wall thickness, etc.)*
proper ***steel*** *(correct metallurgy).*

These features, when incorporated into the layout and design of a refinery, provide a significant degree of safety by mitigating the consequences of process deviations and other incidents. Furthermore, they are, by and large, immune from the adverse effects of human error or other uncalled-for human intervention.

In well laid-out refineries, risk exposures will be limited because of the generous inter-unit distances. The EML (Estimated Maximum Loss) calculations carried out by the insurers in such cases reflect this lower risk, which, in turn, translates into lower premiums.

It can be argued that the ESD credit-taking practice compromises this safety margin. An "undersized" flare header receiving load from several units makes it possible for an equipment over-pressure event (which might lead to an explosion or fire) to occur simultaneously in more than one or all the units connected to the single flare system following a common mode initiating event such as power failure or cooling water failure.

In addition to the possible effect on insurance premiums, another area of concern is the fire-fighting and control capabilities, which need to be provided on site in a refinery. In well laid-out refineries, fire water systems and all other fire-fighting capabilities are based on the general assumption that emergencies will be limited to a single unit or area at a given time. Under-sizing a flare header raises a serious question as to the validity of that assumption.

Over years of disuse and potential neglect, some segments of a flare header system might get partially clogged by sludge deposits or liquid dropping out at low points or pockets in the system (present due to errors in design or construction). If such a system was originally sized to take the full load from all the sources feeding it (i.e., by not taking credit for the ESDs), then it will be more forgiving in the event of a partial blockage than a smaller system based on ESD credit-taking. Note this comment is not to be misconstrued in any way to mean condonation of design flaws (pocketed flare lines, etc.) and/or poor operating and maintenance practices.

5.4 INCOMPATIBILITY WITH SOME TYPES OF ESDS

The primary design basis and objective of some "ESDs" might be to provide furnace protection (i.e., minimize chances of heater explosions). As a result, the process parameters selected for input to such ESD systems may or may not be compatible with ESDs for which credit could be taken in relief system design.

Correct actuation of an ESD does not necessarily mean the relief load gets reduced to zero at the same instant. Residual heat in the fluid contained in a tower will often be sufficient to maintain flow through the relief valve for some time. Also, the time taken to discharge the vapor inventory from the PRV opening pressure down to the reseat pressure is not negligible.

In some cases, a heater ESD may be designed to close a valve in the burner fuel gas supply fitted with a minimum firing restriction orifice around the valve (note that use of these is discouraged nowadays). Furthermore, the heat capacity of the furnace, which depends on the type of refractory, will be another contributing factor to continuation of the relief discharge. It is imperative that all such factors are satisfactorily taken into account in time-line or dynamic analyses carried out to determine the maximum relief load expected from a given installation.

5.5 MULTIPLE-DEVICE UNITS: ONE OUT OF HOW MANY?

Some proponents of ESD credit taking have stressed that there exists a "very large margin of safety" under the method based on the assumption of the largest device failing. An example of this method is shown in Figures 3 and 4. Very large margins of safety would exist only when the largest device represents a large proportion of the total load. Admittedly, it is most likely to be the case in reality too, when the total number of devices or units connected to the common header is small (say, up to 5).

However, for the overall refinery, the assumption of failure of the mitigating device on the largest *single* individual load in the refinery **regardless of the total number of units attached to the combined header** needs to be investigated further. The "largest-load-failure" method theoretically allows an unlimited number of additional process units to be added to the system provided none of the individual relief sources is larger than the governing load.

Since the basic question is to determine if more than one mitigating device will fail concurrently when an initiating event occurs which causes the maximum combined header loading, the answer depends not only on the probability of failure of the individual devices but also on the total number of such devices. The binomial probability distribution function can be used to describe this case. Let "***p***" represent the on-demand failure probability of a single device and "***q***" the probability of the device acting successfully (therefore, ***p*** = 1 − ***q***). For the sake of simplifying the analysis, further assume that failure probabilities of all the devices are equal. Then the probability of "***r***" or more concurrent failures from a total of "***n***" devices is given by:

$$P_r^n = \sum_{j=r}^{j=n} \frac{n\,!}{j\,! \bullet (n-j)\,!} \bullet p^j \bullet q^{(n-j)}$$

An example set of calculations derived from some assumed values of variables ***p***, ***n*** and ***r*** is given in Table 2.

From the data in Table 2 it can be seen that the probability of ***r*** or more failures from a given number of total devices decreases with increments in ***r***. Further, if a certain level of probability can be regarded as negligibly small (for example, say, 10^{-6}), then the number of devices which must be assumed to fail to achieve this negligibly small probability of system failure can also be determined. This is illustrated in Figure 5.

Results from an analysis of probability distribution can also be summarized in the form of data given in Table 3.

It is, therefore, evident that any general rule-of-thumb such as "largest load failure," "largest two loads failure," or "minimum 25% capacity" is, by itself, insufficient to ensure an acceptable level of safety under all situations. The over-riding criterion, therefore, needs to be on the basis of risk estimate derived from quantitative risk analysis.

Table 2. Failure probability distribution

	Probability of r or more failures from a total of n, given $p = 0.05$ and $q = 0.95$, for				
r	$n = 5$	$n = 10$	$n = 15$	$n = 20$	$n = 30$
0	1.00	1.00	1.00	1.00	1
1	2.262e-01	4.013e-01	5.367e-01	6.415e-01	7.854E-01
2	2.259e-02	8.614e-02	1.710e-01	2.642e-01	4.465E-01
3	1.158e-03	1.150e-02	3.620e-02	7.548e-02	1.878E-01
4	3.000e-05	1.028e-03	5.467e-03	1.590e-02	6.077E-02
5	3.125e-07	6.369e-05	6.147e-04	2.574e-03	1.564E-02
6		2.755e-06	5.281e-05	3.293e-04	3.282E-03
7		8.198e-08	3.518e-06	3.395e-05	5.735E-04
8		1.605e-09	1.830e-07	2.857e-06	8.465E-05
9		1.865e-11	7.418e-09	1.979e-07	1.068E-05
10		9.766e-14	2.324e-10	1.134e-08	1.162E-06

6. RELIABILITY OF ESDS

From the discussion included in the preceding sections, it follows that the question of taking credit for ESDs cannot be resolved without taking into account their reliability. Some guidance, therefore, must be given on the desired reliability characteristics of an ESD system. One way to accomplish this would be to provide some information on the minimum acceptable levels of reliability, availability, and maintainability associated with such an ESD system; i.e., the level of integrity of the ESD system.

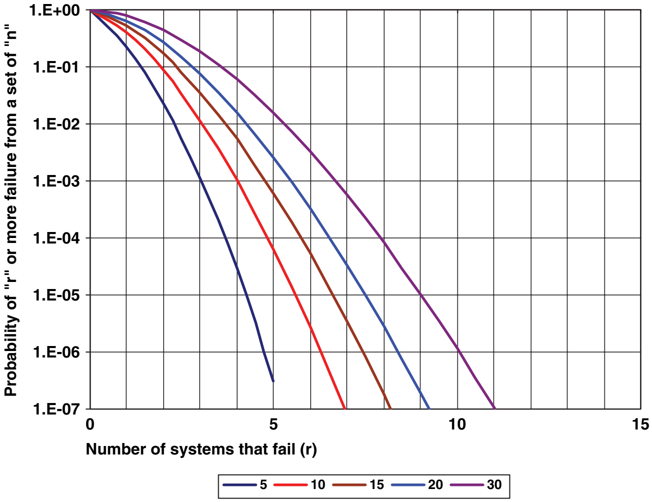

Figure 5. Failure probability distribution "r" failures from a a total of "n" devices

Table 3. Devices assumed to fail

Total number of devices (ESDs) that redice flare load	Number of devices that should be assumed to fail to achieve and extremely low level of overall system failure (10^{-5})
1–4	all
5	4
6–8	5
9–12	6
13–17	7
18–23	8
24–29	9
30–37	10
38–44	11
45–51	12

An easy, workable option from the standpoint of operations management would be to recommend that in each case a detailed reliability analysis be carried out of all instrumentation associated with ESDs for which credit-taking needs to be considered. Such an analysis should be conducted by an approved, qualified consultant. Nonetheless, this is easier said than done.

There are several key issues related to the reliability of ESD systems which need to be addressed by the reliability analyst to the satisfaction of operations management before credit-taking could be accepted.

6.1 HIGH-INTEGRITY ESDS VERSUS RELIABILITY OF PRVS

One claim often made is that in high-integrity systems (i.e., multiple redundant systems) the reliability of the ESD is usually greater than the reliability of pressure relief valves. A PRV tested annually has a *hazard rate* of 4×10^{-3} per year, and a duplicated trip system with weekly testing a *hazard rate* of 5.6×10^{-3} per year as mentioned in Lawley and Kletz (1975) and Lees (1980). From the above, the proponents of ESD credit-taking imply that since ESDs can be designed with high reliability, higher than that achievable with a PRV, therefore credit-taking is justified.

The hazard rate argument for the flare header design is, on the whole, irrelevant. If the decision under consideration was whether a PRV should be installed at a certain process location or not, then the hazard rates can be used as a criterion. The situation can be summed up as follows:

> *If you feel* ***extremely*** *confident that the ESD will work and will not permit an overpressure situation to arise, then don't install a PRV.*

> *If you feel a PRV needs to be installed, then don't undersize it because you feel the probability of it lifting is low due to ESD action. Provide a full-size PRV.* See *Kletz (1984).*
>
> *If you decide to connect the tail-pipe to the flare header, then don't undersize the flare header because you feel the probability of PRV lifting is low. Provide an adequately-sized flare header.*

6.2 RELIABILITY HAS NOT BEEN REALIZED IN PRACTICE

The experience with reliability of ESD systems (even the high- integrity systems) has been varied. With some of the earlier systems, Stewart (1971) reported that: "Sometimes it is shown by the safety assessment that the H.I.P.S. (High-Integrity Protective System) has not achieved its target design specification."

Undoubtedly, reliability of modern ESD systems is higher than that of systems designed in the past. This enhancement is the result of introduction of programmable digital devices, higher reliability of individual components and built-in redundancy and voting arrangements such as "2oo3 (2 out of 3)" and "1oo3." *See* Gruhn (1993) and Beckman (1992, 1993) for safety system reliability terms and calculation methods.

Nonetheless, the promise of high reliability has not materialized in practice. Even those systems that were selected and approved after rigorous FATs (Factory Acceptance Tests) have under-performed upon installation on-site. One major contributing factor is suspected to be poor software reliability.

Beckman (1993) states: "The reliability of the application software is a user responsibility, and it must be tested and validated by the user to ensure that it is free of faults, particularly latent faults (bugs)." Such a statement may find support among the vendors but is not likely to be favored by operating companies, i.e. the users. A significant portion of the responsibility must rest with the vendors. They must ensure the application software is not only free of bugs, but is also robust enough to withstand a certain degree of "rough treatment" in the field.

The operating companies, on their part, must provide accurate information on process variables, generate all deviation scenarios demanding intervention by the ESD system, participate fully in the application software development by the vendor and implement company procedures to carry out regular maintenance and testing of the installed system.

6.3 SPURIOUS TRIPS VIS-À-VIS HUMAN NATURE

Lack of reliable software sometimes results in a significant increase in the rate of spurious trips initiated by an ESD system. The consequential loss of revenue due to these unplanned stoppages can occasionally force an operations manager into taking the rather drastic measure of running the plant with the ESD bypassed. ESDs which are likely to be bypassed or switched over to "inhibit" mode should not be considered for credit-taking in relief header sizing.

One question often asked when designing ESD systems is: "What is an acceptable rate of spurious trips?" Lawley and Kletz (1975) considered a spurious-trip rate of 1.27 trips per year acceptable for the 1oo2 cross-connected high-pressure trip system they had studied. Is this a reasonably acceptable rate for other systems too?

From an end-user standpoint, the answer is given not in terms of spurious-trip rate alone, but in terms of its relationship to the ESD demand rate (i.e., frequency of process parameter deviations requiring ESD intervention). This is because the "perceived" reliability of the ESD system is equally important to the user. When next time the ESD shuts your plant down, are most of your operators convinced that it is a spurious trip? If yes, then they are likely to have little respect for the system installed. Such an ESD will be bypassed at the first opportunity.

A spurious-trip rate of 1 or 2 trips per year is acceptable only if the demand rate is also of the same order of magnitude. In this situation, operators will not regard the ESD system as a mere nuisance because each trip will be perceived as either being spurious or genuine, with equal probability.

If the demand rate is low, say 1 in 10 years (0.1 trips per year), then a spurious-trip rate of 1 per year may turn out to be unacceptably high. Additional cost of building a higher level of redundancy in the system to achieve a lower spurious-trip rate to match the demand rate would be justified here.

6.4 HIGH MTTR (MEAN TIME TO REPAIR)

Another problem created by poor software reliability is that the on-site times taken to diagnose and eliminate software faults have been longer than those predicted at the design stage. Operating companies do not possess software expertise of a level necessary to carry out quick and effective maintenance on these systems. They have to rely on vendor specialists to provide this service on call. The higher MTTRs mean that ESDs remain in a bypassed mode for significant durations of time. Once again, taking credit for such ESDs in relief system design is not advisable.

7. CONCLUSIONS AND PATH FORWARD

While there is no objection to the concept of taking credit for ESDs in the relief and flare header sizing and design, each application needs to be individually scrutinized to ensure plant safety is not compromised. Special attention needs to be given to potential impact on other units sharing the relief header.

The current API recommended practices (RP-520 and RP-521) appear to be silent on this issue. There are no other internationally recognized standards, codes of practice or guidelines which specifically permit taking credit for ESDs in relief system design. There is a need to initiate a dialog with the API and/or hold further discussions under the aegis of some other recognized body, such as the NPRA (National Petroleum Refiners Association), for guidelines to be established and placed on record.

Confirmation should be sought from OSHA that taking credit for ESDs in relief system design does not constitute any violation of the intent of OSHA 1910.119 Paragraph (d)(3)(H)(ii) which states that the employer shall document that equipment complies with recognized and generally accepted good engineering practices; the statement being applicable to relief system design and design basis per Paragraph (d)(3)(D) of the OSHA regulation.

In addition to giving approval to the concept, any future internationally recognized standards or codes must incorporate detailed guidelines on the types of ESDs for which credit-taking would be permissible. These should include reliability targets for high-integrity ESDs or a directive to conduct detailed reliability analyses of such systems.

From an operating company management standpoint, ESD credit-taking is not advisable before this practice is clearly recognized and/or approved in an international standard or code. Lack of such a standard leaves engineers and managers, who permit the design and installation of relief systems taking credit for ESDs, vulnerable to the possibility of adverse comment from official investigations of any loss or injury incidents involving relief system sizing. In a court of law, it would place them in a weak defensive situation.

Even if ESD credit-taking becomes an “approved” practice, operating company management are advised to exercise caution. An extremely risk-aversed inter-unit spacing in a well laid-out refinery is a valuable asset. It presents a natural barrier to the insurer’s EML calculations. Do not erode this barrier by opting for “savings” in the relief header and flare system costs.

Designers and suppliers of ESD systems need to prove that the on-stream availability and reliability of their systems, so readily demonstrable on paper or in FATs, can be reproduced on-site, and are practically immune to environmental factors arising from geographical location or the work ethos of the client company. In a market place of ever-shrinking refining margins, the incessant pursuit of cost effectiveness in all decision-making is not merely a desirable activity, but the key to survival. However, cost effectiveness must never be misconstrued to mean indiscriminate cost-cutting.

LITERATURE CITED

Al-Ansari, Isa G. A., *BAPCO’s Risk Assessment Programme*, Bahrain Society of Engineers, 1990.

American Petroleum Institute (API), *Management of Process Hazards*, Recommended Practice 750, Washington D.C., 1990.

American Petroleum Institute (API), *Guide for Pressure-Relieving and Depressuring Systems*, Recommended Practice 521, Fourth Edition, Washington D.C., March 1997.

American Petroleum Institute (API), *Sizing, Selection, and Installation of Pressure-Relieving Devices in Refineries, Part I. Sizing and Selection*, Recommended Practice 520, Seventh Edition, Washington D.C., January 2000.

American Petroleum Institute (API), *Sizing, Selection, and Installation of Pressure-Relieving Devices in Refineries, Part II: Installation*, Recommended Practice 520, Fifth Edition, Washington D.C., August 2003.

American Society of Mechanical Engineers (ASME), *Boiler and Pressure Vessel Code, Section VIII, Division 1, Parts UG-125 to 136*, Washington D.C., 1992.

Beckman, Lawrence V., *How reliable is your safety system?*, Chemical Engineering, issue January 1992 (pp 108–114).

Beckman, Lawrence V., *More on safety systems. Letters to the editor*, Hydrocarbon Processing, issue December 1993 (p 35).

British Standards Institution (BSI), *Unfired fusion welded pressure vessels, BS-5500,* London, U.K., 1976.

Cassata J.R., Dasgupta S., Gandhi S.L., *Modeling of tower relief dynamics*, Hydrocarbon Processing, Gulf Publishing, Houston, Texas, U.S.A., issue October 1993 (pp 71–76).

CCPA, *Responsible Care Codes of Practice*, The Canadian Chemical Producers' Association, Ottawa, Ontario, 1989.

Center for Chemical Process Safety (CCPS), *Guidelines for Hazard Evaluation Procedures (Second Edition)*, American Institute of Chemical Engineers, New York, N.Y., 1992.

Center for Chemical Process Safety (CCPS), *Guidelines for Chemical Process Quantitative Risk Analysis*, American Institute of Chemical Engineers, New York, 1989.

Center for Chemical Process Safety (CCPS), *Guidelines for Process Equipment Reliability Data*, American Institute of Chemical Engineers, New York, 1989.

Center for Chemical Process Safety (CCPS), *Guidelines for Engineering Design for Process Safety*, American Institute of Chemical Engineers, New York, 1993.

Center for Chemical Process Safety (CCPS), *Guidelines for Safe Automation of Chemical Processes*, American Institute of Chemical Engineers, New York, 1993.

Coker, A.K., *Size Relief Valves Sensibly – Parts 1 and 2*, Chemical Engineering Progress, August 1992 (pp 20–27), November 1992 (pp 94–102).

Goyal R.K., *Probabilistic Risk Analysis – Two Case Studies from the Oil Industry*, Professional Safety, July 1986, American Society of Safety Engineers, Des Plaines, Illinois, 1986.

Goyal R.K., *Practical examples of CPQRA from the petrochemical industries*, The Institution of Chemical Engineers (IChemE), Process Safety and Environmental Protection, Transactions of the IChemE, Vol 71, Part B, Rugby, England, U.K., May 1993.

Gruhn, P., *Safety system performance terms: clearing up the confusion*, Hydrocarbon Processing, February 1993 (pp 63–66).

Hall, Stephen M., *Size and Design Relief Headers*, Chemical Engineering Progress, March 1993 (pp 117–122).

Health and Safety Executive (HSE), *The fires and explosion at BP Oil (Grangemouth) Refinery Ltd.* —A report of the investigations by the HSE into the fires and explosion at Grangemouth and Dalmeny, Scotland, 13 March, 22 March and 11 June 1987, Her Majesty's Stationery Office, London, U.K., 1989.

Kletz, Trevor A., *Myths of the Chemical Industry*, The Institution of Chemical Engineers, Rugby, U.K., 1984.

Lawley, Herbert G. and Kletz, Trevor A., *High-Pressure-Trip Systems For Vessel Protection*, Chemical Engineering, May 1975 (pp 81–88).

Lees, Frank P., *Loss Prevention in the Process Industries*, Volumes 1, 2, 3, Butterworth, London, U.K., Second Edition 1996.

Leung, Joseph C., *Size Safety Relief Valves for Flashing Liquids*, Chemical Engineering Progress, February 1992 (pp 70–75).

Niemeyer C.E. and Livingston G.N., *Choose the Right Flare System Design*, American Institute of Chemical Engineers, Chemical Engineering Progress, New York, N.Y., December 1993 (pp 39–44).

NFPA, *Codes and Standards*, The National Fire Protection Association, Quincy, Massachusetts.

OSHA 29CFR Part 1910.119, *Process Safety Management of Highly Hazardous Chemicals*, Federal Register Vol. 57, No. 36, Washington D.C., February 24, 1992.

OSHA 29CFR (Code of Federal Regulations) Part 1910.119, *Notice of Proposed Rulemaking: Process Safety Management of Highly Hazardous Chemicals*, Federal Register Vol. 55, No. 137, Washington D.C., July 17, 1990.

Papa, Donald M., *Clear Up Pressure Relief Valve Sizing Methods*, Chemical Engineering Progress, August 1991 (pp 81–83).

Stewart, R.M., *High integrity protective systems*, The Institution of Chemical Engineers (IChemE), IChemE Symposium Series No. 34 (pp 99–104), Rugby, England, U.K., 1971.