Harpur Hill, Buxton, SK17 9JN
Telephone: 0129 821 8234
Facsimile: 0129 821 8271

HEALTH & SAFETY LABORATORY

The application of BS EN 61508 to industrial boiler installations: Report 2 – Development of a strategy for the allocation of risk to individual boiler safety functions

CI/05/11

Project Leader: **Dr A M Wray**
Author(s): **A M Wray BSc PhD**
Science Group: **Engineering Control Group**

DISTRIBUTION

Mr G Hawkins	HIDCD5
Mr S Brown	NSD4C
Mr W Black	Blacksafe Consulting Ltd
Mr P Pearson	Dalkia Utilities Services
Mr R Bell (2 copies)	NSD4C
Dr N G West	HSL
Mr P F Heyes	HSL
Dr A M Wray	HSL
Mr R B Lee	HSL
Group 2 circulation	HSL
Registry file	HSL
Library (2 copies)	

This report and the work it describes were funded by the Health and safety Executive. Its contents, including any opinions and/or conclusions expressed, are those of the author alone and do not necessarily reflect HSE policy.

Available to the public

HSL report approval:	Mr P F Heyes
Date of issue:	May 2005
Job number:	JS2003601
Registry file:	CI/RE/51
Filename:	Report2.doc

CONTENTS

1 Introduction....1
2 The BS EN 61508 approach: Brief summary....3
3 Determining the tolerable risk for the installation....5
3.1 Individual, societal risk and cost-benefit criteria....5
3.2 Determination of target risk for the safety functions....6
3.3 The "As Low As Reasonably Practicable" (ALARP) concept....7
4 Initial determination of the target risk reduction for each safety function....9
4.1 Installation 1 (Large Industrial site)....10
4.2 Installation 2 (Hospital)....14
4.3 Installation 3 (Laundry)....15
5 Allocation of the target risk between the safety functions....18
5.1 Installation 1....18
5.2 installation 2....20
5.3 Installation 3....21
6 Allocation of target risk: A simpler approach....22
6.1 Safety Integrity Levels: Points to note....26
7 Conclusions....28
8 References....30

EXECUTIVE SUMMARY

Programmable Electronic Systems (PES) are becoming increasingly commonplace in boiler control and protection. The monitoring and control facilities provided by these systems may be very sophisticated, allowing automatic shutdown, remote monitoring and a facility to automatically indicate at a remote engineering site that a fault has been detected. As a result of this, there is pressure to reduce the manning levels and place an increased reliance on the safety-related control systems.

The existing HSE guidance note, PM5, on automatically controlled boilers predates the use of PES in boiler control and the recently published standards, e.g., BS EN 61508, which cover these technologies.

This report is the second in a series of reports and describes methodologies for allocating the SILs[1] between safety functions, and is intended to provide some of the information that will allow a state-of-the-art revision of PM5 to be made.

This, and the previous, report focused on the determination of safety-integrity requirements, and whether the hardware in current use is likely to be capable of meeting the relevant probability of failure on demand criteria. Further work is needed to determine if the application of the other requirements in IEC 61508, relating to systematic failures, is practicable in the case of boiler installations. The work will need to consider the work processes under which hardware and software are specified and implemented throughout the entire lifecycle from SIL determination through to operation, maintenance and modification.

OBJECTIVES

To consider the analyses of three diverse boiler installations described in the previous report, and determine, using a risk-based approach, how the Safety Integrity Levels should be allocated to the various safety functions.

MAIN FINDINGS

1) A simplified means of estimating the target SILs for various boiler safety functions has been developed for the majority of boiler applications where the consequence of failure is restricted to less than 5 employees. For applications involving more than 5 fatalities to employees, or a fatality to a member of the general public, more fundamental techniques will be needed.

2) Although this assessment has worked through the calculations for the pressure function, this would not currently be required for conformity with current UK legislation, assuming adequate pressure-relief valves are in place.

3) The pressure safety function provides only a small contribution to the overall risk associated with Installations 1 and 2. This safety function is carried out electronically

[1] Safety Integrity Levels

(i.e., shut down the burners) and mechanically via the safety valve(s). Because the safety valves provide a protection channel that is independent of that involving the burner shutdown valves, the shutdown valves provide a less-significant contribution to the overall risk via the pressure function. However, the other safety protection functions rely on the shutdown valves to close down the burners if a malfunction is detected. As a result, the outcome of the risk calculations depends strongly on the failure rate of these valves. Therefore, an accurate estimate of the failure rate of these valves (i.e., not a generic estimate as used in Reference 2 and, as a consequence, also in this report) would be required for an assessment using IEC 61508.

4) Estimates of the safety-integrity-level requirements of the various safety functions of a generic boiler installation have been made. These indicate that the SIL requirement of the low-water protection function (SIL4, or SIL3 if changes are made as indicated in the text) is more onerous than that for the other protection functions, and reflects the high demand rate determined using data from the monitoring systems at Installations 1 and 2, and the predicted consequences. This confirms the critical nature of the safety function that provides protection against low water. Traditionally, this has demanded a high level of manning during the operation of the boiler and will be a key concern in relation to the use of automated systems as a means of reducing manning levels.

5) The achievement and maintenance of SIL4 using complex technology, e.g., programmable electronic devices, will not be easy unless specialist design techniques appropriate to high-integrity protection systems are used. High levels of competency and safety management will also be needed throughout all stages of the safety lifecycle including operation and maintenance. SIL4 systems are currently extremely rare, even in major hazards process plant. This has implications not only for the hardware reliability, but also for the systematic integrity of both hardware and software.

6) The allocation of risk targets for individual safety functions that contribute to the risk control of a common hazardous event can be carried out in a number of ways with a consequent impact on the safety integrity requirements of the various safety functions.

7) Further work is needed to determine if it is practicable to apply the other requirements of IEC 61508 (e.g., associated with systematic failures) to boiler installations. The work will need to consider the work processes under which hardware and software are developed, specified and implemented throughout the whole safety lifecycle from SIL determination through to operation, maintenance and modification.

1 INTRODUCTION

HSL report "The application of BS EN 61508 to industrial boiler installations: Report 1 - Hardware reliability aspects", Reference 2, described the quantitative reliability analyses of the safety-related systems of three boiler installations. The analyses determined that, despite a conservative approach being applied, the hazard rates associated with the installations were generally ALARP[2].

The analyses, intended to form a baseline for future work, predicted the hazard rate expected of the installations. Although the overall aim of the work, of which the analyses formed part, was to assist in the preparation of guidance for a future revision of HSE guidance on this subject (e.g., PM5 - Reference 1) in accordance with the principles of BS EN 61508, the analyses made no reference to this standard. The reason for this is that the analyses were intended to determine the risk presented by current installations. This contrasts with the approach taken by a quantitative analysis according to BS EN 61508, which starts with a target risk and works backwards in order to determine target system failure rates, i.e., is intended to assist the designer in determining the integrity required for the individual functions carried out by the system.

This report describes the approach that would be taken in determining the target risk allocated to each safety function in a boiler installation in order to carry out an analysis based on BS EN 61508; however, the approach will draw heavily on the calculations carried out in the previous analyses. Therefore, it is recommended that the reader becomes familiar with the analyses described in Reference 2.

The author developed the approach with the assistance of Mr W Black of Blacksafe Consulting Ltd under the general direction of a steering group whose members were:

- Mr G Hawkins, HSE HIDCD5;
- Mr S Brown, HSE NSD4C;
- Mr P Pearson, Dalkia Utilities Services;
- Mr W (Bill) Black, Blacksafe Consulting Ltd, and
- Dr A M Wray, HSL.

This report describes each stage of the process of allocating the risk between the safety functions, even though it may be possible to use intuition to avoid some of the (somewhat) iterative processes and still achieve the required goal.

Readers should note that this report is not intended to describe an assessment of the three installations using BS EN 61508. Instead, it is intended to illustrate a methodology for allocating risk between the various safety functions of these installations, so actual values of risk, risk reduction, probability of failure on demand, shown in this report, are for only illustrative purposes.

---

[2] As Low As Reasonably Practicable – see Reference 3. A list of abbreviations will be found at Appendix A of this report.

Whilst this work, and the related report (Reference 2), provide a comprehensive example of quantified reliability assessment and risk analysis as applied to industrial boiler installations, they should not be regarded as indicative of HSE policy, or as guidance towards meeting statutory requirements at the time of publication of this report.

2 THE BS EN 61508 APPROACH: BRIEF SUMMARY

The approach to be followed when designing protection systems using BS EN 61508 takes the following steps. (See Part 1 of Reference 4.)

1) Determine a list of hazards, and hazardous events, appropriate to the installation and the event sequences leading to these hazardous events.

2) Determine the tolerable risk for each hazardous event and then allocate this to the safety functions involved. This can be undertaken using qualitative or qualitative methods. In the UK, criteria for tolerable risk are defined in Reference 3. This document is concerned with overall risk; however, targets for the tolerable risk appropriate to the hazardous events and, hence, to the individual safety functions can be derived from the overall targets given in this document.

3) For low-demand-mode safety functions, determine the initial risk at the installation in the absence of the safety function under consideration, but taking into account other relevant risk reduction measures.

4) The ratio between the results of Item 2 and Item 3 provides the Target Risk Reduction (TRR) that must be provided, as a minimum, by the safety function under consideration. This is the inverse of the Target Probability of Failure on Demand ($TPFD_{av}$) of the protection system, i.e., $TPFD_{av}=1/TRR$, and assumes that the various protection layers have been designed to avoid common-cause failures.

5) The $TPFD_{av}$ [or Target Probability of Failure per Hour (TPFH) if the safety function is operating in high-demand/continuous mode] will fall into one of 4 ranges defined by Table 2 [Table 3] of Part 1 of Reference 4. This table defines the Safety Integrity Level (SIL) required of the safety function.

6) Some aspects of the integrity of the system cannot adequately be defined by the $TPFD_{av}$ or TPFH, for example, software quality. The SIL defines a range of qualitative measures that, based on engineering judgement, are considered to be appropriate for the range of $TPFD_{av}$/TPFH for each SIL. Therefore, the qualitative requirements for each SIL must be applied to the protection system and its design.

7) Having obtained the $TPFD_{av}$ or TPFH, the hardware can be designed such that:

- its predicted Probability of Failure on Demand (PFD) is less than the $TPFD_{av}$, or its PFH is lower than the TPFH, i.e., PFD<$TPFD_{av}$ or PFH<TPFH, depending on the mode of operation (See Reference 4.);

- it meets the qualitative design requirements described at Item 7, for example, the qualitative aspects may require greater redundancy or particular techniques to be used in the production of the software, and

- other aspects associated with the subsequent life-cycle stages of the system can be determined from the $TPFD_{av}$/TPFH, for example, the various proof-test intervals that

must be applied during routine maintenance in order to ensure that the $TPFD_{av}$ is actually achieved.

The methodology in this report describes the development of procedures that will be followed in order to complete Steps 1 to 6 for the three boiler installations described in Reference 2.

Where an electrical safety-related system provides a safety function that operates in a continuous demand mode, it may be inappropriate to determine its $TPFD_{av}$. In this case, its TPFH must be determined.

3 DETERMINING THE TOLERABLE RISK FOR THE INSTALLATION

Reducing Risks Protecting People (Reference 3) will be used as the basis for determining the tolerable risk. Readers are advised to consider this document when carrying out a risk assessment.

Individual risk, societal risk and cost-benefit criteria should all be considered; however, individual risk normally dominates in cases where the risk is restricted to a small number of workers as is the case for the majority of boiler installations.

3.1 INDIVIDUAL, SOCIETAL RISK AND COST-BENEFIT CRITERIA

An examination of the calculations described in Reference 2, shows that the greatest risk is subjected to the workers at each installation and that, in comparison, the public at large would not significantly be affected by any of the three installations that were assessed. Therefore, we shall base our calculations on individual risk in the case of Installations 1 and 2, where only a single boilerman will receive any significant risk from the installation. In the case of Installation 3, more than one person is exposed to the risk. For the purposes of the examination described in Reference 2, the mean individual risk of those persons on site was determined, and was taken to be the total risk divided by the number of persons on site (i.e., 8). Consideration should be given to the fact that a hypothetical person is very unlikely to be exposed for more than 25% of the time. (This assumes: a working week of 48 hours and that 46 weeks are worked per year, allowing for holidays, illness, etc.)

In the case of installations in which the risk to a large number of people would dominate, such as an aeroplane or nuclear power plant, societal risk should be determined. This would generally apply where members of the public were exposed in large numbers, as would be the case if, for example:

- Installation 1 were located close to a school;
- Installation 2 were located within the main hospital building (or there would be significant patient consequences if there were a loss of the steam supply), or
- Installation 3 were located within a laundry forming part of a busy shopping centre.

The risks to on-site workers are shown by Reference 2 to dominate the overall risk at the installations under consideration. For example, the overall risk calculated for the boilerman at Installation 1 was a factor of 5.5 higher than the risk to persons outside the boilerhouse, mainly because of the remote location of the boilerhouse. If the boilerhouse had been located near a busy thoroughfare, the societal risk would significantly have been increased. In such circumstances, the public's perception of risk is not linear with the number of people at risk, leading to a need for proportionally greater risk reduction as the hazard level increases. As individual risk dominates in the installations under consideration, the

risk assessments that will be followed will be based on individual risk and not societal risk[3]. However, the methodology to be described could be applied in either case.

In addition to the normal consideration of risk, if many people are at risk, one must take into account the risk aversion factor. This allows for the public perception of risk rising much faster than the number of people (N) actually at risk. As a general rule, the risk aversion factor is proportional to $N^{1.5}$ or N^2 and societal risk becomes significant where the occupancy is greater than about 5.

If the consequences of any of the hazards are so severe that off-site risks become significant, these risks should be included in the assessment. The off-site risks have not been considered in this assessment only because:

- Reference 2 has already shown them to be small in comparison to the on-site risks,
- there is little, if any, risk to the public;
- the occupancy is <5, and
- to simplify and, therefore, improve the clarity of this report.

In addition, it will be necessary to establish the cost of providing any further reductions in the risk, i.e., the ALARP principle (See Reference 3.) will need to be applied. Since the individual risk is likely to be reduced to a low value, and there are few exposed persons, it is unlikely that there will be a significant benefit (in terms of cost) in reducing the risk further. A cost-benefit analysis can be considered once the residual individual risk has been determined.

3.2 DETERMINATION OF TARGET RISK FOR THE SAFETY FUNCTIONS

Reference 3 indicates that the upper tolerable limit of risk of death to any individual is 1 in a 1000 per annum, but qualifies this by stating that the actual individual risk is normally well below this value. We could choose an arbitrary value of risk as our starting point, in order to ensure that the level of risk was well below the upper limit; however, instead, we shall work downwards from this upper limit. Therefore, our aim is to ensure that the overall individual risk to our boilerman[4] is less than 10^{-3} per year.

This upper limit of risk results from all sources of risk associated with the workplace. In the case of our boilerman, it will include his journey between sites (but not his journey to work), trips and falls, etc. Table 1 gives examples of the workplace risks that our boilerman must face[5].

---

[3] As a general rule, societal risk should be considered in addition to individual risk when the occupancy associated with a hazard exceeds about 5.

[4] If the upper limit of risk of death to any individual is 1 in a 1000 per annum, it follows that the hypothetical individual to which it applies must be the most vulnerable to the hazard. By definition, this must be the boilerman at Installations 1 and 2.

[5] The tables throughout this report are linked to spreadsheets that carry out the relevant calculations. Because of the uncertainty in the calculations, only two significant figures are displayed; however, the underlying

Table 1: Examples of typical workplace risks

Hazard	Risk	Unit of measurement
Risk of injury travelling to work (Reference 3)	7.0E-07	per kilometre
(assume daily trip of 10km between sites)	1.4E-05	per day
(assume 220 workdays per year)	3.1E-03	per year
Risk of death from a road accident: overall	6.0E-05	per year
During journey between sites	2.6E-05	per year
Risk of death: all types of accidents (Reference 3)	2.5E-04	per year

It will be seen that, assuming that our boilerman travels 10km to and from the site of the installation as part of his daily working routine for 220 days of the year, his risk of injury associated with only his journey will be 3.1_{10}-3 per year, and his overall risk of death will be 2.6_{10}-5.

In the design of a boiler control system, we have no control over the work-related risks that are present but which are unrelated to the operation of the boiler. Therefore, to ensure that the risk of failure of the boiler-control functions does not provide a significant contribution to the overall risk, we must ensure that the contribution from the boiler-control functions is significantly below the upper limit. To achieve this, we shall take our target level of risk for all hazards associated with boiler-control functions to be 10% of the upper limit. This leads to the initial target risk associated with the overall boiler installation being 10^{-4}.

The boilerman's risk of death from driving is about $2.6_{10}{}^{-5}$ per year, which is included in his overall risk of death from all types of accident of $2.5_{10}{}^{-4}$ per year. By ensuring that the target risk from the entire boiler installation is less than 10^{-4} per year, we shall automatically ensure that the overall risk of death faced by our boilerman is less than 10^{-3} per year (and probably less than $3.5_{10}{}^{-4}$ per year).

It should be noted that the road-related risk for our boilerman has been assumed to be 2. $6_{10}{}^{-5}$ per year, which is similar to a typical home-to-work journey. However, if it were necessary for our boilerman to visit a large number of sites each for a short period or the sites were in, for example, the Buxton area, where road-related risks are high, the time spent driving between sites may introduce a significant risk that would need to be taken into account in its own right. In this case, suitable precautions would be required, for example, sending drivers on an advanced driving course.

3.3 THE "AS LOW AS REASONABLY PRACTICABLE" (ALARP) CONCEPT

Reference 3 suggests a "Value for Preventing a Fatality" (VPF) of £1,000,000 at 2001 prices. Allowing for inflation, the corresponding value would be about £1,100,000 in 2004. Table 2 shows the calculations, which determine, and use, the target risk in monetary terms to determine the funds available for further risk reduction.

---

calculations will employ greater precision. Therefore, if an attempt to confirm the calculations is made, the correlation may not be exact.

Table 2: Calculation of risk in monetary terms

		Units
Value for preventing a fatality	£1,100,000	per life
Overall risk	1.3E-04	per year
Overall risk in monetary terms	£143	per year
Assume equipment life of, e.g., 7 years	£1,001	
Allow for the number of people at risk, e.g., 2	£286	per year
Assume equipment life of, e.g., 7 years	£2,002	

For the three installations examined in Reference 2, the mean overall risk was 1.3_{10}-4. Table 2 shows that the risk can be converted into a cost per year, which can be totalled over the expected life (e.g., 7 years) of any equipment that is installed. The calculation suggests that £2,002 would be available for risk reduction over the lifetime of the equipment, assuming that two persons were at risk.

In the case of an installation where only the boilerman is at risk, Table 2 suggests that, if a significant (e.g., a factor of 10) reduction in the risk of the entire installation can be obtained by spending £1,138, or less, on the control system then this definitely should be spent.

If the calculation were carried out individually for each safety function (using the contribution to the risk from that safety function), the most cost-effective means of reducing the overall risk could be determined. For example, it may be that the integrity of a single function, which provides a large contribution to the overall risk, can be increased at a relatively low cost.

It should be noted that, in most cases, this will not be practical. To achieve a significant reduction in risk, it will be necessary to reduce the probability of failure on demand by a factor of approaching 10, leading to the next higher safety integrity level. However, as a general rule, the annual capital and maintenance costs required to achieve this are likely to exceed the value of £143/per person/year shown in Table 2.

The Gross Disproportion Factor[6], GDF, can be used to determine the upper limit of cost above which a further risk reduction is unnecessary. In this case, if

Costs / Benefits > GDF

then the cost of implementing the measure cannot be justified by the reduction in the risk, and the resultant cost saving, that it produces. It is unlikely that GDF will have a value in excess of 10, and it may be possible to justify a value less than this. For example, a GDF of 3 may be appropriate for a worker, but a range of 2 to 10 may be applicable to the public, depending on the level of risk involved (e.g., ranging between a single member of the public to many members of the public).

[6] The UK Courts have decided that practicable measures to reduce risk can be ruled out as being unreasonable only if the cost of implementing them would be grossly disproportionate to the reduction in risk - hence, the Gross Disproportion Factor.

4 INITIAL DETERMINATION OF THE TARGET RISK REDUCTION FOR EACH SAFETY FUNCTION

Reference 2 identifies a number of hazardous events associated with each installation, most of which are not under the control of the boiler control/protection system(s). There are 10 hazardous events, which are related directly to the boilers. If we are initially to assume that the same risk should be associated with each hazardous event, we can divide the target risk for the entire installation by 10, as a starting point, in order initially to determine the target residual risk associated with each safety function. The functions should be considered for each individual boiler, and the targets set accordingly, rather than considering, for example, the low-water function applied to all of the boilers together, which would be the case only if a single control/protection system controlled/protected all of the boilers.

The basis of the approach is to ensure that the probability of death, to which our boilerman is subjected:

- associated with all work-related hazards, is less than 10^{-3} per year;
- associated with the single boiler hazard, is less than 10^{-4} per year, and
- associated with any one hazardous event associated with the boiler, is less than 10^{-5} per year.

If the latter is ensured, it can justifiably be argued that the previous criteria are also ensured.

Unfortunately, because of the complex way in which the various safety devices interact (for example, the three safety valves, the two burners and the different operating modes[7] of the burners when providing less than 17% of full output) the safety functions are also complex. Considering only the pressure-related safety function of the electrical system, this must be subdivided into the individual safety subfunctions that protect against the over-pressure event. (It may be possible to neglect some of the operating modes; however, until we have determined their impact on the overall risk, such a possibility can be considered only conjecture at this point.)

The first task to be carried out is to determine the actual risk reduction provided by each individual protection function carried out by the non-electrical[8] protection systems. In effect, we shall estimate the risk if the safety function were not implemented and then calculate the factor by which this must be reduced in order to achieve our target risk for that safety function. To facilitate this, we shall make use of the calculations already described in Reference 2.

---

[7] The risk associated with some of the safety functions must be calculated differently according to the operation of other protections systems or operator presence. Therefore the functions have been divided into subfunctions in order to allow the different risks to be calculated.

[8] This report will not differentiate between an electrical, electronic or programmable-electronic protection system, referring to any as electrical. An example of a non-electrical protection system would be a safety valve.

In the UK, a steam boiler designed and manufactured in accordance with BS 2790: 1992 (Reference 6) must be fitted with an adequately rated safety valve and a pressure control switch linked to the firing system (see clauses 8.1.1.3 and 9.2.2). The purpose of the 'pressure stat.' is to turn the firing system on and off as required to maintain the desired steam pressure (and hence saturated steam temperature). Note that once the firing system has been turned off following a signal from the pressure stat., it may restart automatically once the pressure has fallen below the set point of the switch. Manufacturers of steam boilers may now choose to show compliance with BS EN 12953 (Reference 5), which specifies the use of an adequately rated safety valve and a pressure limiter that will cut off and lockout the heat supply (i.e. following a high pressure trip signal from the boiler the firing system is automatically shut down and must be manually reset before it can restart). In view of the latter, and that Reference 2 examined the boiler over-pressure protection function, this report will continue the calculations for the pressure function right through to the SIL determination. The calculations associated with the over-pressure protection function will be shown in *italics,* which are included for information. It will be found that, because of the additional protection provided by the safety valves, the risk reduction required of the electrical pressure protection function is very small compared to the target risk for the overall pressure protection function.

4.1 INSTALLATION 1 (LARGE INDUSTRIAL SITE)

Details of this installation can be obtained from Reference 2.

Readers should remember that the values used in the calculations for an assessment based on BS EN 61508 should differ slightly from those described in Reference 2, especially in relation to the low-water function, because calculations or comparisons described in this report will take into account that:

- Contactor K4 incorporates redundancy following changes having been made subsequent to the examination described in Reference 2, and
- a 70% confidence level for the failure rate of components is required by BS EN 61508. Therefore, in this report the failure rate of the low-water sensor, used in either Installations 1 or 2, is determined with this confidence level.

4.1.1 Pressure-related hazards

The electrical system providing protection against over-pressurization of the boiler was shown in Reference 2 to provide a number of safety sub-functions according to the combinations of failure of the other control/protection systems. These are:

1) control the pressure when running at <17% of full output;

2) act as a protection system and close the valves for one specific gas train, i.e., the one corresponding to a single runaway burner, if the proportional control system of one burner fails;

3) act as a protection system and close the valves for either gas train, i.e., to shut down one of a pair of runaway burners, if the proportional control systems of both burners fail, or

4) act as a protection system and close the valves for both gas trains, i.e., to shut down both runaway burners, if the proportional control systems of both burners fail.

Rearranging Table A1 of Reference 2 shows that these modes receive demands according to Table 3.

Table 3: The combinations of events/failures leading to demands on the safety sub-functions

Case	Steam load	Proportional controller failure	Safety valve failure	Demand on:
1	<17% only	No failure required	All three valves	Either or both gas trains
2	Any load	One burner	Any two valves	One specific gas train
3		Both burners	Any two valves	Both gas trains
4		Both burners	Any one valve	Either gas train

If we now determine the theoretical demand rate for each of the safety sub-functions, we obtain the values shown in Tables 4A; however, because the safety system operates in continuous demand mode for Case 1, we must calculate the target probability of failure per hour (TPFH) for this particular safety sub-function as is shown in Table 4B.

Table 4A: Determination of the target risk reduction for Installation 1 - Pressure

Case	Safety sub-function	Demand rate	Vulnerability	Occupancy	Boilers	Initial risk	Target risk	TRR
2	Close one specific gas train	*5.8E-04*	*1*	*0.009*	*3*	*1.5E-05*	*2.5E-06*	*6.1E+00*
3	Close either gas train	*6.8E-03*	*1*	*0.009*	*3*	*1.8E-04*	*2.5E-06*	*7.2E+01*
4	Close both gas trains	*2.3E-04*	*1*	*0.009*	*3*	*6.0E-06*	*2.5E-06*	*2.4E+00*

Note: The units of all rates are "per year".

Table 4B: Determination of the target failure rate for Installation 1

Case	Safety sub-function	Target risk	$PFD_{(other)}$	Vulnerability	Occupancy	Boilers	Risk time	TPFH
1	Close either/both gas trains	*2.5E-06*	*1.4E-03*	*1*	*0.210*	*3*	*0.6*	*4.7E-03*

Notes

1) The units of all rates are "per year".

2) Case 1 applies for 60% of the time (standby) and has been taken into account in determining the TFR.

3) Risk time shows the fraction of time during which this sub-function is active.

Tables 4A and 4B show that there are 4 safety sub-functions involved in pressure control. Because pressure control was allocated a target risk of 10^{-5}/year, the initial target risk has been equally divided between them, giving an initial target risk of 2.5×10^{-6}/year for each safety sub-function.

4.1.1.1 Table 4A: Explanation

As described previously, the demand rate on a safety function has been calculated to be the hazard rate assuming that the PFD of the safety function is 1. For example, the demand rate for Case 2 of Table 4A was calculated to be the rate of either burner failing to a high output multiplied by the probability of two of the safety valves concurrently failing.

It is assumed that the boilerman will be killed if a pressure failure of the boiler occurs whilst he is anywhere in the boilerhouse. Therefore, a value of 1 has been assumed for the "Vulnerability" column.

The "Occupancy" column indicates the fraction of all time that the boilerman is in an area of risk. This takes into account:

- days worked per year;
- number of visits per day, and
- the duration of the visits or the duration of risk (e.g. the time taken to shut-down the boiler with a safety valve blowing as the boilerman arrives at the site), as appropriate.

Clearly, the overall risk depends on the number of boilers that contribute to the risk. As there are three boilers at Installation 1, the "Boilers" column is set to 3.

The "Initial risk" column contains the initial risk (in deaths per year) presented by the installation in the absence of the safety function under consideration. In this case, it is the product of the values in the: "Demand rate"; "Vulnerability"; "Occupancy", and "Boilers" columns.

We have already determined the Target risk so, by determining the ratio between this and the initial risk, we can determine by how much the initial risk must be reduced in order to reach the target risk. This is the value shown in the "TRR" column.

In Reference 2, purely to simplify the calculations, the demand rate on the loss-of-forced-draught safety function was considered to be the rate of coincidences between losses of forced draught and failures of the vent valve to open. In the calculations in this report, the demand rate on the loss of forced draught protection is the rate at which the forced draught actually fails.

4.1.1.2 Table 4B: Explanation

Table 4B is very similar to Table 4A. However, in this case, our safety-related system is controlling the boiler temperature, not acting as an independent protection system for another controller. In this case, we must determine the rate of failure instead of risk reduction.

The "Target risk" column was determined as for Table 4A.

The $PFD_{(other)}$ column shows the probability of failure on demand of the appropriate combination of safety valves (in this case, any two).

With the occupancy, vulnerability and boilers determined as for Table 4A, the TPFH can be calculated by dividing the target risk by the values in the: "$PFD_{(other)}$"; "Vulnerability"; "Occupancy", and "Boilers" columns.

4.1.2 Low-water hazards

Table 5, which was calculated in a similar way to Table 4A, shows the theoretical demand rate for the low-water safety functions.

4.1.3 Burner-related hazards

Table 5 shows the theoretical demand rates for the burner-related safety functions.

Table 5: Determination of the target risk reduction for Installation 1 - Low water/loss of flame

Safety function	Demand rate	Vulnerability	Occupancy	Boilers	Initial risk	Target risk	TRR
Low water	3.8E+00	1	0.210	3	2.4E+00	1.0E-05	2.4E+05
Low gas pressure	1.0E-01	0.1	0.210	3	6.3E-03	1.0E-05	6.3E+02
Loss of flame	1.8E+00	0.1	0.210	3	1.1E-01	1.0E-05	1.1E+04
Loss of forced draught (A)	1.0E-01	0.1	0.210	3	6.6E-03	5.0E-06	1.3E+03
Loss of forced draught (B)	1.4E-01	0.1	0.210	3	8.7E-03	5.0E-06	1.7E+03

Note: The units of all rates are "per year".

Notes to Tables 5 and 6

1) It may not be clear to readers as to why a low-water event, which will probably lead to steam/water escaping into the furnace, has a vulnerability of 1 when an explosion within the furnace has been assigned a much lower value. The explanation is that the furnace explosion will lead to a hazard at the front and rear of the boiler as a result, for example, of the burner or flue being blown off the boiler. On the other hand, an escape of superheated water into the furnace will lead to a large volume of steam entering the boilerhouse over an extended period. This will be a major hazard and will eventually overcome the boilerman, especially if he cannot escape because the escaping steam cuts off his escape route. Although the actual vulnerability will be less than 1, it is not considered to be significantly lower.

2) In the initial hazard rate calculations for Installations 1 and 2 described in Reference 2, it was convenient to consider the demand rate on the loss-of-forced-draught protection system to be the rate of coincidences between a loss of forced draught and a failure of the vent valve to open[9] rather than to incorporate the failure rate of the vent valve into the integrity of the protection system. Clearly, in the current calculation, the vent valve must be considered to be part of the protection system, so in Tables 5 and 7, the failure rate of the vent valve does not affect the loss-of-forced-draught demand rate.

3) The demand rate for the low-water protection function of 3.8 demands per year is unusually high for a protection function. Demand rates in excess of 1 per year would normally be considered appropriate to the “high demand or continuous mode of operation” rather than the “low demand mode of operation” (i.e., Table 3 of BS IEC 61508-1 1998 would be used instead of Table 2). However, if continuous mode of operation were assumed, the calculations for this installation would become incompatible with those for the other installations. It will be seen that the low demand mode of operation has been assumed in Table 5; however, the final calculations in Section 6 are based on the lower demand rate obtained from Installation 2.

4) The occupancy is high as a result of the boilerman being present for 8 hours, in the case of Installation 1, or 4 hours, in the case of Installation 2, on each of his working days

[9] A worst-case assumption was made in Reference 2 that the main gas valves would leak and, therefore, that a hazardous event would occur if the vent valve fails to open coincidentally with a failure of the forced draught fan.

4.2 INSTALLATION 2 (HOSPITAL)

Details of this installation can be obtained from Reference 2.

4.2.1 Pressure-related hazards

There are only two safety sub-functions associated with the pressure-protection system of Installation 2. These are:

- operation with a steam load of >17%. In this case, the electrical system acts as a protection system. It is assumed that this mode of failure could apply to any one of the three boilers, or

- operation with a steam load of <17%. In this case, the electrical system acts as a control system, because the proportional control system is throttled back to its limit. Two of the three boilers would be operating in this mode.

Tables 6A shows the calculation of the TRR related to overpressure with a steam load greater than 17%. In the case of overpressure with a load of less than 17%, the safety system operates in continuous mode, so it is necessary to determine the target in terms of failure rate (TPFH) rather than risk reduction (TRR), so the calculation is shown in Table 6B. (For an explanation of the calculations, see Sections 4.1.1.1 and 4.1.1.2.

4.2.2 Low-water hazards

The calculation of the TRR for this function is similar to that for Installation 1. See Table 6A.

Readers may note that the low-water demand rate used in reference 2 is higher than the rate used in this report. The data for Installation 1 included a setting-up period in which there was a number of low-water events that could be explained by steam surge. These initial events were excluded. However, in the case of Installation 2, of the 5 low-water events that were recorded in the period examined, all were included in the analysis, as steam surge was not considered to be a problem at this site.

Of the five events, for two of them, no fault associated with the water level was found by the boilerman on his arrival at the site. These events have been excluded from the calculation of the low-water demand rate used in this report. (Readers may be interested to know that one of the three genuine low-water events was the result of the electrical power [presumably to the water feed pump] being turned off by a site employee. Such [difficult to quantify] maintenance-related faults may need to be taken into account in any theoretical calculations to determine demand rates – such events **will** happen, the question is "How often?" It should be noted that this type of event can often lead to a common-cause failure of more than one protection system.)

4.2.3 Burner-related hazards

The calculation of the TRR for this function is similar to that for Installation 1. See Table 6A.

Table 6A: Determination of the target risk reduction for Installation 2

Safety (sub)function	Demand rate	Vulnerability	Occupancy	Boilers	Initial risk	Target risk	TRR
Low water	6.7E-01	1	0.105	3	2.1E-01	1.0E-05	2.1E+04
Overpressure >17% load	*2.9E-02*	*1*	*0.105*	*3*	*9.3E-03*	*5.0E-06*	*1.9E+03*
Low gas pressure	1.0E-01	0.2	0.105	3	6.3E-03	1.0E-05	6.3E+02
Loss of flame	3.4E+00	0.2	0.105	3	2.1E-01	1.0E-05	2.1E+04
Loss of forced draught	1.1E-01	0.2	0.105	3	6.9E-03	1.0E-05	6.9E+02

Notes: The units of all rates are "per year".
Occupancy assumes 230 days worked per year

Table 6B: Determination of the target failure rate for Installation 2

Safety subfunction	Target risk	$PFD_{(other)}$	Vulnerability	Boilers	Occupancy	TPFH
Overpressure <17% load	*5.0E-06*	*1.4E-03*	*1*	*2*	*0.105*	*1.7E-02*

Notes:
1) The units of all rates are "per year".
2) In general, the two boilers on hot stand-by operate in this mode
3) Occupancy assumes 230 4-hour visits per year.

Tables 6A and 6B show that there are 2 safety sub-functions involved in pressure control. Because pressure control was allocated a target risk of 10^{-5}/year, the initial target risk has been equally divided between them, giving an initial target risk of 5×10^{-6}/year for each mode.

In Reference 2, purely to simplify the calculations, the demand rate on the loss-of-forced-draught protection system was considered to be the rate of coincidences between losses of forced draught and failures of the vent valve to open[10]. In the calculations in this report, the demand rate on the loss of forced draught protection is the rate at which forced draught actually fails.

4.3 INSTALLATION 3 (LAUNDRY)

Details of this installation can be obtained from Reference 2.

Reference 2 determined the average risk actually presented to the on-site workers, by determining the average risk to each worker on the site (including office workers). Reference 3 suggests that the calculation relates to a hypothetical person, who could be the one most exposed to the hazard. Therefore, in relation to Installation 3, we shall consider only the workers in the laundry room and shall not take into account the office workers, who are exposed to a reduced risk.

Section 3.1 suggests that societal risk becomes dominant where the site occupancy becomes greater than about 5. Although we actually have 6 workers in our laundry room, they work for only 8-hours per day, which is a third of the time. Therefore, even if they were to work for every day of the year,

[10] A worst-case assumption was made in Reference 2 that the main gas valves would leak and, therefore, that a hazardous event would occur if the vent valve fails to open coincidentally with a failure of the forced draught fan.

the mean occupancy cannot exceed 2. Therefore, we shall not consider societal risk, but shall calculate the risk faced by a single hypothetical person working a standard shift in the laundry room.

4.3.1 Pressure-related hazards

The electrical safety system for Installation 3, which relates to pressure, operates in continuous mode of operation. Therefore, it is necessary to determine its TPFH, as is shown in Table 7B, and not its TRR.

4.3.2 Low-water hazards

The calculations of the TRR for the low-water safety function of Installation 3 are shown in Table 7A.

4.3.3 Burner-related hazards

Table 7A: Determination of the target risk reduction for Installation 3

Safety (sub)function	Demand rate	Vulnerability	Occupancy	Boilers	Initial risk	Target risk	TRR
Low water	2.8E-01	0.11	0.026	1	7.9E-04	1.0E-05	7.9E+01
Low gas pressure	1.0E-01	0.2	0.026	1	5.3E-04	1.0E-05	5.3E+01
Loss of flame	7.7E-02	0.2	0.026	1	4.1E-04	5.0E-06	8.1E+01
Loss of flame during test	7.7E-02	1	0.002	1	1.3E-04	5.0E-06	2.5E+01
Loss of forced draught	6.3E-02	0.2	0.026	1	3.3E-04	5.0E-06	6.7E+01
Loss of forced draught during test	6.3E-02	1	0.002	1	1.0E-04	5.0E-06	2.1E+01

Notes:
1) The units of all rates are "per year".
2) The occupancy is the mean occupancy per individual employee working for 230 days/year.
3) The vunerability for "low water" allows for the boiler's robustness to this event and the vertical format of the boiler directing escaping steam upwards. (See Reference 2.)

Table 7B: Determination of the target failure rate for Installation 3

Safety (sub)function	Target risk	$PFD_{(other)}$	Vulnerability	Occupancy	Boilers	TPFH
Overpressure	*5.0E-06*	*2.6E-02*	*0.9*	*0.026*	*1*	*8.3E-03*
Overpressure during test	*5.0E-06*	*2.6E-02*	*1*	*0.002*	*1*	*1.2E-01*

Notes:
1) The units of all rates are "per year".
2) The occupancy is the mean occupancy per employee working 230 days per year

Table 7B shows that there are 2 safety sub-functions involved in pressure control. Because pressure control was allocated a target risk of 10^{-5}/year, the initial target risk has been equally divided between them, giving an initial target risk of 5×10^{-6}/year for each sub-function.

Readers will have noted that several of the safety functions have two different modes of operation (i.e., normal and test modes), and that the test mode applies for only a small fraction of the time. Although the values for occupancy take into account the fraction of time that each mode applies, the

target risk has been divided equally between the normal and test modes of operation. This will be taken into account in Section 5.

5 ALLOCATION OF THE TARGET RISK BETWEEN THE SAFETY FUNCTIONS

The calculations described in Section 4 assume that the target risk is divided equally between the safety functions. There will be different costs associated with reducing the risks associated with the various safety functions. Therefore, it is likely to be more cost effective to reduce some risks in preference to others. This may make it appropriate to trade off the allocation of the target risk between the safety functions in order to obtain the most cost-effective solution. Therefore, the initial equal allocation of target risk to each safety function is unlikely to be the most cost-effective approach.

Therefore, at this stage, we can consider the target risk in relation to the safety functions that are available. If, for example, an existing safety function can readily provide a risk reduction that is significantly greater than the initial TRR, the "excess" Target risk can be reallocated to another safety function, as will now be described.

First, we shall compare the target risks with the actual risks presented by the installations for each of their safety functions. This will provide an insight into their contribution to the overall risk so that decisions regarding the allocation of risk can be taken.

5.1 INSTALLATION 1

The "Initial" columns of Figure 8 summarize Tables 4A, 4B and 5. These columns show the initial allocations of risk to the various safety functions and their operating modes, and the TRR/TPFH required to achieve these risks.

The "Actual" columns of Table 8 show the actual risk reductions (or failure rates) that were determined for the existing safety systems in the examinations described by Reference 2. These provide an indication of what has been achieved by each safety function/operating mode.

The "Actual Risk" column (Column 5) includes a running total of the risk excess. Consider the operating mode "Pressure: Close one specific gas train". It will be seen that the initial allocation of risk is 2.5E-6; however, the existing safety system achieves a negligible level of risk. This means that nearly all of the initial allocation is "unused", as is shown in the row immediately below. This excess risk allocation could be re-allocated to another safety function.

This process has been continued down the "Actual Risk" column and it will be seen that an excess of risk allocation is accumulated until the "Low water" function is reached, causing a deficit.

Table 8 shows that the overall risk associated with Installation 1 is approximately double the overall target risk – within the uncertainty of this generic assessment, which has taken a somewhat pessimistic approach. However, this has been achieved as a result of the target risk effectively having being reallocated between the various functions in the "Actual Risk" column.

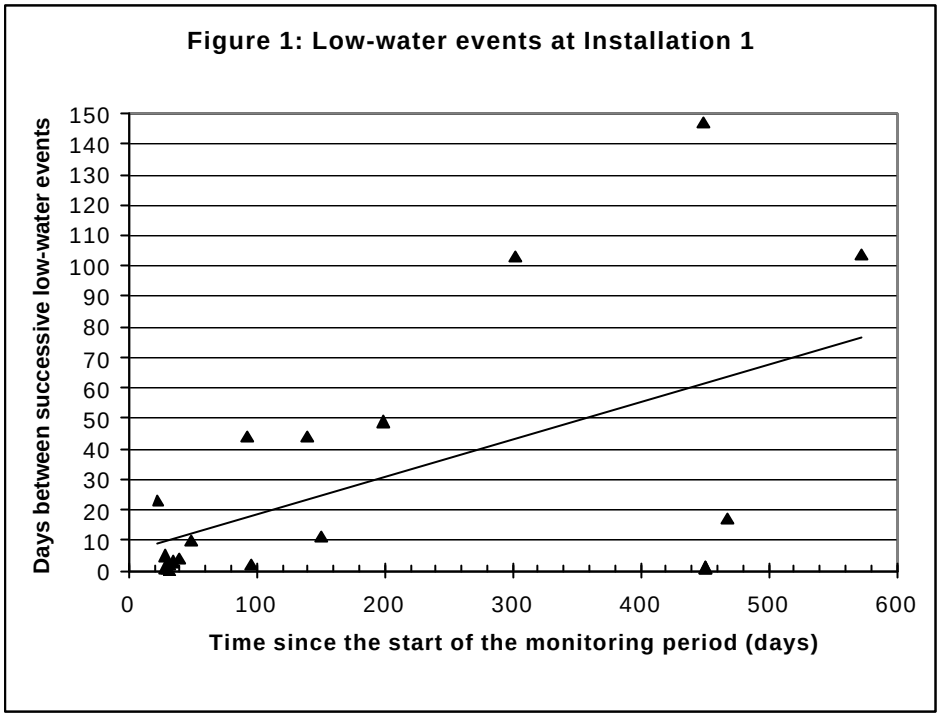
It will be seen that eliminating the pressure function from the calculations appears to make matters worse using this approach. This is because the allocation of 1E-5 is lost, but the actual risk contribution is very low, so there is a net gain of residual risk.

Table 8: Summary of Tables 4A, 4B and 5

	Initial			Actual		
Safety (sub)function	**Target risk**	**TRR**	**TPFH**	**Risk**	**ARR**	**APFH**
Pressure: Close one specific gas train	*2.5E-06*	*6.1E+00*		*1.3E-10*	*1.2E+05*	
Balance of target risk (excess) carried downwards				*2.5E-06*		
Pressure: Close either gas train	*2.5E-06*	*7.2E+01*		*6.5E-08*	*2.8E+03*	
Balance of target risk (excess) carried downwards				*4.9E-06*		
Pressure: Close both gas trains	*2.5E-06*	*2.4E+00*		*2.1E-09*	*2.9E+03*	
Balance of target risk (excess) carried downwards				*7.4E-06*		
Pressure: Close either/both gas trains	*2.5E-06*		*4.7E-03*	*2.1E-06*		*4.0E-03*
Balance of target risk (excess) carried downwards				*7.8E-06*		
Low water	1.0E-05	2.4E+05		5.5E-05	4.4E+04	
Balance of target risk (deficit) carried downwards				*-3.7E-05*		
Low gas pressure	1.0E-05	6.3E+02		5.6E-08	1.1E+05	
Balance of target risk (deficit) carried downwards				*-2.7E-05*		
Loss of forced draught (A)	5.0E-06	1.3E+03		9.9E-06	6.7E+02	
Balance of target risk (deficit) carried downwards				*-3.2E-05*		
Loss of forced draught (B)	5.0E-06	1.7E+03		3.3E-05	2.7E+02	
Balance of target risk (deficit) carried downwards				*-6.0E-05*		
Loss of flame	1.0E-05	1.1E+04		2.1E-05	5.3E+03	
Total target risk	**5.0E-05**			**1.2E-04**		
Overall target risk reduction deficit				-7.1E-05		
Total target risk excluding pressure	4.0E-05			1.2E-04		
Overall target risk reduction deficit excluding pressure				-7.8E-05		

The demand rate for the low-water function at Installation 1 is unrealistically high; however, the author has checked the data and was unable to eliminate any additional low-water events that led to no fault being found by the boilerman when he arrived on site in response to the boiler shutting down.

A linear trend line fitted to the data, plotted in terms of the time between low-water events against time, suggests that the mean time between low-water events increased from about 10 days to about 80 days over the monitoring period of about 18 months. (See Figure 1.) This suggests that, because the period over which the installation was monitored corresponded to the period immediately after the commissioning of the installation, the low-water demand rate used in this report is unrealistically high and the time between low-water events could eventually be 80 days, or above (i.e., the low-water demand rate would reduce from 3.8/boiler/year to 1.5/boiler/year, or below).



5.2 INSTALLATION 2

Table 9 is similar to Table 8, but with values appropriate to Installation 2.

Table 9: Summary of Tables 6A and 6B						
	Initial			Actual		
Safety (sub)function	**Target risk**	**TRR**	**TPFH**	**Risk**	**ARR**	**APFH**
Low water	1.0E-05	2.1E+04		2.8E-06	7.7E+04	
Balance of target risk (excess) carried downwards				*7.2E-06*		
Low gas pressure	1.0E-05	6.3E+02		8.0E-08	7.9E+04	
Balance of target risk (excess) carried downwards				*1.7E-05*		
Loss of forced draught	1.0E-05	6.9E+02		2.3E-07	3.0E+04	
Balance of target risk (excess) carried downwards				*2.7E-05*		
Overpressure <17% load	*5.0E-06*		*1.7E-02*	*1.7E-06*		*5.8E-03*
Balance of target risk (excess) carried downwards				*3.0E-05*		
Overpressure >17% load	*5.0E-06*	*1.9E+03*		*4.8E-07*	*2.0E+04*	
Balance of target risk (excess) carried downwards				*3.5E-05*		
Loss of flame	1.0E-05	2.1E+04		7.3E-05	2.9E+03	
Total	**5.0E-05**			**7.8E-05**		
Overall target risk reduction deficit				*-2.8E-05*		

As with Table 8, an excess of target risk is carried down, in the case of Installation 2 until the "Loss of flame" function, which accounts for much of the actual risk at the installation.

For Installation 2, the overall actual risk is only marginally greater than the overall target risk.

5.3 INSTALLATION 3

Table 10 shows the same parameters as Table 8, but with values appropriate to Installation 3. It will be seen that the overall actual risk is less than the overall target risk for this installation.

Table 10: Summary of Tables 7A and 7B

	Initial			Actual		
Safety (sub)function	**Target risk**	**TRR**	**TPFH**	**Risk**	**ARR**	**APFH**
Overpressure during test	*5.0E-06*		*1.2E-01*	*4.0E-07*		*9.6E-03*
Balance of target risk (excess) carried downwards				*4.6E-06*		
Overpressure	*5.0E-06*		*8.3E-03*	*5.8E-06*		*9.6E-03*
Balance of target risk (excess) carried downwards				*3.8E-06*		
Low water	1.0E-05	7.9E+01		4.7E-06	1.7E+02	
Balance of target risk (excess) carried downwards				*6.5E-06*		
Low gas pressure	1.0E-05	5.3E+01		5.9E-06	8.9E+01	
Balance of target risk (excess) carried downwards				*1.1E-05*		
Loss of flame	5.0E-06	8.1E+01		1.0E-05	3.9E+01	
Balance of target risk (excess) carried downwards				*5.3E-06*		
Loss of flame during test	5.0E-06	2.5E+01		3.2E-06	3.9E+01	
Balance of target risk (excess) carried downwards				*7.1E-06*		
Loss of forced draught	5.0E-06	6.7E+01		2.3E-06	1.4E+02	
Balance of target risk (excess) carried downwards				*9.8E-06*		
Loss of forced draught during test	5.0E-06	2.1E+01		7.2E-07	1.4E+02	
Total	**5.0E-05**			**3.3E-05**		
Overall target risk reduction excess				***1.7E-05***		

6 ALLOCATION OF TARGET RISK: A SIMPLER APPROACH

Whilst the quantitative method of risk allocation described previously can be considered to be an ideal solution, in many circumstances, a simpler qualitative approach may be possible, as will now be described.

Table 11: Target parameters for each safety (sub)function at each installation

Safety (sub)function	Installation 1				Installation 2				Installation 3			
	TRR	TPFH	Occupancy	Vulnerability	TRR	TPFH	Occupancy	Vulnerability	TRR	TPFH	Occupancy	Vulnerability
Pressure: Protection	*7.2E+01*		*8.7E-03*	*1.0E+00*	*1.9E+03*		*1.0E-01*	*1.0E+00*				
Pressure: Control		*4.7E-03*	*2.1E-01*	*1.0E+00*		*1.7E-02*	*1.0E-01*	*1.0E+00*		*8.3E-03*	*2.3E-02*	*9.1E-01*
Low water	2.4E+05		2.1E-01	1.0E+00	2.1E+04		1.0E-01	1.0E+00	7.9E+01		2.6E-02	1.1E-01
Low gas pressure	6.3E+02		2.1E-01	1.0E-01	6.3E+02		1.0E-01	2.0E-01	5.3E+01		2.6E-02	2.0E-01
Loss of forced draught	1.5E+03		2.1E-01	1.0E-01	6.9E+02		1.0E-01	2.0E-01	6.7E+01		2.6E-02	2.0E-01
Loss of flame	1.1E+04		2.1E-01	1.0E-01	2.1E+04		1.0E-01	2.0E-01	8.1E+01		2.6E-02	2.0E-01

Notes

1) The vulnerability for "pressure" at Installation 3 varies by only 10% between subfunctions, so the mean occupancy is used

2) The TRR and TPFH are "per boiler", reflecting a need for a higher integrity at Installations 1 and 2, which have multiple boilers.

3) The daily test contributes only 25% of the loss-of-forced-draught risk at Installation 3, so the entry is based on normal operation

4) The worst-case TRR has been used for "Pressure: Protection" of Installation 1

5) The pressure control function applies when the pressure is being controlled by the safety system whilst the boiler runs at <17% output.

Table 11 shows the target parameters for each safety function at the three installations, after the data have been manipulated to merge the operating modes in order to allow comparison between the installations, together with the appropriate occupancies and vulnerabilities.

If we normalize the data in Table 11 for unit occupancy, unit vulnerability and one boiler per installation, we obtain Table 12.

Table 12: TRR & TPFH normalized to: unit occupancy; unit vulnerability, and one boiler/installation

Safety function	Installation 1		Installation 2		Installation 3		Mean	Range
	TRR	TPFH	TRR	TPFH	TRR	TPFH		
Pressure: Protection	*2.7E+03*		*5.9E+03*				***4.0E+03***	***2.2***
Pressure: Control		*2.9E-03*		*5.3E-03*		*1.7E-04*	***1.4E-03***	***30.2***
Low water	3.8E+05		6.7E+04		2.8E+04		**9.0E+04**	**13.4**
Low water (revised)	1.9E+05						**7.2E+04**	**6.7**
Low gas pressure	1.0E+04		1.0E+04		1.0E+04		**1.0E+04**	**1.0**
Loss of forced draught	2.4E+04		1.1E+04		1.3E+04		**1.5E+04**	**2.2**
Loss of flame	1.8E+05		3.4E+05		1.5E+04		**9.7E+04**	**21.7**

Column 9 shows the range between the maximum and minimum values in Columns 2 to 7. These ranges reflect, for example, the variations between the demand rates at the installations. The range is relatively narrow for most of the safety functions; however, some have a significant spread.

Let us consider each of the rows in turn, which reflect the demand rates on the various systems.

Pressure: Protection/Control: Because of the different safety sub-functions of the protection systems of Installations 1 and 2, it is not easy to determine a single TRR or TPFH for these installations – especially when the fraction of time during which each boiler spends in each operating mode is variable and effectively unknown.

Clearly, if the safety valve (or safety valves) could be relied on to provide an adequate risk reduction (which should be the case if current UK standards are followed), the electrical protection system could be regarded as not being safety related; however, this may not be the case if maintenance (which the author considers to have a major influence on the integrity of safety valves) or design is inadequate (See Reference 2.), or current standards are changed.

Installation 3 must be treated differently to the other installations, as it has no secondary electrical protection system, which makes its target failure rate relatively easy to determine.

As compliance with current UK standards can be achieved by the use of adequately rated safety valves, the values associated with pressure are for interest only.

Low water: The author attempted to eliminate data from the initial "learning" period at Installation 1, when the water level probes were being adjusted to allow for water level variations caused by the boilers at this site coming on-line and going off-line quickly. Nevertheless, this installation still shows the highest rate of low-water incidents and Installation 3 the lowest, leading to an overall range of about 13. In this case, the geometric mean corresponds closely with the value for Installation 2. However, Figure 1 clearly shows that the time between low-water events at Installation 1 increased substantially over the 18-month monitoring period and suggests that a more-realistic demand rate for this site is likely to be no more than half of the value used in the calculations. This can be seen in Table 12 along the low-water (revised) row.

The demand rate used for Installation 3 was based on calculated failure rates, which may not take into account all eventualities, especially those involving human factors. Therefore, the demand rate for Installation 2 may be more realistic than that for Installation 3, with the demand rate for Installation 1

reflecting a greater potential for the effects of steam surge (or the complexity [e.g., additional valves] associated with a need to deal with steam surge).

Low gas pressure: The figure is the same for all installations and reflects the same assumption for the failure rate of the gas supply.

Loss of forced draught: The values for the three installations are closely similar, so it would be appropriate to assume the mean.

Loss of flame: The value for Installation 3 is significantly lower than the values for Installations 1 and 2, which are quite similar. In fact, the value for Installation 3 is more than a factor of 15 below the geometric mean of the values for Installations 1 and 2 ($2.47_{10}5$).

The rate of demands on the loss-of-flame safety function was determined from the site logs at Installations 1 and 2, whereas that for Installation 3 was based on only the failure rate of the ignition system. Clearly, at Installations 1 and 2, the burners were more likely to fail as a result of burner adjustment and operation than a failure of their ignition systems. This would suggest that the loss-of-flame protection system at Installation 3 may require a higher integrity than is indicated by Column 6, so it would not be unreasonable to give greater credence to the values for Installations 1 and 2 by using their geometric mean.

Table 13 summarizes the data according to these assumptions.

Table 13: Summary of normalized target requirements

	Normalized		
Safety function	**TRR**	**TPFH**	**Comment**
Pressure: Protection	*4.0E+03*		Assumes operation similar to Installations 1 and 2, with additional proportional control system
Pressure: Control		*3.9E-03*	
Pressure: Control only		*1.7E-04*	Value used is from Installation 3. Assumes pressure control and safety valve, i.e., no additional protection system.
Low water	6.7E+04		Multiply by 3 if steam surge potentially frequent. The value chosen is from Installation 2 as real data are available for this.
Low gas pressure	1.0E+04		Same for each installation.
Loss of forced draught	1.5E+04		Logarithmic mean of all 3 installations.
Loss of flame	2.4E+05		Logarithmic mean for Installations 1 and 2 as real data were used in the calculations for these sites.

If we now take the values of:

- the normalized TRR, and multiply them by the: fractional vulnerability; the fractional occupancy and the number of boilers in order to get an estimate of the TRR for each safety function. This is the inverse of the $TPFD_{av}$, which can be converted directly to the SIL for the safety function, and

- the normalized TPFH, and divide them by the: fractional vulnerability; the fractional occupancy and the number of boilers, we get an estimate of the TPFH for each safety function, which can be converted directly to the SIL for the safety function.

For example, consider the low-water function, where steam surge is unlikely. The normalised TRR is $6.7_{10}4$. If the installation has 1 boiler (N=1), the boilerman has a vulnerability of 1 (V=1) and his occupancy is 0.15 (O=0.15), then the calculated TRR becomes $1.0_{10}4$ (=Normalized TRR x V x O x N), which corresponds to a PFD_{av} of 9.9_{10}-5 as is shown in Table 14[11].

It will be seen that the low-water safety function has the highest SIL requirement, which results from the relatively high demand rate on this function. Although this function requires the highest SIL of all of the safety functions, the PFD_{av} is only marginally above the threshold for SIL4.

The three demands on the low-water safety function at Installation 2 during the monitoring period of 544 days resulted from:

1) an unknown fault. This may have been spurious but, as the boiler was left isolated by the engineer who attended the fault, the fault cannot be assumed to have been spurious from the available information;

2) power [to the feed pump] being turned off by on-site personnel (i.e., associated with the site but not the boiler installation), and

3) the feed pump having tripped.

If Fault 1 had been indicated to be spurious, the Target PFD_{av} for low water shown in Table 14 would have been about 1.5E-4, leading to a requirement for a SIL of 3.

The target SILs shown in Table 14 are not unreasonable, but there may be difficulty in meeting them using complex technology, whose use will require particular care at all stages in the safety lifecycle.

Table 14: SIL estimates for typical data

Safety function	Normalized		Fractional vulnerability	Estimated		$TPFD_{av}$	SIL
	TRR	TPFH		TRR	TPFH		
Pressure: Protection (>17% load)	*4.0E+03*		*1.0E+00*	*6.0E+02*		*1.7E-03*	*2*
Pressure: Control (<17% load)		*3.9E-03*	*1.0E+00*		*2.6E-02*		*1*
Pressure: Control only		*1.7E-04*	*1.0E+00*		*1.2E-03*		*2*
Low water (Steam surge is unlikely)	6.7E+04		1.0E+00	1.0E+04		9.9E-05	4
Low water (Steam surge is likely)	2.0E+05		1.0E+00	3.0E+04		3.3E-05	4
Low gas pressure	1.0E+04		2.0E-01	3.0E+02		3.3E-03	2
Loss of forced draught	1.5E+04		2.0E-01	4.5E+02		2.2E-03	2
Loss of flame	2.4E+05		2.0E-01	7.3E+03		1.4E-04	3
Number of boilers	1						
Fractional occupancy	1.5E-01						

Note: The units of all rates are per year.

It should be noted that the methodology described in Section 5 allows the risk reduction to be traded between the various safety functions; however, there is a limit to which this can be done. (For example, if there were only two safety functions, the limit would be when one safety function

[11] It will be noted in Table 14 that a TRR of 1.0E+04 does not appear to correspond to a $TPFD_{av}$ of 9.9E-05. The the apparent discrepancy is the result of the rounding required to show one decimal place.

contributed double its equal share leaving the other function to contribute zero. Therefore, in this particular case, an increase of only a factor of 2 is possible, but at great expense in reducing the contribution of the other function. A factor of two is of little consequence when the breadth of a SIL is a factor of 10.)

The methodology described in this section attempts to allocate a similar contribution toward the risk from each safety function; however, as the option of trading risk between safety functions is somewhat limited, the methodology may be a satisfactory means of determining the SIL in the majority of applications.

6.1 SAFETY INTEGRITY LEVELS: POINTS TO NOTE

1) If the $TPFD_{av}$ of a function is in the range 0.001 and 0.01 (and assuming other criteria have been met), this will lead to a SIL of 2. This means that the $TPFD_{av}$ can cover a range spanning almost a factor of 10.

   The SIL defines the qualitative requirements that the equipment providing the function must achieve. These requirements could, for example, define the level of software quality assurance control that is applied to the software or the electrical interference-testing regime. It should be noted that the SIL is determined from the $TPFD_{av}$ and that the SIL gives no indication of the $TPFD_{av}$, other than to the nearest order of magnitude.

   Suppose that we have determined that the $TPFD_{av}$ for a particular safety function is 0.002. This is at the lower end of the range for SIL 2, so we can design the equipment implementing our safety function using the qualitative requirements defined by IEC 61508 for SIL 2. However, we must ensure that the hardware of our system can achieve a PFD_{av} that is no greater than 0.002. It would NOT be acceptable to assume that, as we require "a SIL 2 system", any PFD_{av} within the range 0.001 and 0.01 would be adequate. If it were, this would imply that a PFD_{av} of 0.009, which is 4.5 times the $TPFD_{av}$, would be acceptable, and this is clearly not the case.

   Therefore, the SIL:

   - should be used to define only the qualitative aspects of the design, and
   - should not be used to define the PFD_{av} of the system unless the value used is at the minimum (i.e., highest integrity) end of the range for the SIL in question.

2) Readers may have noted that the boilerman attending Installation 1 attends for two periods of 4 hours, making 8 hours in total, whereas the boilerman who visits Installation 2 attends for one 4-hour period. The analysis considers that the risk associated with the rest of the working day for the Installation 2 boilerman is included in his "other risks". Therefore, the analysis has a slight bias in favour of Installation 2. In the cases examined, this bias represents a factor of only two; however, if a boilerman attended 6 installations each for an hour per day, the error would be significant. One way forward may be to combine the analyses of both of the installations that the Installation-2 boilerman visits in order to determine his overall work-related risk.

3) If members of the public, especially in large numbers, were put at risk by the installations, Table 14 would suggest that current equipment designs might not be suitable for ensuring an adequately low level of risk. (Readers should be aware that the analysis described in this report

is conservative and a more accurate analysis, based on specific, rather than generic, data could change this conclusion.)

4) The relatively high demand rate on the low-water protection function has led to a probability of failure on demand requirement that takes the integrity requirement just into SIL4. A slightly lower demand rate would have led to a requirement of SIL3. It is not 100% clear whether one of the three low-water demands that were considered in the calculations resulted from a spurious indication or a genuine demand. If the indication were spurious, the SIL requirement would have fallen well into the range of SIL3, leading to the qualitative design requirements becoming significantly less onerous.

5) The relatively onerous SIL requirements are not unreasonable when one considers that the equipment used in boiler control is highly specialized and well established, so will reflect feedback from incidents that have occurred over a large number of years. However, such onerous SIL requirements may be a concern in the future if complex control systems are envisaged.

6) The use of complex (e.g., computer-based) equipment will make the achievement of SIL4 difficult unless specialist design techniques are used. The qualitative design requirements of SIL4 will be particularly onerous in relation to the software design, the self-test requirements and the architecture (i.e., redundancy/diversity).

7) As the target SIL increases, the probability of common-cause failures becomes increasingly important. With a target SIL of SIL3 or SIL4, particular care must be taken to avoid common-cause failures associated with sensors and/or the electrical circuitry associated with them.

8) Based on current maintenance regimes, the boiler-control equipment would appear to be, more or less, achieving the requirements[12]. However, an increase in the various examination (proof test) intervals associated with a reduction in maintenance could lead to an increase in risk.

[12] It is important to note that this report has taken into account only the quantitative aspects of the risk assessment process. Having determined the integrity and, hence, the SIL for each of the safety functions, an assessment to IEC 61508 would apply additional qualitative criteria appropriate to the relevant SIL.

7 CONCLUSIONS

1) A simplified means of estimating the target SILs for various boiler safety functions has been developed for the majority of boiler applications where the consequence of failure is restricted to less than 5 employees. For applications involving more than 5 fatalities to employees, or a fatality to a member of the general public, more fundamental techniques will be needed.

2) Although this assessment has worked through the calculations for the pressure function, this would not currently be required for conformity with current UK legislation, assuming adequate pressure-relief valves are in place.

3) The pressure safety function provides only a small contribution to the overall risk associated with Installations 1 and 2. This safety function is carried out electronically (i.e., shut down the burners) and mechanically via the safety valve(s). Because the safety valves provide a protection channel that is independent of that involving the burner shutdown valves, the shutdown valves provide a less-significant contribution to the overall risk via the pressure function. However, the other safety protection functions rely on the shutdown valves to close down the burners if a malfunction is detected. As a result, the outcome of the risk calculations depends strongly on the failure rate of these valves. Therefore, an accurate estimate of the failure rate of these valves (i.e., not a generic estimate as used in Reference 2 and, as a consequence, also in this report) would be required for an assessment using IEC 61508.

4) Estimates of the safety-integrity-level requirements of the various safety functions of a generic boiler installation have been made. These indicate that the SIL requirement of the low-water protection function (SIL4, or SIL3 if changes are made as indicated in the text) is more onerous than that for the other protection functions, and reflects the high demand rate determined using data from the monitoring systems at Installations 1 and 2, and the predicted consequences. This confirms the critical nature of the safety function that provides protection against low water. Traditionally, this has demanded a high level of manning during the operation of the boiler and will be a key concern in relation to the use of automated systems as a means of reducing manning levels.

5) The achievement and maintenance of SIL4 using complex technology, e.g., programmable electronic devices, will not be easy unless specialist design techniques appropriate to high-integrity protection systems are used. High levels of competency and safety management will also be needed throughout all stages of the safety lifecycle including operation and maintenance. SIL4 systems are currently extremely rare, even in major hazards process plant. This has implications not only for the hardware reliability, but also for the systematic integrity of both hardware and software.

6) The allocation of risk targets for individual safety functions that contribute to the risk control of a common hazardous event can be carried out in a number of ways with a consequent impact on the safety integrity requirements of the various safety functions.

7) Further work is needed to determine if it is practicable to apply the other requirements of IEC 61508 (e.g., associated with systematic failures) to boiler installations. The work will need to consider the work processes under which hardware and software are developed, specified and

implemented throughout the whole safety lifecycle from SIL determination through to operation, maintenance and modification.

8 REFERENCES

1) Automatically controlled steam and hot water boilers - Guidance Note PM5 from the Health and Safety Executive, ISBN 0 11 885425 9, December 1989.

2) The application of BS EN 61508 to industrial boiler installations: Report 1 - Hardware reliability aspects, CI/03/23, A M Wray, Health and Safety Executive, September 2003. This report is available for downloading from http://www.hse.gov.uk/research/rrhtm/rr178.htm or can be obtained as a hardcopy.

3) Reducing risks, protecting people, HSE Books, ISBN 0 7176 2151 0, December 2001.

4) BS EN 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems, Parts 1 to 7, 2002. ISBN: Part 1: 0 580 32719 1; Part 2: 0 580 36136 5; Part 3: 0 580 32720 5; Part 4: 0 580 32721 3; Part 5: 0 580 32728 0; Part 6: 0 580 36137, and Part 7: 0 580 36138 1.

5) BS EN12953-6:2002, Shell boilers – Part 6: Requirements for equipment for the boiler, ISBN 0 580 39848 X, BSI Standards.

6) BS 2790: 1992, Specification for Design and manufacture of shell boilers of welded construction, ISBN 0 580 20075 2, BSI Standards.

Appendix A
List of abbreviations

For brevity, a number of abbreviations are used in this report. Although these are explained at the position of their first use, for the convenience of the reader the more important ones are expanded below.

ALARP	As Low As Reasonably Practicable
APFH	Actual Probability of Failure per Hour
ARR	Actual Risk Reduction
FR	Failure Rate
GDF	Gross Disproportion Factor
PES	Programmable Electronic Systems
PFD_{av}	Average Probability of Failure on Demand. Because the PFD is time dependent, it is the average PFD over the relevant period that is important. Therefore, the aim is to ensure that PFD_{av} is less than the target value.
PFH	Probability of Failure per hour - sometimes referred to as the random hardware failure rate.
RR	Risk Reduction
SIL	Safety Integrity Level (See Reference 4.)
$TPFD_{av}$	Target value for the average Probability of Failure on Demand.
TPFH	Target Probability of Failure per hour.
TRR	Target Risk Reduction
VPF	Value for Preventing a Fatality