Robust sensor network design for fault diagnosis

Mani Bhushan\textsuperscript{a,1}, Sridharakumar Narasimhan\textsuperscript{b,2}, Raghunathan Rengaswamy\textsuperscript{b,*}

\textsuperscript{a} Department of Chemical and Materials Engineering, University of Alberta, Canada
\textsuperscript{b} Department of Chemical Engineering, Clarkson University, USA

Abstract

An appropriately designed sensor network is crucial for the success of any fault diagnostic strategy. Strategies for optimally locating sensors based on reliability-maximization and cost-minimization exist. While reliability and cost criteria have been used in selecting optimal sensor networks, the robustness of the network to uncertainties/\errors in the underlying model and probability data have not been considered. In this article, we present robustness enhancing criteria for the design of sensor networks for reliable fault diagnosis. Robustness to modeling errors is incorporated by choosing a distributed sensor network. Robustness to available probability data is incorporated by minimizing the unreliability of fault detection with uncertain probability data. These criteria are incorporated in a lexicographic manner along with the overall reliability-maximization and cost-minimization objectives in a single optimization problem. Solution to this optimization problem results in a solution that is most reliable, robust and cost minimal in a lexicographic sense. The utility of the proposed approaches is demonstrated through the Tennessee Eastman case study.

Keywords: Sensor location; Fault diagnosis; Robust design; Optimization

1. Introduction

Fault detection and diagnosis is important for optimal and safe process operations. The aim of any fault diagnostic strategy is to quickly detect and identify faults. The efficiency of a diagnostic system depends critically on the location of the sensors monitoring important process variables. With hundreds of process variables available for measurement in a typical chemical plant, selection of informative sensor positions for efficient fault diagnosis is an important problem. While extensive research is available on sensor location in general, sensor location from a fault diagnosis perspective has received less attention. While these are related areas, there are still significant differences between them. The aim of sensor location problem as posed and solved in the literature is to identify variables to be measured such that various criteria, \textit{viz}: observability (ability to estimate values of all variables), precision (estimation of certain key variables with minimum variance), residual precision (estimation of certain key variables with required variance even if some sensor measurements are deleted), reliability of estimation of variables (in presence of sensor failure probabilities), gross error detectability (ability to detect gross errors of a certain size), and error resilience (ability to limit the smearing effect of undetected gross errors), are satisfied. An interested reader is referred to Bagajewicz's (2002) review article for further detailed information. As opposed to the above approaches which are mainly variable-centric, the aim of sensor location from fault diagnostic perspective is to identify variables to be measured such that various faults can be detected and diagnosed. Criteria such as resolution, cost, reliability, speed of detection and diagnosis, and false alarm rates are some of the measures that can be incorporated in this framework. Further, these approaches can also be classified based on the types of models used. Qualitative models such as fault trees (Lambert, 1977), (signed) directed graphs (Bhushan & Rengaswamy, 2000b; Raghuraj, Bhushan, & Rengaswamy, 1999), structural relationship models (Chang, Mah, & Tsai, 1993), detailed mathematical models (Alpay & Shor, 2000; Patton, Frank, & Clark, 1989; Watanabe, Sasaki, & Himmelblau, 1985), and data based models such as principal component analysis (Musulin, Bagajewicz, Nougues, &
2. Preliminaries

In this section, the main ideas that are necessary for understanding the proposed formulations are presented.

2.1. Process digraph based modeling and faultsets

A signed digraph (SDG) representation of the process is used in the sensor network design algorithms. A comprehensive discussion on the development and analysis of SDGs can be found in Maurya et al. (Maurya, Rengaswamy, & Venkatasubramanian, 2003a, 2003b). The SDG representation is used in designing a sensor network using the idea of faultsets. A faultset is associated with every fault. It is the set of variables affected by that particular fault. Placing a sensor on any one of the variables in the faultset will ensure that the corresponding fault is observed (Raghuraj et al., 1999; Bhushan & Rengaswamy, 2000b). For fault resolution (or diagnosis), the same idea is extended and faultsets are generated for fictitious fault nodes that represent the ability to resolve between faults pairwise. Placing a sensor on any one of the variables in these faultsets would distinguish between the two faults that are represented by the fictitious fault node (Raghuraj et al., 1999; Bhushan & Rengaswamy, 2000b). The solution to both the observability and resolution problems is the well-known set cover problem. Raghuraj et al. (1999) presented greedy search based heuristic methods for solving this problem.

In the work presented in this article, we will not make a distinction in the formulations between observability or resolution of faults. Also, the faultsets will be represented as a matrix, which will be referred to as fault-variable bipartite matrix \( B \). The rows of this matrix will correspond to faults (can be for observability or for resolution) while the columns will represent the variables. Further, \( B_{ij} = 1 \) if fault \( i \) affects variable \( j \), and is 0 otherwise.

2.2. Constrained optimization for minimization of detection unreliability

Bhushan and Rengaswamy (2000a, 2002a, 2002b) extended the work of Raghuraj et al. (1999) and Bhushan and Rengaswamy (2000b) to account for fault and sensor reliabilities. According to this approach, a reliable fault monitoring system should ensure that the probability of any fault occurring without being detected is low. The only way in which a fault can occur without being detected is if the fault occurs and

Puigjaner, 2003; Wang, Song, & Li, 2002; Wang, Song, & Wang, 2002), have been used.

In our previous work on sensor network design based on digraph (Raghuraj et al., 1999) and signed digraph (Bhushan & Rengaswamy, 2000b) representations, notions of fault observability and resolution were used to select optimal sensors. Later, optimization formulations incorporating various constraints on the sensor network design problem, as well as utilizing quantitative information such as fault occurrence and sensor failure probabilities, and cost constraints for sensor location were presented (Bhushan & Rengaswamy, 2002a, 2002b). While this approach provides an optimal sensor network design in terms of maximizing reliability, the robustness of the sensor network design is not considered. In this article, formulations for incorporating robustness to the uncertain fault occurrence and sensor failure probability data are presented. Further robustness to modeling errors/uncertainties in the underlying digraph models is also considered. These formulations are presented in a lexicographic optimization framework.

Nomenclature

\[ A_i \] set of variables affected by fault \( i \)
\[ B \] bipartite matrix between faults and measurable variables
\[ c_j \] cost of sensor used to measure variable \( v_j \)
\[ C^* \] available cost for sensor location
\[ f_i \] occurrence probability of fault \( i \)
\[ f_i \] fault \( i \)
\[ I \] set of fault indices considered in a formulation
\[ I_f \] set of indices of inaccurate faults
\[ I_s \] set of indices of faults which affect inaccurate sensors
\[ J \] set of indices of all measurable variables
\[ J_s \] set of indices of inaccurate sensors
\[ m \] number of faults in the optimization formulations
\[ n \] number of measurable variables
\[ n_j \] binary variable which is 1 if variable \( v_j \) is measured and is 0 otherwise
\[ N \] total number of variables measured in the process
\[ P \] a large positive constant
\[ s_j \] failure probability of sensor used for measuring \( v_j \)
\[ U_i \] unreliability of detection value of fault \( i \)
\[ v_j \] variable \( j \)
\[ x_j \] decision variable for the optimization problems; value indicates the number of sensors to be used for measuring variable \( v_j \)
\[ x_s \] non-negative slack variable for the cost constraint
\[ y_i \] binary variable corresponding to inaccurate fault \( i \)

Greek symbols

\[ \alpha, \alpha' \] constants used for lexicographic optimization
\[ \beta, \beta' \] \[ \lambda \] \[ \phi \] overall slack
\[ \phi^* \] maximum meaningful value of overall slack
\[ \phi_{i} \] slack for inaccurate fault \( i \)
\[ \phi_{i}^* \] maximum meaningful value of slack for inaccurate fault \( i \)

Subscripts

\[ f \] inaccurate fault probabilities case
\[ fs \] inaccurate fault and sensor probabilities case
\[ s \] inaccurate sensor probabilities case
simultaneously all the sensors detecting the fault fail (Bhushan & Rengaswamy, 2000a). This probability was defined as unobservability of the fault. Assuming that faults occur and sensors fail independently, the unobservability of fault $i$ was defined as:

$$ U_i = f_i \prod_{j=1}^{n} (s_j)^{R_j(x_j)} \tag{1} $$

where $s_j$ is the probability of failure of the $j$th sensor and is defined as $s_j = 1 - R_j$ with $R_j$ being the reliability of the $j$th sensor, i.e. $R_j$ is the probability that the sensor has not failed from time 0 to $t$. Similarly, $f_i$ is the probability of occurrence of $i$th fault and is defined as $f_i = 1 - R_{fi}$ with $R_{fi}$ being the reliability of the $i$th fault. The reason for this change in notation is that in the general fault diagnosis literature, the term unobservability has been used as a “yes/no condition” (fault is either observable or not) (Massoumnia, Verghese, & Willsky, 1989) rather than as an index or degree. In view of this requirement, it can be noted that each of the three objectives however behave differently in this aspect.

In this article, we refer to $U_i$ as unreliability of detection of $i$th fault and not unobservability of $i$th fault. The reason for this change in notation is that in the general fault diagnosis literature, the term unobservability has been used as a “yes/no condition” (fault is either observable or not) (Massoumnia, Verghese, & Willsky, 1989) rather than as an index or degree. In view of this, continued use of term “unobservability” for a quantity (as defined in Eq. (1)) of unreliability of detection, they did not provide any detailed discussion about its interpretation and alternative objective functions. We discuss these issues here to enable better understanding of the existing and proposed work. Towards this end, we define the following two events: $C_i$: Event of not detecting $i$th fault, and $A_i$: Event of $i$th fault occurring.

Detection unreliability is the joint probability of fault occurrence and failure of all sensors detecting the $i$th fault and is given as:

$$ P(C_i \cap A_i) = P(A_i)P(C_i|A_i) \tag{2} $$

where $P$ denotes the probability and $P(A_i) = f_i$ is the probability of fault occurrence while $P(C_i|A_i)$ is the probability that the fault is not detected, given that it has occurred. For this to happen all the sensors observing the fault have to fail and the probability of this is: $\prod_{j=1}^{n} (s_j)^{R_j(x_j)}$. Notice that $f_i$ does not appear in the $P(C_i|A_i)$ expression as the conditional probability means that it is given that $A_i$ has already happened (fault has occurred). Hence, $P(C_i \cap A_i)$ can be written as:

$$ P(C_i \cap A_i) = f_i \prod_{j=1}^{n} (s_j)^{R_j(x_j)} \tag{3} $$

which is the expression given in Eq. (1).

From a viewpoint of performing sensor location, other than $P(C_i \cap A_i)$, two alternative objectives can also be potentially minimized. These are

1. Probability of not detecting a fault, i.e. $P(C_i)$ which is given as:

$$ P(C_i) = P(C_i \cap A_i) + P(C_i \cap \sim A_i) \tag{4} $$

or,

$$ P(C_i) = P(C_i|A_i)P(A_i) + P(C_i|\sim A_i)P(\sim A_i) \tag{5} $$

In the above expression, $\sim A_i$ denotes non-occurrence of event $A_i$, and $P(C_i|\sim A_i) = 1$ based on the implicit assumption of no false positives (no sensor deviates beyond its control limit in the absence of fault). This assumption ensures that the probability of not detecting a fault when it has not occurred is 1. Hence,

$$ P(C_i) = P(C_i|A_i)P(A_i) + P(\sim A_i) \tag{6} $$

or,

$$ P(C_i) = f_i \prod_{j=1}^{n} (s_j)^{R_j(x_j)} + 1 - f_i \tag{7} $$

Note that since $P(C_i)$ is simply the probability of not detecting the fault, it encapsulates both scenarios where fault has occurred (first term in Eq. (7)) as well as when fault has not occurred (second term in Eq. (7)). In comparison, $P(C_i \cap A_i)$ only considered situations involving occurrence of the fault (Eq. (3)).

2. The conditional probability of not detecting a fault given that it has occurred, i.e. $P(C_i|A_i)$ which is given as:

$$ P(C_i|A_i) = \prod_{j=1}^{n} (s_j)^{R_j(x_j)} \tag{8} $$

In the sensor network design problem, the aim will be to place sensors to minimize the unreliability of detection of fault. In view of this requirement, it can be noted that each of the three possible objectives exhibit the correct behaviour (they decrease) with increasing number of sensors (increasing $s_j$) as well as with decreasing sensor failure probabilities ($s_j$).

Additionally, we would also want the unreliability of detection to increase with increasing fault occurrence probability. The three objectives however behave differently in this aspect. While $P(C_i|A_i)$ does not change with increasing $f_i$, $P(C_i \cap A_i)$ increases and $P(C_i)$ decreases with increasing $f_i$. Hence, only $P(C_i \cap A_i)$ has the desirable behaviour. Apart from this, another crucial reason why we choose $P(C_i \cap A_i)$ over the other two objectives for performing sensor location is that it denotes the worst case scenario of simultaneous fault occurrence and sensor failures. $P(C_i)$ on the other hand also incorporates scenario when no fault has occurred. This philosophy of considering worst case scenarios is reflected throughout this article in the way in which various objectives are defined and has also been used in the past in reliability based sensor network design literature (Ali & Narasimhan, 1993).
A good sensor network should lead to low unreliability of detection values for the faults. However, in the presence of cost constraints, arbitrary reduction in unreliability of detection values is not possible. The sensor location design problem is to then “choose the number and location of variables to be measured such that the system unreliability of detection is minimized while satisfying the overall cost constraint”. Consistent with the philosophy of designing for the worst case scenario, the measure of system unreliability of detection chosen by Bhushan and Rengaswamy (2002a) is the maximum unreliability of detection among all the faults. Further, instead of minimizing unreliability of detection, equivalently, log of unreliability of detection can be minimized. The advantage of the log transformation being that the problem becomes linear in the decision variables \( x_j \). This sensor location design problem was then posed as a mixed integer linear programming (MILP) problem (Bhushan & Rengaswamy, 2000a).

2.3. Lexicographic optimization

It was further found by Bhushan and Rengaswamy (2002a) that this problem typically has multiple solutions for unreliability of detection with different costs. Lexicographic optimization is one way of finding the solution with the least cost among these multiple solutions. This is achieved by ordering the objectives in hierarchical levels based on their importance. Such an ordering would mean that a higher level objective is infinitely more important than a lower level objective (Miettinen, 1998). The lexicographic solution is obtained by combining the various objective functions in a single objective function using appropriate weights (Sherali, 1982; Sherali & Soyster, 1983). Bhushan and Rengaswamy (2002a) used an approach similar to Sherali (1982) to combine unreliability of detection minimization and cost minimization objectives in a lexicographic manner in a single objective function as (Bhushan & Rengaswamy, 2002a):

Problem I. One-step optimization

\[
\min \{ U - \alpha x_s \} \\
\text{(9)}
\]

subject to:

\[
U \geq \log U_i; \quad i = 1, \ldots, m
\]

\[
\sum_{j=1}^{n} c_j x_j + x_s = C^* \quad \text{(11)}
\]

\[
x_j \in \mathbb{Z}^+; \quad j = 1, \ldots, n
\]

\[
x_s \in \mathbb{R}^+; \quad U \in \mathbb{R}^-
\]

In the above problem, the objective function \( U \) is the maximum unreliability of detection (on a log scale) among all faults (this is captured by constraints (10)), and \( C^* \) is the available cost for performing sensor location. The problem is linear in the decision variables \( x_j \) since the log of unreliability of detection is being used. Notice that hardware redundancy is incorporated in the above formulation by allowing the variables to take any non-negative integer value. The variable \( x_s \) corresponds to cost saving, and hence the higher the value of \( x_s \), lower is the cost used for sensor location. \( \alpha \) is a positive constant which has to be chosen such that the primary objective (minimizing unreliability of detection) still attains its earlier optimal value. A sufficient range for the value of \( \alpha \) is given in Bhushan and Rengaswamy (2002a), who have also presented constraint reduction techniques for the above problem. The above formulation is applicable for any appropriately generated \( B \) matrix and fault occurrence probabilities (Bhushan & Rengaswamy, 2002a).

3. Robust sensor network design

The sensor network design presented in this article is based on the digraph representation of the process. The digraph model represents cause–effect relationships in the process which even if exactly known at the current operating point, can change as the operating point of the process changes. Hence, some amount of approximation is inevitably involved in the construction of the digraph representation. It is then desirable to choose a sensor network which is robust to some extent to changes/errors in the process model as represented by the digraph. It is worthwhile to point out that even though the approach presented here for incorporating robustness is geared towards digraph based representation of the process, the issue of robustness while designing sensor networks would be valid irrespective of the modeling strategy used.

Robustness to modeling errors is incorporated by preferring a more distributed sensor network. We will demonstrate through simulation studies, later in this article, that distribution leads to robustness to modeling errors. Besides the underlying model, the sensor network design strategy also requires the knowledge of fault occurrence and sensor failure probabilities. In some cases the probability data may be known based only on insufficient past knowledge or lab-scale experiments. It is then desirable to incorporate some robustness to this data while designing a sensor network. We present a novel lexicographic approach for incorporating robustness to inaccurate probability data. The key idea is to choose a sensor network such that the resulting system unreliability of detection is insensitive to imprecise data. This is achieved by ensuring that the constraints involving uncertain data are far from being active at the optimal solution.

3.1. Robustness to available probability data

For robustness to available probability data, three different scenarios are considered:

1. inaccuracies in occurrence probabilities of some faults with all sensor probabilities accurately known;
2. inaccuracies in failure probabilities of some sensors with all fault occurrence probabilities accurately known;
3. combination of situations (1) and (2).

Note that while situations (1) and (2) are special cases of situation (3), they are presented separately to highlight the various issues involved. In the rest of the article, to simplify the notation, a fault whose unreliability of detection calculation
involves inaccurately known or uncertain data, will be referred to as “inaccurate” or “uncertain” fault. A fault can be inaccurate if any of the following three conditions hold: (a) the fault occurrence probability is inaccurately known, (b) the unreliability of detection value of a fault depends on a sensor (or more than one sensor) with inaccurately known failure probability, or (c) both (a) and (b) hold. We use lexicographic optimization to solve these problems.

The primary objective is the minimization of system unreliability of detection calculated using nominal fault occurrence and sensor failure probability values. The secondary objective is the maximization of the slack in the unreliability of detection among all the faults. Hence, it is possible that sensor networks with the same system unreliability of detection have different unreliability of detection values for the individual faults. If some of these faults are inaccurately characterized, then a network which yields a lower unreliability of detection for the inaccurate fault should be chosen. Such a network will lead to a higher slack in the unreliability of detection constraint of the corresponding fault. In general, there can be more than one inaccurate fault. The secondary objective is then to maximize the minimum slack amongst all the slack variables in the unreliability of detection constraints of these faults. Even after optimization of these two objective functions, it is still possible to obtain multiple optimal solutions with possibly different cost required for each solution. The third objective is then to minimize the cost used. The three objective functions are combined in a single-weighted objective function using appropriately computed weighting constants. These formulations for scenarios (1)–(3) listed above are presented next. In all the formulations presented in this and other sections, it is assumed that the objective functions: unreliability of detection, slack: \( \phi_f / \phi_s / \phi_{fs} \), and cost slack: \( x_s \) can take only integer values. The values for the various weighting coefficients \( (\lambda_i, \beta_i, \beta_f, \alpha_i, \alpha_f) \) are given with this assumption. For situations where this assumption is not true, the modified values are provided in Appendix B. Another important observation, true for all the formulations presented in this article is that the calculation of all the weighting constants used in the objective function for lexicographic optimization is based on the problem data and not on the values of the decision variables. One final comment here is that as formulated in Problem I, instead of unreliability of detection, the log of unreliability of detection was minimized. In the robustness formulations presented in this article, log of unreliability of detection is considered everywhere even though we need robustness with respect to unreliability of detection. However, it turns out that the two situations: maximizing robustness with respect to unreliability of detection or log of unreliability of detection, are equivalent as shown in Appendix A.

3.1.1. Robustness to inaccurate fault probability data

**Problem II.** Formulation for incorporating robustness to inaccurate fault probability data

subject to,

\[
\sum_{j=1}^{n} c_j x_j + x_s = C^* \tag{15}
\]

\[
U \geq \log(U_i), \forall i \in I \setminus I_f \tag{16}
\]

\[
U = \log(U_i) + \phi_{fi}, \forall i \in I_f \tag{17}
\]

\[
\phi_f \leq \phi_{fi}, \forall i \in I_f \tag{18}
\]

\[
x_j \in \mathbb{Z}^+; \ U \in \mathbb{R}^-; \ (x_s, \phi_{fi}, \phi_f) \in \mathbb{R}^+ \tag{19}
\]

In the formulation shown above, \( \phi_{fi} \) is the (positive) slack variable of the unreliability of detection constraint for the \( i \)th inaccurate fault. This slack variable is added to the unreliability of detection constraints of the faults (belonging to \( I_f \)) whose occurrence probabilities are not accurately known. The secondary objective is the maximization of the minimum slack \( \phi_f \) among all the faults with inaccurately known probabilities. Constraints (18) and the fact that \( \phi_f \) is being maximized in the objective function (a constant times \( -\phi_f \) is being minimized) ensures that \( \phi_f \) is equal to the minimum value among all individual \( \phi_{fi} \) values. Positive constants \( \lambda_1 \) and \( \lambda_2 \) ensure that the solution to Problem II solves a lexicographic optimization problem with unreliability of detection minimization, slack maximization and cost minimization as the objectives in decreasing order of preference. The values for \( \lambda_1 \) and \( \lambda_2 \) can be derived using the idea presented by Sherali (1982) and are:

\[
\lambda_1 = (1 + \phi_f^*) (1 + C^*) \tag{20}
\]

\[
\lambda_2 = (1 + C^*) \tag{21}
\]

where \( \phi_f^* \) is a constant calculated as in Eq. (23). Notice that in the formulation of Problem II, the objective function could also have been equivalently written as: \( U - \beta \phi_f - \gamma x_s \) where constants \( \beta \) and \( \gamma \) can be calculated in terms of \( \lambda_1 \) and \( \lambda_2 \).

Formulation II as presented above has a problem. It can lead to solutions where the extra cost is spent in increasing \( \phi_f \) to meaningless high values. To understand this, consider a process with one inaccurate fault with nominal fault occurrence probability of \( 10^{-2} \). In the worst case, the actual occurrence probability of this fault will tend to \( 10^0 = 1 \). Considering constraint (17) for this fault, it can be seen that if \( \phi_{fi} \) for this fault is equal to 2 (= \( \log(10^0) - \log(10^{-2}) \)), then even in the worst case, the system unreliability of detection will not be higher than the value calculated using nominal fault occurrence probability data. In other words, if \( \phi_f > 2 \) for this problem, then the unreliability of detection constraint involving the inaccurate fault will never be active, and hence the system unreliability of detection will be insensitive to the true fault occurrence probability of this inaccurate fault, irrespective of the value of system unreliability of detection. Hence, spending extra cost to increase \( \phi_f \) above 2 for this case is not required. One way of incorporating this constraint is to impose a maximum value on \( \phi_f \). For example, for this case, the constraint \( \phi_f \leq 2 \) can be added. In general, each inaccurate fault will have an upper limit for \( \phi_f \). In that case, the
following constraint on the variable $\phi_f$ can be added

$$\phi_f \leq \phi_f^*$$  \hspace{1cm} (22)

where the constant $\phi_f^*$ is given as:

$$\phi_f^* = \max_{(\forall i \in I_f)} \phi_f^*$$  \hspace{1cm} (23)

where $\phi_f^*$ is the maximum meaningful value of the slack variable for the $i$th inaccurate fault. Calculation of $\phi_f^*$ is presented in Appendix C.1.

Constraint (22) only ensures that the maximum value of $\phi_f$ is not more than the maximum meaningful value of all the slack variables. However, since the secondary objective is to maximize $\phi_f$ and $\phi_f$ is the minimum of all $\phi_f^*$, in order for $\phi_f$ to achieve the maximum permissible value ($\phi_f^*$), each $\phi_f^*$ will have to be $\geq \phi_f^*$. But this is not correct since as discussed in the above paragraph, the maximum meaningful value for each $\phi_f^*$ is the corresponding $\phi_f^*$, and hence maximizing the value of $\phi_f$ should not force a solution which results in any $\phi_f^* \geq \phi_f^*$. This is achieved by replacing constraints (18) by the following set of constraints

$$\phi_f \leq \phi_f^* + \phi_f^* y_i, \hspace{1cm} \forall i \in I_f$$  \hspace{1cm} (24)

$$P y_i \geq \phi_f - \phi_f^*, \hspace{1cm} \forall i \in I_f$$  \hspace{1cm} (25)

$$P(y_i - 1) \leq \phi_f - \phi_f^*, \hspace{1cm} \forall i \in I_f$$  \hspace{1cm} (26)

$$y_i \in \{0, 1\}, \hspace{1cm} \forall i \in I_f$$  \hspace{1cm} (27)

In the above constraints, $P$ is a large positive constant (for example, 1000) and $y_i$ is a binary variable. The basic idea behind introducing this binary variable is that if for a fault $k$, the slack variable $\phi_{f_k}$ has a value greater than its maximum meaningful value $\phi_{f_k}^*$, then the value $\phi_f$ is not restricted by value of $\phi_{f_k}$, and increasing $\phi_{f_k}$ further will not increase $\phi_f$. Constraints (25) and (26) ensure that $y_k = 1$ for this case, and this ensures that constraint (24) for fault $k$ is not a limiting constraint on the upper value of $\phi_f$ (compare constraint (24) with constraint (22)). For the case when $\phi_{f_k} < \phi_{f_k}^*$, constraints (25) and (26) force $y_k$ to be 0, and this reduces constraint (24) for fault $k$ to $\phi_f \leq \phi_{f_k}$ as it should be. For the case when $\phi_{f_k} = \phi_{f_k}^*$, constraints (25) and (26) allow $y_k$ to be either 0 or 1, but maximization of $\phi_f$ in the objective function ensures that $y_k$ will be chosen as 1, if the maximum value of $\phi_f$ is being restricted by $\phi_{f_k}$ (refer to constraint (24)).

Note that it may be argued that instead of introducing the binary variables $y_i$, we could have directly imposed constraints on the upper values of $\phi_{f_i}$ as $\phi_{f_i} \leq \phi_{f_i}^*$. But this would not be correct, as these constraints may affect the optimal values for the primary objective (minimizing system unreliability of detection), thereby violating our design philosophy of lexicographic optimization. Constraints (24)–(27) on the other hand, do not force $\phi_{f_i} \leq \phi_{f_i}^*$. They just ensure that increasing $\phi_{f_i}$ beyond $\phi_{f_i}^*$ does not result in increasing $\phi_f$.

To summarize, the formulation that we propose to use for sensor network design while incorporating robustness to fault occurrence probability data is: Formulation II with constraints (22) and (24)–(27) used in place of constraints (18).

3.1.2. Robustness to inaccurate sensor failure probability data

Formulation to incorporate robustness to sensor failure probability data is now considered.

**Problem III.** Formulation for incorporating robustness to inaccurate sensor probability data

$$\min[\lambda_1 U - \lambda_2 \phi_s - x_s]$$  \hspace{1cm} (28)

subject to,

$$\sum_{j=1}^n c_j x_j + x_s = C^*$$  \hspace{1cm} (29)

$$U \geq \log(U_i), \hspace{1cm} \forall i \in I \setminus I_s$$  \hspace{1cm} (30)

$$U = \log(U_i) + \phi_{si}, \hspace{1cm} \forall i \in I_s$$  \hspace{1cm} (31)

$$\phi_s^* = -\sum_{j \in I_s} B_{ij}(\log s_j)x_j, \hspace{1cm} \forall i \in I_s$$  \hspace{1cm} (32)

$$P y_i \geq \phi_{si} - \phi_{si}^*, \hspace{1cm} \forall i \in I_s$$  \hspace{1cm} (33)

$$P(y_i - 1) \leq \phi_{si} - \phi_{si}^*, \hspace{1cm} \forall i \in I_s$$  \hspace{1cm} (34)

$$\phi_s \leq \phi_{si} + \phi_{si}^* y_i, \hspace{1cm} \forall i \in I_s$$  \hspace{1cm} (35)

$$\phi_s \leq \phi_s^*$$  \hspace{1cm} (36)

$$x_j \in \mathbb{Z}^+; \hspace{1cm} (x_s, \phi_s, \phi_{si}, \phi_{si}^*) \in \mathbb{R}^+$$  \hspace{1cm} (37)

$$U \in \mathbb{R}^-; \hspace{1cm} y_i \in \{0, 1\}$$  \hspace{1cm} (38)

In the formulation shown above, constant $\phi_s^*$ is the maximum meaningful value for $\phi_s$ for a given problem. The procedure for calculating $\phi_s^*$ is however more involved than Eq. (23), and a method for calculating $\phi_s^*$ is given in Appendix C.2. Constraint (32) is written for faults affecting variables to be measured by uncertain sensors, and it calculates the maximum meaningful value of slack required in a fault unreliability of detection constraint, based on the chosen sensors. For example, suppose that a fault affects one variable with uncertain sensor, however no sensor is selected for measuring that variable (the corresponding $x$ value is 0). In that case no slack will be required for the unreliability of detection constraint for this fault. As can be seen from Eq. (32), $\phi_s^*$ for this fault will be 0. Constraints (33)–(36) are the same as the constraints used in Formulation II. A formulation to incorporate robustness to both sensor failure and fault occurrence probabilities is considered next.

3.1.3. Robustness to inaccurate sensor failure and fault occurrence probability data

Problem II incorporated robustness only to inaccurate fault occurrence probabilities, and Problem III considered robustness only to inaccurate sensor failure probabilities. A design formulation where both types of uncertainties are considered simultaneously is presented next.
Problem IV. Formulation for incorporating robustness to inaccurate sensor and fault probability data

\[
\min_{(x_j)} [\lambda_1 U - \lambda_2 \phi_{fs} - x_i] \quad (39)
\]

subject to,

\[
\sum_{j=1}^n c_j x_j + x_i = C^* \quad (40)
\]

\[
U \geq \log(U_i), \quad \forall i \in I \setminus (I_f \cup I_s) \quad (41)
\]

\[
U = \log(U_i) + \phi_{fsi}, \quad \forall i \in (I_f \cup I_s) \quad (42)
\]

\[
\phi_{fsi}^s = \phi_{fsi}^s, \quad \forall i \in (I_f \setminus I_s) \quad (43)
\]

\[
\phi_{fsi}^s = \phi_{fsi}^s, \quad \forall i \in (I_s \setminus I_f) \quad (44)
\]

\[
\phi_{fsi} = \phi_{fsi}^s + \phi_{fsi}^*, \quad \forall i \in (I_f \cap I_s) \quad (45)
\]

\[
P_{yi} \geq \phi_{fsi} - \phi_{fsi}^*, \quad \forall i \in (I_f \cup I_s) \quad (46)
\]

\[
P(y_i - 1) \leq \phi_{fsi} - \phi_{fsi}^*, \quad \forall i \in (I_f \cup I_s) \quad (47)
\]

\[
\phi_{fsi} \leq \phi_{fsi}^s + \phi_{fsi}^y_i, \quad \forall i \in (I_f \cup I_s) \quad (48)
\]

\[
\phi_{fs} \leq \phi_{fs}^* \quad (49)
\]

\[
\phi_{fs}^* = -\sum_{j \in I_s} B_{ij}(\log s_j) x_j, \quad \forall i \in I_s \quad (50)
\]

\[
x_j \in \mathbb{Z}^+; \quad (x_s, \phi_{fs}, \phi_{fsi}, \phi_{fsi}^s, \phi_{fs}^y) \in \mathbb{R}^+ \quad (51)
\]

\[
U \in \mathbb{R}^-; \quad y_i \in \{0, 1\} \quad (52)
\]

In the above formulation, \(\phi_{fs}^s\) and \(\phi_{fs}^y\) are as given in Formulations II and III, respectively. Calculation of the constant \(\phi_{fs}^y\) (the maximum meaningful value for the slack) is explained in Appendix C.3. Note that, as expected, the constraints in the above formulation are a combination of constraints of Problems II and III.

A few points are worth noting regarding the Formulations II, III and IV:

- Instead of combining the three individual objectives into one single weighted objective function, equivalently, three sequential optimization problems could have been solved.
- Also, instead of maximizing the minimum slack, a suitably weighted function of slacks in the individual fault constraints, or some other combination could have been used. The idea in using the minimum slack among all inaccurate faults is similar to the idea of using maximum unreliability of detection among all faults. This concept is inspired by the philosophy that “a chain can be no stronger than its weakest link” used earlier in the area of sensor location (Ali & Narasimhan, 1993).
- Redundant constraint removal: a procedure for removing redundant constraints was presented by Bhushan and Rengaswamy (2002a). That procedure needs to be modified for the case when there is uncertainty in some fault occurrence and/or some sensor failure probabilities. For the sake of completeness, this modified procedure is briefly explained in Appendix E.
- The weighting coefficients \(\lambda_1\) and \(\lambda_2\) for Formulations III and IV can be determined similar to that for Formulation II (Eqs. (20) and (21)). This is illustrated in Appendix B.

3.2. Lexicographic approach for incorporating robustness to modeling errors

Formulations to incorporate robustness to inaccurate probability data were presented above. It can also happen that the underlying process model used for generating cause–effect information between faults and measurable variables (matrix \(B\) in our formulations) is not accurate. This may happen, since we have used process SDG which is a qualitative, cause–effect representation of the process. The resulting faultsets are accurate representations of the effect of faults on variables if the underlying qualitative relationships are correct. The SDG can be constructed from the nonlinear model equations representing the process by linearizing the equations around an operating point, and finding signs of the effects of variables on each other based on this linearized model. Unlike a quantitative model, that would be valid in a very narrow range around the operating point, the digraph model would have a much larger region of validity, since the region in which the signs do not change will be much larger than the region in which the numerical values of the derivatives do not change. Still, it is possible to be operating in a region where the underlying qualitative relationships have changed since the process has moved from the original operating point, or the relationships themselves have been wrongly modeled. Further, to reduce the number of spurious solutions (which are inherent to any qualitative representation), Bhushan and Rengaswamy (2002b) incorporated arc-gains in the SDG representation. While this reduces the number of spurious solutions, it is at the expense of making wrong predictions since gains are calculated based on steady state values, and for a nonlinear process, as the process moves away from the steady state, the gains can change significantly.

In view of the preceding discussion, it is clear that some amount of uncertainty/errors are typically present in the generation of the cause–effect matrix \(B\). The efficacy of a selected sensor network will then be affected by these unknown uncertainties. The following example briefly illustrates this issue and the solution that we propose.

Example 1: consider a simple process consisting of two faults \(F_1\) and \(F_2\), and two measurable variables \(v_1\) and \(v_2\). Assume that the sensors available for measuring \(v_1\) and \(v_2\) have the same reliability and cost. Suppose from SDG simulation, we find the faultsets to be \(A_1 = \{v_1^+, v_2^+\}\) and \(A_2 = \{v_1^-, v_2^+\}\). Then, if we want to observe both faults, as well as resolve between the two faults under the single fault assumption, either variable \(v_1\) or \(v_2\) can be measured. The system unreliability of detection in both the cases would be the same. Now, if the cost for placing two sensors is available, then placing two sensors to measure either variable \(v_1\) or \(v_2\) or measuring both variables using a sensor each, the system unreliability of detection and the total
cost used would be the same. For the sake of argument, let us assume that both the sensors are placed on variable \( v_2 \). However, now consider a situation where the actual effect of fault \( F_1 \) on variable \( v_2 \) is positive and not negative as used in our model. Now, since both the sensors are placed at variable \( v_2 \), it will not be possible to resolve between faults \( F_1 \) and \( F_2 \). On the other hand, if a sensor each had been placed on variables \( v_1 \) and \( v_2 \), then it would have been possible to resolve between the two faults, even in the presence of modeling error.

It is seen from the above example that a distributed sensor network is better in general for handling modeling uncertainties. A sensor network is more distributed than some other network, if the total number of distinct variables being measured is more in the former case. The strategy that we then propose to incorporate robustness is to maximize the distribution in the selected sensor network. Once again, this is done in a lexicographic framework, and the formulation that we propose to achieve this when there is no uncertainty in the probability data is similar to Problem I with the following modifications: (a) the objective function is modified to include a term corresponding to network distribution as: \( \min x_{j} \{ (\alpha_1 U - \alpha_2 N) - N \} \) and (b) the following additional constraints are added: \( N = \sum_{j=1}^{n} n_j \), \( n_j \leq x_j, \ j = 1, 2, \ldots, n \) where the variables \( n_j \in \{0, 1\} \). In this formulation, \( N \) is the total number of variables measured in the process, and characterizes the distribution in the process. Variable \( n_j \) is a binary variable, which is 1 if variable \( j \) is measured (irrespective of the number of sensors used to measure variable \( j \)), and is 0 if variable \( j \) is not measured. This is ensured by constraints \( n_j \leq x_j \) and the fact that \( N \) is being maximized in the objective function (or negative \( N \) is being minimized). \( \alpha_1 \) and \( \alpha_2 \) are positive constants which ensure that solution to this problem is optimal in the lexicographic sense with unreliability of detection minimization, cost minimization, and network distribution maximization being the three objectives in decreasing order of priority. These constants can be calculated in a manner similar to Eqs. (20) and (21), and are given as

\[
\alpha_1 = (1 + C^*) (1 + N^*) \tag{53}
\]

\[
\alpha_2 = (1 + N^*) \tag{54}
\]

where \( N^* \) is the maximum number of different sensors that can be selected in the process for a given available cost \( C^* \). A procedure for calculating \( N^* \) is given in Appendix D.

It is also to be noted that in this proposed modification, contrary to formulations presented so far, cost minimization is considered a more important objective than network distribution maximization. The reason for this is that if network distribution maximization is considered as a secondary objective, then this objective forces measurement of as many variables as possible, and hence may not result in significant cost savings. However, if cost savings are not important (as long as the overall cost constraint is not violated), then the network distribution maximization can be made a secondary objective and cost the third objective. This is a design choice that may vary from one situation to other and thus, we can also use the following alternative objective function for achieving distributed network: \( \min x_{j} \{ (\alpha'_1 U - \alpha'_2 N) - N \} \), with the constraints remaining as before. The lexicographic constants \( \alpha'_1, \alpha'_2 \) can be calculated in a manner similar to Eqs. (53) and (54).

In general, multi-objective optimization problems are inherently subjective and often when faced with several objectives, it may be difficult to prioritize them. Hence, the final choice is left to the decision maker. However, in both the network distribution formulations, the primary objective is overall system unreliability of detection minimization and that remains unchanged.

The network distribution formulations discussed above assumed that the probability data is accurately known. Incase, some probability values (either fault and/or sensor) are not accurately known, then depending on the scenario, a network distribution maximization objective can be added to the appropriate formulation in a lexicographic manner. Thus, depending on whether we choose to prioritize distribution over cost or otherwise, we have the following problems:

**Problem Va.** Formulation incorporating network distribution and uncertain probability data

\[
\min x_{j} \{ \beta_1 U - \beta_2 N - N \} \tag{55}
\]

subject to,

\[
N = \sum_{j=1}^{n} n_j \tag{56}
\]

Constraints of Problems II or III or IV depending on the scenario

\[
n_j \leq x_j, \ j = 1, 2, \ldots, n \tag{57}
\]

\[
n_j \in \{0, 1\} \tag{58}
\]

The values for constants \( \beta_1, \beta_2, \beta_3 \) can be calculated using Sherali’s (1982) algorithm as:

\[
\beta_1 = (1 + N^*) (1 + C^*) (1 + M) \tag{60}
\]

\[
\beta_2 = (1 + N^*) (1 + C^*) \tag{61}
\]

\[
\beta_3 = (1 + N^*) \tag{62}
\]

where constant

\[
M = \begin{cases} 
\phi_s' & \text{if uncertainty only in faults (Problem II),} \\
\phi_s' & \text{if uncertainty only in sensors (Problem III),} \\
\phi_{fs} & \text{if uncertainty in both faults and sensors (Problem IV).} 
\end{cases} \tag{63}
\]

**Problem Vb.** Alternate formulation incorporating network distribution and uncertain probability data

\[
\min x_{j} \{ \beta'_1 U - \beta'_2 N - N \} \tag{64}
\]

subject to the constraints of Problem Va. The values for constants \( \beta'_1, \beta'_2, \beta'_3 \) can be calculated similar to Eqs. (60)–(62) as:

\[
\beta'_1 = (1 + C^*) (1 + N^*) (1 + M) \tag{65}
\]

\[
\beta'_2 = (1 + C^*) (1 + N^*) \tag{66}
\]
\[ \beta'_3 = (1 + C^+) \]  

(67)

where constant \( M \) is as given in Eq. (63).

Even though theoretically sound, depending on the values of constants \( N^*, C^*, M \), the use of objective functions (55) or (64) may not be possible, as it may lead to scaling problems due to wide differences in the values of the weighting constants for different objectives. In this situation, the lexicographic solution can be obtained by solving more than one problem in sequence (Sherali, 1982). The Tennessee Eastman case study which demonstrates the utility of the proposed robust designs is presented next.

4. Tennessee Eastman case study

To illustrate the utility of the ideas presented in this article, the well known Tennessee Eastman (TE) process is used as a case study. The TE process was presented originally by Downs and Vogel (1993) as a challenge problem in control, diagnosis and other related areas. A flowsheet of the TE process is given in Fig. 1. The process consists of five major unit operations: an exothermic two-phase reactor, product condenser, flash separator, a reboiled stripper, and a recycle compressor. Two products, G and H and a byproduct F are produced from reactants A, C, D and E along with an inert component B. Ricker and Lee (1995) proposed a reduced model for the TE process. Based on this reduced model, Maurya, Rengaswamy, and Venkatasubramanian (2004) developed an SDG and used it to generate the faultsets for the original faults. From these faultsets, we created pseudo faultsets corresponding to single fault resolution. The results presented in this section correspond to single fault resolution and observability scenario. Possible locations of sensors, sensor failure probabilities, sensor costs, faults considered and probabilities of their occurrences are listed in Tables 1–3. This data has been taken from two references: Bhushan and Rengaswamy (2002b) (cost and probability data) and Maurya et al. (2004) (faults and faultsets), and detailed information about the variables and the faults involved can be obtained from these references.

The following cases are considered (cases are numbered according to the corresponding formulation being considered):

Case I: Baseline scenario, where the objectives are to minimize system unreliability of detection and cost (Problem I).

Case II: Robust design in the presence of inaccuracies in fault probability data (Problem II). It is assumed that the probabilities of occurrence \( f_1 \) and \( f_9 \) of faults \( F_1 \) and \( F_9 \), respectively, are inaccurately known.

Case III: Robust design in the presence of inaccuracies in sensor failure probability data (Problem III). It is assumed that the failure probabilities \( s_3 \) and \( s_4 \) of sensors to be...
used for measuring variables $v_3$ and $v_4$, respectively, are inaccurately known.

Case IV : Robust design in the presence of both fault occurrence and sensor failure probability data (Problem IV). It is assumed that fault occurrence probabilities $f_1$ and $f_0$ and sensor failure probabilities $s_3$ and $s_4$ are inaccurately known.

Case Va : Design incorporating robustness and network distribution (Problem Va). The sensor networks are designed to be robust to the relevant scenario (uncertain fault probability, uncertain sensor failure probability and uncertainty in both sensor failure and fault probabilities).

Case Vb : Design incorporating robustness and network distribution by prioritizing distribution over cost (Problem Vb).

The resulting sensor networks for different available cost $C^*$ along with other relevant information are tabulated in Tables 4, 6 and 8. The quality of robustness as quantified by $\phi_f, \phi_s$, and $\phi_c$ needs further qualification and additional details are tabulated in Tables 5, 7 and 9. Only relevant inaccurate faults are reported in these tables as all other inaccurate faults were found to have lower unreliabilities of detection. Further, the listed unreliability of detection values are on the log$_{10}$ scale.

In all the tables, the selected sensor is just indicated by the corresponding variable number, and the number in bracket after the variable number indicates the hardware redundancy (total number of sensors selected to measure that variable). For example, 3(2) means that two sensors are selected to measure variable $v_3$.

All the formulations are solved using the widely used ILOG-CPLEX solver.

4.1. Inaccurate faults scenario

In the uncertain fault scenario, the values of $\phi_f$ reported in Table 4 are the relevant slacks in the unreliability of detection calculation for inaccurate faults.

Consider the sensor networks for $C^* = 500$. As seen from Table 5, the $\phi_f$ (slack) values for Problem I (measured variable is $v_1$ as listed in Table 4) for faults $F_1, F_{1.7}, F_{1.9}, F_{1.15}$ are respec-
respectively 3, 0, 0, 0. Given that the overall system unreliability of detection is −2 (Table 4), this indicates that the individual unreliabilities of detection for faults $F_1, F_{1.7}, F_{1.9}, F_{1.15}$ are $-5 (= -2 - 3), -2 (= -2 - 0), -2 (= -2 - 0)$, respectively. Here, $F_{1.7}$ refers to a pseudo fault corresponding to single fault resolution between $F_1$ and $F_7$. Since the individual $\phi_f$ values for faults $F_{1.7}, F_{1.9}, F_{1.15}$ are 0, these faults will not be able to tolerate any uncertainty in the fault probabilities $f_1$ and/or $f_9$. Increase in $f_1$ will increase the unreliabilities of detection of $F_{1.7}$ and $F_{1.15}$ above −2, and simultaneous increase in both $f_1$ and $f_9$ will increase the unreliability of detection of $F_{1.9}$ beyond −2, thereby increasing the overall system unreliability of detection. Hence, $\phi_f$ which is the minimum meaningful slack is 0 in this case and is reported as such in Table 4. Thus, the minimum cost sensor network is not robust even to slight increases in fault probabilities.

Now consider the sensor network obtained by solving Problem II which seeks to maximize the minimum slack (as a secondary objective), in addition to minimizing system unreliability of detection (as primary objective) and minimizing cost as the ternary objective. Following the philosophy of lexicographic optimization, this requires that the system unreliability of detection be −2. The resulting sensor network $v_3, v_4$ has overall system unreliability of detection −2 and the network cost is 400. As seen from Table 5, the unreliabilities of detection for faults $F_1, F_{1.7}, F_{1.9}, F_{1.15}$ are respectively −8, −5, −8, −5. In the nominal case, $\log_{10} f_1 = -2, \log_{10} f_9 = -2$. Hence, in the worst case, the unreliability of detection of any uncertain fault can only go up by 2 and the individual unreliabilities of detection of the faults $F_1, F_{1.7}, F_{1.9}, F_{1.15}$ (in the worst case) cannot increase beyond −6, −3, −6, −3. Hence, even in the worst case scenario, the system unreliability of detection remains at −2. In this case then, there is no value in trying to reduce the unreliabilities of detection of these faults any further (for example, by adding more sensors). So, it is meaningless to require that the margin of safety available for uncertain faults be greater than 2. However, this does not mean that the slack $\phi_f$ of any particular fault cannot exceed 2. As minimizing cost is the ternary objective, it only ensures that in the quest for a robust sensor network, additional cost is not diverted to increasing $\phi_f$ beyond 2. Further, the value of $\phi_f$ reported in Table 4 is the maximum meaningful slack and is hence 2 rather than 3, even though maximum of the individual $\phi_f$ values is 3.

### Table 4
**Results: uncertainty in faults**

<table>
<thead>
<tr>
<th>Case</th>
<th>$C^*$</th>
<th>Cost used</th>
<th>$U$</th>
<th>$\phi_f$</th>
<th>$N$</th>
<th>Sensors selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>500</td>
<td>100</td>
<td>−2</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>II</td>
<td>500</td>
<td>400</td>
<td>−2</td>
<td>2</td>
<td>2</td>
<td>3,4</td>
</tr>
<tr>
<td>Va</td>
<td>500</td>
<td>400</td>
<td>−2</td>
<td>2</td>
<td>2</td>
<td>3,4</td>
</tr>
<tr>
<td>Vb</td>
<td>500</td>
<td>400</td>
<td>−2</td>
<td>2</td>
<td>2</td>
<td>3,4</td>
</tr>
<tr>
<td>I</td>
<td>3000</td>
<td>100</td>
<td>−2</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>II</td>
<td>3000</td>
<td>400</td>
<td>−2</td>
<td>2</td>
<td>2</td>
<td>3,4</td>
</tr>
<tr>
<td>Va</td>
<td>3000</td>
<td>400</td>
<td>−2</td>
<td>2</td>
<td>2</td>
<td>3,4</td>
</tr>
<tr>
<td>Vb</td>
<td>3000</td>
<td>2550</td>
<td>−2</td>
<td>2</td>
<td>14</td>
<td>1, 2, 3, 4, 13, 42, 43, 44, 45, 46, 47, 48, 49, 50</td>
</tr>
<tr>
<td>I</td>
<td>6000</td>
<td>4700</td>
<td>−3</td>
<td>0</td>
<td>14</td>
<td>3, 4, 5, 8, 9, 13, 42, 43, 45(2), 46, 47(2), 48, 49(2), 50</td>
</tr>
<tr>
<td>II</td>
<td>6000</td>
<td>5100</td>
<td>−2</td>
<td>2</td>
<td>2</td>
<td>3,4</td>
</tr>
<tr>
<td>Va</td>
<td>6000</td>
<td>5100</td>
<td>−2</td>
<td>2</td>
<td>2</td>
<td>3,4</td>
</tr>
<tr>
<td>Vb</td>
<td>6000</td>
<td>5800</td>
<td>−5</td>
<td>2</td>
<td>17</td>
<td>1, 2, 3(2), 4(2), 5, 8, 9, 13, 42, 43, 44, 45(2), 46, 47(2), 48, 49(2), 50</td>
</tr>
</tbody>
</table>

### Table 5
**Results: $\phi$ values for uncertain faults**

<table>
<thead>
<tr>
<th>Case</th>
<th>$C^*$</th>
<th>Fault $F_1$</th>
<th>$\phi^*_f$</th>
<th>Fault $F_{1.7}$</th>
<th>$\phi^*_f$</th>
<th>Fault $F_{1.9}$</th>
<th>$\phi^*_f$</th>
<th>Fault $F_{1.15}$</th>
<th>$\phi^*_f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>500</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>II</td>
<td>500</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Va</td>
<td>500</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Vb</td>
<td>500</td>
<td>9</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>I</td>
<td>3000</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>II</td>
<td>3000</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Va</td>
<td>3000</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Vb</td>
<td>3000</td>
<td>41</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>I</td>
<td>6000</td>
<td>45</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>12</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>II</td>
<td>6000</td>
<td>51</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>18</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Va</td>
<td>6000</td>
<td>51</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>18</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Vb</td>
<td>6000</td>
<td>59</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>18</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>
Comparing the results obtained by solving Problem Va (where we prioritize cost over distribution) with these results (Problem II), we find no change in the sensor network. However, when we emphasize distribution over cost (Problem Vb), a more distributed sensor network measuring variables v2, v3, v4 is chosen and the cost of this sensor network is 500.

The results for \( C^* = 3000 \) are identical to those obtained for \( C^* = 500 \) for Problems I, II and Va. However, the sensor network obtained by solving Problem Vb is more distributed measuring 14 different variables \( v_1 - v_4, v_{13}, v_{42} - v_{50} \). As mentioned in the previous section, this occurs since the available cost is used up in measuring additional variables and the overall network cost is 2550 as compared to 100, 400 and 400 for networks obtained by solving Problems I, II and Va, respectively. Thus, in this case a distributed sensor network is achieved at the expense of spending significant resources (cost) and this trade-off may be questionable.

When available cost \( C^* \) is increased, as expected, it is possible to include more sensors in the sensor network and the overall system unreliability of detection decreases. In all the cases, the sensor networks obtained by solving Problem I are not robust to (even slight) variations in fault probabilities as seen from the values of \( \phi_f \) which are all 0. However, requiring that the sensor networks be robust ensures that in all the cases, even in the worst case scenario, the system unreliability of detection does not change from the nominal system unreliability of detection. It is important to note that robustness is achieved by including more sensors, but the additional cost is not substantial and the trade-off is very significant. For instance, when \( C^* = 6000 \), the baseline sensor network costs 4700, while the robust sensor network costs 5100.

Robustness to model uncertainties was implicitly assumed by requiring a distributed sensor network, all other objectives (unreliability of detection, robustness to uncertain probability data) being satisfied. Requiring that the sensor network be distributed in order to ensure robustness to modeling errors is a heuristic requirement. Hence, a simple numerical experiment was performed to determine if a distributed sensor network was indeed more robust to modeling errors than a non-distributed one. Two sensor networks obtained by solving Formulations Va and Vb, respectively in Table 4 for \( C^* = 6000 \) were chosen for comparison:

\[
S_1 = \{v_3(2), v_4(2), v_5, v_8, v_9, v_{13}, v_{42}, v_{43}, v_{45}(2), v_{46}, v_{47}(2), v_{48}, v_{49}(2), v_{50}\}
\]

\[
S_2 = \{v_1, v_2, v_3(2), v_4(2), v_5, v_8, v_9, v_{13}, v_{42}, v_{43}, v_{44}, v_{45}(2), v_{46}, v_{47}(2), v_{48}, v_{49}(2), v_{50}\}
\]

In order to simulate a scenario where modeling is uncertain, it was assumed that some randomly chosen unambiguous quantities in the entries in the original cause effect matrix are not known accurately. Denoting \( A_i \) as the set of variables affected by fault \( i \), randomly chosen \( + \) or \( - \) entries in \( A_i \) were modified to \( \pm \). This was done simultaneously for randomly chosen faults. After these modifications, the fault-variable bipartite matrix \( B \) corresponding to single fault resolution was again generated. The system unreliability of detection for this new scenario was determined for both sensor networks. Clearly, it is possible that the overall system unreliability of detection in the new scenario is different (higher) than the original system unreliability of detection, \( -\). This process was repeated for 1000 realizations. The total number of times the system unreliability of detection increased above the nominal \( -5 \) for both networks was computed. It was seen that for the distributed network \( S_2 \), the fraction of times the new system unreliability of detection increases was 7% as against 25% for the non-distributed sensor network \( S_1 \). This provides a justification for requiring that the sensor network be distributed. It should be noted that while we required the sensor network to be distributed, no additional information about the network or the uncertainty was assumed.

### 4.2. Inaccurate sensors scenario

For the case where sensor failure probabilities \( s_3 \) and \( s_4 \) are not accurately known, we arrive at similar conclusions (Tables 6 and 7) as above. However, the value of \( \phi_s \), the minimum slack in the unreliability of detection of inaccurate faults, needs to be interpreted carefully. Consider the case when \( C^* = 500 \) in Table 6. The sensor network obtained by solving Problem I which is the minimum cost network for \( U = -2 \) is \( v_5 \). The system unreliability of detection is \(-2\) and the unreliabilities of

<table>
<thead>
<tr>
<th>Case</th>
<th>( C^* )</th>
<th>Cost used</th>
<th>( U )</th>
<th>( \phi_s )</th>
<th>( N )</th>
<th>Sensors selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>500</td>
<td>100</td>
<td>-2</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>III</td>
<td>500</td>
<td>100</td>
<td>-2</td>
<td>18</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Va</td>
<td>500</td>
<td>100</td>
<td>-2</td>
<td>18</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Vb</td>
<td>500</td>
<td>500</td>
<td>-2</td>
<td>18</td>
<td>5</td>
<td>1, 2, 3, 48, 50</td>
</tr>
<tr>
<td>I</td>
<td>3000</td>
<td>100</td>
<td>-2</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>III</td>
<td>3000</td>
<td>100</td>
<td>-2</td>
<td>120</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Va</td>
<td>3000</td>
<td>100</td>
<td>-2</td>
<td>120</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Vb</td>
<td>3000</td>
<td>2550</td>
<td>-2</td>
<td>120</td>
<td>14</td>
<td>1, 2, 3, 4, 13, 42, 43, 44, 45, 46, 47, 48, 49, 50</td>
</tr>
<tr>
<td>I</td>
<td>6000</td>
<td>4700</td>
<td>-5</td>
<td>0</td>
<td>14</td>
<td>3, 4, 5, 8, 9, 13, 42, 43, 45(2), 46, 47(2), 48, 49(2), 50</td>
</tr>
<tr>
<td>III</td>
<td>6000</td>
<td>5900</td>
<td>-5</td>
<td>9</td>
<td>14</td>
<td>3(4), 4(4), 5, 8, 9, 13, 42, 43, 45(2), 46, 47(2), 48, 49(2), 50</td>
</tr>
<tr>
<td>Va</td>
<td>6000</td>
<td>5900</td>
<td>-5</td>
<td>9</td>
<td>14</td>
<td>3(4), 4(4), 5, 8, 9, 13, 42, 43, 45(2), 46, 47(2), 48, 49(2), 50</td>
</tr>
<tr>
<td>Vb</td>
<td>6000</td>
<td>6000</td>
<td>-5</td>
<td>9</td>
<td>15</td>
<td>1, 3(4), 4(4), 5, 8, 9, 13, 42, 43, 45(2), 46, 47(2), 48, 49(2), 50</td>
</tr>
</tbody>
</table>
detection of inaccurate faults $F_{1,15}$, $F_{15,29}$, $F_{15,30}$ are $-4$, $-5$ and $-2$, respectively. $v_3$ is measured by an inaccurate sensor, and if its failure probability $\phi_s$ were to increase, the unreliabilities of detection of $F_{1,15}$ and $F_{15,29}$ would increase as these faults affect $v_3$. An increase in $\phi_s$ however, does not affect unreliability of detection of $F_{15,30}$ since it does not affect $v_3$. If probability of failure $\phi_s$ were to increase to 0.1 (increase of 2 from its nominal value on the log10 scale), the unreliability of detection of $F_{1,15}$ would increase to $-2$, which is the overall system unreliability of detection. If $\phi_s$ were to increase above 0.1, the fault unreliability of detection would increase above the nominal unreliability of detection. The unreliability of detection of $F_{15,29}$ in the worst case does not increase beyond $-2$. Thus, in the worst case, the system unreliability of detection increases to $-1$. The value of $\phi_s$ is thus the least of all relevant $\phi_s$ and is 2 in this case.

The sensor network obtained by solving Problem III consists of measuring $v_3$ alone. The network cost is the same, but it is more robust compared to measuring $v_3$. This is immediately clear since the probability of failure $f_1$ is accurately known and any changes in probability of failure $s_3$ (or $s_4$) in no way affect system unreliability of detection. Hence, the maximum relevant slacks, $\phi_s^*\setminus s$ are 0 for all inaccurate faults. However, in the optimization formulation, the only binding constraint on $\phi_s$ is that $\phi_s \leq \phi_s^* = 18$ and since $\phi_s$ is maximized, a value of $\phi_s = 18$ is reported in Table 6. Hence, it must not be concluded that the margin of safety is 18, but rather the system is totally robust to changes in sensor failure probability $s_3$ and $s_4$. As in the inaccurate faults scenario, solving Problem Vb results in a sensor network that is robust and highly distributed, the distribution being achieved by using all the available cost.

When $C^* = 6000$, the overall system unreliability of detection is $-5$. The minimum cost sensor network is clearly seen to be not robust to inaccuracy in failure probabilities $s_3$ or $s_4$. Any increase in $s_3$ or $s_4$ would increase the unreliabilities of detection of faults $F_{15,29}$ and $F_{15,30}$, respectively above their nominal levels, viz., $-5$ and $-5$ and thus increase the system unreliability of detection. However, the other sensor networks obtained by solving Problems III, Va and Vb are sufficiently robust to uncertainties which is seen from the higher values of $\phi_s$ and $\phi_s^*$. Again, solving Problem Vb, which emphasizes distribution over cost, results in a more distributed sensor network. Similar conclusions can be drawn by analyzing results for $C^* = 3000$.

### 4.3. Inaccurate faults and sensors scenarios

The results obtained for the scenario where there is uncertainty in the fault probabilities $f_1$ and $f_2$, as well as sensor failure probabilities $s_3$ and $s_4$ are tabulated in Tables 8 and 9. For $C^* = 500$, solving the robust Formulation (IV) gives rise to a sensor network that involves the inaccurate sensors also, unlike the scenario involving only inaccurate sensors. When $C^* = 3000$, unlike the earlier scenarios, the available cost is used to the extent of 2800 in order to ensure robustness to uncertainty in both fault and sensor failure probabilities. The results for higher $C^*$ are similar in spirit to the earlier results.

Thus, in conclusion, solving the minimum cost problem (Problem I) does not guarantee robustness to uncertainties in fault and sensor failure probabilities. In many cases it was seen that even a slight increase in fault occurrence or sensor failure probability would increase overall system unreliability of detection over the nominal levels. Incorporating robustness explicitly in the formulations resulted in networks that were highly robust to these uncertainties. In all the three scenarios, prioritizing cost over distribution (Problem Va) does not lead to any improvement. However, this is problem specific and in other instances

<table>
<thead>
<tr>
<th>Case</th>
<th>$C^*$</th>
<th>Cost used</th>
<th>$U$</th>
<th>$\phi_f^*$</th>
<th>$N$</th>
<th>Sensors selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>500</td>
<td>100</td>
<td>$-2$</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>IV</td>
<td>500</td>
<td>400</td>
<td>$-2$</td>
<td>3</td>
<td>2</td>
<td>3, 4</td>
</tr>
<tr>
<td>Va</td>
<td>500</td>
<td>400</td>
<td>$-2$</td>
<td>3</td>
<td>2</td>
<td>3, 4</td>
</tr>
<tr>
<td>Vb</td>
<td>500</td>
<td>500</td>
<td>$-2$</td>
<td>3</td>
<td>3</td>
<td>1, 3, 4</td>
</tr>
<tr>
<td>I</td>
<td>3000</td>
<td>100</td>
<td>$-2$</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>IV</td>
<td>3000</td>
<td>2800</td>
<td>$-2$</td>
<td>21</td>
<td>2</td>
<td>3(7), 4(7)</td>
</tr>
<tr>
<td>Va</td>
<td>3000</td>
<td>2800</td>
<td>$-2$</td>
<td>21</td>
<td>2</td>
<td>3(7), 4(7)</td>
</tr>
<tr>
<td>Vb</td>
<td>3000</td>
<td>3000</td>
<td>$-2$</td>
<td>21</td>
<td>4</td>
<td>1, 2, 3(7), 4(7)</td>
</tr>
<tr>
<td>I</td>
<td>6000</td>
<td>4700</td>
<td>$-5$</td>
<td>0</td>
<td>14</td>
<td>3, 4, 5, 8, 9, 13, 42, 43, 45(2), 46, 47(2), 48, 49(2), 50</td>
</tr>
<tr>
<td>IV</td>
<td>6000</td>
<td>5900</td>
<td>$-5$</td>
<td>9</td>
<td>14</td>
<td>3(4), 4(4), 5, 8, 9, 13, 42, 43, 45(2), 46, 47(2), 48, 49(2), 50</td>
</tr>
<tr>
<td>Va</td>
<td>6000</td>
<td>5900</td>
<td>$-5$</td>
<td>9</td>
<td>14</td>
<td>3(4), 4(4), 5, 8, 9, 13, 42, 43, 45(2), 46, 47(2), 48, 49(2), 50</td>
</tr>
<tr>
<td>Vb</td>
<td>6000</td>
<td>6000</td>
<td>$-5$</td>
<td>9</td>
<td>15</td>
<td>1, 3(4), 4(4), 5, 8, 9, 13, 42, 43, 45(2), 46, 47(2), 48, 49(2), 50</td>
</tr>
</tbody>
</table>
optimization under uncertainty. In literature (Diwekar, 2003),
nosis. The design problem is actually a problem of performing
has been used to design sensor networks for robust fault diag-
5. Discussions
it may be possible to obtain a more distributed network for the
same cost. Further, if we are ready to prioritize distribution over
cost (Problem Vb), then we get sensor networks where more
variables are measured. This is clearly done by using additional
available cost, thereby compromising on cost saving. This some-
times leads to scenarios where almost all the available cost is
used to achieve distribution. In a multi-objective optimization
problem, analysis of the trade-offs is often subjective and the
final choice is left to the decision maker. However, it must be
pointed out that unless such a multi-objective optimization prob-
lem is solved explicitly, the trade-offs are not at all apparent
to the decision maker. For instance, if we were to solve for mini-
um reliability of detection alone, the other solutions would
never have been uncovered.

5. Discussions

In this article, a lexicographic optimization based approach
has been used to design sensor networks for robust fault diag-
nosis. The design problem is actually a problem of performing
optimization under uncertainty. In literature (Diwekar, 2003),
generally two approaches have been used to perform optimization
under uncertainty: wait and see, and here and now. Wait and
see approach involves solving deterministic optimization prob-
lems for several random values of the uncertain variables and
then combining the results from these individual problems to
obtain a probabilistic representation of the outcome. In contrast
to this approach, the here and now approach requires solving
only one deterministic optimization problem, with the require-
ment that the objective function and constraints be expressed
in terms of some probabilistic representation (such as mean,
variance, etc.). Chance constraint programming is a type of
here and now approach which involves rewriting a constraint
involving uncertain variables in terms of probability of constraint
satisfaction. The approach followed in this article is similar in
philosophy to the here and now approach. However, the uncer-
tainty of parameters is incorporated by an additional objective
function and not by specifying any probability of constraint sat-
satisfaction. The approach is based on the notion of lexicographic
optimization. This is a different, novel approach for dealing with
uncertainty in the data. An important feature to note is that no
assumptions regarding distributions of the uncertain parameters
need to be made in this approach. The chance constraint pro-
gramming approach on the other hand requires the distribution
of the uncertain parameters to be known, stable distributions
(Diwekar, 2003).

Another interesting feature of the sensor network designs
resulting from solving the formulations proposed in this work
is that the robustness is achieved without compromising on the
performance for the nominal scenario. This is possible since
for the type of primary objective function considered for sensor
network design (for characterizing performance for the nomi-
mental parameter values), the formulation invariably has multiple
solutions. The approach for incorporating robustness is to then
select, from amongst these multiple solutions, a solution that
is most insensitive (or robust) to the uncertain parameters. A
drawback of the approach is however, that the selected design
is not necessarily optimal if the values of the uncertain param-
ters change. Still, the designer is guaranteed performance at
the same level, which was achieved with the nominal param-
eter values, provided the change in the uncertain parameters is
within the ranges as given by the respective slacks. Also, the
approach is only concerned with worst case scenarios. Hence,
for cases where the parameter (the probabilities) values actually
decrease, a better sensor network design may be possible, but this
is not considered here. Basically, the idea is to promise a perfor-
mance level to the process engineer and ensure that irrespective
of changes in the uncertain data, that performance is achieved as
far as possible. The idea of incorporating network distribution
in the objective function is another novel, though coarse way of
handling model uncertainty. Again, no assumptions regarding
the type of model uncertainty have been made.

6. Conclusions

An optimization based approach for designing sensor net-
works for robust fault diagnosis has been presented in this article.
We believe that this approach is a novel way of handling uncer-
tainty in the data. The concept of lexicographic optimization has been used for this approach. Uncertainty to some fault occurrence and sensor failure probabilities, and model-plant mismatch were considered. The basic idea for handling uncertainties in the data is to select solutions for which the constraints involving uncertain data are not active at the optimal solution; this is achieved by defining and maximizing appropriate slacks in the relevant constraints. Robustness to model-plant mismatch is incorporated by selecting distributed networks. The application of the proposed approach was demonstrated on the Tennessee Eastman challenge problem. This approach can be a tool in the sensor network designer’s repertoire for generating designs, for performing efficient fault detection and diagnosis, which are highly robust to uncertain data and process model.

Several other issues need further investigation. Specifically, alternate formulations can be developed to address the way unreliability detection has been incorporated at the individual fault and system levels. From the viewpoint of fault diagnosis, an alternate approach is to incorporate the final diagnostic system as part of the initial design process. There are other approaches to integrate the design and decision problems using game theory ideas. Sensor network designs based on these various approaches can also be benchmarked using large stochastic simulations. These issues need further investigation as part of future work in this area.

Appendix A. Robustness with respect to log of unreliability of detection

In this section, we prove that maximizing robustness in unreliability of detection values on log scale is equivalent to maximizing robustness in the original unreliability of detection values.

The unreliability of detection minimization formulation without log transformation is:

A.1. Formulation A

Base formulation

\[
\begin{align*}
\min U \\
U &\geq U_i; \quad \forall i \in I
\end{align*}
\]

where cost constraint and non-negative integer domain for the decision variables is not explicitly listed for the sake of brevity. Let the resulting optimal objective be \(U^*\).

To consider robustness, it can be seen (from definition of \(U_i\) in Eq. (1)) that the uncertainties in fault occurrence and sensor failure probabilities are transferred in a nonlinear way to the unreliability of detection as:

\[
U_i' = (f_i + \Delta f_i) \prod_{j=1}^{n} (s_j + \Delta s_j)^{(b_j/s_j)}
\]

where \(U_i'\) is the new unreliability of detection of fault \(i\), \(\Delta f_i\) and \(\Delta s_j\) are the uncertainties in the \(i\)th fault occurrence and \(j\)th sensor failure probability. Treating the uncertainty in unreliability of detection directly is difficult (in terms of formulating it as suitable optimization problem), hence we approximate unreliability of detection in presence of uncertainty to be of either of the following two forms:

- multiplicative uncertainty
  \[
  U_i' \simeq U_i \times \Delta U_i^m
  \]
- additive uncertainty
  \[
  U_i' \simeq U_i + \Delta U_i^a
  \]

where \(\Delta U_i^m\) and \(\Delta U_i^a\) are multiplicative and additive uncertainties, having different values. Infact, \(\Delta U_i^m \geq 1\) while \(1 \geq \Delta U_i^a \geq 0\), since for positive \(\Delta f_i\) and \(\Delta s_j\), \(U_i'\) should be higher than \(U_i\).

Ensuring a robust design means that the system unreliability of detection \(U\) is governed by the nominal values \(U_i\) and does not change, even though the true fault unreliabilities of detection may change to \(U_i'\) (which is higher than \(U_i\)); the factor \(\Delta U_i\) acts as a buffer in ensuring this.

It is easy to notice that if the uncertainty is considered to be multiplicative, then the slacks \(\phi_i\) as considered in this article are directly equal to \(\log \Delta U_i^m\), and hence maximizing the minimum \(\phi_i\) is the same as maximizing the minimum \(\Delta U_i^m\). We now further show that maximizing robustness in the unreliability of detection on log scale (\(\log U_i\)) is equivalent to maximizing \(\Delta U_i^m\) as well. For this, consider the following robust formulation:

A.2. Formulation B

Robust formulation

\[
\begin{align*}
\max \left\{ \min_{i \in (I_f \cup I_s)} \Delta U_i^a \right\} \\
U = U_i + \Delta U_i^a; \quad \forall i \in (I_f \cup I_s) \\
U \geq U_k; \quad \forall k \in I \setminus (I_f \cup I_s) \\
U = U^*
\end{align*}
\]

Now, consider the robust formulation (B) in the log scale (as we have done in this article):

A.3. Formulation B’

Robust formulation in log scale

\[
\begin{align*}
\max \left\{ \min_{i \in (I_f \cup I_s)} \phi_i \right\} \\
\log U = \log U_i + \phi_i; \quad \forall i \in (I_f \cup I_s) \\
\log U \geq \log U_k; \quad \forall k \in I \setminus (I_f \cup I_s) \\
\log U = \log U^*
\end{align*}
\]

The following theorem now proves the equivalence.

Theorem. Solution (in terms of decision variables) of Formulations B and B’ are the same.
Proof. : For two inaccurate faults $i_1$ and $i_2$, consider a situation where $\Delta U_{i_1}^U \geq \Delta U_{i_2}^U$, or in other words (from Formulation B)

$$U - U_{i_1} \geq U - U_{i_2}$$  \hspace{1cm} (A.14)

which after some straightforward algebraic manipulation can be written as

$$\log U - \log U_{i_1} \leq \log U - \log U_{i_2}$$  \hspace{1cm} (A.15)

or as (Formulation B'),

$$\phi_{i_1} \geq \phi_{i_2}$$  \hspace{1cm} (A.16)

Hence, $\Delta U_{i_1}^U \geq \Delta U_{i_2}^U \Rightarrow \phi_{i_1} \geq \phi_{i_2}$. The implication in reverse can also be easily shown in a similar fashion. In other words, solving Formulation B' is same as solving Formulation B. □

Appendix B. Values for weighting coefficients for various formulations

In the text, the values for weighting coefficients ($\lambda_i$, $\beta_i$, $\beta'_i$, and $\alpha_i$) are given. These have been obtained by applying Algorithm 2 of Sherali’s (1982) article for the case when objective functions: $U, \phi_1, \phi_2, \phi_{i_1}, x_k$ take integer values. For the sake of completeness, this application for Problems II–IV is presented below. For other problems, the ideas simply carry-over.

The problem as posed in Sherali’s article is (for three objective functions):

$$\max \{x_1 c_1 + x_2 c_2 + x_3 c_3\} x$$  \hspace{1cm} (B.1)

subject to other problem constraints. Here $c_1$, $c_2$, $c_3$ are the cost coefficients of the three objective functions, respectively and $x$ are the decision variables. $c_1$ corresponds to highest priority and $c_3$ corresponds to lowest priority. $\lambda_1$ and $\lambda_2$ are weights (constants) to be determined. Our problem is a minimization problem. The algorithm presented by Sherali works for minimization problems as well. The objective function for Problems II, III, or IV in this article is:

$$\min \{\lambda_1 U - \lambda_2 \phi - x_k\}$$  \hspace{1cm} (B.2)

where $\phi$ is replaced by $\phi_1, \phi_2$, or $\phi_{i_1}$ depending on the scenario considered.

Applying Algorithm 2 of Sherali, we get:

$$\lambda_2 = 1 + UB(-x_k)$$  \hspace{1cm} (B.3)

where $UB(-x_k)$ is the maximum difference in the value of $-x_k$ for all feasible solutions of the problem. Since, the maximum value of slack obtained in the cost constraint can be the total available cost ($C^*$) and the minimum value can be zero, $UB(-x_k) = 0 - (-C^*) = C^*$. Therefore, $\lambda_2 = 1 + C^*$. Now, $\lambda_1$ can be calculated as:

$$\lambda_1 = 1 + UB(-x_k - \lambda_2 \phi)$$  \hspace{1cm} (B.4)

Now, $UB(-x_k - \lambda_2 \phi)$ can be calculated as,

$$UB(-x_k - \lambda_2 \phi) = [0 - (1 + C^*)0] - [-C^* - (1 + C^*)M]$$  \hspace{1cm} (B.5)

since the maximum and minimum values of $\phi$ can be $M$ and 0, respectively, where depending upon the scenario, the appropriate value of $M$ (as listed in Eq. (63)) has to be used. Then, $\lambda_1$ is given as:

$$\lambda_1 = (1 + C^*)(1 + M)$$  \hspace{1cm} (B.6)

and the overall objective function to be minimized is:

$$\min \{(1 + C^*)(1 + M)U - (1 + C^*)\phi - x_k\}$$  \hspace{1cm} (B.7)

Similar procedures can be applied to derive values for weighting coefficients for the other formulations presented in this work.

The algorithm of Sherali used above requires the objective functions to be integer valued. This may not be the case in general. For the problems addressed in this article, the following modification can be made (Bhushan & Rengaswamy, 2002a): It is reasonable to assume that each data used in the problem (log of probabilities, sensor costs, total available cost, etc.) is a rational number ($\pm p/q$ where $p$ and $q$ are integers). Then calculate the LCM of all these denominator integers ($q$ values) and let this LCM be $a$. Now, if the problem (objective function and constraints) is multiplied by $a$ throughout, it is easy to see that the modified objective functions

$$U' = aU, \quad \phi' = a\phi, \quad x_k' = ax_k, \quad N' =aN$$  \hspace{1cm} (B.8)

will take only integer values. Now following Algorithm 2 of Sherali (1982) as presented above, the values for weighting coefficients can be calculated easily.

In the Tennessee Eastman case study presented in this article, the data used was such that all the objectives were integer valued.

Appendix C. Values of maximum meaningful slacks for uncertain data

Procedures for calculation of values of maximum meaningful slacks for uncertain data in Formulations II, III and IV are considered in this section.

C.1. Uncertainties in only fault occurrence probabilities (Problem II)

The maximum meaningful slack $\phi_f^\star$ for this case is given as

$$\phi_f^\star = \max_{i \in f} \phi_i^\star$$  \hspace{1cm} (C.1)

where calculation of $\phi_i^\star$ depends on the type of fault and is discussed next. In the following discussion, the nominal probability of the uncertain fault $k$ is denoted by $f_k$.

- Fault $k$ is uncertain and is an actual fault in the process. Then in the worst case, its true occurrence probability can tend towards 1 ($=10^0$), and hence the maximum meaningful slack for this fault is given as:

$$\phi_f^\star = \log(1) - \log(f_k) = -\log(f_k)$$  \hspace{1cm} (C.2)

- Fault $k$ is a pseudo-fault corresponding to single fault resolution of original faults $i$ and $j$, i.e. the set of variables affected by fault $k$ corresponds to being able to resolve between faults
\( i \) and \( j \). If the nominal probabilities of occurrences of faults \( i \) and \( j \) are given as \( f_i \) and \( f_j \), respectively, then the fault occurrence probability of fault \( k \) is calculated as: 
\[ f_k = \min(f_i, f_j) \] 
(Bhushan & Rengaswamy, 2002a). Now consider the following two situations:

(1) Fault \( i \) is uncertain and fault \( j \) is certain with

(a) \( f_i \geq f_j \). Hence, \( f_k = \min(f_i, f_j) = f_j \). For this case, even if the true value of \( f_i \) is higher than that considered in the formulation, it does not affect \( f_k \). Hence, no slack is required for the fault \( k \), or if a slack is considered, its maximum meaningful value \( \phi^*_{f_k} = 0 \).

(b) \( f_i < f_j \). Here \( f_k = \min(f_i, f_j) = f_i \). Hence, if the true value of \( f_i \) is higher than its nominal value then the true value of \( f_k \) would also be higher. But once \( f_i > f_j \), then \( f_k = \min(f_i, f_j) = f_j \), in other words, \( f_k \) cannot be higher than \( f_j \) irrespective of the value of \( f_i \). Hence, the maximum meaningful slack for fault \( k \) is
\[ \phi^*_{f_k} = \log(f_i) - \log(f_j). \]  

(2) Both the original faults \( i \) and \( j \) are uncertain. Then the nominal occurrence probability of fault \( k \) is \( f_k = \min(f_i, f_j) \) which is equal to \( f_i \) or \( f_j \) depending on whichever is lower. However, since both the values of \( f_i \) and \( f_j \) are uncertain, in the worst case, both these values can tend towards one, and hence, the maximum meaningful slack for fault \( k \) is
\[ \phi^*_{f_k} = \log(1) - \min(\log(f_i), \log(f_j)) = -\min(\log(f_i), \log(f_j)) \]  

(C.3)

C.2. Uncertainties in only sensor failure probabilities (Problem III)

The maximum meaningful slack \( \phi^*_s \) for this case is given as
\[ \phi^*_s = \max_{i \in I_s} \left\{ -\sum_{j \in J} B_{ij}(\log s_j)x^*_j \right\} \]  

(C.4)

where \( x^*_j = \lfloor c^*_j \rfloor \) is the maximum number of sensors which can be selected to measure variable \( j \), and is given as:
\[ x^*_j = \lfloor \frac{c^*_j}{\epsilon} \rfloor \]  

(C.5)

where \( |a| \) (where \( a \) is any number) indicates rounding off \( a \) to the nearest integer not higher than \( a \). The calculation of \( \phi^*_s \) is different from that of \( \phi^*_f \). While for the fault uncertainty case, the upper limits on the maximum slack required in each uncertain fault unreliability of detection constraint can be calculated based on the given data (the values of the decision variables \( x \) are not required), for the sensor uncertainty case, the upper limits on the maximum slack \( \phi^*_s \) required in each inaccurate fault unreliability of detection constraint depends on the values of the decision variables and are given as in Eq. (32):
\[ \phi^*_s = -\sum_{j \in J} B_{ij}(\log s_j)x_j, \quad \forall i \in I_s \]  

(C.6)

To understand the above equation, consider a fault \( i \) which affects an uncertain sensor used to measure variable \( j \) with nominal failure probability of \( 10^{-2} \). Also, as a solution to the unreliability of detection maximization problem (the primary objective), let us suppose that three sensors are used to measure variable \( j \). Then, the contribution to \( \log U_i \) of sensors on variable \( j \) is \( x_j \times \log(10^{-2}) = 3 \times (-2) = -6 \). Now, in the worst case, the true failure probability of sensor on variable \( j \) can tend towards \( 1 = 10^0 \). Hence, in the worst case, the contribution of sensors on variable \( j \) to \( \log U_i \) is \( x_j \times \log(10^0) = 0 \). In other words, the difference for the nominal and the worst case is \( 0 - (-6) = 6 \), i.e. the maximum meaningful slack for this fault is 6, as given by the above expression.

Based on Eq. (C.6), it appears that the value for \( \phi^*_s \) can be calculated as
\[ \phi^*_s = \max_{i \in I_s} (\phi^*_{f_{si}}) \]  

(C.7)

However, incorporation of above constraint in Formulation III will not only make the problem nonlinear, it can also lead to different (sub-optimal) solutions as it may result in selection of more uncertain sensors since this increases \( \phi^*_s \), thereby increasing the value of \( \phi^*_n \) which is maximized in the objective function. To avoid this problem we incorporate constraint C.4 to calculate the value of \( \phi^*_s \), since this value does not depend on the decision variables. It should be noted that even though this procedure leads to a loose upper bound on \( \phi^*_s \), it does not change the solution (in terms of the decision variables) of Problem III. However, the resulting \( \phi^*_s \) value has to be properly interpreted (as illustrated in the case study).

C.3. Uncertainties in both fault occurrence and sensor failure probabilities (Problem IV)

The maximum meaningful slack \( \phi^*_{f_{isi}} \) for this case is given as
\[ \phi^*_{f_{isi}} = \max_{i \in I_f \setminus I_s} \left\{ \max_{i \in I_f \setminus I_s} \left( \phi^*_{fi}, \phi^*_{fi} \right), \max_{i \in I_f \setminus I_s} \left( -\sum_{j \in J} B_{ij}(\log s_j)x^*_j \right) \right\} \]  

(C.8)

The value of maximum meaningful slack \( \phi^*_{f_{isi}} \) for fault \( i \) is in general given as:
\[ \phi^*_{f_{isi}} = \phi^*_{fi} + \phi^*_{si} \]  

(C.9)

where \( \phi^*_{fi} \) is the contribution from the uncertainty due to fault occurrence probability (it is 0 if fault is certain), and \( \phi^*_{si} \) is the contribution from uncertain sensors affected by that fault (it is 0 if fault \( i \) does not affect any uncertain sensor). Depending on the fault (original fault or pseudo fault corresponding to single fault resolution between original faults), the appropriate equation from Section C.1 is used for \( \phi^*_{fi} \) calculation, while \( \phi^*_{si} \) is as given in Eq. (C.6).

Note that depending on the actual problem at hand, it may be possible to calculate tighter (smaller) bounds for the maximum meaningful slacks for various formulations as compared
to those calculated here. However, this is not attempted in the case studies presented in this article. The value of these slacks affects the values of weighting coefficients in the lexicographic objective function. Getting a tighter bounds on maximum meaningful slacks will not affect the optimality of the solution, though they may have an effect on computational efficiency (time taken by a given solver to solve the problem) since the weighting coefficients will be different. This remains an open issue which requires further research to be resolved.

Appendix D. Calculation of \( N^* \)

An upper bound on the value of maximum network distribution \( N^* \) is \( n \), the number of measurable variables in the process. While this value can be used, this may result in larger values for the weighting coefficients for problems where network distribution is being maximized (such as Problems Va and Vb). A much tighter (smaller) value for \( N^* \) can be obtained by performing a simple greedy search procedure as follows:

Arrange all the variables in increasing order of sensor cost. Let the variable indices in this order be given by a vector \( Inc \). Initially, the cost used in selecting the sensors is 0. Now, keep selecting one variable in increasing order from the index vector \( Inc \) and keep adding the corresponding sensor cost to cost used. Continue this procedure till either cost used is greater than available cost \( C^* \), or if all variables from \( Inc \) have been selected. In the former case, the number of variables selected is the value of \( N^* \), while in the latter case, \( N^* = n \).

Appendix E. Redundant constraint removal for the optimization problems

The basic idea in (Blushan & Rengaswamy, 2002a) was to remove a fault, say: \( F_k \), from consideration in the optimization formulation if it could be established that, irrespective of the chosen sensor location, the unreliability of detection of \( F_k \) will always be less than or equal to that of some other fault. Since the optimization is based on minimizing the maximum unreliability of detection, the unreliability of detection constraint \( (U \geq \log U_k) \) corresponding to this fault will either be inactive (at the optimal solution), or will be an exact repetition of some other constraint. With some modifications, this idea is applicable even when some fault probabilities are uncertain, and is implemented in this article. The guiding principle in the redundant constraint removal procedure is to remove constraints while making sure that the feasible region is not altered.

References