14th International Conference on Structural Safety and Reliability - ICOSSAR'25
1-6 June, 2025 - Los Angeles California, USA
R. Ghanem, E. Johnson, S. Masri and A. Olivier (Eds)

INFLUENCE OF ATTACKER'S PRIOR KNOWLEDGE ON THE PERFORMANCE OF REDUNDANT SYSTEMS

LEANDRO IANNACONE[1] AND ALEX SIXIE CAO[2,3]

[1] Division of Structural Engineering, Lund University
Klas Anshelms väg 14, 223 63, Lund, Sweden
iannacone.leandro@kstr.lth.se

[2] Empa, Swiss Federal Laboratories for Materials Science and Technology
Überlandstrasse 129, 8600, Dübendorf, Switzerland
alex.cao@empa.ch

[3] Institute of Structural Engineering, ETH Zürich
Stefano-Franscini-Platz 5, 8093, Zürich, Switzerland
cao@ibk.baug.ethz.ch

Key words: Robustness, Redundancy, Reliability, Attack Strategy, Prior Knowledge

Abstract. The main objectives of civil engineering structures are to provide functional spaces for societal activities and shelter from the environment. To ensure the safety of such structures, design standards employ methods derived from structural reliability to achieve a target safety level throughout the operational life of structures for expected loading. However, disruptions may occur to a system that involve the initial damage to one or more components. To manage the consequences of system disruptions, robustness strategies can be used to enhance the robustness of a system. Previous research has shown that targeted risk-reducing measures are the most efficient. Therefore, knowledge on the system disruptions is crucial for informing decision-making on appropriate counter-measures. In this paper, initial damage scenarios to redundant systems with a mix of brittle and ductile components are investigated and the effect of prior knowledge of an attacker are quantified using probabilistic and combinatorial analysis. The results are presented in β–π diagrams, which compare the reliability and robustness of systems in a visual medium. The results show that for the same component reliabilities, brittle systems are less robust than ductile systems. In mixed systems, the initial damage that leads to the lowest robustness is not always the loss of only ductile components, but often a combination of damage to ductile and brittle components. In a deliberate attack on a system, there is a large reduction in the robustness and reliability, depending on the prior knowledge of the attacker and the severity of the attack. This analysis shows the importance of considering the prior knowledge of an attacker on the system performance, and facilitates the development of targeted counter-measures and design strategies.

1 INTRODUCTION

1.1 Background

Ensuring the safety, functionality, and resilience of civil engineering structures throughout their operational life is a fundamental objective. It requires a good understanding and quantification of key system properties, such as the reliability and robustness. Reliability ensures adequate system performance during its operational lifetime for expected loading, and is quantified using the system reliability index $\beta_{\text{sys}} = -\Phi^{-1}[\mathrm{P}(F_{\text{sys}})]$, where $\mathrm{P}(F_{\text{sys}})$ is the probability of system failure and $\Phi^{-1}[\cdot]$ is the inverse cumulative distribution function of the standard normal distribution. Robustness can be defined as the ability of a system to maintain functionality given system disruptions or perturbations, where the function is the preservation of life safety for the users. The properties of reliability and robustness complement each other, where: (i) reliability manages failure under expected operational conditions; (ii) robustness manages failures in case of unexpected system disruptions.

The system reliability β_{sys} depends on the components and system configuration [1]. In general, ductile components enable load redistribution, thereby mobilizing redundant capacity and increasing β_{sys} [2]. Conversely, brittle components fail suddenly and preclude the mobilization of load redistribution mechanisms, leading to a lower β_{sys} [2]. Increasing robustness constitutes an effective strategy for improving system reliability. An enhanced robustness can be achieved through redundancy or segmentation. Redundancy introduces ductility or additional components to a system. Ductility directly increases β_{sys} [2], whereas the addition of more components reduces the importance of each component and the scatter of the system performance [3]. Segmentation is a damage-limiting strategy, where a system is organized in compartments that cannot propagate damage to each other [4].

The concepts of reliability and robustness can be formally characterized by decomposing the total probability of system failure due to progressive collapse, $\mathrm{P}(F_{\text{sys}})$ [5], into its constituent components, as expressed by the following equation, adapted from the risk equation in the Eurocode [6]:

$$\mathrm{P}(F_{\text{sys}}) = \sum_i \mathrm{P}(H_i) \sum_j \sum_k \mathrm{P}(D_j|H_i)\mathrm{P}(F_{\text{sys},k}|D_j), \tag{1}$$

where H_i is hazard i, D_j is an initiating damage scenario j, and $F_{\text{sys},k}$ is an adverse system state k leading to loss of performance. Reliability addresses the hazard H_i and the resulting damage scenario $D_j|H_i$, whereas robustness addresses the system failure following a specific damage scenario $S_k|D_j$. The primary scope of current design standards is managing the reliability.

In robustness, initial developments were focused on non-deliberate accidental loads. However, the focus shifted after the events of September 11, 2001, with the progressive collapse of the World Trade Centers following a terror attack [7]. Since then, deliberate attacks have received increased attention [8]. To reduce the risk of deliberate attacks, targeted and building-specific protective measures are the most cost-efficient methodologies [9]. However, the prior knowledge of an attacker about the system, which can range from *no knowledge* to *complete knowledge*, may affect the choice of optimal risk-reduction measure. For instance, in scale-free networks characterized by a few well connected nodes, the failure of random links does not greatly affect the system performance because of the presence of numerous alternative paths. However, targeted attacks on the links of well-connected nodes quickly lead to system failure [10].

To quantify the performance of a system under expected operational conditions and in case of unexpected system disruptions, Lim et al. [11] introduced a β–π analysis, where the reliability associated with a specific initiating damage scenario, $\beta_{i,j} = -\Phi^{-1}[\mathrm{P}(D_j|H_i)]$, is compared with the robustness index for the same damage scenario, $\pi_{i,j,k} = -\Phi^{-1}[\mathrm{P}(F_{\text{sys},k}|D_j, H_i)]$, in a β–π diagram. In the absence of segmentation measures (e.g., in a Daniels system [1]) the robustness index $\pi_{i,j,k}$ reduces to a redundancy index. A high reliability $\beta_{i,j}$ signifies a lower probability of a specific initiating damage scenario under expected loading conditions, whereas a high robustness $\pi_{i,j,k}$ signifies a lower probability of an adverse system state $F_{\text{sys},k}$ following such initiating event. As such, a β–π diagram enables a direct comparison and potential trade-offs between the reliability β and robustness π of a system.

1.2 Objectives and scope

Although studied in the realm of network theory [10], there is a lack of understanding on the effect of prior knowledge of the attacker on the performance of a structural system. Moreover, structural systems may be characterized by a mixture of different component behavior (such as brittle and ductile) which may lead to a large combination of damage scenarios for an attack involving the failure of multiple components. This study aims to increase the understanding of the complex relationship between the prior knowledge of an attacker, the attacked component(s), and the properties of the system.

This investigation is limited to a Daniels system [1] with ten components which may be brittle or ductile. It uses a combination of probabilistic and combinatorial methods with Monte Carlo analysis. Three case studies are investigated: (i) uniform brittle and ductile systems; (ii) a mixed system with an equal number of brittle and ductile components; and (iii) informed and uninformed attacks on the mixed system. The research contributes to the quantification of the effects of prior knowledge of an attacker on a system, and can be further developed for targeted risk-reducing measures.

2 THEORETICAL FRAMEWORK

2.1 Mechanical model

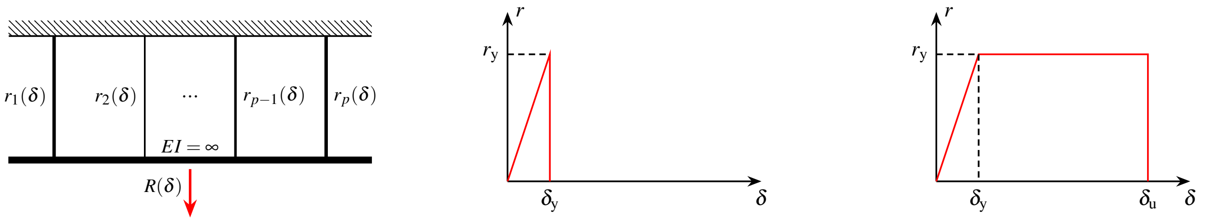
In the redundant system in Figure 1a with n components, the failure of a component D_p does not definitively lead to a system failure F_{sys} because of load redistribution mechanisms [1, 2]. If the components are assumed to behave in a linear elastic ideal brittle manner (Figure 1b), and their resistances $r_{\text{y},p}$ are assumed to be independent and identically distributed, then the probability of exactly $j < n$ components failing can be computed as follows:

$$\mathrm{P}(D_j) = \left[\prod_{p=1}^{j} \mathrm{P}(D_p)\right] \left[\prod_{p=1}^{n-j} (1 - \mathrm{P}(D_p))\right], \tag{2}$$

where $\mathrm{P}(D_p)$ can be determined using reliability analysis considering a hazard H_i with intensity S_i and a component resistance $r_{\text{y},p}$. If component failure is defined as the exceedance of the resistance $r_{\text{y},p}$, the limit state function for a component becomes

$$\mathrm{P}(D_p) = \mathrm{P}\left(r_{\text{y},p} - \frac{S_i}{N} \leq 0\right). \tag{3}$$

Eq. 3 can be solved using any reliability-based method, such as the first-order reliability method or crude Monte Carlo analysis. If the components are assumed to have an ideal plastic behavior following the linear elastic phase in Figure 1c and failure is interpreted as inelastic behavior, then Eqs. 2 and 3 are valid as well.



(a) Redundant system. (b) Linear elastic ideal brittle. (c) Linear elastic ideal plastic.

Figure 1: System and component behaviors $r_p(\delta)$.

2.2 β–π diagram

A β–π diagram is a visual representation of the reliability and robustness of a system [11]. The probability of system failure F_{sys} for a specific hazard H_i can be expressed as [5]

$$\mathrm{P}(F_{\text{sys}}|H_i) = \mathrm{P}(F_{\text{sys}}|D_j)\mathrm{P}(D_j|H_i)\mathrm{P}(H_i) < \mathrm{P}_{\text{dm}}, \tag{4}$$

where D_j is the j-th initiating damage scenario (from Eq. 1), which for the system under investigation corresponds to the simultaneous failure of j components, and P_{dm} is the *de minimis* probability of system failure. Eq. 4 is obtained from Eq. 1 under the assumption that the only adverse system state is the loss of structural capacity of the system. Alternatively, Eq. 4 can be expressed as

$$\Phi(-\pi_{i,j})\Phi(-\beta_{i,j}) < \frac{\mathrm{P}_{\text{dm}}}{\mathrm{P}(H_i)}, \tag{5}$$

In Eq. 5, $\beta_{i,j}$ and $\pi_{i,j}$ are defined as:

$$\beta_{i,j} = -\Phi^{-1}\left[\mathrm{P}\left(D_j|H_i\right)\right], \tag{6a}$$

$$\pi_{i,j} = -\Phi^{-1}\left[\mathrm{P}\left(F_{\text{sys}}|D_j, H_i\right)\right]. \tag{6b}$$

In a redundant system where the behavior of the components $r_p(\delta)$ are identically distributed, Eq. 6a can be interpreted as the reliability index of the initiating damage scenario event D_j for a hazard H_i (using the limit state function in Eq. 3), whereas Eq. 6b is the robustness index of the system for a hazard H_j and initiating damage scenario D_j. In a β–π diagram, $\beta_{i,j}$ is usually plotted on the vertical axis and $\pi_{i,j}$ on the horizontal axis. A β–π diagram with different iso-probability lines P_{dm} is shown in Figure 2.

The probability of the hazard H_i can also be incorporated in the diagram by replacing $\beta_{i,j}$ with an adjusted index $\beta^*_{i,j}$, expressed as [12]

$$\beta^*_{i,j} = -\Phi^{-1}\left[\mathrm{P}\left(D_j|H_i\right)\lambda_i\right], \tag{7}$$

where λ_i is the rate of occurrence of H_i, numerically equal to $P(H_i)$ if $\lambda_i \ll 1$. We can use the new index $\beta^*_{i,j}$ to rewrite Eq. 5 as

$$\Phi(-\pi_{i,j})\Phi(-\beta^*_{i,j}) < P_{\text{dm}}. \tag{8}$$

For the system in Figure 1a, the robustness index $\pi_{i,j}$ in Eq. 6b quantifies the redundancy of the system for a the initiating damage scenario D_j, i.e., the simultaneous failure of j components.

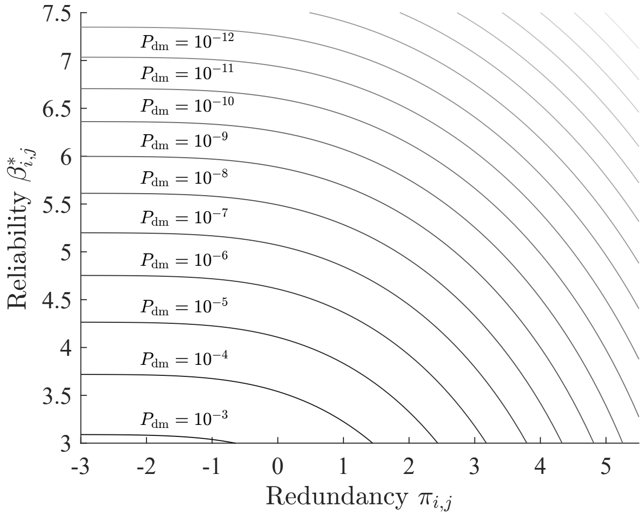


Figure 2: π–β diagram with different iso-probability lines $P_{\rm dm}$.

2.3 Damage scenarios in mixed systems

In systems with mixed component behaviors, a multitude of unique initiating damage scenarios are possible. The system under investigation in this paper comprises n components out of which $n_{\rm B} < n$ are linear elastic ideal brittle (B), with behavior shown in Figure 1b, and $n_{\rm D} = n - n_{\rm B}$ are linear elastic ideal plastic (D), with behavior shown in Figure 1c.

If a system with n components suffers from an instantaneous failure of any $j \geq 1$ components, a total of $2^n - 1$ different initiating damage scenarios can be identified. We define Y_k, with $k = 1, \ldots, K$, as a subset of the initiating damage scenario D_j, characterized by the number of brittle components that have failed. For an initiating damage scenario D_j, the total number of subsets K can be obtained as follows:

$$K = b_{\max} - b_{\min} + 1, \quad \text{with} \quad b_{\min} = \max(0, j - n_{\rm D}),\ b_{\max} = \min(j, n_{\rm B}). \tag{9}$$

Using the hypergeometric distribution from combinatorial analysis, the probability of damaging exactly b brittle components if exactly j components are damaged, $\mathrm{P}(D_{j,k=b}) = \mathrm{P}(Y_k = b|D_j)$, is

$$\mathrm{P}(D_{j,k=b}) = \frac{\binom{n_{\rm B}}{b}\binom{n_{\rm D}}{j-b}}{\binom{n}{j}}, \quad b \in [b_{\min}, \ldots, b_{\max}]. \tag{10}$$

The coordinates $(\beta^*_{i,j,k}, \pi_{i,j,k})$ for the specific damage scenario k, where exactly b brittle components and $j - b$ ductile components fail, can be determined as in Eq. 7, as

$$\beta^*_{i,j,k} = -\Phi^{-1}\left[\mathrm{P}\left(D_{i,j,k}\right)\mathrm{P}\left(D_{i,j}\right)\lambda_i\right], \tag{11a}$$

$$\pi_{i,j,k} = -\Phi^{-1}\left[\mathrm{P}\left(F_{\mathrm{sys},i,j,k}\right)\right], \tag{11b}$$

where $\mathrm{P}\left(D_{i,j,k}\right) = \mathrm{P}\left(Y_k|D_j, H_i\right)$, and $\mathrm{P}\left(D_{i,j}\right) = \mathrm{P}\left(D_j|H_i\right)$. For brevity, the conditional statements $X|H_i, D_j, Y_k$ are simply written as $X_{i,j,k}$ in Eq. 11 and subsequent equations.

The points defined by the coordinates in Eq. 11 can be aggregated to obtain the point associated with the initiating damage scenario D_j, which have the following coordinates:

$$\beta^*_{i,j} = -\Phi^{-1}[\mathrm{P}(D_{i,j})\lambda_i], \text{ with } \mathrm{P}(D_{i,j}) = \sum_{k}^{K} \mathrm{P}(D_{i,j,k}) = \sum_{k}^{K} \Phi(-\beta_{i,j,k}), \tag{12a}$$

$$\pi_{i,j} = -\Phi^{-1}[\mathrm{P}(F_{\text{sys},i,j})], \text{ with } \mathrm{P}(F_{\text{sys},i,j}) = \sum_{k}^{K} \mathrm{P}(F_{\text{sys},i,j,k})\mathrm{P}(D_{i,j,k}) = \sum_{k}^{K} \Phi(-\pi_{i,j,k})\mathrm{P}(D_{i,j,k}). \tag{12b}$$

In turn, the points defined by the coordinates in Eq. 12 can be aggregated to obtain a point that describes the performance of the system subject to *any* initiating damage scenario. We denote this point the *system performance point* for hazard H_i. The coordinates of the *system performance point* can be found as follows:

$$\beta^*_i = -\Phi^{-1}[\mathrm{P}(\hat{D}_i)\lambda_i], \quad \text{with} \quad \mathrm{P}(\hat{D}_i) = \sum_{j}^{J} \mathrm{P}(D_{i,j}) = \sum_{j}^{J} \Phi(-\beta^*_{i,j}), \tag{13a}$$

$$\pi_i = -\Phi^{-1}[\mathrm{P}(F_{\text{sys}}|\hat{D}_i)], \quad \text{with} \quad \mathrm{P}(F_{\text{sys}}|\hat{D}_i) = \sum_{j}^{J} \mathrm{P}(F_{\text{sys},i,j})\frac{\mathrm{P}(D_{i,j})}{\mathrm{P}(D_i)} = \sum_{j}^{J} \Phi(-\pi_{i,j})\frac{\Phi(-\beta^*_{i,j})}{\sum_j^J \Phi(-\beta^*_{i,j})}, \tag{13b}$$

where $\mathrm{P}(\hat{D}_i)$ is the probability of occurrence of *any* initiating damage scenario following hazard H_i, and $\mathrm{P}(D_{i,j}) = \mathrm{P}(D_j|H_i)$ is the probability of damaging exactly j components following hazard H_i.

Finally, the system performance point (β^*_i, π_i) in Eq. 13 can be used to determine the probability of failure of the system due to hazard H_i, $\mathrm{P}(F_{\text{sys},i})$, and the corresponding system reliability index, $\beta_{\text{sys},i}$, as follows:

$$\mathrm{P}(F_{\text{sys},i}) = \mathrm{P}(F_{\text{sys}}|H_i) = \mathrm{P}(F_{\text{sys}}|\hat{D}_i)P(\hat{D}_i) = \frac{\Phi(-\pi_i)\Phi(-\beta^*_i)}{\lambda_i}, \quad \beta_{\text{sys},i} = -\Phi^{-1}[\mathrm{P}(F_{\text{sys},i})]. \tag{14}$$

Attacks on the system are expected to reduce both the reliability and redundancy, effectively shifting the system performance point (β^*_i, π_i) closer to the origin of the β–π space. As a result, certain initiating events that were previously less critical may become dominant. The total effect of an attack can thus be visualized as a displacement of the system performance point (β^*_i, π_i), illustrating the degradation in structural performance.

2.4 Attack strategies

In the context of structural systems, attack strategies refer to intentional actions aimed at compromising system performance by removing or disabling one or more of its components. While originally studied in the realm of network theory [10], the concept of attack strategies has gained increasing relevance in the assessment of physical infrastructure, particularly when considering deliberate attacks, such as sabotage, terrorism, or targeted degradation.

The two main types of attack strategies considered in this paper are the following:

1. **Uninformed attack:** The attacker lacks detailed knowledge about the system configuration and attacks components of the system at random without prior knowledge. As such, the failure of each component is equally likely and occurs at random. This approach is suitable for modeling non-strategic or uninformed disruptions.

2. **Informed attack:** The attacker has full knowledge of the system configuration and intentionally removes components with prior knowledge to maximize the disruption. This approach is suitable for modeling sophisticated and informed threats, where the attacker seeks to maximize the disruption.

From a reliability-based perspective, the effect of an attack can be seen as a system perturbation. As such, the result of a successful attack is a reduced post-attack reliability and robustness for the system. Evaluating these effects can help identify critical components and support the development of targeted counter-measures and defense strategies.

3 CASE STUDIES

We investigate the reliability and redundancy of redundant systems [1] with $n = 10$ components, illustrated in Figure 1a. The components could be either brittle or ductile, with the behaviors shown in Figure 1b and 1c, respectively. Furthermore, we assess the influence of the two attack strategies on the reliability and redundancy of the system. The systems are subject to a constant deterministic load S_i with a rate of occurrence $\lambda_i = 10^{-3}$ year^{-1}, while the resistance of all components is normally distributed with a mean $\mu_r = 2$ and coefficient of variation $V_r = 0.35$, i.e., $r_{\mathrm{y},p} = r_y \sim \mathcal{N}[\mu_r, (\mu_r V_r)^2]\,\forall\, p$. The probability of failure of an individual component can be obtained with Eq. 3, and the corresponding component reliability index is $\beta_p = 2.71$.

The brittle components behave in a linear elastic manner until failure defined by r_y, whereas the ductile components behave in a linear elastic manner until r_y with subsequent ideal plastic behavior. For the ductile components, a ductility $\delta_\mathrm{u}/\delta_\mathrm{y} = \infty$ is assumed and component failure is defined as $\delta \geq \delta_y$ and $r_j(\delta) = r_\mathrm{y}$, as the components are not intended to function beyond their yield points. This assumption reflects a conservative design approach where yielding is considered a loss of structural integrity, and any plastic deformation is treated as unacceptable. However, it should be noted that additional deformation δ may occur beyond the yield point r_y. Therefore, the computed reliability indices ($\beta^*_{i,j}$) should be interpreted as conservative. Nonetheless, the redundancy indices $\pi_{i,j}$ remain representative of system failure $F_{\mathrm{sys},i}$ for both brittle and ductile component behaviors, as yielding in *all* components leads to continued deformation until the ultimate deformation δ_u is reached and the system fails.

3.1 Uniform brittle and uniform ductile systems

This section examines systems that only comprise brittle or ductile components. The β^*–π diagrams for the uniform brittle and ductile systems are shown in Figure 3 with iso-probability lines in the background for reference. The colored numbers beside each circle denote the initial instantaneous failure of j components. For redundancy indices of $\pi_{i,j} < -3$, the points are drawn at $\pi = -3$, for visual clarity.

Figure 3 shows that the ductile system exhibits significantly higher redundancy $\pi_{i,j}$ compared with the brittle system for the same component reliability β_p. The additional redundancy $\pi_{i,j}$ in ductile systems stems from load-redistribution mechanisms originating from the ductility. For initial damage

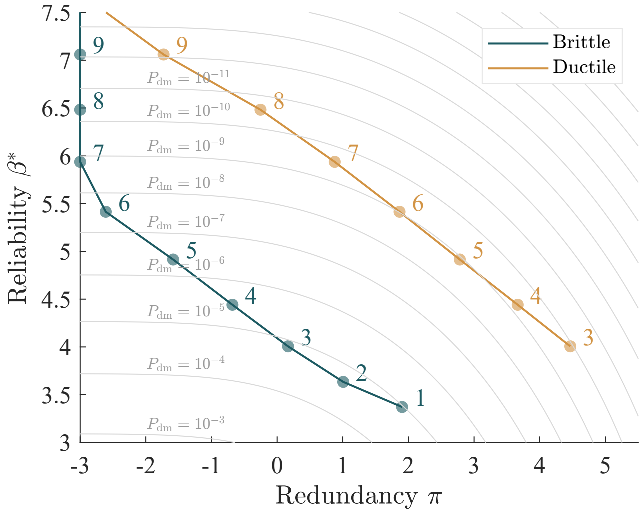


Figure 3: β^*–π plots for the uniform brittle system and the uniform ideal ductile system

j \ k	1	2	3	4	5	6
1	1 B	1 D				
2	2 B	1 B, 1 D	2 D			
3	3 B	2 B, 1 D	1 B, 2 D	3 D		
4	4 B	3 B, 1 D	2 B, 2 D	1 B, 3 D	4 D	
5	5 B	4 B, 1 D	3 B, 2 D	2 B, 3 D	1 B, 4 D	5 D
6	5 B, 1 D	4 B, 2 D	3 B, 3 D	2 B, 4 D	1 B, 5 D	
7	5 B, 2 D	4 B, 3 D	3 B, 4 D	2 B, 5 D		
8	5 B, 3 D	4 B, 4 D	3 B, 5 D			
9	5 B, 4 D	4 B, 5 D				

Table 1: Initial damage k for $n = 10$ components with $n_{\mathrm{B}} = n_{\mathrm{D}} = 5$ for a failure of j components.

scenarios D_j involving damage to $j \ll n$ components, the redundancy becomes $\lim_{j \ll n} \pi_{i,j} = \infty$. As such, the points for $j \in [1, 2] \ll n = 10$ for the ductile system are omitted from Figure 3. This observation is in line with previous research on the system reliability of redundant systems, where the system reliability β_{sys} of ductile systems is higher than for brittle systems [2].

3.2 Mixture of brittle and ductile components

In this section, we examine a mixed system with $n_{\mathrm{B}} = 5$ brittle and $n_{\mathrm{D}} = 5$ ductile components. A large number of initial damage scenarios can be identified. For instance, the initial damage event with damage to $j = 1$ components may correspond to the failure of a brittle component or the failure of a ductile component. The initial damage scenarios $k \in [1, ..., K]$ for damage to $j \in [1, ..., J]$ components and their associated probabilities of occurrence can be determined from Eqs. 9 and 10. A comprehensive list of all initiating damage scenarios is shown in Table 1.

Figure 4 shows the β^*–π diagram of the mixed system. The performance points $(\beta^*_{i,j,k}, \pi_{i,j,k})$ for each of the individual events listed in Table 1 (shown in blue in Figure 4) form clusters depending

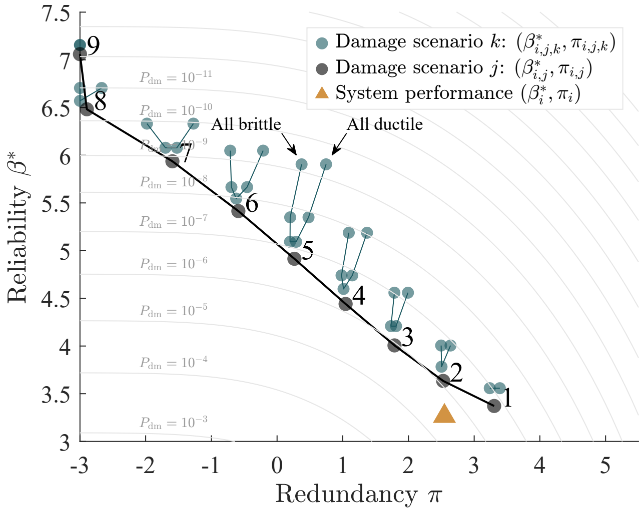


Figure 4: β^*–π plots for the mixed system

on the number of failed components j. In each cluster, two distinct arms can be identified: (i) the left arm is governed by the failure of brittle components and survival of ductile components; and (ii) the right arm governed by the failure of ductile components and survival of brittle components. This is shown in Figure 4 for an initial failure of $j = 5$ components, where the points with the highest reliability $\beta^*_{i,5}$ are: (left) failure of only brittle components; and (right) failure of only ductile components. Surprisingly, the lowest redundancy $\min(\pi_{i,5})$ is obtained with the failure of $b = 4$ brittle and $j - b = 1$ ductile components and not the failure of only brittle components.

The performance points $(\beta^*_{i,j}, \pi_{i,j})$ for the individual damage scenarios D_j are obtained using Eq. 12 and are shown in gray in Figure 4. As expected, the combined reliability $\beta^*_{i,j}$ is lower that the reliability of the individual points $\beta^*_{i,j,k}$. This stems from the cumulative probabilities of each damage scenario in Eq. 12a.

The system performance point (β^*_i, π_i) for the hazard H_i can be computed from Eq. 13 considering all J damage scenarios. For the investigated system and load, the probability of *any* initiating damage scenario considering the rate of occurrence of the hazard is $\mathrm{P}(\hat{D}_i)\lambda_i = 5.5 \cdot 10^{-4}$, corresponding to a reliability index $\beta^*_i = 3.26$. The redundancy is $\pi_i = 2.55$ with a conditional probability of system failure $\mathrm{P}(F_{\mathrm{sys},i}|\hat{D}_i) = 5.4 \cdot 10^{-3}$.

The system performance point lies in the vicinity of the points corresponding to the failure scenarios involving a small number of components (i.e., $j = 1, 2$). This is because the coordinates defined by Eq. 13 represent a weighted average over all initiating damage scenarios D_j, with weights proportional to their probability of occurrence. Consequently, scenarios with low probability and high reliability indices (in this case study $j > 2$) have limited influence on the system performance point, which is therefore generally situated close to the most likely failure events. We remind here that our approach assumes that the failure of one component is independent of the survival state of the neighboring component, which may not reflect realistic hazard-scenarios. For instance, we would expect the survival state of a neighboring component to be correlated to the distance from a failed component in material degradation situations from water damage. Another example is the case of vehicular impact, where the location of potential subsequent impacts would be correlated to the location and other variables of the initial impact. However, the assumption of damage independence could be a good approximation in cases where there is weak or no correlation between the damage to multiple components.

3.3 Uninformed vs. informed attacks

This section investigates the influence of different attack strategies on the mixed system described in Section 3.2. The effect of an attack is modeled by progressively removing $m \in [1, 2, 3, 4]$ components from the system, thereby emulating various severities of attacks. In contrast to earlier sections, the removal of m components in this case results in an actual loss of load-carrying capacity for the ductile components. This reflects a scenario in which the attacked elements are entirely destroyed — rather than merely yielding — as would be the case with explosive or similarly destructive attacks. For each m, the effect of an uninformed and informed attack strategy, as presented in Section 2.4, is assessed.

In an uninformed attack, the attacker lacks system knowledge and members are attacked and removed at random. In terms of probability of each attack, this is treated as presented in Section 2.3 and exemplified in Section 3.2, but for the removal of m components. In contrast, the attacker in an informed attack has full system knowledge and seeks to maximize the system disruption by maximizing the reduction in the system's reliability β and redundancy π. Because the removal of ductile components reduces the system's ability to withstand loads in a substantial manner, in this case, the informed attack strategy corresponds to the loss of m ductile components.

The results of the analyses on informed and uninformed attacks are presented in Figure 5 for the removal of m components. Generally, the removal of more components leads to lower reliabilities $\beta^*_{i,j}$ and redundancies $\pi_{i,j}$. This is evident in the translation of the *informed* and *uninformed attack* curves from the *no attack* curve towards the lower left corners in Figure 5, where

$$\lim_{\beta^*_{i,j} \to -\infty} [\mathrm{P}(D_{i,j})\lambda_i = \Phi(-\beta^*_{i,j})] = 1, \tag{15a}$$

$$\lim_{\pi_{i,j} \to -\infty} [\mathrm{P}(F_{\mathrm{sys},i,j}) = \Phi(-\pi_{i,j})] = 1. \tag{15b}$$

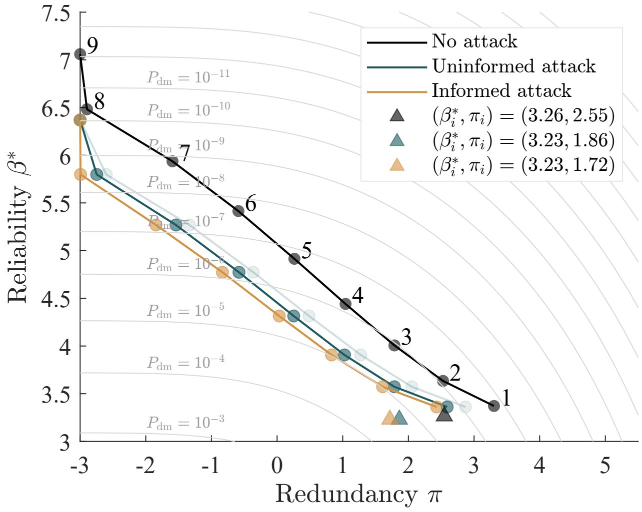
Although the reliability values $\beta^*_{i,j}$ do not reduce dramatically, the redundancy values $\pi_{i,j}$ move from $\pi_{i,j} > 0$ to $\pi_{i,j} < 0$, marking a paradigm shift where system collapse $F_{\mathrm{sys},i}$ is more likely than survival. This is also reflected in the translation of the system performance point, which moves from $\pi_i > 0|_{m \leq 1}$ to $\pi_i < 0|_{m \geq 4}$.

The influence of the attack strategy on the system performance $(\beta^*_i, \pi_i)|m$ is mainly evident in the redundancy π_i, where a greater number of removed components m leads to a larger difference in the system performance points $(\beta^*_i, \pi_i)|m$. This shows that the value of information for the attacker increases with the severity of the attack, with more detrimental consequences for the structure.

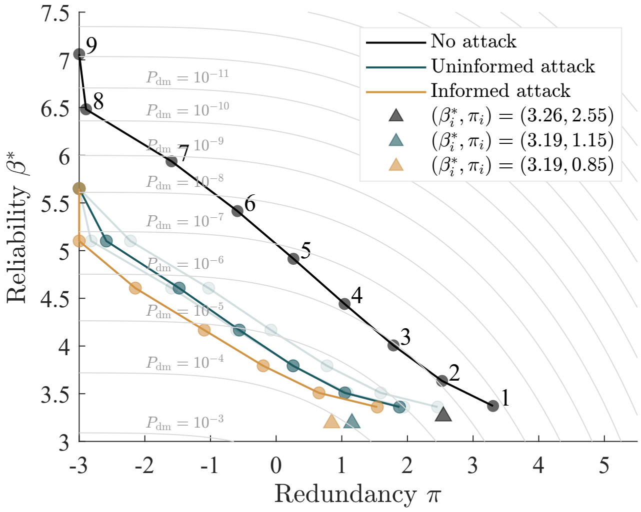
The presented methodology can aid in the development of effective defense strategies against attacks of various severities and prior information about a structure, such as the use of protective structures, key elements, segmentation, redundancy, and more. Moreover, the value of information for an attacker can be quantified to assess the appropriate allocation of resources into counter-measures, such as obscurity, information safety of the structure, and more. As such, this work contributes to the shift from *preventing* to *managing* abnormal and unforeseen hazards.

4 CONCLUSION

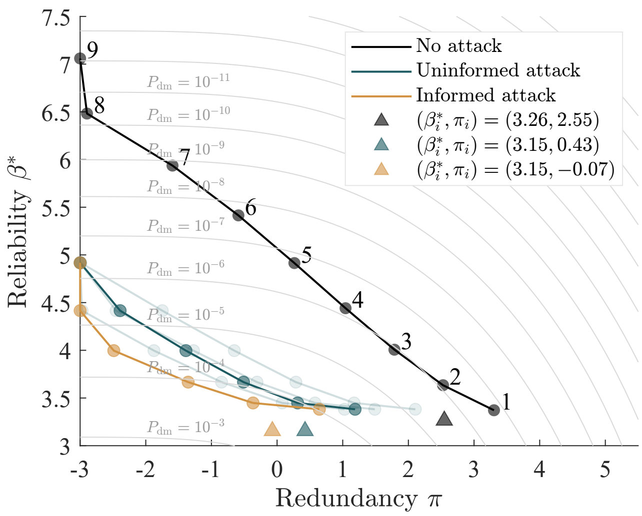
In this paper, we assessed the effect of damage scenarios in mixed systems and the influence of prior knowledge of an attacker in a deliberate attack on a structure. To achieve this goal, probabilistic and



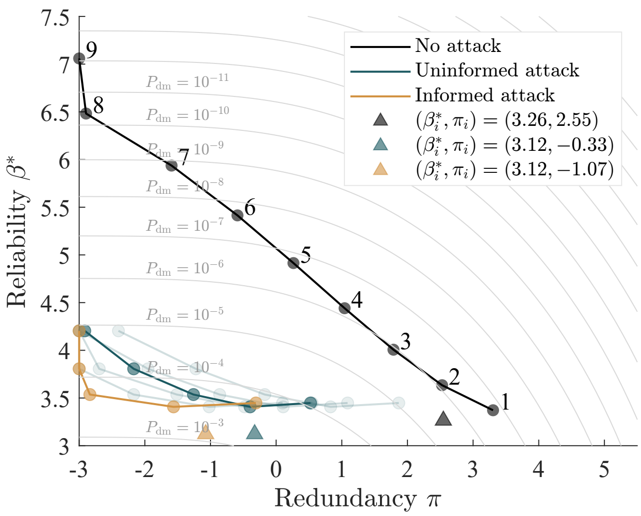
(a) Attack on $m = 1$ component.



(b) Attack on $m = 2$ components.



(c) Attack on $m = 3$ components.



(d) Attack on $m = 4$ components.

Figure 5: Effect of attacks on m components in a system with five brittle and five ductile components.

combinatorial methods were combined with Monte Carlo analysis and the methodology was demonstrated on a redundant system with ten components in three case studies: (i) uniform ductile and brittle systems; (ii) mixed system comprising equal numbers of ductile and brittle components; and (iii) informed and uninformed attacks. The results show that brittle systems are less robust than ductile systems. For mixed systems, the most detrimental initiating event is damage to mostly brittle components and a few ductile components. An informed attack leads to a more severe reduction in the robustness compared with an uninformed attack, and the differences between an uninformed and informed attack grows with the number of targeted components. The paper shows the importance of considering the prior knowledge of an attacker when devising counter-measures and defense strategies. Further research should assess a larger diversity in systems and quantify the value of information for an attacker to devise appropriate targeted counter-measures and defense strategies.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the financial support provided by the Swiss National Science Foundation SNSF and Formas - a Swedish Research Council for Sustainable Development in the project *RelyConnect - Reliable and high-performance modern timber structures with modern connections* (SNSF grant no. 220112, Formas grant no. 2023-01603) , and the COST Action *CA20139 - Holistic design of taller timber buildings (HELEN).*

REFERENCES

[1] H. E. Daniels, "The statistical theory of the strength of bundles of threads, Part I," *Proceedings of the Royal Society A*, vol. 183, no. 995, 1945.

[2] S. Gollwitzer and R. Rackwitz, "On the reliability of Daniels systems," *Structural Safety*, vol. 7, no. 2-4, pp. 229–243, 1990.

[3] A. S. Cao, S. Thöns, R. Jockwer, and P. Palma, "System effects of timber connections comprising multiple fasteners," in *14th International Conference on Structural Safety and Reliability - ICOSSAR'25* (R. Ghanem, E. Johnson, S. Masri, and A. Olivier, eds.), (Los Angeles, USA), 6 2025.

[4] A. S. Cao, *Modelling progressive collapse of timber buildings and its applications*. PhD thesis, ETH Zurich, Zurich, Switzerland, 2024.

[5] B. R. Ellingwood and D. O. Dusenberry, "Building design for abnormal loads and progressive collapse," *Computer-Aided Civil and Infrastructure Engineering*, vol. 20, pp. 194–205, 5 2005.

[6] "Eurocode 1: Actions on structures - part 1-7: General actions - accidental actions," 2006. European Standard.

[7] N. Lalkovski and U. Starossek, "The Total Collapse of the Twin Towers: What It Would Have Taken to Prevent It Once Collapse Was Initiated," *Journal of Structural Engineering*, vol. 148, 2 2022.

[8] J. M. Adam, F. Parisi, J. Sagaseta, and X. Lu, "Research and practice on progressive collapse and robustness of building structures in the 21st century," *Engineering Structures*, vol. 173, pp. 122–149, 10 2018.

[9] S. Thöns and M. G. Stewart, "On the cost-efficiency, significance and effectiveness of terrorism risk reduction strategies for buildings," *Structural Safety*, vol. 85, 7 2020.

[10] M. Tomassini, "Designing robust scale-free networks under targeted link attack using local information," *Physica A: Statistical Mechanics and its Applications*, vol. 615, 4 2023.

[11] S. Lim, T. Kim, and J. Song, "System-reliability-based disaster resilience analysis: Framework and applications to structural systems," *Structural Safety*, vol. 96, p. 102202, 2022.

[12] L. Iannacone, I. Björnsson, S. Thöns, and D. Honfi, "Multi-index method for visualizing robustness of structures," in *Proceedings of the 2025 Symposium of the International Association for Bridge and Structural Engineering (IABSE), Tokyo, Japan*, p. N/A, 2025.