*sustainability*

MDPI

*Article*

# Living with Legacy Risk—The Limits of Practicalities?

**Ben J. M. Ale [1,*], Des N. D. Hartford [2] and David H. Slater [3]**

[1] Department of Values and Technology, Technical University, 2600 GA Delft, The Netherlands
[2] BC Hydro, Burnaby, BC V3N 4X8, Canada; drdeshartford@shaw.ca
[3] School of Engineering, Cardiff University, Cardiff CF24 3AA, UK; davidhslater@btinternet.com
* Correspondence: ben.ale@xs4all.nl

**Abstract:** Legacy risks from infrastructures and industrial installations often reveal themselves when a potential for failure has been discovered much later than at the stage of the design and construction of a structure. In which case, there might already be a problem with the legacy installation, or even a crisis, without having had an accident. When the hazard cannot be taken away, the question arises as to how much effort, if any, should be spent on improving the situation. The usefulness of the three archetypical approaches to this problem: setting a standard, the as low as reasonably practicable approach and a case-by-case discourse approach are discussed for their applicability for these legacy risks. Although it would be desirable to retrofit legacy risks to previously set legal requirements as is the case when acceptability limits are set in law or demonstration of ALARP (As Low As Reasonably Achievable) is demanded, it may be impossible to reduce the residual risk to an otherwise acceptable level without taking away or replacing the infrastructure, which is not acceptable either. Therefore in conclusion the only available solution to persistent legacy risk problems seems to be to have a thorough discussion with all relevant stakeholders until an agreement is in some way found.

**Keywords:** Norm; ALARP; discourse; cost benefit analysis

check for updates

**Citation:** Ale, B.J.M.; Hartford, D.N.D.; Slater, D.H. Living with Legacy Risk—The Limits of Practicalities?. *Sustainability* **2021**, *13*, 3004. https://doi.org/10.3390/su13063004

Academic Editors: Dragan Komljenovic, Georges Abdul-Nour and François Gauthier

Received: 24 February 2021
Accepted: 5 March 2021
Published: 10 March 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

## 1. Introduction

A recurring and persistent problem that risk managers from governments and corporations alike are confronted with are legacy risks from infrastructures and industrial installations. Often the people who are confronted with these risks and have to deal with them have not been part of the original decision as to their acceptability: and rarely have first-hand information about what information was available, what weight was given to the various attributes in that decision; or even, which stakeholders were involved and who were not, and exactly how the decision was reached. For the people and the stakeholders involved only when the risk is revealed, the risk is new, but the situation is old. Such situations are not easy to remedy either. The "new" hazard cannot be taken away without considerable costs, or even damage, to the same stakeholders who are exposed to these risks. This makes decision making in these situations much more difficult than in the new situation.

This confrontation sometimes occurs as a result of an unexpected and unanticipated accident: but more often, it occurs when a potential for failure has been discovered much later than at the stage of the design and construction of a structure. In which case, there might already be a problem with the legacy installation, or even a crisis, without having had an accident. There are several reasons why this can happen. It may be that at the time of the design and construction, aspects of the technology, or of the environment in which it is functioning were insufficiently understood or known. Technology develops and so does the understanding. It might even be that certain risks associated with elements of the behavior of the construction did not occur to the people who designed and built it. Finally, it may be that warnings were issued at the time but dismissed by the then established engineering community.

Given that the hazard cannot be taken away, the question arises as to how much effort, if any, should be spent on improving the situation. It should be borne in mind that in a case where the hazard cannot be taken away, the only remaining option is to reduce the probability. The decision therefore becomes a decision on risk and the acceptability or tolerability of it.

In this paper we consider the usefulness of the three archetypical approaches to this problem: setting a standard, the ALARP (as low as reasonably achievable) approach, and a case-by-case discourse approach [1]. The paper contributes to the understanding of which decision-making methods are most applicable to legacy risks, especially for large infrastructures that cannot be removed nor easily updated.

## 2. Spectrum of Industrial Installation Types

The many types of industrial installation can be considered in terms of a spectrum that ranges from large, fixed installations such as dams, major bridges, and tunnels that are difficult and expensive to remediate; to light industrial installations that can be readily adapted and improved in the light of advances in science and technology. Large complex installations such as nuclear power plants represent an intermediate category, where some aspects of the functioning of the installation can be improved with technological advances.

Structures such as dams, bridges, and tunnels largely function in a passive way, absorbing the forces that are applied to them over a wide range of force fields. All structures share this force absorption characteristic to some degree (e.g., nuclear pressure vessel and tanks in industrial installations). However, as one moves across the spectrum from the large fixed civil infrastructures to light industrial installations, the functioning of the installation often involves processes that require evermore "active" control. The greater the role of technology in the safe functioning of the installation, the more amenable the installation is to function and therefore safety improvements. At the same time, such installations become obsolete relatively quickly in comparison to what can be achieved by more up-to-date installations. Such complex installations can also experience normal accidents, where interactions and interdependencies between the many parts of the system combine to cause an accident, even though each part is operating within its normal limits.

The large fixed passive infrastructures become obsolete much more slowly in comparison to lighter industrial facilities and often provide useful service over multiple economic evaluation horizons. Such infrastructures are often fully depreciated in accounting terms long before their useful life is over.

## 3. Deterministic Standards of Acceptability

The designs of many industrial installations are defined in terms of design rules that are often termed "good practice of the day". These "good practices" that have proven to be reliable over many years have evolved slowly over many years even centuries, sometimes anchored in physical principles that have been understood to varying degrees over millennia. Deterministic analysis aims to demonstrate that an installation is tolerant to identified hazards and faults that are within the "design basis", thereby defining the limits of safe operation.

Deterministic safety analyses are normally supplemented by further specific information and analysis such as information and analysis relating to fabrication, testing, inspection and evaluation of the operating experience. A great deal of nuclear engineering is anchored in deterministic standards. However, nuclear power plants and other similarly designed complex installations can experience normal accidents and catastrophic failures. The fact that such failures can and do occur necessitates a broader view of safety standards than strict adherence to deterministic norms and established good practices. Probabilistic safety analysis is intended to provide an additional contribution to demonstrating that the possible different plant states are acceptable, and that the possibility of certain conditions arising that could lead to some type of failure is remote. This raises the questions of the

meaning of the term "remote", and the means of demonstrating that such a condition has been achieved.

## 4. Risk Standards of Acceptability

In a few countries, levels of acceptable risk are specified by law. The Netherlands is a well-documented example [2–4]. In the Netherlands these levels are expressed as localized risk (LR). Localized risk is defined as the frequency (/yr.) that an individual who is permanently present at a specific location could be killed as a result of an accident, or incident at a nearby hazard source. For sea defenses the maximum allowable LR is $10^{-5}$/yr. For gas-exploitation induced earthquakes, this level is also set at $10^{-5}$/yr. For industrial installations the level is set at $10^{-6}$/yr.

The law does not demand that the levels of risk outside industrial premises, or on any other location cannot be higher than that level. The law however does require that no housing—or buildings with similar vulnerability, such as hospitals—can exist at locations where the acceptable levels are exceeded. This means that no new houses can be built at locations where the acceptable level of risk is exceeded and that should there be houses in such an area, that they have to be removed. This also means that new activities and developments that would lead to exceeding the acceptable level at locations where houses are already present are prohibited.

The difference between acceptability of an order of magnitude between industrial installations on the one hand and flood protection and protection against induced earthquakes, on the other, has a simple reason: available budgets. The original acceptability level for sea defenses dates from the middle of the previous century and was revised early in this century.

### *4.1. Sea Defenses 1950s*

The defense of the Netherlands against floods has a long history. After the second World War and the flood in the 1953 design criteria for these defenses were based on probabilistic reasoning. They were and still are expressed in design overtopping probabilities.

In 1953 a flood in the Netherlands caused serious damage over large areas of the country. On February 1st of that year, as a result of a storm surge combined with spring tide, i.e., a flood level that was increased by astronomical phenomena, the sea defenses in the south west of the Netherlands collapsed. There were 90 large holes and 500 smaller breaches in the dike system. Of the total length of 1000 km almost 500 km was damaged and 23 km was completely washed away. In the disaster 1835 people were killed and 72,000 people were evacuated. A year after the disaster 5565 persons still could not return to their homes. In addition, 47,000 cattle and 140,000 poultry were killed. Of the buildings, 3000 houses and 300 farms were completely destroyed and a further 40,000 houses and 3000 farms were damaged. The total expenditure was 1100 million guilders (Guilders 1953. Today's value: 8.4 billion Euro), of which 390 million guilders was for the repairs to the water defenses.

After the flood disaster in 1953, a commission called the DELTA commission was appointed to advise the government on measures to be taken to prevent the recurrence of such an event. The process that led to the final recommendations of the commissioners remains somewhat hazy. Several authors [5,6] suggest that for the probability of a flood, they found 1 in 10,000 a nice number and that the factor was chosen accordingly. From that followed the height of the defenses. The costs of the works would be 2 billion guilders to be spent over the duration of the works of 25 years, which the commission thought was reasonable given the costs of the 1953 disaster of about 1 billion. The yearly costs would be 0.5% of the GDP. There is no definitive information of what the commission had in mind with respect to the individual risk of death. The estimates on the basis of past floods amount to 1% of the population exposed given a flood [7], which makes the resulting average risk of drowning by floods for the Netherlands population $10^{-7}$/yr. and the maximum approximately $10^{-6}$/yr.

### *4.2. Industrial Risks*

In the late 1970s and early 1980′s several disasters occurred in the chemical industry. In Europe, it was decided to issue a directive to encourage the Member States to explicitly consider the hazards of chemical plants in decision making. The "Directive on Major Hazards" [8] initially only contained provisions regarding mandatory reporting on the hazards. This directive is commonly known as the Seveso directive. In later changes, the scope of the directive was extended to include considerations about probability, reflections on safety management and the obligation to take into account the potential hazards in spatial planning. The most recent version was adopted in 2012 [9].

In the Netherlands the discussion on how to deal with these risks culminated in the document "Premises for Risk Management" [10], which in the preliminary form, was presented as an annex to the Indicative Multi-annual Program for the Environment of 1986–1990 [11]. Later it was presented in the expanded form at the first National Environmental Policy Plan. "Premises"—as the document is commonly called—attempted to offer an organized general solution for risk problems.

In "Premises", limits for the acceptability of individual risks and societal risks were presented. The individual risk limits were among others based on the risk of traffic and the risk of floods. It was generally assumed that the average risk of drowning by floods for the Netherlands population was $10^{-7}$ [10] (p. 7).

Another argument was that the costs of the policy given these limits were not excessive. The maximum individual risk was set at $10^{-6}$/yr. For societal risk the limit, which was already set for LPG activities in 1983 [12], was extended to all man made "environmental (Risks that were in the policy remit of the ministry of environment. This included the safety of chemical installations and the transport of dangerous materials.)" risks—i.e., risks that were in the policy remit of the ministry of environment. This included the safety of chemical installations and the transport of dangerous materials—at $F = 10^{-3}/N^2$ per year where F is the cumulative frequency of accidents with N victims or more [10]. So, it was not a surprise that the major flood defenses adhered to the limits of "Premises" as these limits were in part derived from them. These obligations have been implemented in the Netherlands in the Decree on Major Accidents.

### *4.3. Floods Revisited*

In 1992 another commission was appointed to investigate whether the principles defined by the Delta commission were appropriate. This commission considered the individual risk explicitly and compared them with the risk limits for industrial installations, which were defined in "Premises for risk management [10]". The value derived by the commission was low, as compared to the $10^{-6}$ limit defined in "premises", and therefore they did not consider these risks a problem, even when taking the uncertainties into account [13] (p. 53)

In 2009 the responsibility for flood protection was put in an agency: The Delta Commissariat headed by the Delta Commissioner. All the dyke rings were listed together with the current estimates of the corresponding overtopping frequencies. In parliament it was announced that a further evaluation of risks would lead to an update of these values. The results of these updates prompted the government to rethink the necessary levels of flood protection. The overtopping frequencies were found not only to be much higher that originally assumed, but also they would increase further, due to rising sea levels.

The final word so far has been given in the letter of the minister of April 26, 2013 [14,15] in which the government states that the basis for the policy will be that nowhere, the local individual risk of drowning in a flood will be larger than $10^{-5}$. It is stated explicitly in this letter that this is higher than the limit for industrial installations. This is argued by the fact that flood risks have a natural cause and industrial risks are man-made. Lowering the risks further was deemed too costly although it should also be noted that whereas the original Delta committee deemed a yearly expenditure of 0.5% of the GDP a reasonable cost level, this cost of the water defenses in the early 21st century only amounted to 0.15% of the GDP.

The design criteria for the sea defenses were, and still are, expressed in design overtopping probabilities. Over time there has been considerable confusion as to what these numbers mean in terms of risk for people. Sometimes the probability of flooding is taken as equal to the probability of overtopping, sometimes it is taken as only 10% of these values, although in reality it may be higher. Similarly, the probability of drowning is taken sometimes as 1% of the probability of flood, sometimes as 10%. Sometimes the effect of evacuation is taken into account, sometimes it is not.

The assumption that on average the individual probability of death by drowning from flood was approximately $10^{-7}$/yr. seems to have been too low an estimate. The current design base maximum individual risk of death by floods in the Netherlands was $10^{-5}$/yr. Due to the distribution of the risks in the low-lying parts of the country the average individual risk was lower, but currently along the rivers the risk could be higher than $10^{-5}$.

### *4.4. Induced Earthquakes*

In 1959 an extensive gas reserve was discovered under the Netherlands; specifically, in the province of Groningen. The field proved to be one of the largest in the world. Many more fields were discovered since. They are much smaller. The state of the Netherlands developed joint ventures with private operators to develop and exploit these fields.

Extracting natural gas leads to compaction in the underground and thus to subsidence. In the 1960s it was thought that the subsidence would be some 20 cm. Ten years later the estimate was 100 cm, subsequently corrected to 25 cm (1974). In the years to follow the estimates rose and sank. The current estimate is 50 cm. In all cases it was claimed that there would be no earthquakes and Groningen would stay above sea level.

At the end of 1986 earthquakes started to occur. From then on, the rate of occurrence steadily increased, as did the maximum magnitude. These earthquakes are not only a continued nuisance and disturbing events for the citizens, they also have caused and still cause considerable damage. Although the population density is relatively low, there are some 200,000 houses in the area, many of which are designated monuments.

It took about 30 years before the government decided what to do about the earthquakes and the damage. Finally, in 2017, after the state council judged that the damage levels were unacceptable, it was decided to reduce gas extraction, pay for the damages and reinforce the houses in the exposed areas. For reducing the risk to $10^{-6}$/yr. it would have been necessary to demolish the existing houses and build new ones. This was considered too intrusive and too expensive. Therefore, rather than using the limit of industrial activities, the government used the maximum acceptable level for floods: $10^{-5}$/yr.

### *4.5. Upward Tendency*

It is often stated that the existence of limits of risk would lead to industries letting the risk drift upwards to the limit; and therefore, that limits of acceptability would increase in the longer term. It should be noted though that there are many instances where further limits are introduced to keep negative effects under control, or reduce them. The introduction of maximum speeds in traffic, reduces the consequences of all accidents and thus the frequency of serious accidents and the concentration limits of chemicals keep food quality and the addition of potential harmful additives under control. It is possible that in some isolated instances the effect is the opposite: people tend to drive at the maximum allowed speed even when it would be more prudent to reduce speed. However, on the whole a maximum speed is beneficial.

It should also be noted that under Roman law everything that is not explicitly forbidden is allowed [16]. Clear indications of what the limits are give certainty to entrepreneurs and the population alike, of what is allowed under the law and what is not. This makes processes such as applying and approving a permit largely predictable and gives all parties the legal certainty that forms one of the corner stones of the Roman law system.

### *4.6. Normative Approach*

From these examples it can be seen that a normative approach is possible, but meaningful levels of acceptability can only be set for defined categories of activities, such as major hazard industries, or the transport of hazardous materials.

If it is found that a risk is higher than anticipated—as is the case in the earthquake example—or is increasing—as in the sea defense example—it is often too costly or even completely unfeasible to reduce these risks to bring them in line with existing standards.

While the normative approach is a possible policy option that has several beneficial attributes, it is not always an acceptable policy option. For instance, it may be that the circumstances of an accident frame the acceptability of the risk. For instance, the acceptability of a risk associated with natural hazards such as dike failure caused by unprecedented high tides coupled with severe storms and snowmelt from the highlands, could well be more readily accepted than say a failure of a hydro dam due to mismanagement of the water, even if the numerical values of the preaccident risk are numerically similar.

## 5. As Low As Reasonably Practicable

Many countries have a policy that can be characterized by some form of as low as reasonably practicable (ALARP). In this realm there are more acronyms such as ALAP (as low as possible), ALARA (as low as reasonably achievable), SFAIRP (so far as is reasonably practicable), BPM (best practical means), BTM (best technical means), and BATNEEC (best available techniques not entailing excessive cost). Although they are generally thought of meaning the same thing, the differences are not just linguistic. Further, there is no law of nature that defines these terms, rather they are policy constructs. Their meaning and interpretation in practice is determined by the policy makers in a particular (macro) policy context. The use of one of these terms in one jurisdiction might well be slightly or even significantly different.

### *5.1. ALAP*

ALAP stands for as low as possible [17]. Although initially this was the aim policies directed at the protection of human lives and the environment against the collateral damage of not only technology but also medical procedures and diagnostics. The ALAP principle has its roots in ethical principles of medicine—do no harm—which go back centuries, and may even go back to Hippocrates [18]. However, not doing harm may come at a cost, the ultimate cost being not to embark on a venture that brings collateral damage, even if that venture also brings benefits. The medical corollary that the cure should be better than the illness translates into the more common cost benefit analysis. It should not only be possible—in principle—to lower the collateral damage, it should also be reasonably worth the cost. From this, two principles arise, which often are considered to be the same, but they really are not: ALARA (as low as reasonably achievable) and ALARP (as low as reasonably practicable).

### *5.2. ALARA*

The ALARA principle is directed at reducing the collateral damage as far as possible using reasonable efforts. The ALARA principle can demand a one-off solution to reduce or eliminate the collateral damage, which may have to be designed especially for this one occasion. This implies that one has to look for and investigate in each case whether a solution is possible and make a judgment whether the effort and expense can reasonably be demanded. A derivative of the ALARA principle, first promulgated by the Alkali Inspectorate in the UK in the 1870s, as best practical means, (BPM) [19], is the requirement of using the best technical means (BTM) [20]. In the ALARA approach costs are considered but the main consideration is whether it is technically feasible to reduce the collateral damage. If it is feasible it should be done.

### *5.3. SFAIRP, ALARP, and Tolerability of Risk*

The ALARP principle goes a step further towards considering the costs of damage reducing measures. The practicable element means that a solution should not be a one off. It should be applicable in other, similar situations and it should preferably be done before. The concept of best available techniques (BAT) falls under this approach. Best available techniques (BAT) are defined by EC Directive 96/61 [21] as: "the most effective and advanced stage in the development of activities and their methods of operation which indicates the practicable suitability of particular techniques for providing the basis for emission limit values designed to prevent, and where that is not practicable, generally to reduce the emissions and the impact on the environment as a whole". This definition implies that BAT not only covers the technology used but also the way in which the installation is operated, to ensure a high level of environmental protection as a whole. BAT takes into account the balance between the costs and environmental benefits.

ALARP is the acronym used worldwide for this principle. However, the original British formulation reads so far as is reasonably practicable (SFAIRP). The application and interpretation of the SFAIRP or ALARP principle leans heavily on a verdict on the case of Edwards v. National Coal Board in 1949 [22]. In the case the court stated that "Reasonably practicable is a narrower term than 'physically possible' and seems to me to imply that a computation must be made by the owner in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other; and if it be shown that there is a gross disproportion between them, the risk being insignificant in relation to the sacrifice—the (person on whom the duty is laid) discharges the onus on them (of proving that compliance was not reasonably practicable)". The ruling implied that the risk must be insignificant in relation to the sacrifice (in terms of money, time or trouble) required to avert it: risks must be averted unless there is a gross disproportion between the costs and benefits of doing so.

The application of SFAIRP in the United Kingdom is inextricably linked to the regulatory regime where the UK safety regulatory tradition, to which SFAIRP and ALARP belong, has always involved the regulator negotiating a safe situation with the duty-holder against the background of compulsory powers if the negotiation breaks down. This contrasts with other important approaches, which place critical reliance on fixed non-negotiable standards, conformity with which is held to be "safe".

In essence, SFAIRP implies that nothing is ever wholly "safe", but there has to be a process whereby duty-holders must show that they are doing whatever they reasonably can to reduce risk, taking into account what is technically possible, what is good practice, and what is the cost in money and trouble of doing better. Of course, the SFAIRP approach implies the existence of a powerful, well-informed, and challenging regulator. "Good practice" is regarded as the minimum requirement, so that, for example, a published standard that is accepted by the government will be regarded automatically as reasonably practicable and will be enforced by the regulator.

Although the Edwards judgment referred to a "computation", it did not describe how the computation might proceed. The term ALARP first arose with the UK Central Electricity Generating Board (CEGB) in the context of the British nuclear program as a numerical equivalent to SFAIRP. However, the manner in which the concept was used in the industry and interpreted and enforced by the regulator was considered by the Sizewell B Inquiry (1983–1986) to be incomprehensible to a public increasingly concerned at the risks posed by nuclear plants. The Sizewell Inspector demanded that UK Health and Safety Executive should describe the challenge process that it used in its function as nuclear regulator clearly and also explain why the public should accept the residual risks as "tolerable". The explanation needed to include both the technical and the political dimensions. On that basis, the company was sent away to redesign an automatic safety system to comply with their stated criteria.

The underlying philosophy implies from the start that some degree of risk is always present in any human activity and must be tolerated; and even adherence to good practice

will not alter that situation. A deterministic view that adherence to engineering standards and judgment can be accepted as sufficient in itself, is implicitly rejected. The view, often associated with the deterministic approach, that where a standard includes a numerical goal (as for example with exposure limits for chemicals) the number must be as low as is technically achievable, is also implicitly rejected. Thus, in the negotiation of exposure limits, the approach in the United Kingdom has been that it is best to recognize risk and commercial realities and to favor a higher number while relying on strict but flexible regulation to achieve the best available solution in particular circumstances. This does not exclude decisions that particular hazards should be banned altogether.

The approach assumes a malleable risk situation, and indeed, most situations in industry are malleable. Those that are less so, for example in the case of fixed structures with a long-life expectancy, and which can only be reinforced at great expense, are in principle less suited to the approach. An intermediate category is that of complex, large scale operating plant, as in the nuclear industry in relation to which the "Tolerability of Risk" (ToR) idea originated. Here the approach has been to establish the initial design process and also to secure the establishment and satisfactory maintenance of a "safety case", in reference to which modifications can take place with regulatory concurrence during the plant's lifetime. Such an approach is incorporated in the European Union's major hazard arrangements for non-nuclear high hazard plant. In the case of large fixed installations such as bridges or dams, the "Tolerability of Risk" approach has less applicability. In these latter cases the engineering is usually considerably less complex than in an operating nuclear power plant, and it is perfectly sensible to define an overall risk goal in numerical terms and design to it, while of course maintaining a careful watch to ensure that the risk situation does not deteriorate. In this context, the application of ALARP applies a largely static downward thrust to maintain the risk at an already low level.

When applied to the complex plant, both SFAIRP and ALARP incorporate a dynamic downward thrust, which seeks to ensure that avenues for risk reduction are identified at the design stage and during plant lifetime, and are undertaken if any increment of risk reduction is both technically feasible and its cost can be justified in terms of the expected reduction in risk.

This downward thrust implicit in SFAIRP and ALARP is expressed in the ToR diagram (Figure 1). The diagram incorporates an "ALARP area" below the limit of tolerability where the risk is considered to be tolerable in the interim, and above the area where the risk level is negligible or generally acceptable. The process of risk reduction operates in the "ALARP" area. The diagram also takes account of a secondary idea borrowed from the legal meaning of "SFAIRP", namely that it is not enough to accept a risk on the basis simply that the cost of further improvement is likely to exceed the associated gain in safety; there should be an element of "disproportion" in favor of risk reduction. This idea is incorporated in the ToR concept as applying (only) where the residual risk is thought to be in the upper part of the ALARP spectrum. It takes account of the fact that risk estimates are always approximate—implying that the real level of risk could exceed the limit of tolerability even if the available calculations suggest that this is not the case. This concept of "disproportion" means in effect that greater efforts have to be made and perhaps more expense incurred to get risk levels down so long as they remain high, i.e., not far below the limit of tolerability.

With the application of the ALARP principle, the costs therefore still must outweigh the benefits by a large margin, which is sometimes called excessive. This led to another principle, BATNEEC: best available techniques not entailing excessive cost.

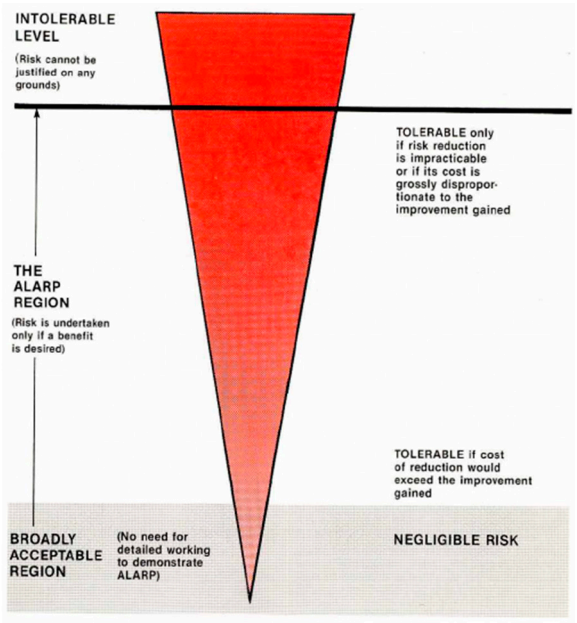


**Figure 1.** Tolerability of risk diagram [23].

### *5.4. BATNEEC*

The BATNEEC principle is used primarily in the UK's Environmental Protection Act and was a more nuanced version of the best practical means (BPM) [23]. Each company must have authorization from the regulatory body, before starting up a prescribed process, or continuing to operate an existing plant under the Environmental Protection (Prescribed Processes and Substances) Regulations 1991 and its subsequent amendments. The company must demonstrate that they are using the best available techniques not entailing excessive cost, (or equivalent to that prescribed in "Guidance Notes" by the regulator) to prevent and minimize the release of any prescribed substances and to render harmless any such release. Available, in this context, means procurable, that is generally accessible but does not necessarily imply that the technique is widely used or only available locally. Therefore, in BATNEEC "available" goes further than "practicable" in ALARP in that BATNEEC does not demand the application of solutions that are difficult to obtain.

### *5.5. Negotiability*

The ALARA type policies have in common that their aspirations and purposes are described in qualitative and often vague terms. What is best in terms of reasonable or practicable demands a judgment call. Such a judgment not only changes over time, for instance because the progress of technology makes techniques more readily available, it also varies depending on who makes the judgment. This is even more so for the expense or cost side of any argument. "Not Entailing Excessive Costs" is very subjective and each case is judged on its own merits. UK law does not provide fixed rules but it is expected that every effort be made to minimize the more serious pollutants. This inherent vagueness conforms to the common law tradition where, at least in principle and maybe with the exception of the maximum speed, nothing is really fixed in law. The real decisions are made by judges in court through verdicts on specific cases. As described earlier the whole concept of what is a reasonable expenditure hinges on a court case from 1949.

As noted previously, the complete absence of predictability worried the authorities in the UK already in the 1980s especially in the case of construction of new nuclear power plants, which met with significant opposition from the population, especially after the Chernobyl accident. In retrospect it is likely that the authorities feared that a court might squash their plans giving more weight to potential accidents and the damage thereof than the continued uninterrupted power supply using nuclear power. In any case the UK authorities curtailed their requirement for ALARP type demonstration by specifying the

boundaries of the negligible and the unacceptable. Only between these boundaries ALARP considerations would be applicable in the regulatory context. This does not mean that reasonably practicable risk reductions cannot be achieved within the negligible region, just that the authorities did not seek such demonstration. In the first version of "Tolerability of risk from nuclear power stations" only individual risk was considered [24]. Additionally, in risk criteria for land-use planning in the vicinity of major industrial hazards guidance was given on individual risk only. Setting standards for societal risk was deemed problematic. In 1992, in the second version of Tolerability of Risk from Nuclear Power Stations, HSE (Heath and Safety Executive) provided notional limits for societal risk based on a study on risk from transportation of explosives through ports [25], but HSE explicitly expressed its preference for a judgmental approach. As can be seen from the first report of the Advisory committee on Major Hazards [26], the idea of limiting the frequency of accidents was inspired by the Netherlands approach of designing sea defenses, which were based on the expected frequencies of certain high sea levels. In any case it is apparent from the documents that HSE considered certain risks to be broadly acceptable and the risk of nuclear power plants was among them.

As of 2005, the UK Health and Safety Executive revised the Safety Case Regulations and clarified the role of quantified risk assessment (QRA), within the safety case. The specific requirement to use "suitable and sufficient" QRA within the safety case was removed and the demonstration requirements focused not simply on ALARP but on the broader regulatory requirements, which were then fully in place to support the safety case requirements. In effect, rather than an abstract requirement simply to demonstrate major hazard risks are ALARP, the duty holder became required to demonstrate how the law is being complied with. The supporting legislation contained all the necessary requirements, which, if fully complied with, would ensure the installation is being operated safely.

### *5.6. Predictability*

The problem that remains is that the status of numerical limits is vague and therefore the decision to be expected on a particular risk problem, is highly unpredictable both for the public and for industry. Everything is open for negotiation and also can be renegotiated after a decision has been made. This means that nothing is ever final and procedures always involve lengthy negotiations.

As advantage of the ALARP approach over an approach with fixed limits is often stated that ALARP provides a dynamic downward force on risk [27]. There is an implicit assumption that risks are only taken for a reason, and that this reason is legitimate. However societal pressure may turn the ALARA principle around to mean as large as regulators allow [16] providing a dynamic upward force only to be stopped by some form of legal limitation.

For legacy risks the ALARP principle is a convenient approach. It provides the escape that "what is done is done". If it is impracticable to reduce the risk it can be allowed, and the practicability or the absence thereof is a situational and temporal judgment call.

## 6. Discourse

An alternative for a generally applicable policy approach is a case-by-case approach. The merits, costs, benefits, and all other relevant aspects of a decision are discussed with every stakeholder identified until a decision is made [27]. This discourse approach usually is reserved for complex, ambiguous problems, but in principle it is applicable to all problems and decisions.

A precondition for a successful application of the discourse approach is that parties have the intention to arrive at a decision and are prepared to at some point accept the result of the process. Given the uncertainty and unpredictability of the result such a commitment is often difficult to get. A discourse process also requires that stakeholders can trust each other. In the decades of discussions about further extensions of the airport near Amsterdam focus groups and joint committees were short lived, because the population found out

again and again that the authorities had already agreed with the airport to allow the extension and that the discourse was just meant to sell the decision [28]. These conditions put demands on the maintenance of correspondence between the various stakeholders before any discussion arises. It should be noted that these stakeholders often are involved in other discussions. The question whether the public trusts the government is a profound one. Interestingly, even if the population expresses mistrust in a government it might vote for their return at the next election. Therefore maintaining good, trusting relationships is a balancing act that has to be upheld over a long time and over many subjects, but is necessary for successfully finding an accepted solution for a future really sticky problem.

The alternative is that parties do not agree and the party with the most—political—power makes the decision go its way. That may solve the problem in the short run, but experience tells that the discussion then never goes away and the problem lingers on until the next time the discussion heats up again.

## 7. Legacy Risks

The discourse approach is especially suitable for legacy risks, especially when they are associated with large infrastructures, without which essential societal services such as electricity cannot be delivered. The discussion about these risks does not arise when the risks are generally accepted. The discussion arises because one of the stakeholders, be it the authorities, the corporation that owns or operates the infrastructure, or the public, finds out that there is a legacy risk that is larger than expected and would according to present standards, general opinion, or even the risk appetite of the corporation be deemed unacceptable.

There are decisions in the past that even at the time they were taken were misguided or even against the rule of law. However, these are exceptions. The introduction of DDT to kill off insects and especially the malaria mosquito was logical, legitimate, and had huge benefits at the time the decision was made. That, in the long run the collateral damage of building up harmful concentrations of the pesticide in higher organisms, mammals and humans would become apparent, could not be expected. Now that it is apparent, it proves impossible to ban the use of DDT globally and thus the discussion between those who are of the opinion that DDT cannot be missed to protect their crops and their health and those who are of the opinion that the collateral damage is serious to the extent that the costs exceed the benefits continues.

Similarly, infrastructure was costly at the time it was constructed. There is no reason to assume that the benefits exceeded the risks—as they were known at the time—and the costs. There is also no reason to assume that the risks were not acceptable at the time and given the fact that the infrastructure exists the risks were accepted generally, even if there was opposition at the time.

However, unknown risks may become known and risk may increase. Climate change and the associated increase in torrential rain and sea level rise may change the risks of high water and flooding. Additionally, the size of the potential damage may rise. The population behind the dykes in the Netherlands was 10 million in 1953, when the first decision on the height was made. Today it is 17 million. The increase in the value of the assets is even larger. Therefore the acceptability of the risks is periodically evaluated, and the costs and benefits of additional provisions. Where necessary, new works are put in place [14,29–31].

There is also the possibility that retrofitting an existing legacy facility to account for a recently discovered risk or a recent change in the magnitude of a previously known risk, might create a new risk that is difficult to quantify and is not necessarily of the same type as the risk that the retrofit accounts for. Such a situation might exist where civil works to improve river or canal discharge capacity can introduce new geotechnical risks in the foundation of the new discharge structure.

When these infrastructures are unique as is the case with hydropower dams, there also is no specific frame of reference to assess what level of risks are accepted elsewhere or earlier,

with similar structures, such as is possible with industrial installations handling hazardous chemicals. If moreover it is discovered that in the vicinity of these structures generally accepted levels of risks for the population are exceeded the situation gets really problematic.

## 8. Conclusions

Legacy risks from infrastructures and industrial installations often reveal themselves when a potential for failure has been discovered much later than at the stage of the design and construction of a structure. In which case, there might already be a problem with the legacy installation, or even a crisis, without having had an accident. When the hazard cannot be taken away, the question arises as to how much effort, if any, should be spent on improving the situation. In this paper we considered the usefulness of the three archetypical approaches to this problem: setting a standard, the ALARP approach and a case-by-case discourse approach.

Setting standards or acceptable levels of risk gives certainty to entrepreneurs and the population alike, of what is allowed under the law and what is not. This makes processes such as applying and approving a permit largely predictable and gives all parties the legal certainty that forms one of the corner stones of the Roman law system. It would be desirable if a legacy risk can be adapted to contemporary standards with reasonable effort and expenditure or even if the risk can be taken away, but more often than not the risk cannot be taken away or reduced in a cost-effective way.

Many countries—especially those who have a common law system—have a policy that can be characterized by some form of as low as reasonably practicable (ALARP). In this realm there are more acronyms such as ALAP, ALARA, SFAIRP, BPM, BTM, and BATNEEC. Although they are generally thought of meaning the same thing, the differences are not just linguistic. ALARP is the acronym used worldwide for this principle. However, the original British formulation reads so far as is reasonably practicable (SFAIRP). In essence, SFAIRP implies that nothing is ever wholly "safe", but there has to be a process whereby duty-holders must show that they are doing whatever they reasonably can to reduce risk, taking into account what is technically possible, what is good practice and what is the cost in money and trouble of doing better. Of course, the SFAIRP approach implies the existence of a powerful, well-informed and challenging regulator. When applied to complex plant, both SFAIRP and ALARP incorporate a dynamic downward thrust, which seeks to ensure that avenues for risk reduction are identified at the design stage and during the plant lifetime, and are undertaken if any increment of risk reduction is both technically feasible and its cost can be justified in terms of the expected reduction in risk. In practice though, large static infrastructures are left alone sometimes for decades and the downward thrust for risk, which can be applied to new developments, may not have applied to legacy infrastructures with the result that legacy risks are rarely spontaneously addressed.

An alternative for a generally applicable policy approach is a case-by-case approach. The merits, costs, benefits, and all other relevant aspects of a decision are discussed with every stakeholder identified until a decision is made. This discourse approach usually is reserved for complex, ambiguous problems, but in principle it is applicable to all problems and decisions. A precondition for a successful application of the discourse approach is that parties have the intention to arrive at a decision and are prepared to at some point accept the result of the process. The discourse approach is especially suitable for legacy risks, especially when they are associated with large infrastructures, without which essential societal services such as electricity cannot be delivered. The discussion about these risks does not arise when the risks are generally accepted. The discussion arises because one of the stakeholders, be it the authorities, the corporation that owns or operates the infrastructure or the public, finds out that there is a legacy risk that is larger than expected and would according to present standards, general opinion, or even the risk appetite of the corporation be deemed unacceptable. Unknown risks may become known and risk may increase. When these infrastructures are unique there also is no specific frame of reference

to assess what level of risks are accepted elsewhere or earlier, with similar structures, such as is possible with industrial installations handling hazardous chemicals.

Therefore in conclusion the only available solution to persistent legacy risk problems seems to be to have a thorough discussion with all relevant stakeholders until an agreement is in some way found. Although the result may not really satisfy all parties concerned, when a solution is found it is in the spirit of ALARP: the best reasonable solution available given the circumstances.

**Author Contributions:** Writing: All authors. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Data sharing not applicable.

**Acknowledgments:** The material of SFAIRP, ALARP and ToR benefited from the advice provided to the 2nd Author by J.D. Rimington, the former Director General of the UK Health and Safety Executive who led the development of the Tolerability of Risk approach.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Renn, O. *Risk Governance: Coping with Uncertainty in a Complex World*; Earthscan: New York, NY, USA, 2008; ISBN 9781844072927.
2. Bottelberghs, B. Risk analysis and safety policy developments in the Netherlands. *J. Hazard. Mater.* **2000**, *71*, 59–84. [CrossRef]
3. Ale, B.J.M. Risk analysis and risk policy in the Netherlands and the EEC. *J. Loss Prev. Process Ind.* **1991**, *4*, 58–64. [CrossRef]
4. Ale, B.J.M. Dealing with risks of fixed installations in the Netherlands. *Cryogenics* **1993**, *33*, 762. [CrossRef]
5. Ten Brinke, W.B.M.; Bannink, B.A. *Risico's in Bedijkte Termen, een Thematische Evaluatie van Het Nederlandse Veiligheidsbeleid Tegen Overstromen. (Dutch Dikes and Risk Hikes. A Thematic Policy Evaluation of Risks of Flooding in the Netherlands)*; RIVM rapport 500799002; RIVM National Institute for Public Health and the Environment: Amsterdam, The Netherlands, 2004.
6. Yska, D. Van Deltacommissie tot Deltacommissie: De rol van Adviescommissies in de Besluitvorming over Veiligheidsnormen voor Hoogwaterbescherming. Master's Thesis, University of Twente, Enschede, The Netherlands, 2009.
7. Jonkman, S.N. Loss of Life Estimation in Flood Risk Assessment, Theory and Applications. Ph.D. Thesis, Technische Universiteit Delf, Delft, The Netherlands, 2007.
8. Council of the European Union. *Council Directive 82/501/EEC of 24 June 1982 on the Major-Accident Hazards of Certain Industrial Activities*; 87/216/EEG (Pb EG 1987, L85) ("Seveso directive"); Council of the European Union: Strasbourg, France; Brussels, Belgium, 1982.
9. Council of the European Union. *Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the Control of Major-Accident Hazards Involving Dangerous Substances, Amending and Subsequently Repealing COUNCIL Directive 96/82/EC Text with EEA Relevance*; Council of the European Union: Strasbourg, France; Brussels, Belgium, 2012.
10. Tweede Kamer. *Omgaan met Risico's Vergaderjaar 1988–1989; (Premises for Risk Management Session 1988–1989)*; Tweede Kamer: Amsterdam, The Netherlands, 1988; p. 21137.
11. Tweede Kamer. *Indicatief Meerjarenprogramma Milieubeheer 1986–1990*; Tweede Kamer: Amsterdam, The Netherlands, 1986; pp. 166–167.
12. Integrale Nota LPG. *Tweede Kamer der Staten Generaal, Vergaderjaar 1983–1984*; SDU: Den Haag, The Netherlands, 1983; pp. 1–2.
13. Wijbenga, J.H.A.; Lambeek, J.J.P.; Mosselman, E.; Nieuwkamer, R.L.J.; Passchier, R.H. *Toetsing Uitgangspunten Rivierdijkversterkingen*; Delft University of Technology: Delft, The Netherlands, 1993.
14. Ministerie van Infrastructuur. *Letter of 26 april 2013, Ministerie van Infrastructuur IENM/BSK 2013/19920*; Ministerie van Infrastructuur: The Hague, The Netherlands, 2013.
15. Tweede Kamer. *Tweede Kamer der Staten-Generaal Vergaderjaar 2011–2012; Nr 27 625 Waterbeleid, Nr. 262 Motie Van de Leden Van Veldhoven en Lucas Voorgesteld*; Tweede Kamer: Amsterdam, The Netherlands, 2012.
16. Ale, B.J.M. Tolerable or Acceptable: A comparison of risk regulation in the UK and in the Netherlands. *Risk Anal.* **2005**, *25*, 231–241. [CrossRef] [PubMed]
17. International Standard EN ISO 14971-2012. Available online: http://www.bonnier.net.cn/download/d_20170814141318.PDF (accessed on 8 March 2021).
18. Primum Non Nocere. Available online: https://en.wikipedia.org/wiki/Primum_non_nocere (accessed on 13 January 2021).
19. Hill, M. The role of the British alkali and clean air inspectorate. In *International Comparisons in Implementing Pollution Laws*; Springer: Berlin/Heidelberg, Germany, 1983; pp. 87–106.

20. Council of the European Union. *Council Directive 86/280/EEC of 12 June 1986 on Limit Values and Quality Objectives for Discharges of Certain Dangerous Substances Included in List I of the Annex to Directive 76/464/EEC*; Council of the European Union: Strasbourg, France; Brussels, Belgium, 1982.
21. EC Directive 96/61. Available online: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A31996L0061 (accessed on 3 March 2021).
22. Edwards vs. The National Coal Board 1 A11 ER 743. 1949. Available online: https://en.wikipedia.org/wiki/Edwards_v_National_Coal_Board#:~{}:text=Edwards%20v.,fall%20in%20a%20coal%20mine (accessed on 3 March 2021).
23. Riley, P. The Principles of Environmental Law as They Affect Engineering Decision Making. *Eng. Manag. J.* **1996**, *1996*, 237–241.
24. Stone, A. The Tolerability of risk from nuclear power stations. Version 1. *Atom* **1988**, *11*, 8–9.
25. HSE. *The Tolerability of Risk from Nuclear Power Stations, Version 2*; Her Majesties Stationary Office: London, UK, 1992; ISBN 0118862681.
26. HSC. *Advisory Committee on Major Hazards, First Report*; Her Majesties Stationary Office: London, UK, 1976; ISBN 0118808842.
27. Hartford, D.N.D. Tolerability of Risk and ALARP: Origins, Intent and Implications for Dam Safety Assessment. In Proceedings of the ICOLD 2021 88th Annual Meeting of ICOLD & Symposium on Sustainable Development of Dams and River Basins; International Commission on Large Dams, New Delhi, India, 2 November–3 December 2020.
28. Steinmetz, S. *Schiphol, Biografie Van Een Luchthaven*; Atlas Contact: Amsterdam, The Netherlands, 2020; ISBN 9789045040226.
29. Di Bona, G.; Forcina, A.; Falcone, D.; Silvestri, L. Critical risks method (CRM): A new safety allocation approach for a critical infrastructure. *Sustainabilty* **2020**, *12*, 4949. [CrossRef]
30. Di Bona, G.; Silvestri, A.; De Felice, F.; Forcina, A.; Petrillo, A. An Analytical Model to Measure the Effectiveness of Safety Management Systems: Global Safety Improve Risk Assessment (G-SIRA) Method. *J. Fail. Anal. Prev.* **2016**, *16*, 1024–1037. [CrossRef]
31. *Maatschappelijke Kosten-Baten Analyse Waterveiligheid 21e Eeuw*; Report for the Dutch Goverement; Deltares: Delft, The Netherlands, 2011; 1204144-006-ZWS-0012, 31 March 2011. Available online: https://edepot.wur.nl/346743 (accessed on 3 March 2021).