MDRB Multi Disciplinary research bulletin: Volume 02, Issue 02 | April 2023 | ISSN 2583-5122 (online)

An overview and comparison of engineering disciplines' Safe-by-Design policies

Author: Asst. Prof. Zofail Hassan, NDIIT, New Delhi
CO- Author: Akhilesh Pal, Civil Engineer, Shobhit university

Abstract: In this article, we provide an overview of the Safe-by-Design concept and its practical implementation across a wide range of engineering disciplines. We talk about how these practises vary from one another, how they have things in common, and how they provide opportunities for mutual learning. We also suggest different approaches to put these disciplinary outlooks into context. Construction engineering, chemical engineering, aerospace engineering, urban engineering, software engineering, bio-engineering, nano-engineering, and finally cyber space engineering are the engineering disciplines that are taken into consideration in the order of historically developed technologies. The important technology is presented, the prominent risks are analysed, the societal challenge(s) are noted, and the relevant innovations in the area are discussed. Each discipline is then briefly introduced. The risk management techniques, design concepts that encourage safety or safety awareness, and related techniques or tools are explored within each field. Problems that the discipline's designers may encounter are emphasised. The discussion of possibilities and obstacles in addressing safety concludes each discipline. Investigations of similarities and contrasts amongst engineering fields focus on design techniques for which empirical data have been gathered. According to our argument, Safe-by-Design is best seen as a particular development of Responsible Research and Innovation, with a clear emphasis on safety in connection to other crucial engineering goals like well-being, sustainability, fairness, and affordability. By actively integrating safety concerns into engineering procedures and straddling the line between technological optimism and excessive caution, Safe-by-Design offers an intellectual space for social science and the humanities (SSH) to work on technology advancements and innovation. As a result, Safe-by-Design is a useful tool for shaping governance structures that accommodate and reward safety while fully accepting uncertainty. It is also a tool for policymakers and risk assessors.

Keywords: safe-by-design; secure-by-design; risk-based design; design for values; responsible research and innovation; uncertainty

1.0.Introduction

Funding has been growing for research and innovation concentrating on society's most urgent problems, such as poverty, climate change, renewable energy, mobility, and health difficulties [1]. These challenges include poverty, mission-oriented research, and UN Sustainable Development Goals. Furthermore, it is not anticipated that the technologies used to address these concerns would in and of themselves result in new issues and dangers. Therefore, key concepts in research and innovation governance, like Responsible Research and Innovation (RRI) [2] and Science With and For Society [3], advance the notion that research and innovation should be reflective, anticipatory, forward-looking, and responsive while also taking into account societal needs and public values [4-6].

Safety is a fundamental public value that influences technical advancements, and the RRI idea of "Safe-by-Design" is devoted exclusively to safety. Although it is still a new idea, it has to

be explicitly tested in practise and further developed. The primary tenet of Safe-by-Design is that, on all relevant metrics, avoiding damage is preferable than treating its effects, hence while innovating, we should aim to foresee hazards as much as possible in order to either prevent them from occurring or to reduce their possibility. As a result, we suggest that Safe-by-Design be seen as a heuristic notion that supports preventative design approaches and builds on the advantages of foresight, inclusiveness, and responsiveness as noted in the literature on the policies encouraging RRI. With this paradigm, risk and safety concerns may be approached in a forward-looking way that forces engineers and innovators to consider any possible risks and hazards that can arise during a product's lifecycle. Additionally, it encourages a more in-depth conversation about safety in the context of other significant public objectives, such as sustainability, well-being, fairness, and affordability, to which engineering design may contribute.The authors of this study, who include engineers from diverse fields, risk experts, experts on how science and society interact, as well as Dutch policymakers and risk regulators, have been talking about safe-by-design for a long time and are still talking about it today. In this article, we provide an overview of the Safe-by-Design idea and approach, or how safety has been conceptualised and operationalized in several engineering disciplines. We contend that Safe-by-Design may provide valuable insights for highlighting the importance of designing for the value of safety from the outset, while also taking other significant engineering values into consideration; this approach aids the designer and policy-maker in being more aware of the potential value conflicts and to address them as proactively as possible. As a result, it makes it easier to make educated choices concerning risks in both engineering and policy.It has always been difficult to lessen the uncertainties connected to the hazards that have been generated. Different ways have been explored to address this difficulty, ranging from employing probabilistic approaches focused on lowering the likelihood of certain dangers to adding a deterministic safety factor (as a recognition of uncertainties). Probabilistic techniques assume that engineers are familiar with the nature of the risk and are capable of calculating the likelihood that it will occur. The next step is to attempt to identify prospective scenarios, classify them into fault and event trees, illustrate how those scenarios can result in the system failing, and remove or, to the greatest extent feasible, decrease the likelihood of those scenarios occurring. When "knowledge of all failure mechanisms (as well as subsequent) unpleasant effects that may arise" is unavailable, however, things get more challenging [7]. This poses a control issue that is more broadly characterised by the Collingridge paradox: the more quickly new technologies are developed, the more acquainted we will get with them (and the hazards they pose), yet the less controllable they become [8]. Since the late 1980s, a new branch of research on the precautionary principle and consideration of caution in innovation has appeared in both academic literature and policy texts (PP). Since then, this idea has been a key topic in discussions about how to manage unknown risks. The Rio Declaration on Environment and Development (1992) has a key definition of the PP, which reads in part, "lack of complete scientific knowledge must not be used as a rationale for delaying cost-effective steps to avert environmental deterioration." The PP literature is replete with instances of "late lessons from early warnings," including as health issues linked to leaded gasoline and asbestos-containing building materials that were addressed years after the first issues were noticed [9]. The precautionary viewpoint, including its more complex interpretations, makes the assumption that it is mainly possible to foresee and minimise the hazards associated with new technology. This proves to be challenging in reality, and this is particularly true for new and developing technologies [10,11]. Trade-offs with other goals, such as equality, sustainability, and financial expenses, are also necessary for risk avoidance. As a result, talks concerning proportionality are always part of the prudence the PP advocates.

A recent movement in European policy is supporting the so-called innovation principle since the PP is often seen as being limiting for innovation (IP). For instance, a call for ideas for EU's Horizon 2020 programme specifically instructed academics to "confront the PP with the IP, by which possible advantages of innovation should be preferred when balanced against potential dangers." Strong proponents of innovation often counter that researchers cannot choose not to innovate at all due to potential hazards and that technical solutions are the best way to handle the risks of future innovations. The topic of how Safe-by-Design can strike a balance between encouraging innovation as much as possible and making sure that innovations don't pose hazards or have unintended effects is the subject of this study. How to connect such a broad normative starting point to the real-world problems that various engineering disciplines face is a crucial topic in this regard. We shall present an overview of several operationalizations of Safe-by-Design that have been factually implemented in this work. Safe-by-advantages, Design's disadvantages, and blind spots are highlighted by the cutting-edge implementations in several engineering fields. We suggest a technique for leveraging the Safe-by-Design idea moving forward in order to align innovation with caution, building on this study. Here, two points need to be made. First, depending on the academic sectors, the term "Safe-by-Design" has sometimes been referred to as "Safety-by-Design" or "Design for Safety" [12, 13]. We see these variations as mostly semantic in nature; the fundamental tenet of all of these strategies is to proactively identify and fix safety-related concerns. We shall continuously use Safe-by-Design throughout this essay. Second, although safety is the main emphasis of our conception, security-related topics will sometimes be implied as well. In our view, security includes a deliberate component, while safety is the aftermath of an accident. For instance, we included "vandal proof design," or designing against (deliberate) vandalism, in Table 1 where several design methodologies for creating safety have been considered. Security is an essential critical value that has to be expressly addressed, even if it is sometimes mentioned in our methods and conversations. Using the same scenario again, engineering designs may be the target of terrorist attacks or assaults by hostile governments even if "vandal proof design" aids in protecting against vandalism.

The structure of the essay is as follows. We first provide aquick overview of some of the main ideas in this paper (Section 2), then describe our study strategy (Section 3). Then, we provide a general overview of how Safe-by-Design is developed and used across many engineering fields (Section 4). Our many discoveries from various engineering fields come together in Section 5. Before listing a variety of design techniques we have seen from various engineering viewpoints, we first explore their differences and similarities (Table 1). The manifestations of various methods in various fields are then looked at (Table 2). In Section 6, we make our final argument that Safe-by-Design is best seen as a particular development of Responsible Research and Innovation, with an explicit emphasis on safety in connection to other crucial principles in engineering design. By actively integrating safety considerations into engineering practises while straddling the extremes of technological optimism and excessive caution, Safe-by-Design could thus offer an intellectual space where social science and humanities (SSH) can work together on technological developments and innovation

2.0.Basic Concepts

This article's main structure builds on a specific understanding of several basic concepts—engineering, safety and security, and addressing safety and security—which we will briefly introduce here.*Engineering*: Engineering is concerned with the creation of systems, devices, and processes. Engineering disciplines and professions apply scientific theories, mathematical models, and empirical evidence to design, create, and analyze

technological solutions useful to and sought by society. Engineers therefore need to be familiar with not only natural laws but also safety risks, juridical laws, and regulations as well as a wide variety of (human) factors pertaining to needs, values, perception, acceptance, usability, and costs. Engineering is conventionally subdivided into the branches of civil, chemical, electrical, and mechanical engineering [14]. The Accreditation Board for Engineering and Technol- ogy (ABET) distinguishes between engineering design and engineering science. They define engineering design as a process of devising a system, component, or process to meet desired needs and specifications within constraints [15–17]. It is an iterative, cre- ative, decision-making process in which the basic sciences, mathematics, and engineering sciences are applied to convert resources into solutions. Engineering design involves identifying opportunities, developing requirements, performing analysis and synthesis, generating multiple solutions, evaluating solutions against requirements, considering risks, and making trade-offs for the purpose of obtaining a high-quality solutions under the given circumstances. Engineering sciences are based on mathematics and basic sciences but carry knowledge further toward creative application needed to solve engineering problems. These studies provide a bridge between mathematics and basic sciences on the one hand and engineering practices on the other.

Safety and security: Safety is an important value in any engineering design. It is the

state of being "safe", the condition of being protected from harm, or other non-desirable outcomes. Safety can also refer to the control of recognized hazards to achieve an acceptable level of risk. These can be hazards of any type, including natural hazards, technological hazards, exposure hazards due to toxic emissions, and hazards caused by human action or inaction. Safety is distinct from security in that the former relates to unintentional and random factors, while the latter is related to intentional and malicious factors.

Addressing safety and security: Safety and security can be addressed at all phases of

the life cycle of any product, process, or system (i.e., plan, conceptual design, detailed design, optimized design, test, implement/build, operate, maintain, dispose, or reuse). By definition, Safe-by-Design concentrates on the plan and design phases. It aims at including safety as a value to be translated into design requirements from the earliest stages of product and process development onwards. This implies addressing questions such as the following: What could go wrong with this design in its intended or unintended use? Which components and structures are potentially dangerous? How can the design be adapted to prevent the occurrence of risks, for instance, by replacing, changing, or reducing components? If things do go wrong, how can adverse effects be prevented or controlled?

We approached this exploration of the significations given to Safe-by-Design with these understandings in mind. The following section describes our approach

3.0.Research Approach

Based on an inventory of meanings assigned to danger, safety, and Safe-by-Design at eight engineering faculties at the Delft University of Technology, we were able to identify similarities and contrasts in conceptions of Safe-by-Design as well as potentially transferrable insights from our study. Technology, Policy and Management (TPM), Industrial Design Engineering (IDE), Civil Engineering and Geosciences (CEG), Architecture and the Built Environment (A&BE), Applied Sciences (AS), Aerospace Engineering (AE), Mechanical, Maritime and Materials Engineering (3mE), and Electrical Engineering, Mathematics, and Computer Science (EEMCS) are among these faculties

(EEMCS). Representatives from each of these faculties provided the detailed disciplinary descriptors presented in Section 4 as a contribution to this inventory. The same set of questions, which were prepared together over the course of a series of workshops and meetings conducted between June 2018 and May 2020, were answered by every researcher. In these sessions, politicians from the Dutch Ministry of Infrastructure and Water Management and academics from the Dutch National Institute for Public Health and the Environment frequently addressed the idea of Safe-by-Design, the promise it contains, and the concerns it does not (simply) solve (RIVM).

The items 18tilized to gather relevant data for each field included in this research are shown in Box 1. These components provide the framework for bottom-up explanations of the significance that the disciplines attach to particular notions in order to comprehend how Safe-by-Design is or might be operationalized and to investigate the extent to which Safe-by-Design is currently in use. Our goal was to comprehend the safety risks that exist across disciplines and the requirements for addressing risks early on in research and innovation without overly directing those accounts based on an intricate and predefined notion of Safe-by-Design. By combining these accounts, it is possible to gain a thorough understanding of the relevant similarities and differences among these disciplines as well as the potential traits that each discipline may have that could contribute to a deeper understanding of the meaning(s) that Safe-by-Design may have. The co-authors of this essay and the subject matter experts who provided their disciplinary viewpoints are all (associate) professors in their respective disciplines who now or formerly worked at Delft University of Technology.

4.0.Disciplinary Perspectives

The eight subsections that follow provide a number of ways to think about safety hazards as a result of the research strategy that was previously explained. To help us further our conception of Safe-by-Design, individual co-authors were given and have exercised considerable latitude in elaborating what they see as the pertinent context of their disciplinary domain. The same is true of their conceptions of the system that their work is focused on and the future outlook of their discipline. As a result, this part demonstrates the most cutting-edge techniques in today's procedures for addressing safety hazards in quite different fields of research. If the Safe-by-Design conceptualization proposed here does not agree with the viewpoints discussed here, it is because there is still opportunity for development.

Let's make one more preliminary observation and say that this discipline categorization is a little rudimentary. We feel that at the current point of conceptualising Safe-by-Design, a finer and more precise grouping will needlessly confuse the conversation, even while this undoubtedly affects what safety concerns are recognised as well as the descriptions of how they are to be dealt with.*Construction Engineering*

5.0.Context: Human Factors in Distributed Settings

Buildings, infrastructure, and other engineering structures like wind turbines and pipelines are designed, engineered, and built by the building industry. This sector contributes around 10% of the nation's GDP in The Netherlands.These constructions fail all over the planet. Although there is an extremely minimal chance that any one person would die as a result of a structural collapse, failures are thought to raise the cost of building a structure by around 10%.When a structure is subjected to loads that are greater than it can withstand—such as wind, earthquake, live loads, etc.—a failure results.

Investigations have shown that collapses happen less often in columns and more frequently in foundations, floors, and facades. The structural design that was created before execution is often where failures are found. Failures may also happen during the design and building stages, as well as during usage. Although force majeure is a part in a lot of failure scenarios, the human element still plays a big role.According to the findings of many studies, design and construction mistakes throughout the building process were the primary reasons for collapses and other minor failures. According to Terwel and Janssen [18], organisational factors such as interactions between project partners, particularly a lack of communication and cooperation, a lack of control mechanisms, a lack of responsibility assignment, a lack of structural risk management, a lack of safety culture, and a lack of knowledge infrastructure are the main influencing factors for structural safety during the design and construction process..

6.0.Focus: Structural and Organizational Measures

The design and engineering portion of the construction business is known as structural engineering. According to estimates, these mistakes account for around 50% of structural breakdowns. The design process for the complex structural engineering system focuses on the following levels, which may be broken down into distinct categories:macro level: external elements like law, the environment, politics, and culture;Meso level: business and project elements including working environment and safety culture Micro level: human characteristics like skill, ability to handle stress, knowledge, and attitude.According to the Eurocodes, safety calculations in the European construction industry are based on load and material considerations. About 90% of failures are due to user mistake and design flaws, but these are not taken into account in the calculations. As a result, more non-structural and structural measures are required. Using ductile rather than brittle materials and over-designing the structure are two structural strategies that may boost structural safety (e.g., by adding redundant elements). A strong or resilient structure is one that won't completely collapse even after little harm has been done to it. Additionally, non-structural methods may improve structural safety. Examples include decreasing mistakes in the design process by the appointment of an integral design officer or skilled coordinating structural engineer, defining roles, and providing additional supervisory control actions. A minimal level of expertise may be guaranteed via certification for engineers.The nine guidelines listed below may further improve structural safety in upcoming building projects:Keep the building project and procedure simple; provide enough resources and qualified personnel to handle the project's complexity; Make a comprehensive list of duties, then tick each off as you perform them; Give the main function Object() { [native code] } sufficient accountability and responsibility; pursue routine kinds of cooperation; raise knowledge of safety;Ensure efficient information and knowledge exchange Implement a methodology for successful risk management;Support (international) efforts for structural safety and, if feasible, integrate them in contracts.The trade-offs that designers must make between costs and safety provide a serious challenge. A construction project includes a wide range of parties and players, and often, several small contractors are hired to do a task at the lowest cost. In addition, there is an anti-authoritarian ethos in the construction industry. The financial responsibility of the engineers is minimal and does not exceed the overall value of the contract. Safety precautions are often seen as extra expenses and are thus typically reactive in their application; precautions are adopted as soon as anything goes wrong.Outlook: Digitalization and AutomationOne challenge for the industry is increasing the use of RFID technology (radio fre- quency identification), BIM (building information modelling), and computers, all of which offer opportunities for complex design and increases

engineering speed. These technolo- gies may bring benefits [19] by improving real-time information visibility and traceability to the management of people, materials, and machinery for construction projects. However, the construction industry has been slow to adopt these technologies mainly because of the many technical, financial, and ethical hurdles involved. These technologies also require a thorough understanding and checking of designs.

7.0.Chemical Engineering

7.1.Context: Large-Scale Industry Response to Accidents and Pollution

The conversion of raw materials into other products is an issue for the chemical industry. Accidents in the process sector have the potential to destroy both property and human life [20]. The big accidents "Seveso," "Bhopal," and "Sandoz" are three examples. According to Taylor [21], chemical characteristics, operational problems, human mistake, or poor process design are the main contributors to accidents in the process sector.The chemical industry is now making significant investments in developing safer manufacturing processes and products. Alongside these initiatives, ever-stricter legal restrictions exist (such as REACH). Major chemical makers and suppliers, including BASF, DSM, Dow, and Evonik, are investing considerably in ethical production.In chemical process facilities that deal with hazardous materials, such as refineries and oil and gas (onshore and offshore) production installations, Safe-by-Design focuses on preventing leaks, spills, fires, explosions, equipment malfunction, over-pressures, over-temperatures, corrosion, and similar conditions.

7.2.Focus: Consolidated Principles for Safe and Green Chemistry

Process design is concerned with the selection and ordering of bulk resources to change materials in the appropriate physical and chemical ways. Process flow diagrams are used in the design process, and they often incorporate a material and energy balance that displays typical or design flowrates, stream compositions, and equipment pressures and temperatures. Additionally, the design includes piping and instrumentation diagrams that depict each and every pipeline, together with information on the piping class, pipe diameter, and valving, as well as the positions of the instruments and process control plans.The performance of the process industrial system is influenced by organisational and human variables in addition to its technical components. The process industry applies performance-shaping elements at descriptive, observational, and prescriptive levels to human performance at various task complexity levels and in a variety of safety culture categories.Seven qualitative factors for intrinsically safer design were suggested by Kletz [22]. Reduce the quantity of hazardous material present at any one moment (for example, by working in smaller batches);. Substitute: Using a less dangerous substance in place of an unsafe one (for example, washing with water and detergent instead of a flammable solvent);. Moderate: Lessening the intensity of an effect (e.g., employing a diluted rather than concentrated version of a substance, or using a cold liquid at high pressure instead of a gas);. Simplify: Getting rid of issues from the start rather than adding tools or features to address them. employing complicated techniques and fitting choices only when absolutely essential;. Increase fault tolerance by designing machinery and procedures to withstand potential flaws or design deviations.. Limit consequences: Modifying equipment design, placement, or transportation to make the worst-case scenario less dangerous (e.g., letting gravity carry leaks to safe locations; using bunds; preventing knock-on effects); Make foolproof: Prevent wrong assembly; make it simple to use.e following 12 principles were created as a consequence of Anastas and Warner's [23] addition of sustainability-related

considerations to the aforementioned seven operationally focused principles (preventing accidents): Less hazardous chemical synthesis, designing safer chemicals, safer solvents and auxiliaries, designing for energy efficiency, using renewable feedstocks, reducing derivatives, catalysis, designing for degradation, real-time analysis for pollution prevention, and inherently safer chemistry for accident prevention are just a few of the principles that should guide synthesis planning. These guidelines may be used in a variety of situations: fundamental rethinking of the design of chemical synthesis pathways is required for less dangerous chemical synthesises. One important pillar in this is new catalytic pathways that reduce the amount of synthesis steps. Other adjustments include utilising safer alternatives in place of hazardous (reactive or ecologically dubious) solvents and chemicals and employing catalysis to decrease reaction temperatures and hence lessen explosion risks. The use of novel ideas like flow chemistry or cascade reactions, which minimise the number of individual synthesis steps including downstream processing, is growing.eating more secure chemicals for use in higher-quality goods (i.e., lower amounts or absence of unidentified and potentially toxic by-products). A crucial component in reaching this objective is catalysis in particular. Additionally, utilising selective catalysts (particularly biocatalysts) enhances the reaction's selectivity, producing fewer or no unwanted byproducts. This eliminates or significantly lowers the need for stages in the derivatization process and the need to take auxiliaries out of the finished product.o "satisfy today's requirements without compromising the resources of future generations" [24], product production must be sustainable.Utilizing non-noble metal catalysts and auxiliaries will preserve fossil resources just as new energy-efficient syntheses will do the same (e.g., avoiding non-renewable phosphates or helium).Additionally, there is a growing tendency toward a more comprehensive definition of product performance. Although this phrase has typically been used to refer to the intended use of a certain product, it is now now being used to refer to the earlier and later stages of the product's life. For instance, novel feedstocks are being investigated as potential replacements for polymers made from fossil fuels. The present initiatives to create polymers with inbuilt preset breaking points to assist recycling and their natural breakdown if exposed to the environment are equally significant (avoiding massive accumulation of wastes in the oceans, for example).he goal of process designers is to increase throughput rate, process yield, and product purity while minimising space requirements, capital, operation, and maintenance expenses, safety problems, environmental implications, and the creation of pollutants and trash. The minimal levels of dependability, redundancy, flexibility, and expected unpredictability in input and output must also be taken into account. As instruments for loss prevention and risk management in chemical processes, a number of hazard indices have emerged. Each offers a relative, dimensionless index value that may be coupled with a decision analysis tool to determine priorities.Outlook: From Safety and Sustainability to Non-Toxic and Circular Economy

The future of chemical engineering is heading towards a circular economy in which “waste” as a concept will disappear. Wastes will be perceived as feedstocks for new products. Therefore, the design of tomorrow’s chemicals and materials should take sustainability into account. Chemicals and materials and their production processes must be:Based on non-depleting resources: that is, transitioning from fossil-based chemicals to renewable feedstock. Moreover, anthropogenic CO_2 will be used as feedstock.Non-toxic: necessitating more predictive models for structure-activity relationships.Non-persistent: built-in (bio)degradability of products that are ultimately distributed into the environment (e.g., consumer products such as cosmetics and active pharma- ceutical ingredients).In the chemical engineering domain, the above design principles are frequently used by academic and industrial researchers as a “tick list” to prove safety and “greenness”. However, a holistic

and quantitative evaluation and comparison with existing alternatives is necessary to be able to claim environmental, safety, or societal benefits.Today, some of the principles have been standardized in “life cycle analysis” ap- proaches (e.g., ISO 14040:2006), but these require extensive data and are consequently too laborious and costly for researchers. Simpler semi-quantitative methods such as the “E-factor” are available and should be used more frequently [25].Furthermore, several measures of inherent danger have been developed and are infurther development by researchers such as Gentile et al. [26], Khan and Amyotte [27], and Tugnoli et al. [28]. One of these measures is the DOW fire and explosion index (F&EI), which relies mainly on the material factor, consisting of the flammability and reactivity of chemical substances. The DOW F&EI assesses the hazardousness of a process unit (e.g., a storage tank) merely on the basis of the type and inventory of the contained chemical without considering the process unit’s impact on adjacent units via potential domino effects.Reliable metrics based on graph theory (e.g., out-closeness and betweenness) have therefore been developed to assess the criticality of process units with regard to domino ef- fects [29]. The integration of graph metrics with the DOW F&EI is expected to reflect a more realistic and accurate measure of the hazardousness of a process unit in chemical/process units, which in turn can be considered during the fail-safe/fail-secure designing of chemical plants or in the optimal allocation of safety/security measures.

8.0.Aerospace Engineering

8.1.Context: Integrated Sector and Safety Culture

One of the safest ways of transportation is commercial aviation [30]. Even though flying is generally safe, accidents do happen, and sometimes they result in a large number of casualties, which magnifies the impact that these events have on society and the public's impression of the safety of air travel. As a result, there is now a very strong safety culture in aviation, and several regulatory agencies are in charge of monitoring training programmes, aircraft maintenance, and design and operation. When compared to the number of final assembly manufacturers, the commercial aviation industry is characterised by a widely dispersed network of component suppliers and operations (airlines)..

9.0.Focus: Flight Control Systems as Part of a Layered Safety Approach

A multi-layered strategy called "Safe-by-Design" for aircraft covers a wide range of subjects, including material choice, structures, stability and control, fault detection and isolation, human-machine interface design, pilot training, air traffic control, maintenance, and certification. We will concentrate on the layered safety approach in general and on the design of flight control systems in particular due to the multiplicity of these many elements.The redundancy of crucial systems is the cornerstone of aeroplane safety. There are multiple redundant modes in the software systems, such as the multiple flight control laws in Airbus aircraft, as well as double, triple, and occasionally quadruple redundant systems for the critical flight control components (sensors, flight control computers, and control surfaces like elevators, flaps, or ailerons).The airframe itself is constructed in such a way that it is inherently stable in flight, in addition to the redundancy in subsystems. Thus, the aircraft will glide in a steady way and reject perturbations, such as those from gusts, even in the absence of any control surface or engine inputs from the human pilot or the automated pilot.Authorities in charge of airworthiness are also essential to aviation safety. They regulate the whole "chain," from design and production through operations and maintenance, including pilot licencing and air traffic control, and they make sure the aircraft complies the airworthiness standards. Airworthiness laws include a number of

safety-related design requirements, such as those relating to handling qualities (features of a flight vehicle that determine the ease and accuracy with which a pilot is able to complete a flying activity) [32]. In a certification procedure, aircraft manufacturers must prove that their products meet these requirements.Automation's involvement in preserving the safe flying envelope is a crucial decision in aircraft design. It is difficult for the pilot to provide the aircraft inputs that would be deemed to be too risky since Airbus has a greater automation philosophy that carefully monitors and checks pilot input. Boeing, on the other hand, has always placed a greater emphasis on manual control, giving pilots more latitude in how they fly while also alerting them when they are getting close to the edge of the safe flying envelope. Engineers' confidence in automation is reflected in this design decision. We see mishaps that were partially caused by people but might have been easily prevented by automation. Accidents have, however, also been predominantly brought on by automation, in which the human is so remote from the main functioning of the system that, even when automation is turned off, the lessened awareness of the (upset) situation still results in accidents.

10.0.Outlook: Safe Automation

Through the rising use of unmanned aerial vehicles and the development of intelligent adaptive flight control systems for manned aviation, such as personal air vehicles, recent years have seen a rise in the autonomy of aerial vehicles. The difficulty in creating autonomous aerial vehicles is dealing with operational phase circumstances (such as malfunctions or disturbances) that were not anticipated during the design phase. Human pilots operating these vehicles manually may modify their approaches to deal with these circumstances. The control system of a traditional automated flight control system is only intended to respond to predetermined, known circumstances; it is unable to change its course on its own.Designing adaptive control systems for autonomous cars may be done using the framework of machine learning methods known as reinforcement learning (RL), which is based on human-like learning through experience. Although there have been some early uses of RL in the construction of autonomous flight control systems [33,34], the key difficulty is ensuring the safety of learning. Errors must be committed in order to learn from them since real-world learning primarily involves trial and error. However, the errors must not be so severe that further learning is impossible. This problem is also known as safety of exploration in the literature [35].There is a trade-off between the control system's ability to adapt, which boosts aircraft safety in unforeseen circumstances, and the inherent dangers of learning from experience, which may lower safety. Future intelligent flight control system designers will need to strike a balance between the two and impose limitations to the adaptive system's authority or adaptability in order to assure safety. Since present laws are not created to accommodate adaptive systems, airworthiness authorities also play a significant role in this situation. This indicates that further work must be done on their end before these adaptive systems may get certification.

11.0.Urban Environment

11.1.Context: Crime Prevention as a Distinct Aspect in Urban Design

Secure-by-design in the urban built environment refers to how buildings and public areas are arranged and designed so as to either attract or deter criminal activities and unwanted conduct. The approach of modifying the built environment to produce safer areas is known as "crime prevention through environmental design" (CPTED). Around 1970 [36], when urban regeneration efforts were seen to be destroying the social structure necessary for

self-policing, it first appeared in the US. It is based on ideas from criminology and architecture (with the idea of "defensible space"). Robberies fell by 30–84% in US communities with CPTED efforts compared to those without them, according to Casteel and Peek-meta-analysis Asa's of multiple-component CPTED projects [37].The design firm, which includes architects, urban planners, members of the law enforcement community, and criminologists among others, focuses on the constructed urban environment. It focuses on physical modifications made to the built environment, but from a technical and sociological perspective that alters how people perceive danger, such as by adding trees and bushes, employing proper lighting, and promoting foot and bicycle traffic.

11.2.Focus: Inhibiting Crime

In the urban setting, three non-codified architectural concepts may raise levels of safety and security: Natural Surveillance: If people are aware that they are being watched, they are less likely to engage in aggressive or unlawful behaviour. This may be accomplished by maintaining enough lighting, stepping up presence in busy locations, and getting rid of hiding spots. The separation between public and private spaces may be clearly delineated by fence, planting, and signage to emphasise territorial borders and limit access. Vehicles is directed by well designated sections, and passing by non-local traffic is discouraged on private property. Maintenance: This is the swift removal of garbage and graffiti, the replacement of broken windows, the clearing of school halls, and the upkeep of the landscaping necessary to keep buildings in good condition. According to the theory, "signs of disorder" draw disorderly behaviour that might escalate to violent actions. Secure-by-design in the built environment necessitates standard measures like increased room, lighting, etc., which directly affect the price of developing such urban areas. The cost of implementing secure-by-design may be decreased when it is included at the initial design stage of the physical environment rather than thereafter. Modifying an existing environment to conform with the CPTED principles might be expensive. CPTED concepts become highly appealing and cost-effective by taking into account the possible cost reduction in crime prevention.

11.3.Outlook: Limits to Security?

There are opportunities to further improve secure-by-design principles' performance in urban settings and to derive new best practises. However, they are constrained by the issue of how much crime prevention is really necessary in a given location. How much freedom should a society give up in order to live without the worry of crime, often articulated in terms of freedom of movement and gathering options? Some stakeholders have said that a risk management strategy may be preferable than a strategy based on fear. In addition, the usage of video systems in public areas and the number of gated or guarded communities are increasing globally.

12.0.Software Engineering

12.1.Context: Safety as Performance Requirement

Software is used in an increasing number of societal activities. Therefore, it is crucial to make sure that such software is safe; that is, that it does not crash, that it is secure, that it functions as planned, and so on. Regrettably, software development is an error-prone process, and mistakes often find their way into finished products. As a result, fixing and maintaining flawed software costs a lot of money, and flaws that go undiscovered might

have severe repercussions (e.g., Heartbleed [38] and Toyota [39]). The Safe-by-Design approach emphasises the value of creating methods and tools early in the software development process to avoid software faults.Software must meet a variety of requirements depending on the application area in order to ensure its safety. The programme, for instance, has no flaws that may make it stop working or behave incorrectly (e.g., race conditions, dead locks, or buffer overflows).The programme operates in accordance with a description of its behaviour, meaning that given an input that fulfils P, the software will produce an output that satisfies Q.The programme complies with certain performance requirements, such as those relating to memory use or worst-case execution time (WCET).• The programme provides security features including availability, integrity, and secrecy.These rights may be violated, which may result in financial loss, loss of privacy, loss of life, or other accidents. To achieve a sufficient degree of confidence in these qualities, a suitable set of measures is needed.

12.2.Focus: Trade-Offs and Choices in Safety Approaches

Software safety is achieved via a mix of techniques used by software developers: dynamic evaluation and analysis This method verifies if software fulfils the necessary attributes by running it on a real platform (testing) or an instrumented platform (dynamic analysis). This strategy may be applied to the level of individual software modules (unit testing), interfaces between modules (integration testing), the whole programme (system testing), or the level of interaction between the software and the physical system (acceptance testing). Testing or dynamic analysis can never provide a guarantee that there are no software flaws since there are a limited number of inputs that can be tested. Therefore, it is essential to create representative tests that result in adequate coverage of the various software components. Analysis of static data and formal verification This method seeks to create attributes at the source code level without actually executing the programme. Static analysis or formal verification, in contrast to testing, can guarantee that properties hold for any input. There is a cost associated with this, however. This method typically establishes either fairly weak properties, like the absence of anomalies (through static analysis methods like abstract interpretation or type systems), in a fully automatic manner; or strong properties, like correct input/output behaviour (through formal verification methods like model checking, deductive verification, or theorem proving), with a significant amount of human guidance. Design patterns and coding conventions: This strategy uses reusable patterns for common issues (design patterns) and adheres to certain organisational standards to build software in an organised manner (coding conventions). This strategy often works in tandem with testing during the early stages of development (test-driven development) and employing static analysis to ensure that certain patterns are being utilised consistently (e.g., through linter tools).There are many options when using these strategies. What characteristics the programme should have is the first conundrum. While certain features, like the absence of anomalies, are independent of the application domain and simple to declare, others, like programme behaviour attributes, are reliant on the application domain and very challenging to define.The second conundrum is how to go about verifying these features. The amount of time/money needed, the type of properties that are guaranteed to hold, whether the properties are guaranteed to hold probabilistically or for any input, whether the properties hold for the real system or a model of the system, how much human guidance is required, and other factors all need to be considered.A variety of safety techniques should be employed to develop a combination of characteristics for application areas where safety is crucial. There isn't much agreement on what these combinations should be for conventional software, but for safety-critical software, numerous standards outline the techniques to follow in order to establish a specific degree of trust: DO-178B/C (airborne systems), IEC-15408 (security), IEC-61508

(electronic systems), and ISO-26262 (road vehicles).Outlook: Software Solutions for Software SafetyIn a perfect world, software engineers would devise methods for producing code that is 100% error-free. This, however, is not feasible. The first step would be to carefully define what it means for software to be "error-free," which is a challenging challenge that calls for foresight into every potential pitfall. Second, Rice's theorem [40] proves that it is impossible to automatically determine that software has non-trivial requirements even when such specifications are available. In other words, software engineers are unable to create a programme that verifies that a different programme has all the attributes they need. As a result, excluding software faults always requires human effort. Future research should focus on improving formal verification and static analysis techniques so that they can build more robust attributes with minimal human intervention. There has been significant progress made in this area during the last several years. For instance, programmers have been able to statically validate robust specifications of essential software like operating systems and compilers (CompCert) (L4verified).Additionally, enhancing the environment in which software is developed such that breaches of safety characteristics are found early on may serve as an alternative to depending on programming discipline and make software "Safe-by-Design." The development of safe software may be supported by a variety of complimentary approaches. Creating programming languages that are more suited for certain areas is one example.

13.0.Conclusions

It is difficult to conceptualise and implement Safe-by-Design in reality because of the variations and similarities among safety measures used in many engineering fields. On the one hand, all of the tales in are connected to very certain historical growth trajectories. It would be helpful to have a deeper awareness of these disciplinary and regulatory histories in order to comprehend how the value of safety is realistically applied in many professions. For example, establishing resilient societies that can withstand the stresses of a global pandemic or aligning safety standards with other crucial principles at the core of societal concerns need such context-specific knowledge. There is still much to learn about how to do this realistically, such how to uncover value overlaps or how to make decisions when trade-offs are inevitable. Some types of learning by doing must be avoided in order to advance due to the inherent constraints of anticipating. This might entail, for example, a collaboration between researchers, developers, and regulators to create, test, and evaluate how various safety-oriented design approaches and dedicated governance arrangements for ensuring safety and security perform in various contexts, as well as to look into the most effective ways to modify such approaches in response to both lessons learned and changing circumstances [83].On the other hand, this same diversity in the histories of the many disciplines necessitates the conceptualization of general aspects in Safe-by-Design methods. Here, new research directions could also take a more normative path, examining what it would entail if Safe-by-Design were used as a conceptual yardstick to compare disciplinary practises against rather than looking into the meanings Safe-by-Design is practically given in various fields and the reasons behind those. Thus, we present a first suggestion for such a Safe-by-Design conception as we wrap up this essay. This conception is based on all of the material that has come before it and on ideas from Section 1's discussion of the challenge of control in technological advancements.

14.0. Acknowledgement :I am thankful to god and my guide for giving me this opportunity in my life. I would also like to thank those who have directly or indirectly helped me in my work

.15.0.References

1. Schot, J.; Steinmueller, W.E. Three frames for innovation policy: R&D, systems of innovation and transformative change. *Res. Policy* **2018**, *47*, 1554–1567.
2. Stilgoe, J.; Owen, R.; Macnaghten, P. Developing a framework for responsible innovation. *Res. Policy* **2013**, *42*, 1568–1580. [CrossRef]
3. Van Oost, E.; Kuhlmann, S.; Ordóñez-Matamoros, G.; Stegmaier, P. Futures of science with and for society: Towards transformative policy orientations. *Foresight* **2016**, *18*, 276–296. [CrossRef]
4. Klaassen, P.; Rijnen, M.; Vermeulen, S.; Kupper, F.; Broerse, J. 4 Technocracy versus experimental learning in RRI. In *Responsible Research and Innovation: From Concepts to Practices*; Routledge: Oxfordshire, UK, 2018; pp. 77–98.
5. Taebi, B.; Correlje, A.; Cuppen, E.; Dignum, M.; Pesch, U. Responsible innovation as an endorsement of public values: The need for interdisciplinary research. *J. Responsible Innov.* **2014**, *1*, 118–124. [CrossRef]
6. Van de Poel, I.; Asveld, L.; Flipse, S.; Klaassen, P.; Scholten, V.; Yaghmaei, E. Company strategies for responsible research and innovation (RRI): A conceptual model. *Sustainability* **2017**, *9*, 2045. [CrossRef]
7. Van de Poel, I.; Robaey, Z. Safe-by-design: From safety to responsibility. *Nanoethics* **2017**, *11*, 297–306. [CrossRef]
8. Collingridge, D. *The Social Control of Technology*; Frances Pinter: London, UK, 1980.
9. EEA (European Environment Agency). *Late lLessons from Early Warnings: Science, Precaution, Innovation*; EEA Report No. 1/2013; EEA: Copenhagen, Denmark, 2013.
10. Randall, A. *Risk and Precaution*; Cambridge University Press: Cambridge, UK, 2011.
11. Hansson, S.O. The Precautionary Principle. In *Handbook of Safety Principles*; Möller, N., Hansson, S.O., Holmberg, J.E., Rollenhagen, C., Eds.; John Wiley & Sons: Hoboken, NJ, USA, 2018; Volume 9, pp. 258–283.
12. Serksnis, T. Safety by Design. In *Designing Electronic Product Enclosures*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 181–186.
13. Doorn, N.; Hansson, S.O. Design for the value of safety. In *Handbook of Ethics, Values and Technological Design*; Van den Hoven, J., Vermaas, P., van de Poel, I., Eds.; Springer: Dordrecht, The Netherlands, 2015; pp. 491–511.
14. Klein, G.; Elphinstone, K.; Heiser, G.; Andronick, J.; Cock, D.; Derrin, P.; Elkaduwe, D.; Engelhardt, K.; Kolanski, R.; Norrish, M. seL4: Formal verification of an OS kernel. *Commun. ACM* **2010**, *53*, 107–115. [CrossRef]
15. Pool, R. *Forum on Proposed Revisions to ABET Engineering Accreditation Commission General Criteria on Student Outcomes and Curriculum (Criteria 3 and 5): A Workshop Summary*; National Academies Press: Washington, DC, USA, 2016.
16. Olson, S. *Engineering Societies and Undergraduate Engineering Education: Proceedings of a Workshop*; National Academies Press: Washington, DC, USA, 2017. [CrossRef]

17. ABET. Criteria for Accrediting Engineering Programs, 2019–2020. Available online: https://www.abet.org/accreditation/ accreditation-criteria/criteria-for-accrediting-engineering-programs-2019--2020/ (accessed on 16 April 2020).

18. Terwel, K.C.; Jansen, S.J. Critical factors for structural safety in the design and construction phase. *J. Perform. Constr. Facil.* **2015**,

29, 04014068. [CrossRef]

19. Zhang, S.; Sulankivi, K.; Kiviniemi, M.; Romo, I.; Eastman, C.M.; Teizer, J. BIM-based fall hazard identification and prevention in construction safety planning. *Saf. Sci.* **2015**, *72*, 31–45. [CrossRef]

20. Crowl, D.A.; Louvar, J.F. *Chemical Process Safety: Fundamentals with Applications*, 3rd ed.; Pearson Education: London, UK, 2011.

21. Taylor, J.R. Statistics of design error in the process industries. *Saf. Sci.* **2007**, *45*, 61–73. [CrossRef]

22. Kletz, T.A. *Cheaper, Safer Plants or Wealth and Safety at Work: Notes on Inherently Safer and Simpler Plants*; The Institution of Chemical Engineers: Rugby, Warwickshire, UK, 1985.

23. Anastas, P.T.; Warner, J.C. *Green Chemistry Theory and Practice*; Oxford University Press: New York, NY, USA, 1998.

24. Brundtland, G.H. *Our Common Future*; Oxford University Press: Oxford, UK, 1987.

25. Sheldon, R.A. The E factor 25 years on: The rise of green chemistry and sustainability. *Green Chem.* **2017**, *19*, 18–43. [CrossRef]

26. Gentile, M.; Rogers, W.; Mannan, M. Development of a fuzzy logic-based inherent safety index. *Process Saf. Environ. Prot.* **2003**,*81*, 444–456. [CrossRef]

27. Khan, F.I.; Amyotte, P.R. How to make inherent safety practice a reality. *Can. J. Chem. Eng.* **2003**, *81*, 2–16. [CrossRef]

28. Tugnoli, A.; Cozzani, V.; Landucci, G. A consequence based approach to the quantitative assessment of inherent safety. *AIChE J.***2007**, *53*, 3171–3182. [CrossRef]

29. Khakzad, N.; Landucci, G.; Reniers, G. Application of Graph Theory to Cost-Effective Fire Protection of Chemical Plants During Domino Effects. *Risk Anal.* **2017**, *37*, 1652–1667. [CrossRef] [PubMed]

30. Hubbard, S. Safety Culture: Examination of Safety Attitudes Across Transportation Modes. *Transp. Res. Rec.* **2016**, *2582*, 61–71.[CrossRef]

31. Goupil, P. AIRBUS state of the art and practices on FDI and FTC in flight control system. *Control Eng. Pract.* **2011**, *19*, 524–539.[CrossRef]

32. De Florio, F. *Airworthiness: An Introduction to Aircraft Certification and Operations*, 3rd ed.; Elsevier: Oxford, UK, 2016.

33. De Vries, P.S.; Van Kampen, E.-J. Reinforcement learning-based control allocation for the innovative control effectors aircraft. In Proceedings of the AIAA Scitech 2019 Forum, San

Diego, CA, USA, 7–11 January 2019.

34. Helmer, A.; de Visser, C.C.; Van Kampen, E.-J. Flexible Heuristic Dynamic Programming for Reinforcement Learning in Quad-Rotors. In Proceedings of the AIAA Information systems—AIAA, Kissimmee, FL, USA, 8–12 January 2018.

35. Garcıa, J.; Fernández, F. A comprehensive survey on safe reinforcement learning. *J. Mach. Learn. Res.* **2015**, *16*, 1437–1480.

36. Oscar, N. *Defensible Space: Crime Prevention through Urban Design*; Macmillan: New York, NY, USA, 1972.

37. Casteel, C.; Peek-Asa, C. Effectiveness of crime prevention through environmental design (CPTED) in reducing robberies. *Am. J. Prev. Med.* **2000**, *18*, 99–115. [CrossRef]

38. Durumeric, Z.; Li, F.; Kasten, J.; Amann, J.; Beekman, J.; Payer, M.; Weaver, N.; Adrian, D.; Paxson, V.; Bailey, M. The matter of heartbleed. In Proceedings of the 2014 Conference on Internet Measurement Conference, Vancouver, BC, Canada, 5–7 November 2014; pp. 475–488.

39. Koopman, P. A Case Study of Toyota Unintended Acceleration and Software Safety. Ph.D. Thesis, Carnegie Mellon University, Pittsburgh, PA, USA, 18 September 2014.

40. Hopcroft, J.E.; Motwani, R.; Ullman, J.D. *Introduction to Automata Theory, Languages, and Computation*; Addison-Wesley: Boston,MA, USA, 2006.

41. Schmidt, M. Diffusion of synthetic biology: A challenge to biosafety. *Syst. Synth. Biol.* **2008**, *2*, 1–6. [CrossRef]

42. Robaey, Z. *Dealing with Risks of Biotechnology: Understanding the Potential of Safe-by-Design*; Dutch Ministry of I&W: The Hague, The Netherlands, 2018.

43. Stemerding, D.; Betten, W.; Rerimassie, V.; Robaey, Z.; Kupper, F. Future making and responsible governance of innovation in synthetic biology. *Futures* **2019**, *109*, 213–226. [CrossRef]

44. Asin-Garcia, E.; Kallergi, A.; Landeweerd, L.; dos Santos, V.A.M. Genetic Safeguards for Safety-by-design: So Close Yet So Far.*Trends Biotechnol.* **2020**, *38*, 1308–1312. [CrossRef]

45. Teunisse, W.; Robaey, Z.; Asveld, L. Potentiële Safe-by-Design Strategieën door Directed Evolution. Onderzoeksrapport voor het Ministerie van Infrastructuur en waterstaat. 2019. Available online: https://www.rijksoverheid.nl/documenten/rapporten/2019/12/13/potentiele-safe-by-design-strategieen-door-directed-evolution (accessed on 10 June 2021).

46. Robaey, Z.; Spruit, S.L.; Van de Poel, I. The Food Warden: An Exploration of Issues in Distributing Responsibilities for Safe-by-Design Synthethic Biology Applications. *Sci. Eng. Ethics* **2017**, *24*, 1673–1696. [CrossRef]

47. Bouchaut, B.; Asveld, L. Safe-by-Design: Stakeholders' Perceptions and Expectations of How to Deal with Uncertain Risks of Emerging Biotechnologies in the Netherlands. *Risk Anal.* **2020**, *40*, 1632–1644. [CrossRef] [PubMed]

48. Salameh, S.; Gomez-Hernandez, J.; Goulas, A.; Van Bui, H.; van Ommen, J.R. Advances

in scalable gas-phase manufacturing and processing of nanostructured solids: A review. *Particuology* **2017**, *30*, 15–39. [CrossRef]

49. Buffat, P.; Borel, J.P. Size effect on the melting temperature of gold particles. *Phys. Rev. A* **1976**, *13*, 2287. [CrossRef]

50. Monikh, F.A.; Chupani, L.; Vijver, M.G.; Vancová, M.; Peijnenburg, W.J. Analytical approaches for characterizing and quantifying engineered nanoparticles in biological matrices from an (eco) toxicological perspective: Old challenges, new methods and techniques. *Sci. Total Environ.* **2019**, *660*, 1283–1293. [CrossRef]

51. Jantunen, A.P.K.; Gottardo, S.; Rasmussen, K.; Crutzen, H.P. An inventory of ready-to-use and publicly available tools for the safety assessment of nanomaterials. *NanoImpact* **2018**, *12*, 18–28. [CrossRef]

52. Soeteman-Hernandez, L.G.; Apostolova, M.D.; Bekker, C.; Dekkers, S.; Grafström, R.C.; Groenewold, M.; Handzhiyski, Y.; Herbeck-Engel, P.; Hoehener, K.; Karagkiozaki, V. Safe innovation approach: Towards an agile system for dealing with innovations. *Mater. Today Commun.* **2019**, *20*, 100548. [CrossRef]

53. Morose, G. The 5 principles of "design for safer nanotechnology". *J. Clean. Prod.* **2010**, *18*, 285–289. [CrossRef]

54. Yan, L.; Zhao, F.; Wang, J.; Zu, Y.; Gu, Z.; Zhao, Y. A Safe-by-Design strategy towards safer nanomaterials in nanomedicines. *Adv. Mater.* **2019**, *31*, 1805391. [CrossRef] [PubMed]

55. Zhang, Q.; Huang, J.Q.; Qian, W.Z.; Zhang, Y.Y.; Wei, F. The road for nanomaterials industry: A review of carbon nanotube production, post-treatment, and bulk applications for composites and energy storage. *Small* **2013**, *9*, 1237–1265. [CrossRef] [PubMed]

56. Reijnders, L. Safer-by-design for nanomaterials. In *Nanotoxicity*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 215–237.

57. Galfetti, L.; De Luca, L.; Severini, F.; Meda, L.; Marra, G.; Marchetti, M.; Regi, M.; Bellucci, S. Nanoparticles for solid rocket propulsion. *J. Phys. Condens. Matter* **2006**, *18*, S1991. [CrossRef]

58. Liu, X.T.; MU, X.Y.; WU, X.L.; Meng, L.X.; Guan, W.B.; Qiang, Y.; Hua, S.; Wang, C.J.; LI, X.F. Toxicity of multi-walled carbon nanotubes, graphene oxide, and reduced graphene oxide to zebrafish embryos. *Biomed. Environ. Sci.* **2014**, *27*, 676–683.

59. Ma-Hock, L.; Strauss, V.; Treumann, S.; Küttler, K.; Wohlleben, W.; Hofmann, T.; Gröters, S.; Wiench, K.; van Ravenzwaay, B.; Landsiedel, R. Comparative inhalation toxicity of multi-wall carbon nanotubes, graphene, graphite nanoplatelets and low surface carbon black. *Part. Fibre Toxicol.* **2013**, *10*, 23. [CrossRef]

60. Hanley, C.; Thurber, A.; Hanna, C.; Punnoose, A.; Zhang, J.; Wingett, D.G. The influences of cell type and ZnO nanoparticle size on immune cell cytotoxicity and cytokine induction. *Nanoscale Res. Lett.* **2009**, *4*, 1409–1420. [CrossRef]

61. Nel, A.E.; Mädler, L.; Velegol, D.; Xia, T.; Hoek, E.M.; Somasundaran, P.; Klaessig, F.; Castranova, V.; Thompson, M. Understanding biophysicochemical interactions at the

nano–bio interface. *Nat. Mater.* **2009**, *8*, 543–557. [CrossRef]

62. Rabolli, V.; Thomassen, L.C.; Princen, C.; Napierska, D.; Gonzalez, L.; Kirsch-Volders, M.; Hoet, P.H.; Huaux, F.; Kirschhock, C.E.; Martens, J.A. Influence of size, surface area and microporosity on the in vitro cytotoxic activity of amorphous silica nanoparticles in different cell types. *Nanotoxicology* **2010**, *4*, 307–318. [CrossRef]

63. Savolainen, K.; Alenius, H.; Norppa, H.; Pylkkänen, L.; Tuomi, T.; Kasper, G. Risk assessment of engineered nanomaterials and nanotechnologies—A review. *Toxicology* **2010**, *269*, 92–104. [CrossRef]

64. Kane, G.; Bakker, C.; Balkenende, A. Towards design strategies for circular medical products. *Resour. Conserv. Recycl.* **2018**, *135*,38–47. [CrossRef]

65. Hansen, S.F.; Sørensen, S.N.; Skjolding, L.M.; Hartmann, N.B.; Baun, A. Revising REACH guidance on information requirements and chemical safety assessment for engineered nanomaterials for aquatic ecotoxicity endpoints: Recommendations from the EnvNano project. *Environ. Sci. Eur.* **2017**, *29*, 14. [CrossRef] [PubMed]

66. Schwirn, K.; Tietjen, L.; Beer, I. Why are nanomaterials different and how can they be appropriately regulated under REACH?*Environ. Sci. Eur.* **2014**, *26*, 4. [CrossRef]

67. Labille, J.; Feng, J.; Botta, C.; Borschneck, D.; Sammut, M.; Cabie, M.; Auffan, M.; Rose, J.; Bottero, J.-Y. Aging of TiO_2 nanocomposites used in sunscreen. Dispersion and fate of the degradation products in aqueous environment. *Environ. Pollut.* **2010**, *158*, 3482–3489. [CrossRef] [PubMed]

68. Sarkawi, S.; Dierkes, W.K.; Noordermeer, J.W. Elucidation of filler-to-filler and filler-to-rubber interactions in silica-reinforced natural rubber by TEM Network Visualization. *Eur. Polym. J.* **2014**, *54*, 118–127. [CrossRef]

69. Siriwardena, P. Security by design. In *Advanced API Security*; Apress: Berkeley, CA, USA, 2014; pp. 11–31.

70. Cavoukian, A. *Privacy by Deisgn*; Information and Privacy Commissioner of Ontario: Ottawa, ON, Canada, 2009.

71. Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed.; Wiley: Indianapolis, IN, USA, 2008.

72. Pieters, W. Security. In *Routledge Handbook of Philosophy of Engineering*; to appear; Routledge: London, UK, 2020.

73. Van den Hoven, J.; Blaauw, M.; Pieters, W.; Warnier, M. Privacy and information technology. In *The Stanford Encyclopedia of Philosophy, Summer 2018 ed.*; Zalta, E.N., Ed.; Metaphysics Research Lab, Stanford University: Stanford, CA, USA, 2018.

74. Sindre, G.; Opdahl, A.L. Eliciting security requirements with misuse cases. *Requir. Eng.* **2005**, *10*, 34–44. [CrossRef]

75. Petitcolas, F.A.P. Kerckhoffs' Principle. In *Encyclopedia of Cryptography and Security*; van Tilborg, H.C.A., Jajodia, S., Eds.; Springer: Boston, MA, USA, 2011.

76. OWASP. *A Guide to Building Secure Web Applications and Web Services (ver. 2.0.1)*; Free

Software Foundation: Boston, MA, USA, 2005.

77. Kirlappos, I.; Parkin, S.; Sasse, M.A. "Shadow Security" as a tool for the learning organization. *ACM SIGCAS Comput. Soc.* **2015**,*45*, 29–37. [CrossRef]

78. Pieters, W.; Hadžiosmanović, D.; Dechesne, F. Security-by-experiment: Lessons from responsible deployment in cyberspace. *Sci. Eng. Ethics* **2016**, *22*, 831–850. [CrossRef]

79. Sanders, W.H. Quantitative security metrics: Unattainable holy grail or a vital breakthrough within our reach? *IEEE Secur. Priv.***2014**, *12*, 67–69. [CrossRef]

80. Ahmed, M.A.; van den Hoven, J. Agents of responsibility—Freelance web developers in web applications development. *Inf. Syst.Front.* **2010**, *12*, 415–424. [CrossRef]

81. Bauer, J.M.; Van Eeten, M.J. Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommun. Policy* **2009**, *33*,706–719. [CrossRef]

82. Rutherford, D.B., Jr. What do you mean it's fail safe? In Proceedings of the Rapid Transit Conference, Atlanta, Georgia; 1990.

83. Evans, S.W.; Beal, J.; Berger, K.; Bleijs, D.A.; Cagnetti, A.; Ceroni, F.; Epstein, G.L.; Garcia-Reyero, N.; Gillum, D.R.; Harkess, G. Embrace experimentation in biosecurity governance. *Science* **2020**, *368*, 138–140. [CrossRef] [PubMed]

84. Van den Hoven, J.; Vermaas, P.E.; Van de Poel, I. *Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains*; Springer: Dordrecht, The Netherlands, 2015.