About Concept of Big Safety

V.S. Kharchenko
National Aerospace University "KhAI", Kharkiv, Ukraine
v.kharchenko@csn.khai.edu
•
M.A. Yastrebenetsky
State Scientific and Technical Center for Nuclear
and Radiation Safety, Kharkiv, Ukraine
ma.yastreb2013@gmail.com

Abstract

Concept of Big Safety (BS) is discussed. BS is a result of crossing of the following 10 Bigs: Big property (nuclear safety, radiation safety, functional safety, information (cyber) security, fire safety, physical security, infection safety, safety from natural hazards, etc.); Big/complex environment (a lot of factors of influence and parameters); Big/complex system; Big value of a fatal failure or event; Big number of causes of failure; Big data to be processed; Big number of requirements to safety; Big time and process complexity of system development ; Big toolbox for safety assessment and assurance; Big resources for assurance and recovery. General principles and methods for assessing and assurance of Big Safety are described considering experience of different critical domains, first of all, NPPs. Some well-known accidents in the context of Black Swan theory are analyzed. Strategies of Black Swan tolerance are proposed.

Keywords: Big safety, cyber security, infection safety, diversity, defense-in-depth, Black Swan.

I. Introduction

Over the last 12 months, the global news trend is related to the COVID-19 pandemic, which affects hundreds of thousands of people every day on all continents. The pandemic has caused a serious economic crisis, the effects of which have yet to be assessed, survived and returned to the growth point. It certainly affects the stable functioning of entire industries and industrial facilities, including those commonly referred to as critical, such as aviation, maritime and railway transport, chemical plants and oil and gas utilities, nuclear power plants, etc. These circumstances make it is necessary to address the safety of critical objects and the systems that control them in the face of new COVID-19-related and not related challenges.

This paper is an elaboration of the ideas of the [1] written at the beginning of the coronavirus quarantine and dealt with the safety of nuclear power plants (NPP) and the so-called Big Safety in the time of COVID-19. The authors began to develop the concept of Big Safety (BS), which integrates different kinds of safety of information and control systems (ICS), controlled objects and infrastructures, and formulated some provisions of Big Safety taking into account its new component - infection safety. We had some doubts as to whether such issues would be relevant in the context of coronavirus in a few months' time. Unfortunately, it is even more urgent now given, first, the dynamics of the pandemic and, second, the global safety challenges that have developed before and during the pandemic.

In addition, this paper is a natural extension of the results obtained over, the past decades and published in two books by US publisher IGI Global in 2014 and 2020 [2,3]. They focus on the functional safety and information (cyber) security aspects of NPP ICS. NPPs and their multiple control systems are perhaps one of the most complex, critical and well developed from safety point of view objects. NPPs, in turn, are part of the critical energy infrastructure and the critical infrastructure of the state as a whole, and are therefore an excellent case study for understanding Big Safety.

An additional motivation was also that this problem is now being addressed at many online events. In particular, at the 11th International IEEE Conference "Dependable Systems, Services and Technologies" professor A. Rucinski [4] held a round table "Trusted Dependability, Safety and Security in COVID-19 Time", which started the formation of a platform dedicated to the discussion of BS by experts from Ukraine, USA, UK, France, FRG, Poland, Bulgaria and other countries.

There are two trends in every science - centrifugal (aimed at clarifying and justifying ways of solving problems related to specific classes of objects and their individual properties, in particular safety components) and centripetal (aimed at combining and generalizing the to a broader class of objects the results obtained). Colossal number of papers have been written on various aspects of safety. In late 2020, the number of references to the word "Safety" on the Internet was 3.010.000.000, to the word Security - 6.630.000.000. Note that the number of articles and references on the Internet, to combinations of these terms with such popular ones as "Bid Data", "Internet of Things", "Artificial Intelligence" is growing very fast, - only for 2017-2019 their number has increased by ten times [5], For example, the number of citations for phrase "Big Data for safety" increased by 7.2 times (123.000.000 citation in 2018). Some aspects of application of Internet of Things, Big Data technologies for safety of critical systems, in particular NPPs. were addressed in [6,7].

There are disproportionately fewer works on general safety issues. to which this article is devoted. Close to our ideas is the book "Reliability of power systems" [8], by Y. Rudenko and I. Ushakov, where a methodical approach to the analysis of reliability of various power systems, including coal, oil and gas systems, is used. Besides, many papers view aspects of complex safety considering different types of influence on systems and complexity of the systems, for example [9,10]. Papers [11-13] discuss directions of safety science and describe methods of scientometric mapping for the safety science community taking into account huge number of publications.

This paper belongs the centripetal trend. Methodological aspects of safety analysis of large critical systems, such as rocket and space complexes, have been studied by NASA specialists, in particular by its leading expert N. Levenson [14]. She proposed the concept of comprehensive functional safety of such complexes and even patented a special term "safeware". It is somewhat similarly with "hardware", "software" and other kind of X-ware and defines a set of measures and tools to ensure safety including systems and computer safety. It should be noted that aspects of cyber security and some other types of BS have not been addressed in this methodology.

A separate direction in safety theory has developed in the last 20 years in relation to critical infrastructures - energy grids, transport complexes, and other [15-17], including the context of building resilient systems [18]. Many articles are devoted to human activity in emergency situations, where natural disasters and accidents of various man-made objects and methods of disaster and accident tolerance analysis and assurance are described [19-21].

Note that the term "Big Safety" has been mentioned in the context of big data analysis and the development of the SIEM (Security Information and Event Management) concept [22] and implied primarily the aspects of integrity, confidentiality and other attributes of information security and its management. In this work we are trying to change the methodological approach to safety analysis, namely to go to its cognition not only, and maybe not so much depending on the prevalence of the scale of the analyzed object, when a pair of concepts "big system" and "safety" automatically generates the concept "big safety". We believe that it is necessary to be based on the prevalence of

scale, multidimensionality of safety itself in all its manifestations for different systems, that allow using the adjective "big". This makes it advisable to form general concept of BS, taking into account different types of objects and different types of safety.

An important approach to shaping and making sense of BS is the use of the principle of comparativistics, i.e. comparing methods for assessing and ensuring the safety of different purposes objects for selection and dissemination. Such studies have been conducted previously for control systems of NPP and carrier rockets [23], and later for NPP and rocket-space complexes [24]. It is also important to consider the impact of COVID-19 on the emergence of new safety deficits in the context of modern technology [25].

Thus, the purpose of this research is to develop the concept of BS, analyze its attributes and interconnection of safety types, some principles and methods for its assessment and assurance, based on the experience gained in the nuclear power industry, in particular in the digital ICS of NPP, which form their IT infrastructure.

The paper is structured as follows. Section II analyzes the concept of BS, describes its attributes and classifies the objects and types of BS. Section III discusses the principles and methods of BS analysis and assurance, taking into account the experience of providing functional safety and cyber security of NPP ICS. Section IV discusses the important Black Swan phenomenon in terms of BS and considers some principles for mitigating its effects. Section V concludes the paper and outlines further research directions.

II. Concept and Features of Big Safety

10 B Attributes of Big Safety

By BS we will understand the multi-species (informational, functional, physical, infection, etc.) safety of technical and organization-technical systems in which: many functions are performed and many safety-critical processes are carried out; a significant amount of heterogeneous, rapidly changing and safety-critical data is generated, transmitted, stored and processed; disruption of functioning processes and data circulating in systems can cause a transition to a critical emergency state, which can lead to significant material losses, risks to human health and life, and environmental disasters.

.Big Safety is a result of crossing of the following 10 "Big":

1. Big/Complex Property (BPR). Big safety combines different types of safety and security such as

- nuclear safety (NS),
- radiation safety (RS),
- functional safety (FnS),
- information (cyber) security (InS),
- fire safety (FrS),
- physical security (PS),
- infection safety (IfS),
- safety from natural hazards (disasters): seismic safety (SsS), flooding safety (FIS) etc.,
- transport safety (TS),
- ecological safety (ES),
- chemical safety (ChS),
- food safety (FdS), etc.

Different types of safety for different critical systems interact with each other in different combinations. A typical example of an object in which different types of safety interact is an NPP, for which the first 9 safety types listed are essential. Note that transport safety is important because

of the need to transport fresh and spent nuclear fuel. By definition, NPP safety is the property of not exceeding the established limits of radiation impact on the personnel, residents of nearby houses and the environment during normal operation of an NPP, operational disturbances and design basis accidents, as well as limiting radiation impact during beyond design basis accidents [26].

The set of NPP BS types is shown on Figure 1. The narrows illustrate interconnection of BS types.

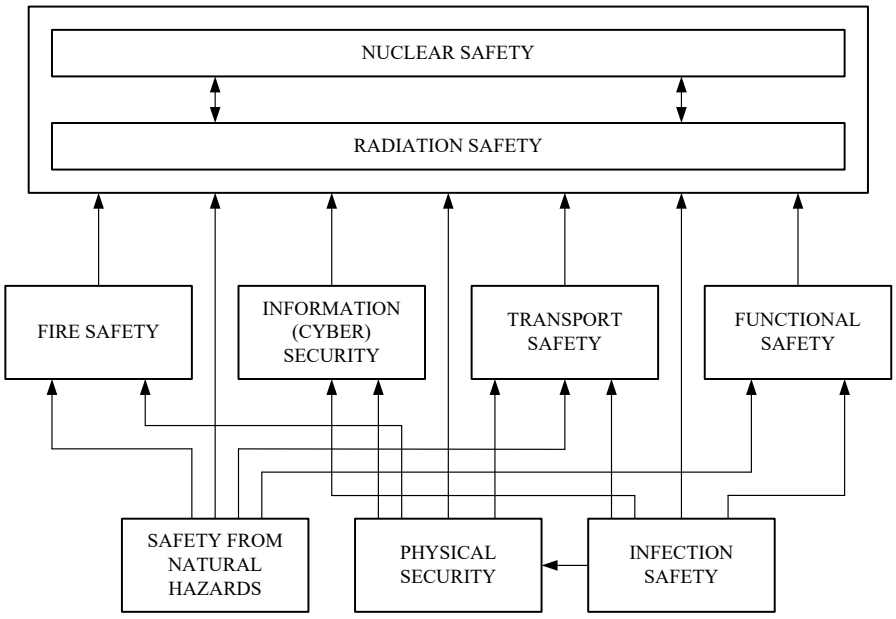

Figure 1: *Interconnection of Big Safety properties for NPP*

The hierarchy of big safety properties depends on the scope of critical systems such as safety critical, security critical, availability critical, etc.

2. Big/Complex Environment (BEN). The concept of BS is characterised by the fact that the behaviour of a (large) system is considered in a complex environment which influences the system - carries out impacts - of various types: physical (with a large number of different parameters - temperature and humidity, vibration, seismic, electromagnetic, radiation....), informational (changing input data, unauthorised impacts through data entry, changes in control panel elements, attacks on vulnerabilities), nuclear and radiological, biological (induction of the system to a potentially dangerous or dangerous - emergency state). Each of these impacts or combinations of impacts can result in the system entering a potentially dangerous or hazardous - emergency state.

3. Big/Complex System (BSS). Most often, BS is characteristic of a large/complex system, which consists of a large number or complex interrelated software, technical, ergative components and subsystems/systems. Each of these components, subsystems is characterised by a certain level of reliability and safety. In this case, we can talk about positive or negative safety synergy at the component-subsystem-system level, which is assessed by different indicators.

In large systems, the safety object consists of two parts: controlled (e.g. process equipment, level of operation technologies, OT) and controlling (level of information technologies. IT) which have become more and more convergent in recent years. Controlling (or instrumentation and control) systems are generally human-machine systems, and the personal factor is a very important part of the systems in terms of safety and security. A controlling system can also be categorised as a big system.

4. Big Failure/ Big or Huge Value of a Fatal Failure or Event (BFV). BS is characterised by the fact that it is considered in relation to so-called critical objects - critical failures or other events with serious material loss, loss of health or threat to human life. That is, such objects and their control systems are systems of great responsibility.

5. Big Number of Reasons/ Causes of Fatal Failure (BRF). A large number of causes usually lead to a large number of breaches of safety. Various safety violations often overlap over time ("trouble does not come alone") or are disrupted in a domino effect.

6. Big Data (BDT). Large amounts of data from tens or hundreds of thousands of sensors, other sources of information that can change dynamically, have high variability, etc. They are described by letter V number (from 3 to 7). In order to obtain and process these data, safety control systems are built into the object of analysis and maintenance of safety based on cybernetic principles and big data processing, implementing predictive analytics methods.

7. Big Number of Requirements to Safety (BRQ). Today's safety-critical systems must comply with hundreds and thousands of requirements of industrial, national and international standards that are designed for different domains and common to all systems. Examples of such "universal" standards are: IEC 61508 [27], ISO/IEC 15408 [28], ISO 62443 [29].

8. Big Time and Process Complexity of Development Implementation and Operation of Safe Systems (BTP). A distinctive feature of the critical systems in question is that they are built over a long time, involving a large number of engineers, managers and inspectors. Reliability of systems is built up during development, ensured during production and maintained during application. In the case of a high level of safety, it is incorporated, produced and maintained during development, production and use. Regulatory, (independent) verification and validation processes are also mandatory here.

9. Big Toolbox (set of methods, techniques and tools) for Safety Assessment and Assurance (BMT). A large number of different methods techniques and tools are used for safety assessment and assurance at different stages of system life cycle. Universal methods and techniques used for safety assessment include analysis of failure modes and effects, block diagram based assessment fault tree analysis, Markov's chain based assessment and others [3, 30].

10. Big Resources for Assurance and Recovery (BRR). BS requires colossal resources. Developing and implementing safety systems for such facilities such as NPP cost tens or hundreds of millions of dollars. It the cost will be even higher more in the event of a breach. Japan's economy, trade, and industry ministry recently (as of 2016) estimated the total cost of dealing with the Fukushima disaster at ¥21.5 trillion (US$187 billion), almost twice the previous estimate of ¥11 trillion (US$96 billion) [31].

Big Safety Objects

BS objects are divided into global and local depending on the size of the object and the consequences of safety violations.

Global Objects. In this case there may be dangers to humanity as a whole. Examples are infections, volcanic eruptions and earthquakes, a celestial body falling to earth, a nuclear disaster (war with nuclear weapons). The most pressing hazard that has affected and continues to affect humanity as a whole is COVID-19. According to research the COVID-19 pandemic will likely end up costing between S8.1 trillion and S15.8 trillion worldwide [31]. As of 1/01/2021, some 1.8 million people had died of COVID-19.

Local Objects. For these objects, the impact is on a group of people in a specific area. Examples: accidents at nuclear power plants, hydroelectric plants (dams, hydroelectric power plants), chemical, oil and gas production facilities, transport accidents.

One of the most recent accidents was a nitrate explosion in Beirut that destroyed a large part of the city. Note that the boundary between BS for global and local objects is difficult to delineate. The consequences of accidents at local facilities, such as NPP, can take on a national and cross-national character.

Analysis of Big Safety Types

The concept of BS consists in its representation taking into account the scale and importance of the system, the volume and sensitivity of the system data, the variety of factors and channels of unacceptable violations of the system. Formation and implementation of the BS concept should take into account concepts that are already in use and defined in the existing standards (in particular [28]):

- system assets (AoS), i.e. its resources that are critical in terms of various types of BS and to be protected;
- safety space (SoS) and perimeter (PoS). The former defines a multi-dimensional space characterised by the values of information, signalling, physical and other parameters at which the system is in a safe state; the SoS is the space in which AoSs are embedded. PoS is characterized by the limit values of these parameters;
- threats, causes, factors, channels of disruption of different types of BS (ToS). Each type of BS is characterised by a different set of threats;
- The consequences of a safety violations (EoS) - determined by the amount of loss due to such a violation (failure, unauthorised access and deformation of assets, accident).

Table 1 provides a description of some types of BS using the above for local objects concepts. Thus, the BS concept includes the definition, attributes (10 B), types and additional concepts of assets, space, perimeter, causes and consequences of violation of BS or its types.

III. General principles and methods for assessing and assurance of BS

BS assessment

To assess Big Safety and its types using by qualitative or quantitative approaches the most widely used methods of assessing functional safety and cyber security can be applied. There are a lot of safety/security assessment techniques [1,9,27-29] that can be generalized for BS assessment by the following way.

Technique TE. **X** Modes and Effects C/D (Criticality/Diagnostics) Analysis abbreviated as **X**ME(C/D)A), where **X** = {Failure, Software failure, Intrusion,...}. In general **X** can be interpreted as an event which is reason for the violation of one or another type of BS. So this method analyses events X (failures, intrusions/attacks, infections etc.), its modes and effects, possibilities of detection, identification or diagnosis and criticality (probability and severity) of the events.

Technique TD. **X** Block Diagrams (**X**BD), where **X** = {Reliability, Safety, Security, Trustworthiness....}. The most known assessment method is based on reliability block diagrams (RBD). It can generalized as XBD depending on assessed BS type or subtype X.

Technique TT. **X** Tree Analysis (**X**TA), where **X** = {Failure, Attack, Non-availability,...}. In this case X can be presented as an event similar XME(C/D)A and other events considering anomalies of BS properties.

Technique TI. **X** Injection/insertion Testing (**X**IT), where **X** = {Fault, Software fault, Vulnerability,...}. The method is based on injection into analysed system anomalies X to assess one of the BS types.

Table 1: *Analysis of Big Safety types*

BS types	AoS	SoS	PoS	ToS	EoS
Information (cyber)	Data, information and knowledge critical to the system	Information space (cyberspace for cyber security)	Information perimeter is defined by data entry and exit points as well as access points to system assets	Violations, unauthorised access, blocking of data or functions in progress	Material damage from loss or disruption of data, accident
Functional	ICS. sensors and actuators, personnel	Parameter and signal space, describes the safe functioning of the ICS	Maximum permissible values of parameters, determining the safe operation of the ICS	Untimely system actuation, resulting in an accident	Material losses from failures, accident
Physical	Premises, equipment, personnel	Physical space in which the systems, personnel are located	Physical boundaries of the area, facilities where the systems, personnel are located	Trespassing on protected equipment, destruction, threat to personnel	Material losses from intrusion, can lead to an emergency situation, loss of assets
Infectious	Personnel	Space to which person-nel have access and through which they can become infected	Perimeter that ensures that no infection can occur	Threat to the health and life of the personnel, inability to perform duties	Loss of health and life, can increase the risks of an accident

Technique TH. Hazard Operation Analysis (HAZOP(**X**)), where **X** = {Safety. Security,...}. The method allows to assess hazards of system operation and can be applied for analysis in point of different types X of BS.

Technique TC. Common Cause **X** Analysis (CC(**X**)A), where **X**={Failure, Vulnerability, Intrusion,...}. The method is aimed at identifying the reasons and events X why and when there may be a simultaneous violation of BS or its types of several redundant systems used for BS assurance.

Technique TM. Markov's Models (MM(**X**)), where **X** = {Availability, Dependability, Safety, Security}. Well-known Markov's model based method can be applied to assess different types of BS. Main restriction of MM or semi-MM techniques application to assess BS is correctness of conditions and representativeness of the initial data for obtaining such models.

There are other techniques based on model checking, formal methods and so on which can be adapted as well. The described set of techniques ST = {TE, TD, TT, TI, TC, TM} can be aggregated using a special framework FW ={SI, F, SO} [3]. Each technique Ti ϵ ST is presented by sets of input SIi and output SOi information and transformer Fi. It transforms input information, for example, set of components and functional structure of system to reliability block diagram presented as a scheme of connected components considering influence on up/down states (output information).

The techniques can be joined using a directed graph G = {N, L}, where a set of nodes N is described by set of the techniques ST (and transformers F) and set of edges L are links between the same outputs and inputs of the corresponding techniques. Thus, the graph G allows getting:

-a set of the possible paths SP = {Pj} to provide the required output information of final technique using available input information of initial technique. For example the techniques TE can be initial and its outputs can be inputs for the techniques TD, TI, TT and so on;

-a set of pairs of the paths Pj. Pk ϵ SP to compare the results obtained when using combinations of techniques corresponding to different paths. If allows improving trustworthiness of assessment.

BS assurance

For all the different objects and the dissimilarity of BS types, there are a number of general principles for its ensuring which have already been tested for functional, information and other types of safety, including for NPP. This is further supported by the [25] on the role of the Internet of Things, artificial intelligence, drones and other modern technologies in addressing Covid-19. Table 2 provides a comparison of some types and common principles of BS safety assurance.

Redundancy. *Redundancy is* the most common principle for ensuring the reliability, and subsequently the safety, of a wide class of local objects. Let's note, that one of the authors of the first handbook on reliability, where different ways of redundancy are considered, was published in 1966 by I.A. Ushakov [33], the founder of Gnedenko-Forum https://gnedenko.net/. This handbook was subsequently reprinted and expanded many times and translated into several languages.

Table 2: *Types and principles of safety assurance*

BS assurance principles	Types of Big Safety						
	NRS	FnS.	InS	FrS	PS	IfS	SsS, FIS and others
Redundancy	+	+	+	+	+	+	-
Diversity	+	+	+	+	+	+	-
Defence-in-Depth	+	+	+	+	+	+	-
Reserves of resistance	+	+	+/-	+	+	+	+
Independent verification and validation	+	+	+	+	-	+	+
Platform based decisions	+/-	+	+	+/-	+/-	+	-

Diversity. Due to the fact that common cause failures have become one of the main hazards, particularly in computer (software) based systems, the principle of diversity has been widely developed in the last 40 years. It is based on the simple idea "the same products/processes have the same anomalies, the different product/processes have different anomalies" [34,35]. "Different" means that products have the same functionality and processes have the same goals but are developed and implemented by different ways. Diversity is a principle of multi-version computing based on the following concepts [36]:

- version is an option of different product or/and process realization of function(s); version redundancy (VR) is a type of redundancy when different versions are used: diversity or multiversity is provided using several versions multi-version system (MVS) is a system in which redundant channels implement two or more versions; multi-version technology (MVT) is a set of the rules and

design actions in which a few versions-processes leading to development of two or more intermediate or end-products are used;

- strategy of diversity is a collection of general criteria, metrics and rules defining principles of formation and selection of version redundancy types and volume or MVTs; diversity metric is indicator to assess level of diversity.

There are the following types of diversity [34-36]:

- design (different technologies, design approaches, architectures);
- equipment (different manufacturers and design technologies) etc;
- functional (different underlying mechanisms, logics, actuators);
- human (different design companies; different managers, designers, programmers, testers and maintenance teams);
- signal (different sensed parameters, physical effects, different manufacturers and sensor designs, different set and location of sensors);
- software (different algorithms, operating systems, languages) etc.

Tabie 3 illustrates domains for diversity principle application according with this classification. MVSs are used in space (Shuttle computer control systems, International Space Station (ISS)), aviation (Airbus and Boeing on-board computer control systems), railway automatics (signalling, centralization and blocking computer-based systems, SCB), chemical industry (Center for Chemical Process Safety, CCPS), defense systems (military information and control systems, MICS), power plants (electrical grid, distributed and embedded control computer systems), NPPs (reactor trips systems, RTS and Engineered Safety Features and Auxialiary Systems, ESFAS), e-commerce (web-service-oriented architecture based systems, WSOA with diverse target web-services) [3,35,36].

Table 3: *Application of diversity principle*

Kinds of diversity (NUREG 6303 [28])	Diversity application domains										
	Space		Aviation		Rail-way	Chemical industry	Defense	Power Plants	NPP		e-Com-merce
	Shuttle	ISS	Airbus A380	Boeing 777	SCB	CCPS	MICS	Electrical Grid	RTS	ESFAS	WSOA
Design											
Equipment											
Function											
Human											
Signal											
Software											
Others											

It can be assumed that, for infectious safety, diversification is realised through a variety of vaccines developed by different organisations and countries and implemented according to different principles.

Defence-in-Depth. Defence-in-Depth includes a set of consistent physical barriers to the spread of hazards (e.g. radioactive substances and ionizing radiation) combined with technical means and organizational measures aimed at preventing deviations from normal operating conditions], preventing accidents and limiting their consequences. Thus, for nuclear and radiation safety of NPPs, the system of consecutive physical barriers includes fuel matrix, fuel element cladding, boundary of reactor compartment (RC) coolant circuit, containment of RC. biological protection. The strategy of NPP Defence -in-Depth is implemented at five levels:

- prevention of operational disruptions;
- ensuring safety in the event of disturbances and preventing emergencies:

- prevention and elimination of accidents;
- management of beyond design basis accidents;
- emergency preparedness and response.

For infectious safety, a system of consistent physical barriers includes state borders, regional borders, city borders, and company borders. For information and physical security, consistent barriers include control of access to territory or premises, systems, control of access to information resources, etc.

Independent Verification and Validation (IV&V). The introduction of Independent Verification and Validation, as well as multiple techniques to assess the functional and information safety of NPP Instrumentation and Control systems has enabled the implementation of another echelon of verification and protection of these systems against residual software and systems in general, in fact, IV&V is another option to implement process diversion and protection in depth to reduce risks of undetected defects and CCF in general. This experience is very important in an environment where safety systems for critical facilities have become digital and software-driven.

Thus the principles diversity, Defence-in-Depth (D3) and IV&V can be presented as a common approach to decreasing of CCF risks (Figure 2) on the stages creation and operation of system [24]. Techniques IV&V of developed or modernized I&C systems and hardware, software, FPGA components, platforms etc. allow minimizing risks of undetected design and physical faults and vulnerabilities.

D3 is a horizontal/vertical echelon consisting of n sub echelons e_i and m version redundancy types vr_i and providing protection of critical assets.

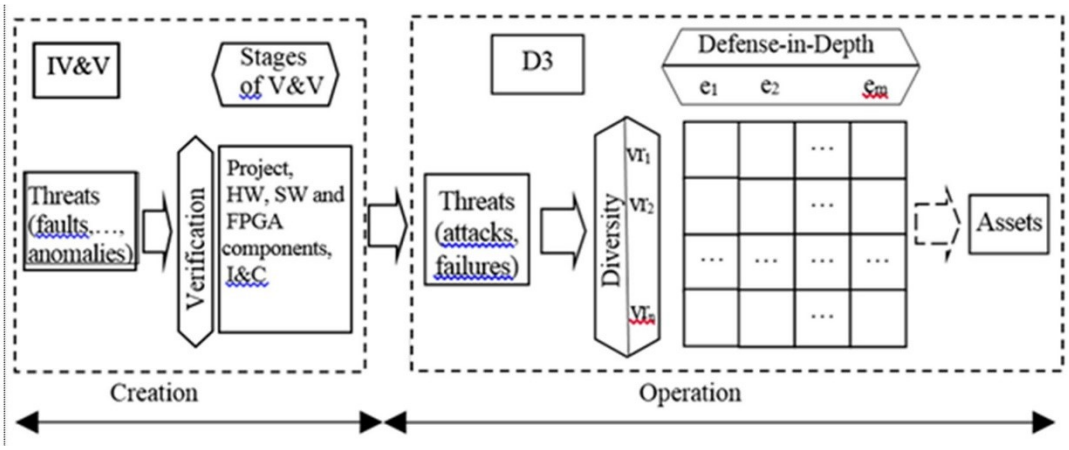

Figure 2: *Two echelons of CCF protection: independent verification and validation and D3 (Defence-in-Depths and diversity) approach: ei - echelons of protection in depth, vr - types of version redundancy*

Reserves of resistance. Reserves of resistance against external impacts (seismic, flooding, hurricanes, falling aircraft and other aircraft etc.) are probably the most obvious safety principle for a number of impacts. Unfortunately, this principle has not always been used to its full potential (as evidenced, for example, by the Fukushima accident). Its implementation is associated with high additional costs.

Platform based decisions. The concept of *"platform* (family of equipment)" has become widespread in recent years for the development of NPP control systems [3]. A platform is a set of hardware and software components that can work together in one or more defined configurations (structures) designed to implement a predefined set of specific control systems of different purposes. A feature of the platform is functional, structural and design completeness for the main application area.

The completeness of the platform is determined by the possibility to create on its basis a variety of information and control systems, which by the composition of performed functions, structure, constructive realization, technical parameters and characteristics in advance can satisfy the requirements of a wide enough, though limited range of specific customers. Such approach allows during development, introduction and justification of safety of each concrete system to concentrate its applied functions, relying at realization of basic functions on the technical decisions accepted at creation of the platform and tested in the course of its application [3].

To the surprise of the authors - nuclear and radiation safety specialists the concept of "platform" was used in vaccine development, including against COVID-19, when previously tested antiviral platforms were used to develop vaccines against new infectious diseases, greatly simplifying and accelerating their development.

BS regulation

The term “regulation” in relation to the activities and names of organisations implementing governmental safety policies is now commonly used for a number of types of safety. The term has been adopted by legislation in many countries, such as the United States - US Nuclear Regulatory Commission, Ukraine - State Nuclear Regulatory Inspectorate, international organizations. For example, Regulatory Committee on Nuclear Activities (CNRA) is an international committee of the Nuclear Energy Agency (NEA) including OECD- Organization for Economic Co-operation and Development. It was created in 1989 to guide the NEA programmes concerning the regulation, licensing and inspection of nuclear installations with regard to safety.

Safety regulation includes:

- safety standardisation (development of international, national and industry standards, regulations, rules and guidelines with safety requirements). Safety requirements are specified in the form of quantitative safety indicators (probabilistic and deterministic, e.g. limits on external influences) and in the form of regulations and rules;
- safety licensing, consisting of the examination, verification and assessment of compliance with safety requirements for the granting of licences (permits for all safety-related activities);
- monitoring compliance with safety requirements in accordance with the terms of licences issued.

Regulatory features:

- independence of the Regulatory Body (RB) from either the facility operator or the facility equipment designers;
- RB is usually a state organization;
- the existence, in some cases, of inter-state regulatory organisations.

An example of a big safety control scheme for a NPP (involving RB) is given in Figure 3.

The RB which reports only to the government, has two types of impacts on the NPP:

- during normal operation - documents (safety standards and regulations, licences, temporary operating permits, various ordinances, etc.);
- in case of an accident and/or emergency- instructions coming to the NPP crisis centre (these links are shown as dotted lines in Figure 3).

The RB receives information from the NPP describing the plant safety as well as information from the suppliers of equipment and services.

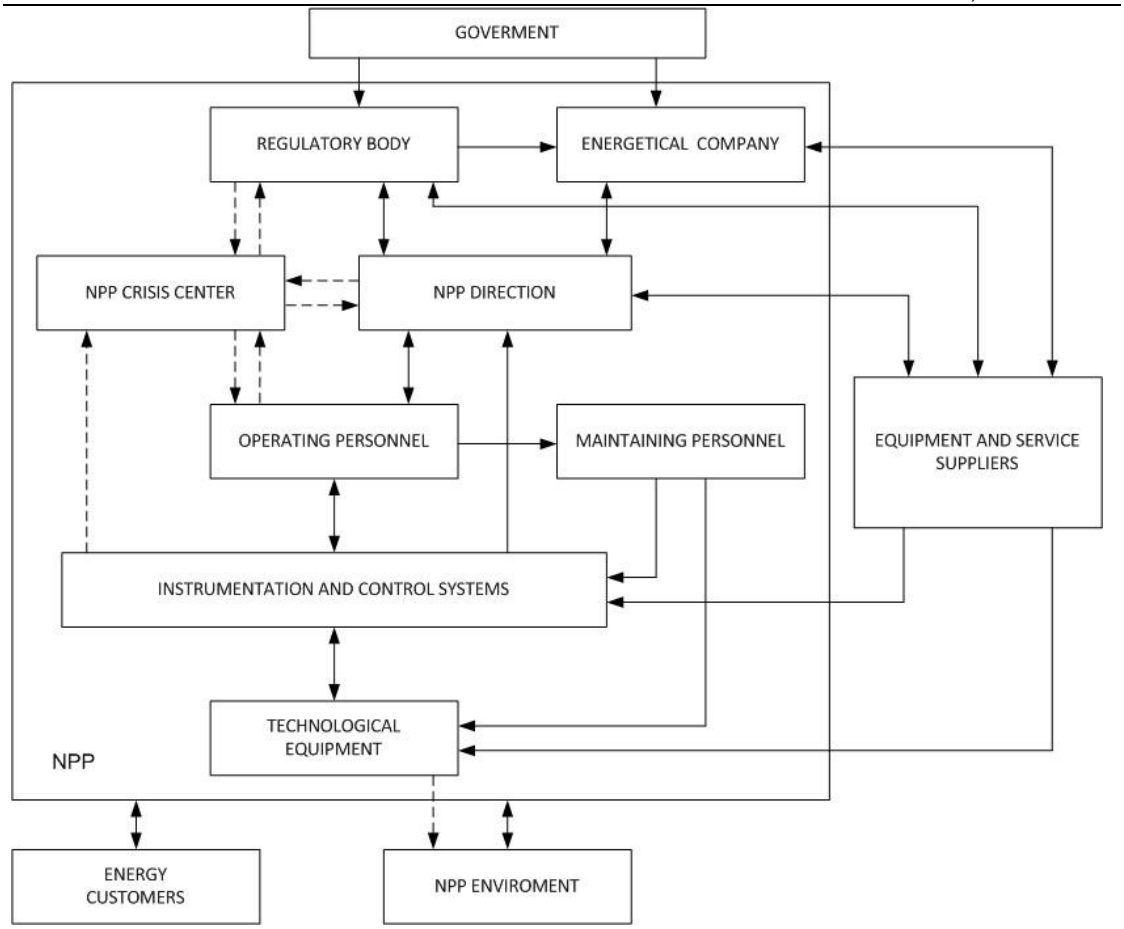

Figure 3: *Example of Big Safety control scheme for an NPP*

IV. Big Safety and Problem of Black Swan

Accidents as a Black Swan

The BS concept, the experience gained in the field of ensuring the safety of NPP and other critical systems can be used to find solutions to another methodological problems. Large man-made accidents in general and accidents at NPP's, in particular, are considered by many experts in the context of the Black Swan effect [37, 38]. According to this theory, the author of which is Nassim Taleb [39], events with the following features are called 'Black Swans":

- Ch1: these events are anomalous, as nothing in the past has foreshadowed them;
- Ch2: they have a significant impact because they are characterised by large material consequences, threats to the health and lives of many people;
- Ch3: An explanation for an event is found ('invented') after it has happened.

Let us analyse examples of events that could be considered as candidates for Black Swan recognition [1,5]. Table 4 summarises the results of the analysis in terms of identifying causes and assessing these events in terms of Ch1-Ch3 attributes. The markings "+" and "–" indicate the presence or absence of a relevant cause or attribute, "+/–" and "–/+" indicates a preponderance of positive or negative responses. This table was constructed taking into account expert judgement [5].

Table 4: *Accidents in context of Black Swan*

Accident	Country	Accident reasons				Is it Black Swan?			
		Comple-xity	Design anomaly	Human factor	Environment	Ch1	Ch2	Ch3	Yes/No
Three Mile Island. 1979	USA	-/+	+	+	-	+	-/+	-/+	Rather No
Chemo-byl. 1986	Formed USSR (Ukraine)	-/+	+	+	-	+/-	+	+	Rather Yes
Fuku-shima 2011	Japan	-/+	+/-	+/-	+	+/-	+	+	Rather Yes
Covid-19	218 countries	-	-	+/-	-/+	+	+	+	Yes

Add comments on the coronavirus pandemic.

Ch1. During the influenza epidemic of 1918-1919 years, 22 million people died worldwide. The world learned nothing from epidemics of lesser consequences. A number of countries lacked dedicated infectious disease hospitals and public anti-infection services. Global solutions must be implemented to control infection.

Ch2. The impact of the coronavirus infection is well known - a pandemic began and within a few months had spread to more than 200 countries on all continents. The death toll is approaching 2 million. Many countries are partially paralysed. Losses amount to tens of trillions of dollars.

Ch3. There is still no unequivocal explanation for the cause and mechanism. Note that Nassim Taleb himself did not refer to the coronavirus as a "black swan" because, in his view, the consequences of the pandemic were predicted at its inception and could have been prevented on this scale [40].

The strategies of Black Swan tolerance assurance

Many authors have analysed possible strategies to reduce the effects of the Black Swan effect [37]. "Black swans" become a kind of dataset that is used to train a "world" neuro-model for (support) decision-making systems. After receiving each new dataset, the "intelligence" of the model is increased, however, it is limited to the appearance of a predictable and intelligent response of the system to the arrival of a similar "black swan".

There are several strategies for Black Swan tolerance (StrT) [1].

A posteriori strategy (AsStrT). It is based on a comprehensive and detailed analysis of causes and effects, developing measures to reduce the risks of occurrence and minimise damage from the "black swan" that has "arrived". The results are formation and implementation of a set or set of sets for neuro-model training.

A priori, proactive strategy (ApStrT). The strategy consists of classifying and object-orienting analysis of “black swans” to form scenarios for future behaviour (earth meeting a major asteroid, a worldwide flood, the arrival of aggressive aliens, etc.). It is clear that the attempt to be proactive based on predictions of new black s wans runs counter to their very nature and Ch1 attribute, and is an attempt to erase the boundary between the part of probability theory that deals with rare events and the fundamental (by definition) unpredictability of these events. What is at stake here, however, is not an attempt to find a mathematical solution to the problem or to come close to solving it, but to

typify the solution procedure itself. A “set" is then formed for another “neuro-model", which will support decisions to improve this procedure.

A 'colour change' strategy (CStrT). In this it is worth revisiting Nassim Taleb's characterisation of the coronavirus as a ‘‘White swan”. It is worth highlighting a construct in his judgement that relates to the very possibility of a change of “colour” and the formation of an appropriate strategy on this basis. If consists of analysing, predicting, devising and implementing mitigation measures, i.e. changing the colour from black to grey or white, in the event of a time-bound event that may have the characteristics of a "black swan".

Swarming strategy (FStrT). The above strategies are based on the assumption of "ordinariness" of the black swan flow. A more complex situation is when two or more black swans arrive at the same time or with a delay that makes it impossible to react to the consequences of the previous black swan. At the same time, they can be from the same "swarm" (i.e. of the same type. e.g. a NPP accident), or from different ones (accident and pandemic). A combination of actions based on the strategies discussed above, taking into account the negative synergy of Black Swans from the swarms, is needed here. If situation “a Black Swan by Black Swan” happens, i.e. a known domino effect with Black Swans occurs, people should try to change the colour of at least the next Swan.

It is clear that implementing such strategies will involve enormous costs. However, dealing with the consequences of Black Swans is always immeasurably greater than the cost of defending against them.

V. Conclusions

1. The introduction of the concept and formation of the BS concept is an objective necessity related to trends in the development of critical systems in various areas of human activity and stimulated by the emergence of the coronavirus pandemic. It is not a tribute to fashion in the use of the word BIG. For all the different objects of safety and diversity of types of BS, there are a number of common principles for its assurance and assessment.

2. The BS problem becomes a global one because:

- has global causes and consequences;
- cannot be predicted and warned about outside the global context:
- cannot be solved by a single organization, region or country;
- consequences cannot be dealt with by local efforts.

It requires a global organizational and technical platform based on the BS concept, its legal and financial support, and teams of analysts and experts - "strategists and tacticians" (the experience of the Fukushima Daiichi accident in 2011 demonstrated this).

3. In the 2000s, the sustainable development movement began in the world. The coronavirus pandemic seems to be interrupting sustainable development trends. However, the lessons to be learned will help return to sustainable development with ‘greater sustainability'.

4. Nuclear power plant is an example of a local BS object. The nuclear power industry has accumulated invaluable experience in evaluating and providing various types of BS, which should be used by other critical areas. The same lessons learned in these areas need to be analyzed and applied to the safety of nuclear power plants and other critical objects consequently, it is important to develop comparative approach in framework of BS.

5. When analyzing and improving the BS concept, the importance of the human factor should be noted once again. The coronavirus situation already allows us to draw a simple conclusion: we should always take care of people, because people are both the object and the instrument of safety assurance.

6. It must be taken into account that information and communication technology and software are often the vectors of "danger". Sometimes accidents in different systems are caused by failures of their IT component. There is a need for an "amplifier of positives" and a "filter" of safety deficits caused by the introduction of new technologies (Internet of Things, artificial intelligence, man-machine cooperation, Big data, etc.) and concepts (Industry 4.0, 5.0...). Thus, it is important to rule out a situation that could be called as “the technology coronavirus” when new technologies can become reason of cyber or other kinds of threats and effects in point of global point view.

7. It is important to rule out the formation of any myths related to BS. Since the introduction of digital technology, the closed systems of nuclear power plants and other critical objects have led to a persistent judgment that cyber attacks are impossible, which has been debunked more than once. Now it is time to analyze the infectious safety with which the threats of creating bio-channels of influence on such systems, their human component, are linked.

8. BS is a safety without borders that are geographical, informational, technological, human. Its concept needs to be refined and filled in the face of new threats. It requires refinement and expansion of the set of countermeasures to counter additional threats in line with the strategies considered. It is necessary to make sure that "black swans" in the sphere of BS do not become absolutely black, to change their color towards grey or white, ensuring black swans-resilience of humanity, which should be proactive.

9. During last year a few papers have been published which discuss problems of safety of structurally complex systems [10], future of safety science [11] in general. The increase in the number of critical industries, the globalization of BS problems requires the development of a theory of big safety. This need is also related to the growing damage caused by hazards. The history of humanity, at least in the 21st century, has probably never known greater damage than that caused by COVID-19.

Notes. The authors understand the discussion nature of some provisions of the paper and, first of all, the very concept of Big Safety. The paper reflects our views on this problem, which are also being formed and developed, taking into account its multidimensional issue. We would be grateful for any feedback and comments.

Acknowledgements. The authors very appreciated to Professor Andrzej Rucinski (University of New Hampshire, USA), Professor Coen van Gulijk (University of Huddersfield, UK), Ambassador Krzysztof Paturej (International Centre for Chemical Safety and Security, Poland) and DrS Aleksandr Bochkov (Gnedenko Forum) for interesting discussion and valuable advices in context of Big Safety problem. We thank to staff of State Center of Nuclear and Radiation Safety and Department of Computer Systems, Networks and Cybersecurity of National Aerospace University «Kharkiv Aviation Institute» for participation in discussions related to topics of this paper.

References

[1] V. Kharchenko, M. Yastrebenetsky (2020). NPP Safety and big Safety in the Time of Covid-19. *Nuclear and Radiation Safety*, 3(87): 74-87.

[2] M. Yastrebenetsky, V. Kharchenko (edits), Nuclear Power Plant Instrumentation and Control Systems for Safety and Safety, Hershey, Pennsylvania, United States of America, IGI Global, 2014, 450.

[3] M. Yastrebenetsky, V. Kharchenko (edits), Safety and Safety of Nuclear Power Plant Instrumentation and Control Systems, Hershey, Pennsylvania, United States of America, IGI Global, 2020, 501.

[4] A. Rucinski. Global Trusted Dependability as a Grand Challenge. Proceedings of the 11th IEEE Conference on Dependable Systems, Services and Technologies, DESSERT2020, Ukraine, Kyiv, May 14-18, 2020: 9-10.

[5] V. Kharchenko (2018). Big Data and Internet of Things for Safety Critical Applications: Challenges, Methodology and Industrial Cases. *International Journal on Information Technologies and Safety*, 4: 3-16.

[6] Yastrebenetsky, M., Dybach, O. (2019). Prospects of using Big Data Technologies in nuclear energy of Ukraine. *Nuclear and Radiation Safety*, 2(82): 9-13.
[7] Illiashenko, O., Kolisnyk, M., Strielkina, A., Kotsiuba, I., Kharchenko, V. (2020). Conception and Application of Dependable Internet of Things Based Systems. Radio electronics, *Computer Science and Control*. 4 (57): 139-150.
[8] Rudenko, Y., Ushakov, I, Reliability of Power Systems. Science, Moscow. 1986, 254.
[9] Bochkov A.V. (2020).On the method of risk synthesis in the safety management of structurally complex systems. *Dependability*. 20(1): 57-67.
[10] Bochkov A.V. On the methods of qualitative estimation of the safety state of structurally complex systems (2020). *Dependability*. 20(3): 34-46. https://doi.org/10.21683/1729-2646-2020-20-3-34-46.
[11] Paul Swuste, Jop Groeneweg, Coen van Gulijk, Walter Zwaard, Saul Lemkowitz, Yvette Oostenthdorp (2020). The future of safety science. *Safety Science*. 125(3):104593: 1-9.
[12] A. Ian Glendon (2021). Safety Science directions: The journal. *Safety Science*. 135(3):105127: 1-8.
[13] Jie Li, Floris Goerlandt, Genserik Reniers (2021). An overview of scientometric mapping for the safety science community: Methods, tools, and framework. *Safety Science*. 134(2):105093: 1-11.
[14] Leveson N. Safeware: System Safety and Computers. – Addison–Wesley, 1995, 680.
[15] Alcaraz, C., Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, 8: 53–66.
[16] Harvey, C., Stanton, N., Safety in System-of-Systems: Ten key challenges (2014). *Safety Science*, 70, December: 58-366.
[17] Kharchenko, V., Sklyar, V., Brezhnev, E. Safety of Information and Control Systems and Infrastructures: Models, Methods and Technologies. Palmarium Academic Publishing. Germany, 2013, 529.
[18] Rehak, D., P. Senovsky, P., Slivkova, S. (2018), Resilience of Critical Infrastructure Elements and Its Main Factors. *Systems*, 6(2): 21-32.
[19] Severe accident management programs for nuclear power plants: safety guide. — Vienna, International Atomic Energy Agency, 2008.
[20] Shropshire, J. and C. Kadlec, Developing the IT Disaster Recovery Planning Construct. Journal of Information Technology Management, 2009. 20(4): 37-40.
[21] Charit, I. Accident Tolerant Nuclear Fuels and Cladding Materials. JOM 70: 173–175 (2018). https://doi.org/10.1007/s11837-017-2701-3
[22] The SIEM Buyer's Guide for 2021, Splunk, 2020 https://www.splunk.com/en_us/form/the-siem-buyers-guide.html.
[23] Isenberg, J., Yastrebenetsky, M. (2002). Comparing of principles of safety assurance of control systems for carrier rockets and NPPs. *Space Science and Technology*, 8, № 1: 4–8.
[24] Sklyar, V., Kharchenko, V., Yastrebenetsky, M. (2004). Digital Instrumentation and Control Systems of NPPs and Rocket-Space Complexes: Comparative Analysis, Tendencies of Development, Safety Assurance. *Nuclear and Radiation Safety*, 10 (2): 12–16.
[25] V. Chamola, V. Hassija, V. Gupta and M. Guizani, A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact," n *IEEE Access*, vol. 8: 90225-90265.
[26] NP 306.2.141-2008. Nuclear and Radiation Safety Standards and Regulations. General Safety Regulations for Nuclear Power Plants, Ukraine, Kyiv, 2008.
[27] IEC 61508. Functional safety of Electrical/Electronic/Programmable Electronic safety-related systems.
[28] IEC 15408 ISO / IEC 15408-1: 2005 Information technology-Safety techniques-Evaluation criteria for IT safety - Part 1: Introduction and general model.
[29] IEC 62443-1-1: 2009 Industrial communication networks - Network and system safety - Part 1-1: Terminology, concepts and models.
[30] Kharchenko, V. Independent Verification and Diversity: The Echelons for Assurance of Cyber Physical Systems Safety, Proceedings of the 2nd International Workshop on Information-Communication Technologies and Embedded Systems (ICTES 2020), Mykolaiv, Ukraine, November 12, 2020: 19-29.
[31] 2.4 trillion yen in Fukushima crisis compensation costs to be tacked onto power bills // December 10, 2016 (Mainichi Japan) https://mainichi.jp/english/articles/20161210/p2a/00m/0na/002000c

[32] Jeremy Schwab. Fighting COVID-19 could cost 500 times as much as pandemic prevention measures World Economic Forum, August 03, 2020. https://www.weforum.org/agenda/authors/jeremy-schwab
[33] Kozlov, B., Ushakov, I., Manual on estimation of radio-electronic and automatics equipment, Moscow, 1975, 472.
[34] NUREG/CR-6303. Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems. Lawrence Livermore National Laboratory, Livermore, CA, USA. 1994
[35] NUREG/CR-7007. Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems. ORNL/TM-2009/302. 2008.
[36] Kharchenko, V., Siora, A., Sklyar, V., Volkoviy, A., Bezsaliy, V. Multi-Diversity Versus Common Cause Failures: FPGA-based Multi-Version NPP I&C Systems. Proceedings of the 7th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC&HMIT 2010). Las Vegas, USA, November 7-11, 2010: 1081-1093.
[37] Avinash M. Nafday, Strategies for Managing the Consequences of Black Swan Events. Leadership Manage. Eng., 2009, No. 9(4): 191–197.
[38] Barry Brook. Black Swan theory and the anti-nuclear sentiment https://bravenewclimate.com/2012/02/01/black-swan-anti-nuclear/
[39] Nassim Nicholas Taleb. The Black Swan: Second Edition: The Impact of the Highly Improbable. Random House Trade Paperbacks, Retrieved November 5, 2017.
[40] Nassim Taleb Says 'White Swan' Coronavirus Pandemic Was Preventable. Bloomberg. July 10, 2020. URL: https://www.bloomberg.com/news/videos/2020-03-30/nassim-taleb-says-white-swan-coronavirus-pandemic-was-preventable-video.