

SYSTEM AND METHOD FOR MODELLING AND ASSESSING RISKS

TECHNICAL FIELD

[0001] The present disclosure relates to a system and method for modelling and assessing risks.

BACKGROUND

[0002] The following discussion of the background is intended to facilitate an understanding of the present disclosure only. It should be appreciated that the discussion is not an acknowledgement or admission that any of the material referred to was published, known or is part of the common general knowledge of the person skilled in the art in any jurisdiction as of the priority date of the invention.

[0003] Risk modelling and assessment are necessary activities throughout the lifecycle of a component, device or system. One method includes manually documenting potential hazards and possible mitigation of such hazards. Although tool support such as spreadsheets may be available to support the documentation process, tool support is typically utilized for managing the documentation and not available for performing deep semantic analysis or performing the decision processes automatically. In addition, manual documentation of risk identification can be labour intensive – this can result in increased costs, reduced efficiency or human errors.

[0004] In addition to the manual approach as mentioned, various approaches to model and evaluate risks have been contemplated, for example model-based engineering methods. In general, such model-based engineering methods aim to provide notations and tools to model functional and safety relevant properties in one overarching system design, integrating design and risk assessment. This link between “designing a system” and “assessing a system” is especially problematic for independent review. Furthermore, the integration unnecessarily limits risk assessment and evaluation to the elements included in the model. Consequently, any protective measure that exists in the environment, but is not part of the system

design, will be missed. In addition, the model-based engineering method also falls short to analyse system-of-systems of dynamically or spontaneously interacting systems. Furthermore, the engineering methods usually requires all vendors to design their components with the same methodology, which may be an unrealistic assumption.

[0005] Another approach, summarized as “run-time methods”, propose various ways to estimate risk of a system under assessment at run-time and change system behaviour accordingly. It is to be appreciated that such methods do not evaluate a protective measure but instead implement the same.

[0006] Another approach, summarized as “formal methods”, rely on formal modelling of the underlying system. However, such models are generally difficult to use because risk assessors may not be versed in formal modelling. In addition, known formal models may be limited in their application and involve the use of intensive computational resources due to the computational complexity associated with formal modelling. Existing formal approaches may not be able to handle dynamic changes and interacting elements within the system under assessment desirably.

[0007] In summary, existing systems and methods have significant shortcomings for modelling and assessing risks. Depending on the method used, they are unable to achieve complete independence from the system under assessment, are unable to achieve complete modelling of risks, and are typically domain specific.

[0008] There exists a need for an improved system and method to alleviate one or more of the aforementioned problems.

SUMMARY

[0009] This disclosure provides for a system capable of automatically assessing the safety and/or security compliance of inter-acting industrial assets in an adaptive or dynamic manner.

[0010] It addresses safety and/or security challenge posed by Industry 4.0

paradigm, i.e. increased inter-connectivity, flexibility and adaptability to change, with the aim to maximize asset efficiency and value generation.

[0011] The system features a method to model the safety and security risks of an industrial asset as defined in existing standards. In a physical safety domain, a risk may be associated with harm in the form of physical injury or other consequences to the health of living beings, such as human beings. The method can additionally model and assess safety risks associated with physical damage to property and/or environment. Overall, it enables assessment of application specific safety and security risks arising from the interaction of any pair of assets. The disclosure is suited for improving the speed and flexibility of risk assessment in a manner so as to reduce human error. The system and method may be deployed in various operational use cases.

[0012] The system can be integrated with traditional workflow of safety and/or security assessment. It can also form part of the development activities for the design and manufacturing of components, products, and sub-systems in the context of industrial internet of things (IIoT).

[0013] The system may also be used for future standardization efforts. It is appreciable that the system and method provides a formalism that is easy to understand for subject matter experts but is still formally correct. It overcomes the challenge to be accessible by people and by machines.

[0014] The system can be deployed alongside an already validated system application in terms of safety and/or security to dynamically re-evaluate conformance when certain properties or parameters within the system under assessment (SUA) change.

[0015] The system models one or more risks (hazards/threats) in terms of mapping natural language to a machine-interpretable semantic that are based on functional and operational adjustments of the SUA. Such a mapping formalizes risk assessment (which may include risk analysis, risk estimation and risk evaluation) in a machine-readable language to allow adaptive risk assessment, risk reduction and as a result ideally automatic safety certification.

[0016] The system semantic can be formally defined as a risk model associated with the SUA. Each layer in the abstraction hierarchy of the risk model can be reduced to lower-level constructs, providing precise semantic meaning. At the lowest level, the hazard modelling as well as risk assessment and reduction according to the present disclosure is based on the mathematical rigor of set theory, type theory, and structures.

[0017] Other aspects and features of the disclosure are described in the following description of specific embodiments in conjunction with the accompanying figures. It will be appreciated and understood by those of ordinary skill in the art that the embodiments are non-limiting examples.

BRIEF DESCRIPTION OF DRAWINGS

[0018] In the figures, which illustrate, by way of example only, embodiments of the present invention,

[0019] Fig. 1 shows a conceptual overview of a relationship between the risk modelling and assessment system of the present disclosure and a system under assessment.

[0020] Fig. 2 is a system diagram of the risk modelling and assessment system according to an embodiment.

[0021] Fig. 3a, 3b, 3c and 3d illustrate a possible structure of an electronic model specification 120 for use with the risk modelling and assessment system. Fig. 3a illustrates a syntax of the electronic model specification 120 in XML format, Fig. 3b tabulates top-level elements of the modelling language, Fig. 3c tabulates the base language elements of the modelling language, and Fig. 3d tabulates the base types of the type system.

[0022] Fig. 4 shows the components of an extensible application programming interface (API) that can be used for the implementation of risk modelling and risk assessment according to some embodiments.

[0023] Fig. 5 shows an embodiment of the modelling language components used for the creation of one or more electronic model specifications.

[0024] Fig. 6 illustrates an embodiment of a support tool, in the form of a graphical interface, to facilitate the creation of one or more electronic model specifications.

[0025] Fig. 7 illustrates a hardware embodiment of the risk modelling and risk assessment system in the form of an integrated circuit chip (IC).

[0026] Fig. 8 illustrates an embodiment wherein the risk modelling and risk assessment system is distributed and deployed as a service over a network.

[0027] Fig. 9 is a flow chart depicting an embodiment of a method for modelling risks associated with a system under assessment.

[0028] Fig. 10 is a flow chart depicting an embodiment of a method for risk assessment associated with a system under assessment.

DESCRIPTION OF EMBODIMENTS

[0029] As used herein, the term “comprise” or variations such as “comprises” or “comprising” will be understood to imply the inclusion of a stated integer or group of integers but not the exclusion of any other integer or group of integers.

[0030] As used herein, the term “include” or variations such as “includes” or “including” will be understood to imply the inclusion of a stated integer or group of integers but not the exclusion of any other integer or group of integers.

[0031] As used herein, the term “may” or “can” will be understood to imply the inclusion of a stated integer or group of integers but not the exclusion of any other integer or group of integers.

[0032] As used herein, the term “system under assessment” (SUA) refers to any system that is suitable to be interfaced with the risk modelling and risk assessment system of the present disclosure. Non-limiting examples of SUA

includes a production system, a manufacturing system, a logistic system, a chemical plant/reactor system, a waste incineration system, an explosion protection zone, a construction site, a nuclear plant, an oil refinery, a gas refinery, a cyber security system, an automation and control system, and one or more combinations of the aforementioned systems. An SUA can be as small as a single machine, vehicle and/or a product. The SUA may refer to the entire system that is being evaluated, regardless of its hierarchical or heterarchical composition. The SUA can also include two or more systems that interact with one another during operation.

[0033] As used herein, the term “element of an SUA” can refer to a constituent of the SUA. Non-limiting examples include a physical facility such as a room, a building, a shelf; a vehicle such as an automated guided vehicle, a forklift, a transport vehicle; one or more machines; and/or a part of or a section of the physical facility, vehicle, machines, etc. The element of an SUA also includes logical constituents such as one or more of the following: operating system, network driver, software application, encryption service, safety function, etc.

[0034] As used herein, the term ‘risk’ includes a safety breach, hazard and/or a security breach, hazard. As used herein, the term ‘risk’ also include instances of safety and/or security gaps against tolerable risk levels as defined in current technical standards. Non-limiting examples of such risks includes entrapment risk (i.e. human operator trapped by one or more machines), explosion risk, fire risk, theft, unauthorized entry into a premise, unauthorized obtainment of confidential information etc.

[0035] As used herein, the term ‘risk related property’ refers to an attribute that is associated with one or more types of risk in the context of an SUA. For example, a risk related property can be a spark within a room of flammable materials that can lead to an explosion risk, a vehicle in a path of an object/person that can lead to a collision risk, etc. Risk related property can also include an attribute for mitigating the risk (e.g. safety functions and security countermeasures), as well as general context information (e.g. gravitational force of Earth).

[0036] As used herein, the term ‘natural language’ includes one or more languages that has been developed naturally in use by human beings and can include languages such as English, Chinese, Japanese, German. The term ‘natural language’ can also include dialects and colloquialism.

[0037] As used herein, the term ‘system semantic’ refers to a semantic utilized within the context of an SUA. The system semantic comprises syntax that can be understood by a human person and can also be interpreted by suitable computer compilers/processors and its meaning for the system.

[0038] As used herein, the term ‘condition’ represents a proposition expressed in natural or pseudo-natural language and mappable to a system semantic. The proposition comprises one or more expressions that can give rise to a risk. If the condition is evaluated to a ‘true’, an unacceptable/ unmitigated risk associated with the condition exists. If the condition is evaluated to a ‘false’, the risk associated with the condition is deemed “tolerable”, hence additional safety and/or security measures are not necessary.

[0039] As used herein, the terms ‘risk assessment’ and ‘risk evaluation’ are understood to be intentionally separated and independent from the design of the SUA. In addition, the terms ‘risk assessment’ and ‘risk evaluation’ are separate and independent from the recommendations to mitigate any identified risks. Risk assessment and risk evaluation results are primarily used to verify and/or validate a design and list non-conformances. In particular, the term risk assessment includes risk analysis, evaluation and/or risk reduction.

[0040] As used herein, the term ‘network’ can be any means of providing communication between one or more devices and/or content stored elsewhere. As used herein, network can be a personal area network, local area network, a storage area network, a system area network, a wide area network, a virtual private network, and an enterprise private network. The network can include one or more gateways or no gateways. The network communication can be conducted via published standard protocols or proprietary protocols.

[0041] As used herein, communication of data through any network can be: (i)

encoded or unencoded; (ii) encrypted or unencrypted; (iii) delivered via a wired network, a wireless network, or a combination of wired and wireless networks. Wireless communication can be accomplished in any practical manner including a Wi-Fi 802.11 network, a Bluetooth™ network, or mobile phone network (such as 3G, 4G, LTE, and 5G). The terms “connect”, “connected”, and “connecting” as used herein refer to a communication link between at least two devices and can be accomplished as discussed in this paragraph.

[0042] As used herein, the term “associate”, “associated”, and “associating” indicate a defined relationship (or cross-reference) between at least two items. Such defined relationship may be expressed in one or more mathematical equations and/or formulas.

[0043] As used herein, the term “computing device” may be a single stand-alone computer such as a desktop computer or a laptop computer, a thin client, a tablet computer, an embedded computer or a mobile phone. The computing device may run a local operating system and store computer files on a local storage drive. The computing device may access files and application through a gateway to one or more content repositories, the content repository can host files and/or run virtual applications and generate a virtual desktop for the computing device.

[0044] As used herein, the term “server” may include a single stand-alone computer, a single dedicated server, multiple dedicated servers, and/or a virtual server running on a larger network of servers and/or cloud-based service. A server may also include virtual machines, and can include one or more computing services hosted on cloud. Cloud could be either private or public commercial cloud.

[0045] As used herein, the term “run time” is used in the context of a computer processing term in relation to the implementation and execution of the present system. The run time may or may not be required to meet real time requirements.

[0046] As used herein, the term “parameter” includes variables, constants, any measurable (quantitative or qualitative) quantities, and the derivatives of any of the aforementioned.

[0047] As used herein, the term “physical property” refers to a property that is measurable, whose value describes a state of a SUA. Non-limiting examples of physical property includes temperature, colour, pressure, distance, response time, memory consumption of a computer, etc.

[0048] As used herein, the term “functional property” refers to the performance, accuracy and consistency of an output of a system in response to an input. For example, a car braking system may be required to brake within a certain distance (output) when an input braking force is applied.

[0049] According to an aspect of the disclosure there is a system for modelling and assessing risks comprising: at least one electronic model specification associated with an SUA, the electronic model specification comprises an application section associated with at least one element of the SUA; the application section includes at least one of a safety section and a security section associated with the at least one element; wherein at least one of a safety section and security section comprises a plurality of risk related properties; the plurality of risk related properties mappable from a natural language to a system semantic, the system semantic associated with a physical or functional property of the SUA; and a condition section specifying at least one condition associated with at least one of a safety breach and a security breach to materialize; wherein the at least one condition comprises at least one of the plurality of risk related property; an evaluation engine configured to evaluate the at least one condition associated with the at least one of a safety breach and a security breach to determine if a risk exists.

[0050] Fig. 1 shows a conceptual overview of a relation between the risk modelling and assessment system 100 of the present disclosure and a SUA 1900. The system 100 may be arranged in communication with the SUA 1900 to obtain information from the same, so as to at least partially derive an input. The communication between the system 100 and SUA 1900 can be wired or wireless. Alternatively the system 100 may not be in communication with the SUA 1900 and inputs are provided manually to the system 100. The system 100 is independent from the SUA 1900 in the sense that the SUA is not influenced in its workings by

the presence, usage or interaction with the system 100. The system 100 is configured to model and assess the SUA 1900. If at least one risk exists, the system 100 models at least one risk in the form of a list of conditions, such as a conjunctive list of conditions that causes the risk to materialize, for a user's action. If a risk can arise due to multiple possibilities or multiple risks are present, the conjunctive list of conditions may be combined using disjunction. It is appreciable that the list of conditions includes a plurality of risk related properties.

[0051] As shown in Fig. 1, the system 100 models and obtains parameters of the SUA 1900. Where any changes are made to the SUA, the system 100 may obtain changed parameters during run-time. The system 100 may also be configured to obtain changed parameters whenever a change event is detected, for example via a trigger. Alternatively or in addition, the system 100 may also be configured check the SUA 1900 at every predetermined time interval to detect any changes. It is contemplated that the system 100 may also be configured to check the SUA 1900 at various system states of the SUA 1900, such as run-time / design phase / batch-mode / on-line vs off-line / simulation states. The system states may correspond to various system life cycles stages of the SUA 1900.

[0052] As shown in Fig. 2, the system 100 comprises an electronic model specification 120 for modelling the SUA and associated safety and/or security risks that can arise in the SUA 1900.

[0053] It is appreciable that each SUA may be different and there can be a plurality of electronic model specifications 120 created for each SUA depending on operating scenarios or additional components to be added to the SUA. In situations where multiple electronic model specifications 120 are created, each of the plurality of electronic model specifications 120 may be regarded or referred to as a fragment. It is appreciable that multiple fragments of the electronic model specification 120 may be created from different remote sources and combined. Such combination may be performed via referencing in one electronic model specification fragment, one or more other electronic model specification fragments. For example, users such as equipment vendors may choose to make an electronic model specification 120 available through a web resource, such as a uniform

resource locator (URL) of their company's domain. The system 100 may be configured to detect any newly added electronic model specification 120 for the SUA 1900 for remodelling. It is appreciable that each electronic model specification fragment shares the same base components as other electronic model specification fragments.

[0054] Creation of the electronic model specification 120 may be performed manually (e.g. by risk assessors, equipment vendors, system integrators, risk assessment experts) or automatically (e.g. by simulation engines, or reasoning engines). A semi-automatic process of electronic model specification creation via computer-assisted tools, such as a graphical editor, is also contemplated. In some embodiments, the reasoning engines may include one or more artificial intelligence (AI) engines to model a risk assessment expert(s).

[0055] The electronic model specification 120 is created in accordance with a modelling language. The modelling language has a predefined semantic, set of rules and structure to facilitate the modelling of risks. The modelling language defines the way in which one or more properties of an SUA 1900 may be documented in a way so as to meet requirements of expressiveness, correctness, and user understandability. The documented properties may be relevant for risk assessment and/or evaluation.

[0056] The modelling language may be regarded as a meta-model that can be realized in various specification language syntaxes. The meta-model may be managed by a component which forms part of an application programming interface (API). An example of a suitable syntax is the Extensible Markup Language (XML), a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. Other suitable syntax can include the JavaScript Object Notation (JSON) and the YAML Ain't Markup Language (YAML) syntax.

[0057] It is contemplated that the modelling language meta model includes rules that define a valid electronic model specification document in the desired language realization. This means that the modelling of risks, for example a safety

hazard is specification language-independent as long as a matching realization parser or syntax analyser is available. Such flexibility allows existing tools, frameworks, and concepts to be utilized under the overall defined structure of the electronic model specification. For example, XML-editors, document validation, XPath and XLink specifications, Resource Description Framework (RDF), etc. can be utilized.

[0058] The electronic model specification 120 comprises an application section 140 associated with at least one element of the SUA. The application section 140 provides a context of usual operation of each element of the SUA, including the scope of use of at least one element. For example, where the element of the SUA is a tool such as a chainsaw, the application section 140 provides for a proper use of the tool. For example, a chainsaw for stirring a liquid is not proper use of the chainsaw. The application context therefore needs to be modelled in addition to the element.

[0059] The application section 140 includes at least one of a safety section 142 and/or a security section 144 associated with the at least one element; wherein the at least one of a safety section 142 and security section 144 comprises a plurality of risk related properties. The plurality of risk related properties is mappable from a natural language to a system semantic, the system semantic associated with a physical or functional property of the SUA.

[0060] As an example of such mapping of natural language to a system semantic, consider the natural expression of a risk related property 'a person is in the path of an automated guided vehicle (AGV)'. While easily understood by a natural person, i.e. a human user documenting such risk, this expression has to be transformed into a machine-readable system semantic that fits the context of the SUA. An example of such mapping may be modelled in the form as a physical property such as distance between the person and the AGV. Whether the statement 'person is in the path of an AGV' is true can depend on a predefined threshold (e.g. 3 metres - distance apart). Such predefined threshold may change or be affected by other physical properties such as speed or weight of the AGV. For example, if the speed of the AGV is high, a longer distance between the person

and the AGV may be defined as the threshold. Likewise, if the load carried by the AGV is heavier, the distance required between the AGV and the person may be longer in order to prevent a collision.

[0061] Another example of a mapping is the natural expression of a risk related property 'flying spark'. While sparks may be generated in the normal course of certain operations such as a milling machine, depending on the context of SUA this may contribute to a safety risk in for example an open room without any proper barrier(s) to isolate the flying spark. Whether or not the flying spark will be evaluated to constitute a risk will depend on the modelling or mapping in the form of function property such as whether an appropriate barrier is closed or opened.

[0062] The electronic model specification also comprises a condition section 146 specifying at least one condition associated with at least one of a safety breach and a security breach to materialize. The at least one condition comprises at least one of the plurality of risk related property. As an example, a condition may be expressed as a conjunctive list of conditions as shown in Equation 1:

$$(\text{person_is_in_path_of_agv}) \wedge (\text{agv_cannot_brake}) \quad (1)$$

[0063] Equation 1 is a simplified example of a hazard model. All elements within Equation (1) must be evaluated to be true for the hazard to take effect or materialize. The risk related property 'person_is_in_path_of_agv' may be defined through the physical and/or functional composition as explained. For example, the "in-path" proposition can simply be modelled as a distance between the person and the path of the AGV that is less than a given threshold. The condition may be modelled in Equation 2, which defines a simplified "in_path_of" proposition based on two parameters (person, AGV). The condition is true when the distance between the person and the path of the AGV is less than a threshold. Symbols prefixed with a '\$' sign denote variables. It is appreciable that the full hazard description is more elaborate than the example given below is SUA dependent.

$$(\text{in_path_of } \$\text{person } \$\text{AGV}) := (< (\text{distance } (\text{location } (\$ \text{person}) (\text{path_of } \$\text{AGV})) \$\text{threshold}) \quad (2)$$

[0064] The risk related property 'agv_cannot_brake' or 'agv_cannot_brake_in_time' can be a function of the AGV's braking system, floor properties and weight of the AGV. Where there are multiple hazards in an SUA, they may be combined using disjunction (i.e. an 'OR' operation). Any of the hazards may invalidate the conformance of the entire system.

[0065] Fig. 3a, 3b, 3c and 3d illustrate various embodiments of the electronic model specification 120. Fig. 3a illustrates an example syntax of the electronic model specification 120 in an XML format, Fig. 3b tabulates top-level elements of the modelling language used to create the electronic model specification, Fig. 3c tabulates the base language elements of the modelling language, and Fig. 3d tabulates the base types of the type system of the modelling language.

[0066] Fig. 3b illustrates additional sections of the electronic model specification in addition to the application, safety, security and condition sections. The additional sections may include a definition section and a world section.

[0067] The definition section introduces default and user defined constructs. For example, the modelling language may allow the definition of basic elements such as types for values and composite elements such as a new type of a robot.

[0068] The world section is the section of the electronic model specification 120 that lists any other relevant properties of an SUA for the assessment that are neither uniquely risk nor mitigation. The world section comprises at least one general property of the SUA 1900. Such general property may not be directly related to any risk of the SUA but can be a physical and/or functional property that can affect the risk assessment of the SUA. A non-limiting example of a general property is gravitational force of earth.

[0069] Fig. 3c shows a table of semantic language elements of the electronic model specification 120. One or more of the language elements may be utilized for risk modelling and definition. In particular, the language element import may be used to reference external electronic model specification fragments.

[0070] Fig. 3d shows a table of different types as part of the specification

language used to create the electronic model specification 120.

[0071] A solution to each condition which gives rise to a safety or security hazard, as listed in the condition section or defined within the safety/security sections, may be found within a search or solution space. To this end, the system 100 comprises an evaluation engine 160 to define a search space and to evaluate the condition to a true/false answer. In some embodiments, the evaluation engine 160 includes a script evaluator 162 and a solver evaluator 164. In some embodiments, the evaluation engine may determine the acceptability of SUA based on modelling the risks of the SUA 1900 as an optimization problem to reduce overall computational complexity. Suitable algorithms that may or may not utilize a search space may be contemplated. Non-limiting examples include evolutionary algorithms such as genetic programming/algorithm; regression algorithms; neural networks; fuzzy logic systems, etc.

[0072] The script evaluator 162 consolidates the input for the solver evaluator 164. In some embodiments script evaluator 162 operates to reduce the search space of each condition, through, for example, substitution and removing redundant or duplicate solutions. For example, two or more solutions having distance between a person and an AGV less than a predefined threshold of Equation (2) may evaluate the risk related property 'person_is_in_path_of_agv' to be true. The script evaluator 162 operates to remove the redundant solutions from the search space so as to reduce computational resource required for evaluation.

[0073] As another example of reducing the complexity or solution space, consider the AGV of Equation (1) and (2). Assume there is a formula/mathematical expression that calculates the braking distance (expressed in metres) of an AGV expressed as a function three parameters: the AGV's current speed, the AGV effective weight which includes the weight of any load carried by the AGV, and the braking force applied (i.e. $f(\text{speed, weight, force})$). The formula outputs the distance that the AGV will need to come to a complete stop. Assuming there is a condition generated in the constraint solver: $(f(\text{speed, weight, force}) < 2)$ meaning that the AGV has to stop within 2 meters of the person. Calculating non-linear functions in the constraint solver may be computationally expensive. The script

solver can simplify the formula or completely replace it with the result if all parameters are known. Imagine that f evaluates to 1.5 meters. Then $(1.5 < 2)$ is simply “true”. It is appreciable that by simplifying the formulas or completely replacing them, the script solver reduces the number of variables the script solver has to consider.

[0074] The solver evaluator 164 evaluates each condition to either a ‘true’ or a ‘false’. If the condition is evaluated to ‘true’, a risk associated with the corresponding condition exists and the SUA therefore cannot be accepted, i.e. non-conformance is detected. Put in another way, the solver evaluator 164 thus functions as a constraint solver to find an assignment to each risk related property that will make the entire condition to be evaluated to ‘true’. The found assignment then automatically constitutes an argument as to why the SUA cannot be accepted.

[0075] It is contemplated that the risk model can be represented as a deterministic model, such as, but not limited to, a Satisfiability-Modulo-Theories solver (SMT) model. In addition, the assessment process is formally verifiable.

[0076] In some embodiments, the evaluation engine 160 may be configured to receive present or updated parameters from the SUA before each condition is evaluated. In some embodiments, one or more of the risk related property may be mapped into a constraint within the SMT model.

[0077] In some embodiments, a protective section 147 may be developed in association with the safety section and a mitigation model 148 may be developed in association with the security section. The protective measures (in the safety domain) or countermeasures (in the security domain) section may be modelled analogously to safety/security risks as conjunctive formulas. The risk modelling language defines mitigation in terms of contradictions to constituents of risks. Using Equation (1) and (2) as examples, a valid safety function can make sure that the AGV is always able to brake or decelerate in time. This could be realized by a safety function that lowers the speed of the AGV to invalidate the “agv_cannot_brake” condition. Another option may be a safety function that addresses the risk related property ‘person_is_in_path_of_agv’. The mitigation

model can assure that the distance between person and AGV path never becomes too short (i.e. collision avoidance). Such modelling methodology establishes a clear and traceable semantic relationship between protective measures and mitigation that explains why it is valid for a given safety or security hazard.

[0078] For the mitigation to be effective, the system 100 makes sure that each protective measure (formula) is satisfiable by itself. This is another important requirement as an invalid protective measure may result in the assessment of the SUA giving a 'false', hence wrongly assessing the SUA to be in conformance even when there is a presence of one or more unmitigated risks that remain in the system. It is appreciable that the mitigation model may be used in addition with the risk model to evaluate conformance of the SUA.

[0079] In some embodiments, the formalism of the electronic model specification may be based on components listed in Fig. 4, in the form of an application programming interface (API) 400. The API 400 is organised into three categories: (1) interface 402, (2) run-time 404, and (3) language 406.

[0080] Components in the interface category define how the electronic model specification 120 and evaluation engine 160 is packaged, used, and interfaced with. The system configuration includes a variety of settings, including environment settings such as modelling language configuration 411, interpretation of input, execution paths, logging levels, authentication, network settings and others. The executable 412 is the binary executable compiled for the target platform (i.e. SUA 1900) of execution. Several modes of interaction are contemplated, including execution as command line tool and as web service. Furthermore, the executable as a library can be embedded in, or called by, supplementary tools such as system design tools or manufacturing execution systems (MES).

[0081] Components in the Run-Time category 404 enable the execution of the system 100, i.e. they implement the algorithms of the system 100 including receiving parameters from the SUA, generating a risk model associated with the SUA, and generating a search space. A registry component 413 controls the set of language elements supported during an evaluation run. The registry component

413 allows the generalization over language elements by alias and by type, a core feature for the extendibility of the language and methodology. The Context component 414 implements an execution scoping mechanism that includes defined types, variables, and functions. A model collector component 415 implements the algorithm to create a risk model associated with an SUA, which is evaluated by two evaluation passes, implemented through the script solver 416 and the model solver 417, respectively. The result of the evaluation is formatted and passed through the configured interface back to the caller.

[0082] Components of the modelling language category 406 implement the risk modelling language itself. A single electronic model specification fragment 418 is the root component from which all others are derived in an object-oriented fashion. An embodiment of a simplified start of the inheritance hierarchy tree is shown in Figure 5. Each construct of the modelling language is realized by a specialization of an electronic model specification fragment. Each component defines its contribution to a system model and a matching interpreter to construct a result for the evaluation.

[0083] Fig. 5 shows an embodiment of the modelling language components forming the structure of the electronic model specification 140 or a part thereof (i.e. fragment), based on object oriented principles. Fig. 5 also depicts the relationships, including inheritance relationships, between different components in the electronic model specification 140. It is to be appreciated that arrow hats (shown as Δ) are only overlapping to simplify the overview. Each inheritance relationship should be understood as a parallel line. Distinguishing features of the inheritance relationships include the following:

[0084] The type system is completely configurable to suit the needs of an SUA. This goes as far as the ability to redefine what "Boolean" type is (e.g. true/false, on/off, one/zero, etc.) It is contemplated that any type can be redefined, modified or excluded. The rigor of the modelling language makes sure that no invalid statements result from this flexibility.

[0085] The type 'system' is not limited to the types that typical constraint

solvers allow. This is noteworthy for the modelling flexibility, expressiveness and usability of the system 100. Theoretically, all risk assessors could be taught to express an SUA model in the domain of constraint solvers. However, this may be impractical and counterproductive as many inconsistencies can arise. Among the many ways risk assessment can be mapped to constraint solvers, the present disclosure of mapping a risk related property to a system semantic and a conjunctive list of conditions, and subsequently into a constraint space, makes sure that the various expressions remain compatible and interoperable.

[0086] Two or more types of variables may be contemplated to model the different evaluation steps. Script variables (for subsequent reduction of the solution or search space via the script solver) may hold local or remote values, generalizing over the concept of a variable. Script variables hold a value. Solver variables do not hold a single value but reference a family of possible assignments. Hence, they are the search parameters for the model evaluation step.

[0087] It is contemplated that safety and security concepts can share many common features (e.g. the concepts of risk and mitigation) but are also specialized to model their distinguishing differences. For example, safety functions need to conform to a target performance level and safety integrity level, while countermeasures need to conform to a security level.

[0088] The hierarchy is extendible, enabling the features of the API 400, modules, libraries, and graphical editors to assist in the process of creating the electronic model specification.

[0089] In some embodiments, software extensions may be defined to extend the functionality of the base modelling language. There are at least two major categories of extension: (1) Content modelled in the modelling language itself, and (2) extensions of the modelling language using the API 400. The first category is referred to as modules, and the second may be referred to as libraries. Modules are more portable but are limited to the configured constructs. Libraries fully subsume modules and additionally allow extension to the language.

[0090] Modules can be a way to codify existing standards and dynamically

import them in the evaluation process. Hence, if an SUA should conform to a given standard, a user, who may be an assessor, may simply import the respective module(s). Standards are typically published by international standardization organizations such as ISO and IEC. For example, analyzing the requirements for safety related control systems in ISO 10218-2, such requirements, as shown in Equation (3), may be translated to an electronic model specification fragment via formation of conjunctive and disjunctive formulas as discussed.

$$\begin{aligned}
 &(\text{No_SingleFault_may_lead_to_loss_of_safety_function}) \wedge \\
 &(\text{SingleFault_shall_be_detected_before_next_demand}) \wedge \\
 &(\text{SingleFault_triggers_safety_function_and_maintain_until_fault_is_corrected}) \wedge \\
 &(\text{All_foreseeable_faults_shall_be_detected})
 \end{aligned} \tag{3}$$

[0091] The target performance requirement can be expressed in the modelling language as well in the following syntax:

```

<SafetyRelatedControlSystem>
    <PerformanceLevel>D</PerformanceLevel>
    <StructureCategory>3</StructureCategory>
    <SafetyIntegrityLevel>2</SafetyIntegrityLevel>
</SafetyRelatedControlSystem>

```

[0092] Based on the aforementioned constructs, the modelling language defines structure and content of safety and security profiles for components of an SUA. For example, a safety profile may include one or more of the following: type of components, safety targets or thresholds, safety measure classification, safety measure properties, reliability requirements (Performance level or Reliability level for mechanical parts), availability over time.

[0093] A security profile may include one or more of the following: type of component, security targets (e.g. confidentiality, integrity, availability), security measure classification, security measure properties, security level requirements, availability over time.

[0094] While it is appreciable that an electronic model specification can be created using a rudimentary text editor, depending on the chosen realization of the language, tool support can be introduced to ease the burden of a user. For example, there are several tools available to edit XML, JSON, and YAML documents, including syntax checkers, validation, and graphical representations.

[0095] Fig. 6 shows an example of a specialized editor in the form of a computer aided design tool 600 provided to a user in assisting the modelling and assessment/evaluation of risks. Fig. 6 illustrates an example prototype visualization of a 2D editor for managing a factory layout.

[0096] The 2D editor is utilized to create and manage the electronic model specification document. Using the 2D editor, a user can drag and drop elements of the SUA, such as equipment onto a space 602. In the background the editor manages an electronic model specification document and adds required fragments to the SUA specification. Figure 6 depicts a reasonably complex application with several machines, a robot, warehouses, shelves, personnel, and AGVs. The marked areas 604, 606 and 608 represent hazard zones that are imported or explicitly specified for the application. Marked area 604 represents an oil puddle, marked area 606 represents a work bench and marked area 608 represents a conveyor belt.

[0097] An example of the effectiveness of the system 100 can be observed in the narrow corridor 610. In case only one AGV is present in the factory, the only area with an entrapment risk is "shelf 2" 612. If a person enters the "shelf2" area 612 and an AGV 614 enters after the personnel, the personnel would have no way to get out of shelf2 area 612, and therefore no escape route. This represents an unacceptable risk. Such an unacceptable risk can be mitigated by an entry control safety function to the shelf. However, upon adding another AGV 616 of the same type as the first AGV 614, a new hazard zone appears in the corridor 610. This may be surprising at first since only acceptable and already certified systems are participating. However, there is a possibility of new emerging hazard in which a person may be trapped between two AGVs along the corridor 610. For a human assessor, it might be difficult to identify such emerging hazards of multiple

interacting systems.

[0098] In some embodiments, the system 100 may be realised directly in hardware, for example via the use of field-programmable gate array (FPGA) for composable safe and secure systems. Each critical component of a system could be embedded with or connected to an integrated circuit (IC) chip 700 (see Fig. 7). The IC chip 700 comprises the electronic model specification and an embedded engine configured to perform the functions of the evaluation engine 160. The electronic model specification can be compiled by the evaluation engine 160 at run time to form a risk model which can contain all relevant hazards and mitigation of the component, including its safety and security profile.

[0099] In some embodiments, the system 100 can also be deployed as a service over a network 800 (see Fig. 8). A node in the network 800 can be hosting the evaluation engine 160. The node provides an entry point for the execution of the risk evaluation. The electronic model specification 120 and associated fragments may be hosted by various network nodes 820 in the network 800. A non-limiting example of a node 820 is a vendor's website. The system 100 service engine 160 may consolidate or combine all the electronic model specification fragments. The service engine can provide judgements for received documents on demand.

[00100] In some embodiments, the system can be realized as a plugin for a design tool to assess conformance of the SUA throughout various phases of the design (see for example the editor of Fig. 6).

[00101] In normal operations, the system 100 may not be considered or offered as an active safety function and/or security countermeasure in operation to ensure independence with respect to the SUA. However, it is contemplated that the system 100 has the capabilities to provide useful information of existing gaps to be fixed by the user in a passive manner.

[00102] Notwithstanding the above, the system 100 can potentially be raised to the level of an active safety function and actively assure safety and security of an SUA where independence may still be achieved.

[00103] According to another aspect of the disclosure there is a method for modelling risks associated with a SUA. Fig. 9 shows an embodiment of the method 900, comprising the steps of: (a.) defining an application section associated with at least one element of the SUA (step s902); (b.) defining within the application section at least one of a safety section and a security section associated with the at least one element, the at least one of a safety section and/or security section comprises a plurality of risk related properties (step s904); (c.) mapping the plurality of risk related properties between a natural language to an system semantic, the system semantic associated with a physical or functional property of the SUA (step s906); (d.) specifying at least one condition associated with at least one of a safety breach and a security breach to materialize (step s908); and forming an electronic model specification (step s910).

[00104] In some embodiments, the method 900 may include the step of specifying a definition section defining a plurality of general elements associated with the SUA (step s912).

[00105] In some embodiments, the step of defining an application section further includes the step of specifying a world section (step s914), the world section comprises at least one non-risk related property *per se*. Examples of a non-risk related property include law of physics, environmental parameters such as temperature and pressure etc. Although non-related related properties may not be risk related property, they may be utilized as threshold for risks to materialize. For example, a temperature threshold may be set such that exceeding the temperature threshold will result in the materialization of an explosion risk.

[00106] The method 900 may be supplemented with a method 1000 for assessing risks associated with a SUA (SUA). With reference to Fig. 10, the method 1000 commences with the step of generating or creating an electronic model specification in accordance with method 900 (step s1002). The method 1000 then proceeds to a step of configuring the system 100 (step s1004). The configuration determines the boundary conditions of the execution of the evaluation (e.g. which features are being used in the execution of the evaluation, types of interfaces that are available, mode of execution, etc.)

[00107] After the configuration is done, the next step involves the step of parsing the electronic model specification documents according to the rules of the modelling language (step s1006) to generate a specification 120 associated with the SUA. The parsing step includes a step of interpreting the parsed document to process the definitions specified in the electronic model specification (step s1008). The structure and implementation of the modelling language results in a modular and extendible specification. For example, the electronic model specification may define custom types to model an SUA. The definitions might also modify how values are being interpreted (e.g. metric vs imperial unit system). The parsing step may also include the step of combining or consolidating all referenced specification fragments via an import function (step s1010). It is appreciable that the referenced electronic model specification fragments may be locally available or may be remotely available. For example, equipment vendors might choose to make an electronic model specification (fragment) available through a unique URI of their company's domain. Any loaded fragment will be recursively evaluated using the same process. It is appreciable that if there is no specification fragment to be imported, the consolidating step may be skipped.

[00108] After all relevant (or necessary) electronic model specifications have been imported, the most generic version of the risk model is available. The risk model then undergoes script evaluation and solver evaluation to identify one or more unmitigated risks associated with the SUA. The following steps s1012 and s1014 facilitate adaptive and optimized risk assessment. First, all referenced parameters from an SUA are collected (step s1012) so that the most current or recent parameters of the SUA are accounted for at run time. These might include, among others, current operating conditions, tasks to execute, and derived or predicted parameters from a simulation. Once the data collection process has completed all derived expression (conjunctive formulas) can be processed via script evaluation and constraint solvers (step s1014). For example, an expression "total weight of an AGV" may be an expression of the sum of its components and its current transport load. The "script" evaluation step first narrow down computational complexity associated with, for example, whether the total weight of the AGV exceeds a predetermined constraint (e.g. weight limit) before solver

evaluation. Traditional constraint solvers suffer from a huge increase of state space when applied to large, real-world problems. The "script" evaluation phase reduces the complexity for constraint solvers.

[00109] After the script and solver evaluation, a deterministic model, such as an SMT model, is generated (step s1016) which represents the input for the solver to find unmitigated risks. For example, the model solver might find an assignment of solver variables that would constitute an unacceptable possibility, which constitutes a hazard that can inflict harm. (e.g. "the user stands in-front of the machine" AND "the machine is on" AND "the door is open" AND "user has one hand free" THEN "user might get cut by rotating equipment"). The results of the model solver phase are parsed, and an evaluation report is generated. The report generation is flexible to cater to the needs of further automatic processing (e.g. by design tools) or for interpretation of a human assessor.

[00110] The method 900 and/or method 1000 may be implemented on a computer readable medium, such as one or more computer devices. As an example, the generation of an electronic model specification via a text editor or graphical editor may be performed on a computing device and the assessing steps in method 1000 implemented on a host server. In some embodiments, to mitigate possibilities of tempering of evaluation process and results, the method 900 and/or method 1000 may be implemented in a blockchain network.

[00111] It is contemplated that the system 100 and method 900, 1000 may be used to support various use cases as follows:

[00112] Risk assessment— The system 100 can be integrated in the traditional workflow of safety and security assessment. It replaces the way risks (hazards and/or threats) and mitigations or countermeasures are documented and formalizes and restructures the risk assessment process. Instead of human-only readable documentation, the system 100 formalizes the documentation and provides a list of conjunctive formulas such that automatic assessment becomes feasible. It is contemplated that the system 100 can be part of the R&D activities for the design and manufacturing of components, products and sub-systems destined

for IIoT contexts.

[00113] Run-time risk monitor— The system 100 can be deployed alongside an already validated system application in terms of safety and security to dynamically re-evaluate conformance of the SUA when parameters of the SUA changes. The main value is derived from optimizations that become possible due to parameterized assessments and relaxing of worst-case assumptions. Even if the system 100 does not accept an SUA, the operator might still decide to run it anyway at his own discretion and taking responsibility of the flagged risks.

[00114] Black box assessment— The system 100 may be used in a black-box assessment mode. In this mode, part of the electronic model specification is either remotely available and/or may be encrypted, such as binary encrypted. A user of a piece of equipment that forms part of an original SUA electronic model specification might decide to modify a part of the equipment. Such modifications may include the replacement of one or more motors, or adding a new piece of equipment. However, the user may not have access to the risk assessment of the original SUA. This might be for reasons of intellectual property protection, or simple economic reasons. The system 100 can allow the user to proceed anyway. Using the modelling language, the user can create an electronic model specification fragment containing only his changes. As the electronic model specification fragment includes additional conjunctive conditions representing the risks attributed by the new equipment, the evaluation engine 160 can re-evaluate the entire system 100 with the newly added electronic model specification fragment, without disclosing any of the details of the original system 100. For example, if the modification may be rejected because the modification which includes a new motor draws more power, which in turn increases the temperature of the power supply, which then creates an unmitigated risk. The original SUA vendor may define level of details for the assessment report. If the vendor does not want to give away specification of the power supply, the system could simply be rejected without further explanation.

[00115] Assistive tool— The method 900 for risk modelling and/or the method 1000 for risk assessment may be integrated with existing system design tools. The computer-aided tool illustrated in Fig. 6 may be used as an example. At various

stages of system design, the system 100 may be invoked to gather insights of the SUA's hypothetical acceptability. The assessment will likely be only indicative as the electronic model specification 120 at various stages may not yet be complete and therefore not approved by a TIC expert. In some embodiments, the methods 900 and 1000 will only be able to judge that an SUA 1900 has an unmitigated risk but will not be able to propose a solution. It will, however, be able to judge the solution as far as it has been modelled based on the modelling language.

[00116] Scenario testing and What-if analysis— By offering a parameterized conformity assessment, the system 100 and methods 900, 1000 can be used to model and evaluate different what-if scenarios and explore implications of modifications for SUA acceptability. Such studies could further support the improvement or optimization of the system design, e.g. by highlighting if acceptability is only achieved in a narrow parameter space.

[00117] In some embodiments, the method 900 and/or the method 1000 can be encoded in the form of software computer codes or computer programs. The computer programs include processor-executable instructions that are stored on at least one non-transitory computer-readable medium. The computer programs may also include or rely on stored data. The computer programs may encompass a basic input/output system (BIOS) that interacts with hardware of the special purpose computer, device drivers that interact with particular devices of the special purpose computer, one or more operating systems, user applications, background services, background applications, etc.

[00118] It should be further appreciated by the person skilled in the art that variations and combinations of features described above, not being alternatives or substitutes, may be combined to form yet further embodiments falling within the intended scope of the invention.

CLAIMS

1. A system for modelling and assessment of risks comprising
at least one electronic model specification associated with a system under
assessment (SUA), the electronic model specification comprises
an application section associated with at least one element of the SUA;
the application section includes at least one of a safety section and a security section
associated with the at least one element; the at least one of a safety section and
security section comprises a plurality of risk related properties; the plurality of risk
related properties mapped from a natural language to a system semantic, the system
semantic associated with a physical or functional property of the SUA;
a condition section specifying at least one condition associated with at
least one of a safety risk and a security risk to materialize; wherein the at least one
condition comprises at least one of the plurality of risk related properties; and
an evaluation engine configured to evaluate the at least one condition
associated with the at least one of a safety risk and a security risk to determine if an
unmitigated risk exists, wherein the evaluation engine is configured to receive a set
of reference parameters from the SUA to define a search space associated with the
at least one condition, and wherein the defined search space represents a set of
solutions that comprises one or more unmitigated risks.
2. The system of claim 1, wherein the defined search space is reduced by
substitution and removing redundant or duplicate solutions.
3. The system of claim 1 or 2, wherein the electronic model specification
comprises a definition section defining a plurality of general elements associated
with the SUA.
4. The system of any one of the preceding claims, wherein the application section
comprises a world section, the world section comprises at least one general
property.

5. The system of any one of the preceding claims hosted by a network, wherein the at least one electronic model specification resides in a first network node and the evaluation engine resides in a second network node.
6. The system of any one of the preceding claims, further comprises a plurality of electronic model specifications, wherein each of the plurality of electronic model specifications is associated with at least one of an equipment, an operation, a facility, an infrastructure, a vehicle, a furniture of the SUA.
7. The system of any one of claims 1 to 6, wherein the search space is represented as a deterministic model.
8. The system of claim 7, wherein the deterministic model is a SMT model.
9. The system of claim 7 or 8, wherein the deterministic model is evaluated to a Boolean result.
10. The system of claim 1, wherein the at least one condition is represented as a Boolean formula of the plurality of risk related properties.
11. The system of claim 10, wherein the evaluation engine is operable to generate an evaluation model, the evaluation model includes the Boolean formula.
12. The system of claim 9 and 11, wherein if the Boolean formula is evaluated to a Boolean "True", the evaluation engine evaluates that an unmitigated risk is present, and wherein if the conjunctive formula is evaluated to a Boolean "False", the evaluation engine evaluates that the unmitigated risk is not present.
13. A method for modelling risks of a system under assessment (SUA) comprising the steps of:
 - (a.) defining an application section associated with at least one element of the SUA;
 - (b.) defining within the application section at least one of a safety section and a security section associated with the at least one element, the at least one of a safety

section and security section comprises a plurality of risk related properties;

(c.) mapping the plurality of risk related properties from a natural language to a system semantic, the system semantic associated with a physical or functional property of the SUA;

(d.) specifying at least one condition associated with at least one of a safety risk and a security risk to materialize;

(e.) receiving a set of reference parameters from the SUA to define a search space associated with the at least one condition, wherein the defined search space represents a set of solutions that comprises one or more unmitigated risks; and

(f.) forming an electronic model specification associated with the SUA.

14. The method of claim 13, further including the step of specifying a definition section defining a plurality of general elements associated with the SUA.

15. The method of claim 13 or 14, wherein the step of forming the electronic model specification includes the step of combining a plurality of electronic model specification fragments.

16. A method for assessing risks associated with a system under assessment (SUA) comprising the steps of:

(a.) creating an electronic model specification associated with the SUA;

(b.) configuring the electronic model specification for assessment of at least one risk associated with the SUA;

(c.) parsing the electronic model specification according to the rules of a modelling language to generate a risk model associated with the SUA, the risk model comprises at least one risk; and

(d.) evaluating the risk model to determine if at least one unmitigated risk exists

wherein the generation of the risk model comprises the step of defining a search space associated with at least one condition, wherein the search space represents a set of solutions that comprises one or more unmitigated risks.

17. The method of claim 16, wherein the step of parsing the electronic model specification includes the step of consolidating at least one referenced electronic

model specification fragment via an import function.

18. The method of claim 16 or 17, wherein the step of defining a search space comprises the step of generating an SMT model.

19. A non-transitory computer readable medium comprising instructions which cause the execution of the method of any one of claims 16-18 when the instructions are executed by a processor.

20. A non-transitory computer readable medium comprising instructions which cause the execution of the method of any one of claims 13-15 to create an electronic model specification.