Meta-modelling for Ecosystems Security

Tristan Caulfield[1(✉)], Marius-Constantin Ilau[1], and David Pym[1,2]

[1] University College London, London, UK
{t.caulfield,marius-constantin.ilau.18,d.pym}@ucl.ac.uk
[2] Institute of Philosophy, University of London, London, UK

Abstract. As the world has evolved to become ever more dependent on complex ecosystems of large, interacting systems, it has become ever more important to be able to reason rigorously about the design, construction, and behaviour not only of individual systems—which may include aspects related to all of people, process, and technology—but also of their assembly into ecosystems. In such situations, it is inevitable that no one type of model—such as mathematical models of dynamical systems, logical models of languages, or discrete event simulation models—will be sufficient to describe all of the aspects of ecosystems about which rigorous reasoning is required. We propose here a meta-theoretical framework, the 'triangle framework', within which different types of models may be categorized and their interactions, especially during the construction of models, can be understood. Its explicit goals are to facilitate a better understanding of the nature of models and to provide a more inclusive language for the description of heterogeneous models. Specifically, we identify three qualities of models, each derived from modelling goals—conceptuality, mathematicality, and executability—and explain how models will, typically, have all of these qualities to varying extents. We also show how the framework supports an analysis of how models can be co-designed by their various stakeholders within an identified translation zone within the process of model construction. We explore our ideas in the concrete setting of models encountered in a range of surveyed security papers, drawn from a diverse collection of security conferences. Although descriptive in nature, we envision this framework as a necessary first step in the development of a methodology for heterogeneous model design and construction, diverse enough to characterize the myriad of model types used in the field of information security while at the same time addressing validation concerns that can reduce their usability in the area of security decision-making.

Keywords: Systems · Ecosystems · Models · Qualities · Methodology · Co-design · Translation zone · Security · Modelling

This work has been partially supported by the UK EPSRC research grant EP/R006865/1.

D. Jiang and H. Song (Eds.): SIMUtools 2021, LNICST 424, pp. 259–283, 2022.
https://doi.org/10.1007/978-3-030-97124-3_22

1 Introduction

There is a famous quote from Grace Hopper:

> 'Life was simple before World War II. After that, we had systems.'

Now, systems are pervasive. They interact with and depend on each other and we, in turn, depend on them. It has become important to be able to think about not just a single system, but also its interactions with other systems—it has become necessary to think of *ecosystems*.

From the perspective of security, it is particularly significant that our ecosystems of concern are *socio-technical*, encompassing not only technical components, but also economic, human, and policy or regulatory aspects.

It is of increasing importance to be able to reason rigorously about the design and behaviour of systems and ecosystems. In particular, is of increasing importance to be able to reason rigorously about the security of systems and ecosystems. A key approach to reasoning about systems is based on the idea of modelling.

Systems models can take many forms. Here we discuss what, we shall argue, are the key categories of models.

- Models may, of course, be expressed in the language of mathematics—perhaps using tools such as differential and integral equations, stochastic processes, or even the methods of abstract algebra—in order to understand the structure of a system.
- Models may also be essentially computational, expressed in a programming language for the purpose of being executed—perhaps as simulations, such as in the *Monte Carlo*-style—in order observe the behaviours of the system.
- Models may be essentially conceptual, perhaps expressed using rigorous natural language or pictorial representation.

Different types of models are appropriate for capturing different types of questions about different types of models. However, it is often the case that combinations of different types of models are not only useful, but essential. For example, within security economics, it may be necessary to combine an executable model of a system, together with a mathematical/economic model of the value of different policy régimes, all based on a conceptual model of the choice of applicable policies and their implementation. See, for example, [11,13,14]. Similarly, Beautement et al.'s 'compliance budget' [8] combines a conceptual model of employees' behaviours within an organization and an economic model of the consequences of their behavioural choices for productivity.

In this paper, we present a meta-theoretical framework within which we can categorize the different types of ecosystem models that are available and understand their relationships to one another in general and the interactions of types of models of particular ecosystems. We argue that this framework represents an important first step in the development of a methodology for heterogeneous model design and construction because it offers a common language for the description of basic properties of models from different research traditions. Furthermore, the application of such a methodology on information security models

requires an important, yet often omitted debate about validation. To even be able to define what validation is in the context of heterogeneous models requires at least a way of describing model properties in relation to model goals and types of knowledge employed. This is exactly what our framework focuses on. In the future, we hope to produce more practical results such as correlations between a model's goals, the types of knowledge it employs, the means of design in its translation zone, its triangle configuration, and its success of implementation and deployment in the real world. However, the domain exploration carried out using this approach in Sect. 5 shows that it manages to encompass the domain's diversity, making it a reasonable alternative for the description of information security models.

We begin, in Sect. 2, by considering the classical characterization of perspectives on modelling in terms Logical Empiricism and Relativism. We explain some of the philosophical background of the two paradigms and describe the methodological and practical issues that lead to a need for combining them in the context of modelling ecosystems.

In Sect. 3, by introducing the 'triangle' framework, we construct a conceptualization of the nature of models that characterizes the key categories of models according to three anchor points of properties:

- **Conceptuality**: describing the components of an ecosystem, their interrelationships, and their evolution in informal, yet rigorous, terms. For example, a careful description of a river system, including its sources, its estuaries, and its flood plains, together with an explantion of the circumstance in which they might be overwhelmed.
- **Mathematicality**: describing the components of an ecosystem, their interrelationships, and their evolution in the language of mathematics. For example, a detailed hydro-mechanical description, using the mathematics of fluid dynamics, of a system of sluices that controls flows within a water distribution network.
- **Executability**: describing the components of an ecosystem, their interrelationships, and their evolution in languages that can be interpreted and executed by machines. For example, A computer program that simulates the effects of excess rainfall within the watershed of a river system, demonstrating graphically the expected extent and duration of flooding.

We explain our interpretation of the properties and their qualitative nature and provide some directions regarding the importance of the framework outside its use for classification.

In Sect. 4, we explain how models are constructed within the context of the triangle framework and how the rôle of co-design, within a translation zone for the different stakeholders in the modelling process, is central to the use of the framework.

In Sect. 5, we explain how ideas we are suggesting play out in the setting of security modelling. In particular, we report on how the triangle framework gives an account of the modelling that can be found in a wide array of papers in a diverse range of security conferences. Our choice of security for empirical

analysis is at once both specific and generic: although the papers considered deal with specific security problems, the topic of security can be seen as providing a generic perspective on the behaviour of systems.

In Sect. 6, we consider the implications of using our framework for validating models, especially in the context of modelling large-scale ecosystems.

Finally, in Sect. 7, we summarize our contribution and briefly consider some directions for developing further the ideas we have introduced.

2 Philosophical Aspects of Models

There are predominantly two traditions on the nature of models, logical empiricist and relativist, dating back to the rationalist and empiricist schools of thought of the 16th century, and being further developed during the 19th and 20th century philosophical split between continental and analytical philosophy.

- *Logical empiricism.* Models are understood as an objective and absolute representations of systems. Validation is a process that is formal, algorithmic, and focussed on the accuracy of both the structure and outputs of the model. A single structural misrepresentation is enough to invalidate the model, regardless of its outputs. The overall modelling process is believed to reveal the truth if performed adequately.
- *Relativism.* Models are subjective; that is, they are just singular instantiations from a continuum of possible representations of the system. Validation is semi-formal, 'a gradual process of building confidence in the usefulness of a model' [6]. Such models do not attempt to reveal absolute truth, but rather produce a useful model given the modeller's goals.

Neither of these two views can solely be used for constructing diverse enough models for ecosystems security. Some of the reasons for this derive from some quite basic problems with, or objections to, each of these views.

Problems with Logical Empiricism. Theoretically, Logical Empiricism is struggling to overcome the epistemic and methodological implications of Kuhn's description of the acceptance of scientific theories and Popper's theory of falsification. Both the acceptance of Kuhn's thesis—stating that scientific progress is not achieved through the accumulation of knowledge but rather subjective community paradigm shifts—and Popper's view that scientific advancement can only be achieved through falsification rather than proving absolute truths, greatly reduce the focus on truth that logical empiricism held of a highest importance. Additionally, some of its practical caveats come from the difficulty of working with knowledge elements that have not been fully proven, completely accepted by the research community or that are yet unquantifiable because the underpinning theoretical work is not mature enough.

In the specific case of security, the most common such elements are related to the uncertainty introduced by human actors—either attackers or non-malicious actors—or the discovery of new technical attack vectors.

Also, logical empiricism requires an extremely powerful validation process which is not always possible in the case of complex cyber-physical systems. Particularly the structural representation criterion can lead to the invalidation of models that are producing seemingly viable results, which can be considered a quality upper bound, but certain phenomenons introduced by humans do not fit this type of approach because they lack the theoretical certainty.

In the best case scenario, a purely logical empiricist model can be used in well defined and seemingly stable conditions, for example when used to determine the trajectory of a rocket given the precise atmospheric conditions, but in today's cyber-physical ecosystems, this is rarely the case.

Problems with Relativism. Under a different set of circumstances, relativist stances hold the figuratively theoretic high ground in modern philosophy of science, in the sense that the subjectivity of knowledge and truth and the social construction of reality are well established notions.

However, this interpretative way of viewing reality also suffers from multiple caveats when singularly employed as paradigm for model construction.

First of all an ecosystemic model is composed of a high number of sub-models, each with their own primary goal, resources, processes, etc. To be able to obtain the relativistic notion of knowledge about those sub-systems, lengthy processes of data collection—interviews, debates—must be carried out by the modeller for the better understanding of the reality as seen by all the parts involved in the system under study. Although methodologically this might not be considered an actual problem, we must consider the fact that models are used today for tackling real world issues in reduced time-frames. The early usage of predictive models at the start of the Covid pandemic can be seen as a relevant example.

Secondly, and possibly the strongest advantage of this method, its openness, can also be its biggest problem in practice. If each sub-model is constructed with a different understanding of reality (the ones of the actors involved in it)—this can be seen in studies about the formal and alternative power structure of organisations—their integration becomes a serious issue. Albeit not directly concerned with models constructed based on a relativist philosophy of science, works such as [13,14] or [11] provide a practical approach of this issue by using interfaces to specify the desired type of output moving between sub models without trying to alter the underlying notions of knowledge that led to the production of that output.

Thirdly, models constructed in this paradigm are complicated to use when trying to determine why certain decisions have been taken. Applying a simple root cause analysis method on a decision taken by such a model might lead either to a return to the real world simulated actors—if they are humans—for further explanations or to uncertainty.

On one hand, although methodologically sound, returning to the simulated actors is a lengthy process that can end up greatly delaying model implementation and should only be used in cases where there exists an evidence of a lack of understanding.

On the other hand, a model whose decisions cannot be certainly explained will hardly be accepted by decision makers who might prefer to use their own understanding of the system because it manifests a smaller degree of uncertainty. Studying which method would outperform the other is not the goal of this paper.

A New Perspective is Needed. As seen above, neither logical empiricism nor relativism alone offer a suitable methodology for modelling the dynamical systems of today. In a certain sense, the former approach places models under a set of too-powerful constraints, whereas the latter presents difficulties in choosing a set of constraints or quality measures usable in practice.

The logical empiricist perspective can provide speed and trace-ability by structure and method where the available system knowledge is suitable: the main phenomenons to be included in the model have been previously studied by the scientific community and an accepted theory has been formulated, and the phenomenons can be translated to quantifiable data types.

On the other hand, the relativist perspective provides better descriptive power and increases the overall comprehensibility of the model. Therefore, we believe that the need of a modelling framework that balances both views is justifiable.

In the next section, we introduce the Triangle Framework.

3 The Triangle Framework

The development of the logical empiricist and relativist views of models was driven by a desire to understand the nature, method of obtaining and validation of scientific truth. These perspectives were developed before the advent of computational modelling, which includes approaches to understanding dynamical systems such as discrete event modelling and Monte Carlo simulation.

Although computational models exhibit aspects of both logical empiricist and relativist views, we argue that their executable aspects give rise to a distinct perspective. As a result, we propose a new framework—the triangle framework—in which the perspective provided by executable models stands alongside that provided by the logical empiricist and relativist views of models with equivalent significance.

The triangle framework, as depicted in Fig. 1, identifies the key or core components of models, and the relationships between them, in terms of three qualities: conceptuality, mathematicality, and executability.

– *Conceptuality*—Aligned with the cognitive science perspective, we define concepts as mental representations of phenomena. The conceptuality of a model then refers to the degree to which its core components and the relationships between them exist and are directly expressed as such representations, through rigorous natural language, pictures, or diagrams, for example. In relation to the other qualities, the degree of conceptuality decreases as the key components of the model are expressed in an increasingly mathematical or executable way.

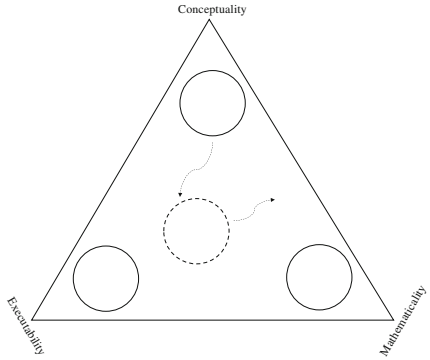


Fig. 1. The triangle framework

- *Mathematicality*—This refers to the degree to which the elements and relationships of a model are expressed using mathematical constructs. For example, models might be expressed as systems of equations or logical formulae.
- *Executability*—This represents the degree to which the elements and relationships of a model are simulated in a physical or computational environment.

These qualities can exist in combination—models may have components that exhibit characteristics of all three. They also trade off against one another; that is, a highly conceptual model will be less mathematical and executable, or a highly executable one will be less conceptual and mathematical. Although we talk about degree, we don't mean a strict measure—there are no units of mathematicality, executability, or conceptuality, and they are quantified subjectively. However, these qualities, and the triangle framework more generally, give us a language for organizing and talking about models. Fig. 1 illustrates how we think of these three types of model and their relationships: in a given model, the relative significance of each of the components determines, by proximity, the position of the model within the triangle; furthermore, the position of the model may change as it evolves during its construction.

We explore empirically the appropriateness of these qualities for describing the components of models, in the setting of security, in Sect. 5.

We suggest that the importance of our proposed framework goes beyond its use for categorization, and hence understanding the relationships between, extant models and types of models. Specifically, we suggest that it can

- guide an on-going modelling process, helping the stakeholders to decide on what property to focus, to increase the chance of better representing the system, in accordance to their goals;
- reduce the risk of producing a model that cannot be practically used to achieve the goals of the modelling;
- can be used as common reference point during co-design: stakeholders from various domains will have a common point for their arguments; serves as a common language for structuring the process;

– offer a way of analysing a model through all the design and construction stages rather than just at the end and therefore, complement an agile testing methodology, providing the following advantages: reduced development time because both the customer and modeller have a common way of understanding how the model evolves and can offer focussed feedback or directions, easier for the customer to formulate requirements, constant focus on common quality metrics derived from the framework, ability to assess the model at any time; and
– lead to a way of comparing models based on the properties of sub-models.

We have mentioned again here the rôle of co-design in the modelling process and how the triangle framework serves to support it. We consider this issue in greater detail in Sect. 4.

4 Model Construction

Whereas the previous section was focussed on model description and interpretation according to a small subset of properties, the current one will examine the necessary methodological elements for the construction of ecosystem models.

Traditionally, in mathematical modelling, models have been constructed using the classical construction cycle depicted in Fig. 2. Succinctly, this represents an iterative process based on multiple stages:

– observing the phenomenon domain,
– constructing a candidate model based on the observations,
– deducing the mathematical consequences of the model,
– interpreting the consequences of the model in the domain, and
– comparing, for validation, the correspondence between these interpretations and the observed reality of the domain.

These stages are repeated until a criterion of adequacy for the intended purpose of the model, often determined by the judgement of the modellers, is passed and the model is considered to be a good enough representation of the system under study. Classical examples of this modelling approach can be observed in [5] as an application for global supply chain management, [46] as a tool for analysing credit scoring or [23] production scheduling.

The efficacy of this modelling process depends on certain key, usually unstated, assumptions about the modelling task:

– The structure and behaviour of the domain is clearly understood in conceptual or engineering terms. For example, the corrosion over time of a metal piston inside a diesel engine is a well-researched phenomenon attributed to the formation of sulphuric acid at the contact between low-grade fuels and water. Such a phenomenon is a good candidate for mathematical modelling, perhaps in the context of testing different materials for the construction of engine parts.

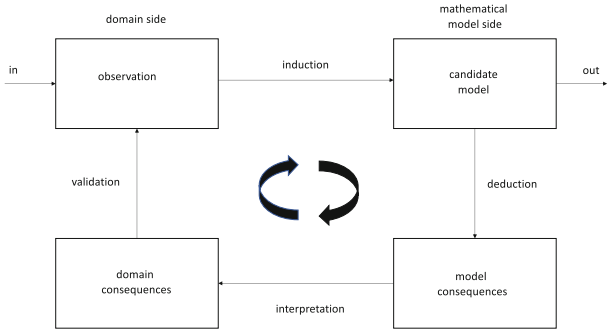


Fig. 2. The classical mathematical modelling cycle (see, e.g., [33])

- The data that can be collected about the domain is essentially unambiguously identified. For example, modelling an organization's employees productivity levels for the sake of improving them might prove an extremely complicated task for mathematical modelling since, essentially, employees might be motivated by extremely subjective concerns and the interpretation of those concerns might differ from person to person.
- The questions that the model is intended to address are identified independently of the detailed design choices required for the construction of a model. For example, building a model for the purpose of optimizing the production time of hardware components in a fully automated manufacturing environment is well suited for the traditional modelling methodology described above. Contrarily, simulating the same system for the purpose of understanding its behaviour and only then deciding what can be optimized—for example, for a reduction of costs—would be more suited to a different approach.

The ecosystems with which modellers in the modern world are presented pose much richer challenges for the form, design, and construction of models. Such ecosystems contain not only components that are clearly susceptible to mathematical modelling, but also include components—such as people and organizations, policies, and economic influences—which require models to have conceptual and computational (i.e., executable) components. In [39], Pidd puts this diversity of components on behalf of the design of human activity systems and Mingers [35] argues for a 'multimethodological' approach for the exploration of such systems. For example, one might imagine a model investigating the impact of malware infection on an organization's profits. However, the probability of infection of a machine is influenced both by the behaviour of the employees given a security policy and by technical elements such as the last installed patch on the machine. Furthermore, the malware spreading pattern heavily depends on network segmentation or existing countermeasures and the impact cannot be directly computed because of factors such as reputation loss. Therefore, one can easily observe that to understand the phenomenon of malware infection and its impact on an organization using a model requires distinct approaches for at least the above described components—employee behaviour, security policy, state of patching, network configuration, reputation loss.

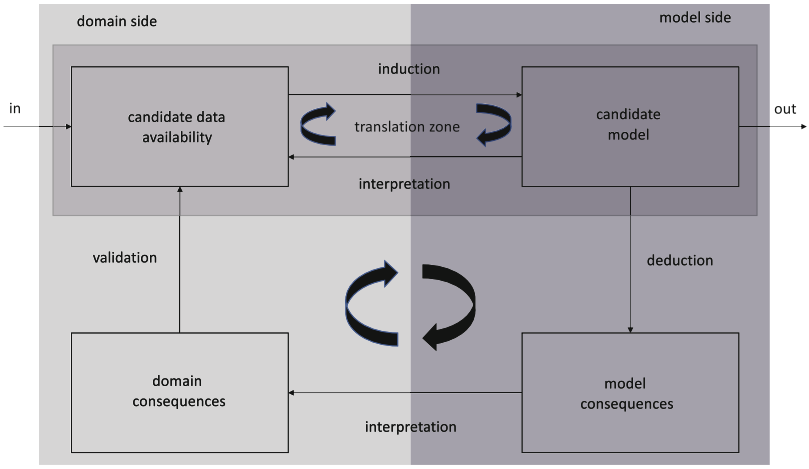


Fig. 3. Co-design in the translation zone

Moreover, it is in the very nature of such domains that the assumptions upon which the basic mathematical modelling cycle depends, as sketched above, do not necessarily hold:

- The structure and behaviour of the domain may depend on the behaviours of individuals and organizations, subject to incentives and policy constraints.
- It may be unclear what data is available for collection.
- It may be unclear, prior to the observation of the ecosystem, what questions can be properly formulated, depending on behaviours and the availability of data.

The key consequence is that a richer methodology of model construction is required in order to establish the cycle of model construction. A wide-ranging collection of articles on approaches to modelling and its challenges may be found in [19].

In the absence of such a priori foundations, we argue that a methodology that is grounded in the principles of co-design is required. What does this mean in the setting of ecosystems modelling? First, the classical modelling cycle, which need not be restricted to wholly mathematical models, should not be abandoned. Once a candidate model has been established, it provides the basis of the cycle of development that leads to an acceptable model. Second, it must, however, be adapted to account for the co-design process by which an initial candidate model is established.

Three key changes are required, all of which constitute proper generalizations of their counterparts in the basic modelling cycle. First, the observation of the domain involves essentially the discovery of the domain's structure and behaviour. Second, the initial postulation of candidate models is contingent upon this discovery process. Third, there is an induction-interpretation feedback loop

between domain observation and candidate model postulation. This situation is depicted in Fig. 3.

In the literature regarding organizational learning, this type of problem-structuring as continuous exploration has been explored in works such as [4] or [29] and represents an important element of modelling methodologies such as Checkland's soft systems methodology [15], cognitive mapping [1,18], or qualitative system dynamics [47].

These structural alterations to the methodology are not, however, sufficient alone. Whereas in the basic modelling cycle experts in the domain will have a relatively limited rôle of supplying information to the modellers, in the co-design sub-cycle their rôle is one of equal significance, forming a component of the modelling process, by identifying the structure and behaviour of the domain together with its policy constraints alongside the modellers' ability to model both the domain and its policies.

Thus, the cycle of domain observation and candidate model construction, as depicted in the upper half of Fig. 3, forms the *translation zone* of the dialogue between the domain experts and the modelling experts, which may have different perspectives and understandings of the domain and of models, and use different languages for expressing those perspectives. The translation zone enables the development of a shared understanding—in a controlled way that is focussed on the needs of the modelling project, managing the expectations of both the domain experts and model experts—as a consequence of the process.

Overall, this establishes a co-design process that

- ensures the participation of both modellers and domain experts, whose requirements are identified, characterized, and (possibly) modified according to the constraints of model design, construction, and deployment,
- identifies modelling objectives, including questions about the domain that are to be addressed, according to the identified requirements,
- designs and constructs appropriate models, and
- ensures that the available data that are identified during the process support the requirements of the models that are constructed.

As with the basic (mathematical) modelling cycle, as depicted in Fig. 2, the description of the co-design cycle—with a translation zone, as depicted in Fig. 3—does not specify the exit criteria for determining that a sufficiently accurate model has been constructed. In both cases, the criteria must be determined case-by-case, but always respecting a few key general considerations relative to which the notion of accuracy must be calibrated: remembering that 'the map is not the territory' [30]; appropriate level of detail; timeliness; and cost-effectiveness.

We argue that the triangle framework provides a conceptual setting within which the development of models through co-design in the translation zone can be characterized. First, the triangle offers the prospect of a common conceptual space—to some extent, even, a common language—to the domain and model experts. Second, while the three properties that anchor the corners of the triangle are difficult to quantify, the modeller, together with the domain expert, must

nevertheless decide what spread of properties is required in order to deliver the objectives of the project: this is an essential aspect of modelling complex, socio-technical ecosystems, for which a model of one conceptual type is unlikely to be adequate in most situations. Third, as the co-design process via the translation zone proceeds, the choices presented in the initial model will, typically, evolve, thereby moving the model's location within the triangle.

A model's evolution during its construction can be seen as a sequence of configurations of the three qualities, with the evolution being driven by the co-design interaction of the stakeholders in the translation zone of Fig. 3.

As an example of this, recent (as yet unpublished [12]) work focuses on modelling the surge capacity of hospital emergency departments to help them prepare for major incidents, when a large number of seriously-injured patients arrive in a short amount of time. Building such a model requires the combined expertise of modellers and medical professionals and results in a model with conceptual, mathematical, and executable components. From the medical side, detailed knowledge of which procedures are needed by patients with different types of injuries and how teams of hospital staff with different skill sets are assembled (and reassembled, as patient flows evolve) to treat them is required. Gathering and using this information provide a good illustration of the translation zone and the way models change as they are constructed. Initially, largely conceptual 'paper-based' models were used in interviews with medical professionals, who explained their strategies for assigning teams of staff to treat patients. These were then codified initially into sets of rules and eventually embedded within executable models of the hospital emergency department. These rules and models—all considered candidate models—were presented to medical staff and evolved based on this feedback.

Some of these ideas will be illustrated in Sect. 5, where we consider a range of security examples.

5 Modelling in Security

In the previous sections, we have described the modelling triangle theoretically, and have explained how models move around the triangle during their construction.

In this section, we explore the modelling triangle in the concrete setting of security, exploring where different types of security models are placed within the triangle. We do this by looking at existing models published in recent security-related conferences and placing them on the triangle. This has several purposes: we want to get a sense of the types of models used in security, we want to understand if there is a relationship between the intended purpose of a model and its location on the triangle, and, lastly, we want to test the triangle approach.

5.1 Methodology

We select papers from five security conferences from 2020: BlackHat USA, NSPW, ACSAC, WEIS, and Gamesec. We select these conferences as they cover

a range of topics and security traditions; we look at all the papers from each conference in 2020. In total, we look at 212 research papers encompassing a range of security topics: behavioral and security management, security policy, technical exploits, machine learning, economics, and more.

For each paper, we want to: (1) determine whether or not it contains a model; (2) understand the purpose and type of model; and (3) determine an appropriate location on the triangle for the model. As a methodological basis, we use a grounded theory approach. Grounded theory has two variants: one that focuses on the emergence of properties from the data coding process guided by a theoretical understanding of the domain of study and another that denies the need of any prior domain exploration. Kelle [28] illustrates both approaches. Since we did perform a prior domain-exploration by analysing the main philosophical positions regarding models and know the properties we are looking for—conceptuality, executability, mathematicality—we adopt the first method and perform the selective coding and classification processes with the properties described above in mind.

We have chosen this study methodology for a number of reasons:

1. Grounded theory is integrative as long as the coding process is consistent. This is extremely important, since it allows the analysis of models constructed using various methodologies. 'According to Ralph, Birks, and Chapman [42], grounded theory is "methodologically dynamic" in the sense that, rather than being a complete methodology, grounded theory provides a means of constructing methods to better understand situations humans find themselves in.'
2. Grounded theory provides ecological validity. This means that theory produced using this approach is representative of the underlying body of literature surveyed. Although not as powerful as when conducted through interviews with practitioners—since in that case additional questions about the subject of study could have been asked—the novelty of the papers shows the 'state of the art' in the security field at the moment.
3. Grounded theory maintains parsimony. Namely, in a situation where multiple hypothesis exist about a certain phenomenon, the one with the smallest amount of assumptions is preferred. This allows us to maintain a relatively small number of properties, since we aim to provide practical and simple explanations of complex phenomena by attempting to link those phenomena to abstract constructs and hypothesizing relationships among those constructs.
4. Although employing both qualitative and quantitative techniques, the nature of the analysis remains qualitative and facilitates the interpretation of conceptual aspects of the models under study.

We followed the following process. First, we analysed every paper to decide whether or not it contains a model, according to our definition from Sect. 1. We used a broad understanding of 'model' to ensure we captured conceptual as well as technical and formal models and as such were quite inclusive in the papers we accept. For example, papers that construct and reason about a structured

representation of the phenomenon under study, even if descriptive, were considered models. Papers that did not include such a representation, such as those focussed on problem solving or tool building in a very specific and mostly technical focussed case were not included. Lastly, some papers included small models used for explanatory purposes, such as showing where their work fits within a system. These are also included in our analysis.

For the papers that contain models, we performed subjective coding focusing on the model description, the techniques employed in the model construction, the model purpose, and the topic. Since we wished to maintain some of the grounded theory ethos, we did not use a pre-established coding scheme in this step, and instead generated the codes as we went through the papers.

After that, we performed selective coding by linking the previously computed codes with our three primary categories—conceptuality, executability, mathematicality. At this point, we derived the 'triangle configuration' of the model under study, with the important note that we did not simply quantitatively analyse the size of the resulted categories. Deciding the relevance of the underlying codes with respect to the overall modelling goal remains a qualitative process and therefore the constructed configuration is subjective.

5.2 Findings

The intent of this study is to understand better the nature of the models employed in the information security field in 2020. Following the methodology described above, we discovered that 67% (142) of the total 212 surveyed papers did indeed employ models. The initial topic analysis and coding have produced 65 different topics that were further reduced to 35. For example, topic codes such as 'social behaviour', 'social engineering', 'community analysis', 'problem solving' or 'human oriented design' were included in the 'human oriented security' category. Table 1 illustrates the most encountered five topics for models in each conference, ranked by their total number of occurrences and having duplicates removed. Subsequently, the most encountered topics were 'attacks/exploits' and 'privacy'.

It is important to note that a model is not limited to a single topic: if one specifically focuses on attacks that affect user privacy, it would be assigned as having both the 'attacks/exploits' and 'privacy' topics. Also, the development of models for the purpose of better understanding machine learning in general can be seen as an interesting attempt at using descriptive models to understand other models.

By analysing the model's topic, goal, and construction procedure, we have produced triangle configurations for each of the surveyed conferences, which can be observed in Fig. 4. These configurations largely correspond to the publicly described conference tradition—for example, the models in Gamesec had a tendency towards mathematicality—with an interesting aspect identified in Blackhat: even though the models tackled many 'attacks/exploits' and 'hardware security' aspects—as it can be seen in Table 1—they are complemented by models with a tendency towards conceptuality that attempted to explain their functionality. Furthermore, we classified the models according to their construction method and modelling goal into five categories.

1. **Descriptive models:** Models in this category are mainly constructed using natural language descriptions, qualitative reasoning and sometimes graphs, charts or other means of visual representation. They construct a subjective representation of reality which can vary in complexity and can include both qualitative and quantitative studies as a starting point. Their primary goal is to simply describe or analyse phenomenons that are hard to quantify and therefore focus on topics such as 'human aspects of security', 'security management', 'philosophical aspects of security' or 'security policies'. However, the analysis process has revealed that such models can be used also for describing other models, not necessary phenomenons directly. As illustrated in Table 2 and Fig. 5a, models in this category represented roughly 21% of the total models encountered and had a strong tendency to be placed close to the upper corner of the triangle because of their highly descriptive nature.
2. **Simulation models:** This category contains two different types of models that have a common construction method—experimental simulations and practical demonstrations. They are comprised of interpretative executable code, constructed manually by a developer and reflecting a human interpretation of a certain phenomenon. With respect to their goal, they can either be used for experimentation, such as simulation based models coming from the dynamic systems tradition, attack demonstrations or enforcing qualitative reasoning. They focus on topics such as 'IoT', 'network security', 'software security', 'operation systems emulation', 'malware' or 'attacks/exploits' because the phenomenon under study can be quantified and represented using graph-like structures. As illustrated in Table 2 and Fig. 5b, models in this category represented roughly 26% of the total models encountered—the largest category—and were placed closer to the center of the triangle. They did not manifest a higher tendency towards the left corner because the model construction was manual and in some cases, the model was run a single time to illustrate that a certain attack was possible.
3. **Statistical models:** Models in this category are constructed using executable code that includes statistical algorithms, data science techniques, natural language processing, and even some traditional machine learning techniques not including deep learning. They construct a complex, stochastic interpretation of reality, usually employed for better understanding or making predictions about a phenomenon that is either extremely complex or would take too much time or analysis power to be understood individually. Furthermore, their most relevant aspect is that their method of producing results can be traced back and understood, with the important note that the results do not directly lead to some automated real world consequence, but require additional interpretation. The most relevant topics to this category were 'privacy', 'security management', 'economics' and 'human oriented security'. As shown in Table 2, statistical models represent almost 20% of the total surveyed models and Fig. 5e depicts them as having balanced triangle configurations, with some slight tendencies towards either conceptuality or mathematicality based on the nature of their input data. For example, a model employing natural language processing and principal component analysis techniques over qualita-

tive data obtained from interviews was placed closer to the conceptuality corner, whereas a Bayesian analysis of security investments was placed closer to the mathematicality corner.

4. **Deep Learning models:** Models in this category are constructed using deep learning and neural networks approaches and they construct a representation of reality that is similarly to statistical models, with the primary difference being the difficulty of interpreting or justifying the produced results. Because of this, they tend to be used for automated problem solving in areas such as offensive security or threat detection. Their triangle placement can be similar to that of simulation models, as Fig. 5d with the important difference that they do not manifest the slight conceptuality tendency since their phenomenon interpretation is particularly hard to understand. However, they do manifest the strongest tendency towards executability, and represent almost 20% of the total models surveyed. However, taken into account the current focus on the development of artificial intelligence explainability methods, we could observe a significant amount of models moving from the deep learning category to the statistical models one.
5. **Game-theoretic models:** This category is primarily comprised of mathematical models constructing game-theoretic interpretations of phenomena. Some of the observed models did produce analytical solutions for solving the represented games, whereas others were simply used for problem setting. In the second case, other types of model were used to produce the desired strategies in the game setting. They were usually employed in areas such as 'network security', 'risk' or 'attacks/exploits', but mostly provided the theoretical setting for another type of model to interpret. We observed the interpretation they produced was used as a setting for either deep learning or simulation models. For example, a game theory model was used to formalise the concept of cyber deception as a multi-party stochastic game and then a simulation model was used to illustrate a successful winning strategy. However, another approach was to construct a deep reinforcement learning model of the involved parties and execute it in multiple epochs such that the actors could develop increasingly better strategies while learning from their own mistakes. As Table 2 and Fig. 5c illustrate, these models can have both balanced triangle configurations and heavy tendencies towards mathematicality and represent roughly 13% of the models surveyed.

Moreover, some additional observations can be drawn when analysing the average and complete model types placement on the triangle in Figs. 6a and 6b. For example, the conceptual, deep learning and game-theoretic models can be seen as having the strongest manifested tendencies towards the triangle's corners. Subsequently, the simulation and statistics models manifested the most balanced configurations for two different reasons: simulation models had the most open approach and used internal sub-models that would have been assessed differently in isolation—for example a stochastic module for agent behaviour or an economics module for determining the risk of an actor's action—but produced balanced overall models, whereas statistical models used extremely varied input

data that introduced an additional degree of conceptuality to the mathematical methods used.

However, Fig. 6b clearly shows that the model categories are not entirely delimited by their triangle configuration: for example, models in Kaczmarczyck et al. [27], Noor et al. [34] and Xiao et al. [48] have similar, central triangle placements even though they are members of the deep learning, statistical and respectively simulation categories. Furthermore, even though their topics are also different, namely automated malware family identification, illustrating a mechanism for key distribution on automotive networks and analysing the forensic validity of approximated audit logs, they all obtain a more balanced configuration by introducing qualitative reasoning about their inner workings.

We believe that this balancing process leads to models that are easier to understand, and therefore that become more suitable for security decision-making, but that requires further work to be validated. However, at the end of this exploration of the information security domain, we can draw several conclusions.

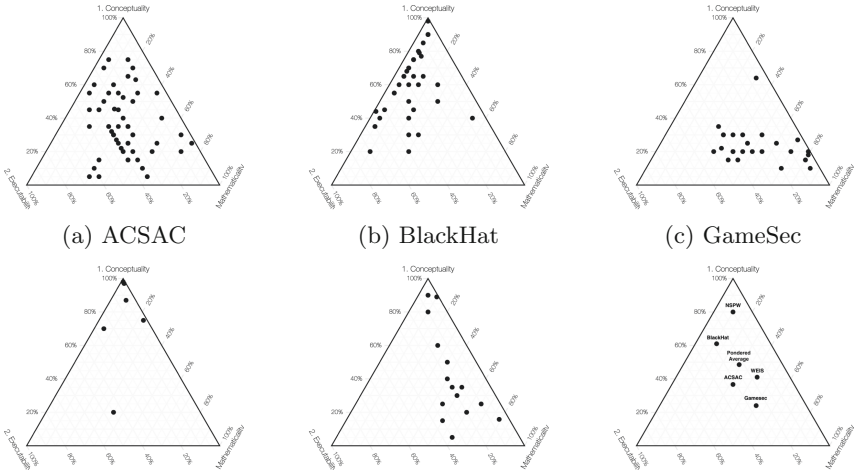
1. Models are an important tool for information security today.
2. Usually, models remain focussed on very specific problems.
3. Some models directly interact with or complement other models. This raises the question of how should models communicate with one another.
4. Some meta-modelling attempts exist, but only at theoretical level. For example, highly mathematical or conceptual models of machine learning algorithms.
5. Simulation models seem to provide a good base for constructing models with components of different types.

Table 1. Top 5 topics per conference

	Blackhat	Nspw	ACSAC	WEIS	GameSec	Total
Attacks/Exploits	19	1	12	2	3	37
Privacy	5	3	17	1	2	28
IoT	5	0	14	1	3	23
Human oriented security	7	5	5	3	2	22
Network Security	7	0	8	1	6	22
Economics	1	0	4	12	3	20
Policy	6	2	7	2	1	18
Hardware Security	10	0	3	0	4	17
Software Security	5	2	8	0	1	16
Machine Learning (as topic)	6	2	6	0	1	15
Theoretical Security	0	0	2	1	10	13
Systems architecture	6	0	2	0	4	12
Risk	2	0	4	4	1	11
Management	2	0	3	5	0	10
Game Theory	1	0	0	0	8	9

Table 2. Model types per conference

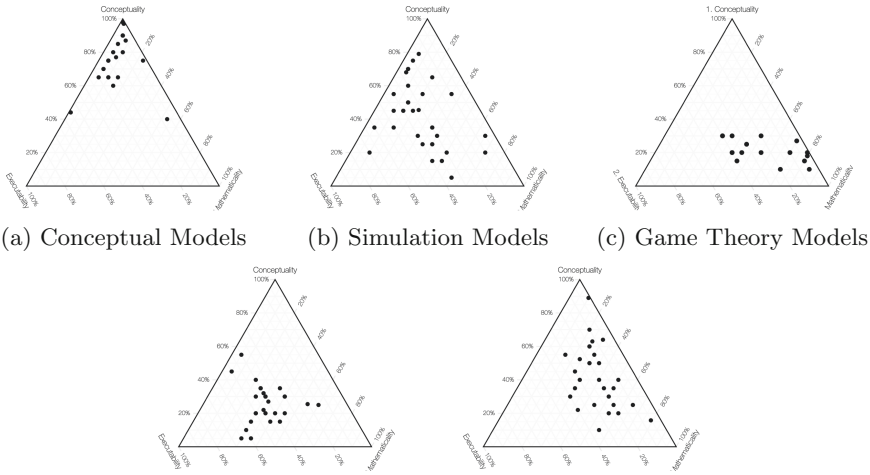
	Blackhat	Nspw	ACSAC	WEIS	GameSec	Total per type
Simulation Models	8	1	25	2	1	37
Descriptive Models	21	6	1	2	0	30
Statistical Models	2	0	15	11	1	29
Deep Learning Models	6	1	15	0	6	28
Game Theory Models	0	0	0	0	18	18
Total per conference	41	8	58	15	26	142



(a) ACSAC (b) BlackHat (c) GameSec

(d) NSPW (e) WEIS (f) Conference Averages

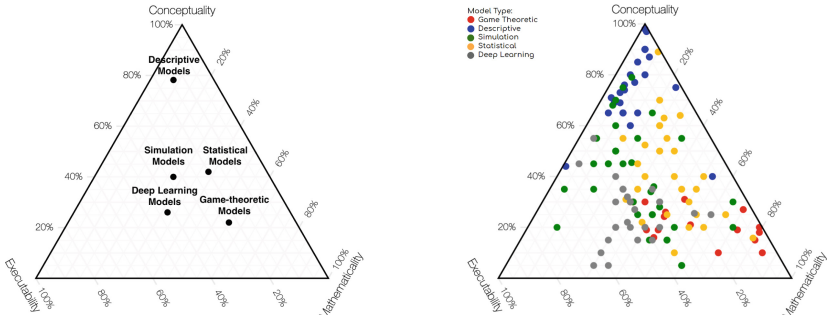
Fig. 4. Positions of papers from different conferences on the triangle



(a) Conceptual Models (b) Simulation Models (c) Game Theory Models

(d) Deep Learning Models (e) Statistical Models

Fig. 5. Positions of different model types on the triangle



(a) Average Model Types (b) Model Types

Fig. 6. Positions of different model types on the triangle

6 Implications for Validation

In the previous sections, we have focussed on constructing an integrated modelling framework for characterizing models according to three primary properties—conceptuality, mathematicality, and executability—that are directly linked to the relevant philosophical and modelling literature. We have described how these properties change during the model-construction cycle and have attempted to use this approach to explore a part of the present-day space of information security models. In the sequel, we seek to understand some of the implications that our vision might have on the ongoing debate regarding the validation of models, especially in the case of modelling large-scale ecosystems.

The validation of a model, at a general level, consists in the deployment of a set of processes that is used for testing that the model performs according to its original goal. As expressed in [6], models can be separated into at least three categories according to their primary goal: modelling for the purpose of improving a certain performance indicator of a system, modelling for testing a scientific theory, and modelling for the sake of understanding or learning about a certain system.

However, it is not the goal alone that determines the type of model to be constructed, but also the nature of the system or phenomenon under study and the available input data types and their collection process. These elements—the goal, the available data and the nature of the phenomenon under study—corroborated with the underlying philosophical implications illustrated in Sect. 2—have led to the development of different and sometimes opposing model validation methodologies in disparate domains of science. To illustrate some of these differences, we present some arguments from the economics, management science, and system dynamics literature that are of great importance for an information security context.

Starting with the management science domain, it can easily be observed that a singular position with respect to validation does not exist. For example, Naylor et al. [37] argue for a validation process that combines rationalist, empiricist and

positive economics [21], but has a primary empiricist assumption: 'A simulation model, the validity of which has not been ascertained by empirical observation, may prove to be of interest for expository or pedagogical purposes, but such a model contributes nothing to the understanding of the system being simulated' [37]. Their position is furthermore aligning to the logical empiricist ethos by the utilisation of a truth based criterion for validation. Oppositely, work such as Mitroff [36] place validation under the philosophical spectrum of experimentalism and focus on the relativity of the philosophy of science position held by the modeller. As Mitroff [36] states, 'a researcher's philosophy of science is as characteristic of him as it is of the phenomena he typically studies' and the same elements chosen as relevant for the construction of the model should be the same ones used for validation. A more practical position, directly related to the need of validating large scale models in a reasonable amount of time can be seen in House and McLeod [24]. There, the authors follow Friedman's principle [21] that assumptions can serve as scientific hypotheses even if 'unrealistic' as long as they can produce significant predictions and focus on the utility of a model rather than its relationship with truth. In the authors' own words 'A businessman cannot afford to discount a "hoped-for" infinite return as the result of an unknown expenditure for a near perfect model today. Our business world exists in the present, so the businessman will be satisfied to buy a somewhat less than a perfect model for a known cost.'

The same heterogeneity of positions with respect to validation can be seen in the economics literature. As already described, Friedman's position with respect to the need of validation for scientific hypothesis is of great importance. In the author's view, scientific assumptions do not need to be verified since they can only be validated by their own predictive power. Since models can be considered a preliminary step in the formation of scientific theories—see Grim and Rescher [22] for a more detailed discussion—Friedman's assumption has been translated to models. A subtle distinction from this criterion of predictive power can be seen in the work of Cyert and Grunberg [16]. Following Popper's falsification thesis [40], the authors believe that a model's predictive power does not necessary validate its position as scientific truth. Therefore modelers should rather focus on constructing models with high descriptive power. Nevertheless, different variations of these criteria can be found in comprehensive literature overviews such as Dhrymes et al. [17] or Radzicki [41]. Of a particular relevance is the conclusion of Dhrymes et al.: 'validation becomes a problem-dependent or decision-dependent process, differing from case to case as the proposed use of the model under consideration changes' [17].

Last but not least, we discuss some of the validation approaches employed in the system dynamics literature. Compared to management science or economics, the system dynamics literature is much more comprehensive in its attempts to tackle philosophical aspects of model validation. An important starting point is the work of Forrester [20], which can be seen as a relativist take on system dynamic validation that was primarily done in a logical empiricist fashion before him. Forrester makes the claim that 'the validity of a model should not

be separated from the validity and the feasibility of its goals' [20], and since the feasibility of the goals cannot be determined through a formal process, validation becomes 'a problem of social discussion' [7]. Furthermore, following a thesis similar to Kuhn's [31], he argues that 'Any "objective" model validation procedure rests eventually at some lower level on a judgment or faith that either the procedure or its goals are acceptable without any objective proof.' [20] and that qualitative model validation techniques must be used in practice, given the fact that 'a preponderant amount of human knowledge is in non quantitative for' [20]. However, Forrester's position was contested by works such as Ansoff & Slevin [3] or Nordhaus [38] that deem it unscientific on a logical empiricist basis and ask questions such as 'Does it represent the judgmental approach of a particular scientist?' [3]. Furthermore, Ansoff & Slevin [3] point out that Forrester does not clearly states a clear criterion of validity or a specific degree of correspondence between the model and the represented system. Additional details about this philosophical debate in the system dynamics field can be found in [2,9,10,43,44] or [45].

As seen above, the fields of economics, management science and system dynamics have been encountering this philosophical debate on model validation for a long period of time, and yet a singular integrative approach has not been designed. What is more interesting is that economic, management science and system dynamics models have been consistently used in information security without the necessary debate about validation.

The field of information security manifests, as shown in Sect. 5, the diversity of encompassing all these different types of models, with respect to both goals and method. For example, Yeo et al. [49] construct a system dynamics model for the sake of reducing the negative impact of security policies on the effectiveness of operations in ports, conceptual work such as Inglesant and Sasse [25] complemented by the modelling in Beautement et al. [8] has informed the theory that cyclic password ageing techniques lead to increased password security and the executable, language based model of Jachim et al. [26] can be used for understanding the behaviour changes of Twitter trolls during the Covid-19 pandemic.

Although a handful of examples, these are already enough to manifest different approaches on validation: [49] uses a system dynamics paradigm and both structural and behavior oriented validation techniques, [8] construct a model that can be placed in between the economics and management science traditions but admits the need of further validation stemming from the subjectivity of the input data obtained from interviews and [26] uses traditional machine learning validation metrics such as k-fold cross-validation.

However, none of the above examples are truly about ecosystems. One can imagine the need of constructing an information security model that combines multiple of the above described directions. Efforts in producing a practical, modular modelling approach that is both open to qualitative interpretation and at the same time constructed on a rigorous mathematical foundation can be seen in [13] or [14]. The relevant aspect of the method presented is that sub modules can

be constructed using significantly different philosophical assumptions as long as the produced output is standardised by the use of interfaces.

Nevertheless, validating a model with sub-modules built according to different philosophic assumptions will not be a trivial task. Given the researched streams of literature concerning validation, it is a plausible assumption to make that such a process will not be unitary in nature. Therefore, the model description offered by the framework described in Sect. 3 and Sect. 4 becomes a roadmap for the selection of validation techniques on a case by case basis—[6,32,44] offer comprehensive overviews of practical validation tests. Therefore, our position is close to Dhrymes et al. [17], with the addition that the model description given by our framework can be used for guiding the selection of validation tests. In a certain sense, Mingers' 'multimethodology' [35] idea is being translated to the issues of validation. Additionally, this can facilitate the construction of validation loops from the early model design and implementation phases, thus bringing the advantages of an agile testing methodology. Furthermore, our belief is that the analysis procedure required to construct the model description and the process of choosing validation tests according to it can increase the believability in the usefulness of the constructed model, by design.

However, the modularity offered by this method comes with a need of using both sub-module validation and overall model validation. The selection of validation tests for sub-modules is guided by the description offered by the above presented framework. When considering overall validation, more experimentation with the framework is required for an attempt to derive a criterion. Nonetheless, our belief is that such a criterion should take into account both descriptive power and believability and cannot be purely based on logical empiricism.

7 Concluding Discussion

As the world has evolved to become ever more dependent on complex ecosystems of large interacting systems, it has become ever more important to be able to reason rigorously about the design, construction, and behaviour not only of individual systems—which may include aspects related to all of people, process, and technology—but also of their assembly into ecosystems. In such complex situations, it is inevitable that no one type of model—such as mathematical models of dynamical systems, logical models of languages, or discrete event simulation models—will be sufficient to describe all of the aspects of ecosystems about which rigorous reasoning is required.

We have proposed here a meta-theoretical framework, the 'triangle framework', within which different types of models may be categorized and their interactions, especially during the construction of models, can be understood. Specifically, we have identifed three qualities of models—conceptuality, mathematicality, and executability—and have explained how in practice models typically have all of these qualities to varying extents. We have conducted an empirical study of the models deployed in a range of security conference papers and have classified these models according to the framework.

We have also discussed how the triangle framework supports an analysis of how models can be co-designed by their various stakeholders within an identified translation zone within the process of model construction. We have explored how our ideas play out in the concrete setting of models that we find in range of security papers, drawn from a diverse collection of security conferences. Lastly, we have started the much needed debate on validation methods that the information security field has been avoiding for far too long.

Much further work is suggested, including on the following:

- the structure of the triangle and its component models;
- the evolution of models within the triangle as they are developed, especially in respect of the rôles of the stakeholders;
- the structure of the translation zone, again, especially in respect of the rôles of the stakeholders; and
- empirical studies of the co-design process in the context of the triangle and the rôles of the stakeholders.

Moreover, as we have already discussed, we hope to produce practical results such as correlations between a model's goals, the types of knowledge it employs, the means of design in its translation zone, its triangle configuration, and its success of implementation and deployment in the real world.

The results of these studies should be expected to inform a reformulation of the triangle, the co-design process, and their integration.

References

1. Ackermann, F., Eden, C., Cropper, S.: Getting started with cognitive mapping. Banxia Software (1992)
2. Andersen, D.F.: How differences in analytic paradigms can lead to differences in policy conclusions. In: Elements of the System Dynamics Method, pp. 61–75 (1980)
3. Ansoff, H.I., Slevin, D.P.: An appreciation of industrial dynamics. Manag. Sci. **14**(7), 383–397 (1968)
4. Argyris, C.: Productive and counterproductive reasoning processes. The Executive Mind: New Insights on Managerial Thought and Action, Jossey-Bass, San Francisco, CA, pp. 25–58 (1983)
5. Arntzen, B.C., Brown, G.G., Harrison, T.P., Trafton, L.L.: Global supply chain management at digital equipment corporation. Interfaces **25**(1), 69–93 (1995)
6. Barlas, Y.: Formal aspects of model validity and validation in system dynamics. Syst. Dyn. Rev. **12**, 183–210 (1996)
7. Barlas, Y., Carpenter, S.: Philosophical roots of model validation: two paradigms. Syst. Dyn. Rev. **6**(2), 148–166 (1990)
8. Beautement, A., Sasse, M.A., Wonham, M.: The compliance budget: managing security behaviour in organisations. In: Proceedings of the 2008 New Security Paradigms Workshop, NSPW '08, pp. 47–58. Association for Computing Machinery, New York (2008). https://doi.org/10.1145/1595676.1595684
9. Bell, J.A., Bell, J.F.: System dynamics and scientific method. In: Elements of the System Dynamics Method, pp. 3–22 (1980)

10. Bell, J.A., Senge, P.M.: Methods for enhancing refutability in system dynamics modeling. TIMS Stud. Manag. Sci. **14**(1), 61–73 (1980)
11. Caulfield, T., Pym, D.: Improving security policy decisions with models. IEEE Secur. Priv. **13**(5), 34–41 (2015)
12. Caulfield, T., Fong, K., Pym, D.: Systems modelling for surge capacity in emergency medicine [working title] (2021, in preparation)
13. Caulfield, T., Pym, D.: Modelling and simulating systems security policy. In: SIMUTOOLS 2015: 8th EAI International Conference on Simulation Tools and Techniques, ICST (2015)
14. Caulfield, T., Pym, D., Williams, J.: Compositional security modelling. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 233–245. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07620-1_21
15. Checkland, P.B.: Soft systems methodology. Human Syst. Manag. **8**(4), 273–289 (1989)
16. Cyert, R.M., Grunberg, E.: Assumption, prediction, and explanation in economics. Behav. Theory Firm **298**, 311 (1963)
17. Dhrymes, P.J., et al.: Criteria for evaluation of econometric models. In: Annals of Economic and Social Measurement, vol. 1, no. 3, pp. 291–324. NBER (1972)
18. Eden, C.: Cognitive mapping. Eur. J. Oper. Res. **36**(1), 1–13 (1988)
19. Pidd, M. (ed.): Systems Modelling: Theory and Practice. Wiley, Hoboken (2004)
20. Forrester, J.W.: Industrial dynamics. J. Oper. Res. Soc. **48**(10), 1037–1041 (1997)
21. Friedman, M.: The methodology of positive economics. Essays in Positive Economics (1953)
22. Grim, P., Rescher, N.: How modeling can go wrong: some cautions and caveats on the use of models. Philos. Technol. **26**(1), 75–80 (2013). https://doi.org/10.1007/s13347-012-0082-7
23. Hendry, L., Fok, K., Shek, K.: A cutting stock and scheduling problem in the copper industry. J. Oper. Res. Soc. **47**(1), 38–47 (1996). https://doi.org/10.1057/jors.1996.4
24. House, P.W., McLeod, J., McLeod, J.: Large-Scale Models for Policy Evaluation. Wiley, New York (1977)
25. Inglesant, P.G., Sasse, M.A.: The true cost of unusable password policies: password use in the wild. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '10, pp. 383–392. Association for Computing Machinery, New York (2010). https://doi.org/10.1145/1753326.1753384
26. Jachim, P., Sharevski, F., Treebridge, P.: Trollhunter [evader]: automated detection [evasion] of twitter trolls during the COVID-19 pandemic. In: New Security Paradigms Workshop 2020, NSPW '20, pp. 59–75. Association for Computing Machinery, New York (2020). https://doi.org/10.1145/3442167.3442169
27. Kaczmarczyck, F., et al.: Spotlight: malware lead generation at scale. In: Annual Computer Security Applications Conference, ACSAC '20, pp. 17–27. Association for Computing Machinery, New York (2020). https://doi.org/10.1145/3427228.3427273
28. Kelle, U.: "Emergence" vs. "forcing" of empirical data? A crucial problem of "grounded theory" reconsidered. Historical Social Research/Historische Sozialforschung. Supplement, pp. 133–156 (2007)
29. Kolb, D.A.: Problem management: learning from experience. The executive mind 28 (1983)
30. Korzybski, A.: Science and Sanity: An Introduction to Non-Aristotelian Systems and General Semantics. Institute of GS (1958)

31. Kuhn, T.S.: The Structure of Scientific Revolutions. University of Chicago press, Chicago (2012)
32. Martis, M.S.: Validation of simulation based models: a theoretical outlook. Electron. J. Bus. Res. Methods **4**(1), 39–46 (2006)
33. McColl, J.: Probability. Butterworth-Heinemann/Elsevier, Oxford (1995)
34. Michael, N., Mink, J., Liu, J., Gaur, S., Hassan, W.U., Bates, A.: On the forensic validity of approximated audit logs. In: Annual Computer Security Applications Conference, ACSAC '20, pp. 189–202. Association for Computing Machinery, New York (2020). https://doi.org/10.1145/3427228.3427272
35. Mingers, J.: Multimethodology. In: Wiley Encyclopedia of Operations Research and Management Science (2010)
36. Mitroff, I.I.: Fundamental issues in the simulation of human behavior: a case in the strategy of behavioral science. Manag. Sci. **15**(12), B-635 (1969)
37. Naylor, T.H., Finger, J.M., McKenney, J.L., Schrank, W.E., Holt, C.C.: Verification of computer simulation models. Manag. Sci. **14**(2), B92–B106 (1967). http://www.jstor.org/stable/2628207
38. Nordhaus, W.D.: World dynamics: measurement without data. Econ. J. **83**(332), 1156–1183 (1973)
39. Pidd, M.: Tools for thinking–modelling in management science. J. Oper. Res. Soc. **48**(11), 1150–1150 (1997)
40. Popper, K.: The Logic of Scientific Discovery. Routledge, London (2005)
41. Radzicki, M.J.: Institutional dynamics: an extension of the institutionalist approach to socioeconomic analysis. J. Econ. Issues **22**(3), 633–665 (1988)
42. Ralph, N., Birks, M., Chapman, Y.: The methodological dynamism of grounded theory. Int. J. Qual. Methods **14**(4), 1609406915611576 (2015). https://doi.org/10.1177/1609406915611576
43. Richardson, G.P., Pugh, A.L., III.: Introduction to system dynamics modeling with DYNAMO. J. Oper. Res. Soc. **48**(11), 1146–1146 (1997)
44. Senge, P.M., Forrester, J.W.: Tests for building confidence in system dynamics models. Syst. Dyn. TIMS Stud. Manag. Sci. **14**, 209–228 (1980)
45. Sterman, J.D.: The growth of knowledge: testing a theory of scientific revolutions with a formal model. Technol. Forecast. Soc. Chang. **28**(2), 93–122 (1985)
46. Thomas, L., Banasik, J., Crook, J.: Recalibrating scorecards. J. Ope. Res. Soc. **52**(9), 981–988 (2001)
47. White, A.S., et al.: Qualitative system dynamics as a tool in accessible design. J. Softw. Eng. Appl. **4**(01), 69 (2011)
48. Xiao, Y., Shi, S., Zhang, N., Lou, W., Hou, Y.T.: Session key distribution made practical for CAN and CAN-FD message authentication. In: Annual Computer Security Applications Conference, ACSAC '20, pp. 681–693. Association for Computing Machinery, New York (2020). https://doi.org/10.1145/3427228.3427278
49. Yeo, G.T., Pak, J.Y., Yang, Z.: Analysis of dynamic effects on seaports adopting port security policy. Transp. Res. Part A: Pol. Pract. **49**, 285–301 (2013). https://doi.org/10.1016/j.tra.2013.01.039. https://www.sciencedirect.com/science/article/pii/S0965856413000463