model into a real-world system, we contend that the real-world system will exhibit patterns that are caused by the modeling patterns from which it has been realized. Some of those patterns may be of unknown vulnerabilities. Therefore, there is potentially a linkage between a modeling language and patterns of unknown vulnerabilities in systems that are realized from such modeling language. We believe that this does not occur when multiple modeling languages are used, because they act as a kind of randomizer.

This linkage yields a critical security threat for systems that rely on an integrated modeling approach or a digital twin. Imagine an attacker focuses on *hacking* or understanding the vulnerabilities that stem from the modeling language. Then, an attacker can envision a vector attack that is *independent* of the system to be attacked. In other words, all systems developed with a given modeling language may be vulnerable to such attack vector. Furthermore, because the modeling language is open, the vector may be generated without knowing the specifics of the system under attack. Protection against this type of vulnerabilities needs an understanding of the fundamental behavior of the modeling language. This has seeded our interest to pursue the work planned in this paper.

23.4 A Research Plan for Discovering Patterns of Unknown Vulnerabilities in SysML

23.4.1 Research Goal and Overview

The research for which a plan is presented here has the goal to discover patterns of unknown vulnerabilities that are inherent to modeling using SysML. The research consists of two main activities. First, we will explore the emergence of unknown vulnerabilities during the realization of systems using a formal mathematical framework. Second, we will use the mathematical framework to identify patterns of unknown vulnerabilities associated to the modeling patterns inherent to SysML.

It should be noted that we present a general plan of the research approach and that several questions about its actual implementation remain open at this time.

23.4.2 Formal Exploration

We will use Wymore's mathematical framework [22] to explore the mathematical properties associated to transforming models into real-world systems. The basic structure for the mathematical elaborations is formed on the definition of system and the concept of homomorphism. Adapted definitions are given below.

Definition 1 (Adapted) A discrete system is a quintuple$z = (SZ, IZ, OZ, NZ, RZ)$, where z is the name of the system, SZ is the set of its states, IZ is the set of its inputs,

OZ is the set of its outputs, NZ is its next state function, and RZ is its readout function that specifies the outputs for each state.

Definition 2 (Adapted) The system z_1 is a homomorphic image of the system z_2 with respect to a set of inputs $I_2 \subseteq IZ_2$, a set of outputs $O_2 \subseteq OZ_2$, and a set of states $Q_2 \subseteq SZ_2$ if and only if:

1. There exists a surjection $hi : I_2 \rightarrow I_1$, where $I_1 \subseteq IZ_1$,
2. There exists a surjection $ho : O_2 \rightarrow O_1$, where $O_1 \subseteq OZ_1$,
3. There exists a surjection $hq : Q_2 \rightarrow Q_1$, where $Q_1 \subseteq SZ_1$,
4. $hq(NZ_2(x, i)) = NZ_1(hq(x), hi(i)), \forall x \in Q_2, i \in I_2$,
5. $ho(RZ_2(x)) = RZ_1(hs(x)), \forall x \in Q_2$.

A model of a real-world system is a homomorphic image of the latter. As indicated in the definition of the concept, a model captures a subset of the transformations that the real-world system will perform. Therefore, a model is actually a homomorphic image of an infinite number of systems. We will therefore explore this problem by looking at divergent patterns that derive from the model itself, as well as convergent patterns that result from a large amount of different real-world systems. Once the patterns have been found, we will classify them as vulnerable or free of vulnerabilities. Vulnerable patterns will be those in which the real-world system allows for an input trajectory that results in a behavior that is different from the one predicted by the model. Patterns free of vulnerabilities will be those in which, although they may exhibit behavior in addition to that predicted by the model, the behavior predicted of the model is also exhibited for the system for all input trajectories.

23.4.3 Identify Vulnerability Patterns

We expect the previous activity to provide insights on the behaviors in relation to vulnerability patterns to which modeling languages may lead. This activity centers on identifying those specific to SysML. We will collect various SysML models from different modelers in order to randomize the effect of the modeler. We plan to verify their consistency and adequacy by an independent panel of experts in SysML. We propose the following process.

23.4.3.1 Transform SysML to Wymore's Framework

The SysML model will be transformed into Wymore's mathematical models. In particular:

- *Sequence diagrams* will be transformed into sets of inputs and input trajectories, sets of outputs and output trajectories, and potentially modes.