THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

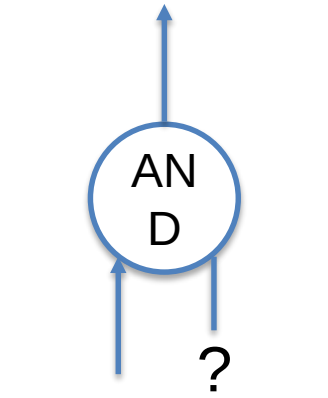
Leveraging SysML for reliability analysis with category theory

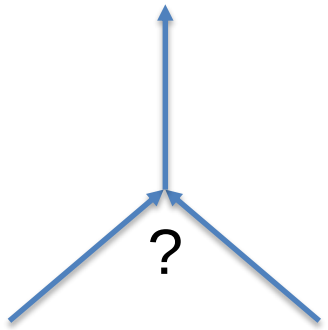
David Perner (UAH), Jonathan Patrick (UAH), Bryan Mesmer (UAH)

RAM XIII Training Summit, Nov 30th - Dec 1st 2021

Limits of SysML for reliability analysis

- Currently, SysML has a loose connection to reliability, used as a reference by practitioners generating reliability analyses
- Extensions to SysML modeling environments like MagicDraw attempt to generate artifacts like fault trees, but have had issues such as[1]:
  - Events combined without logic gates
  - Logic gates having single inputs



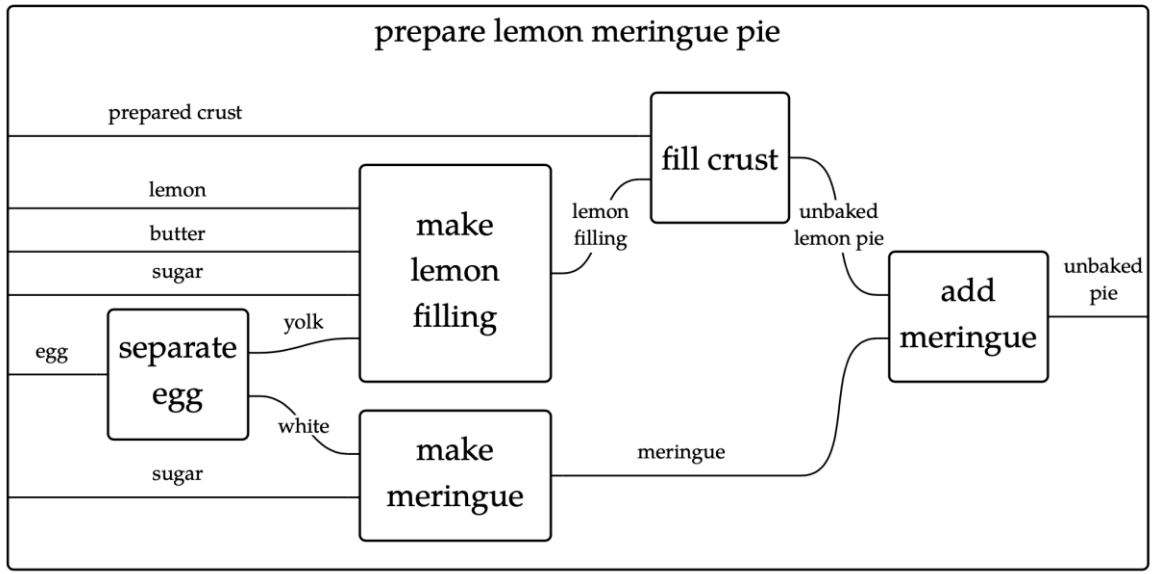


Advantages of a category theoretical approach

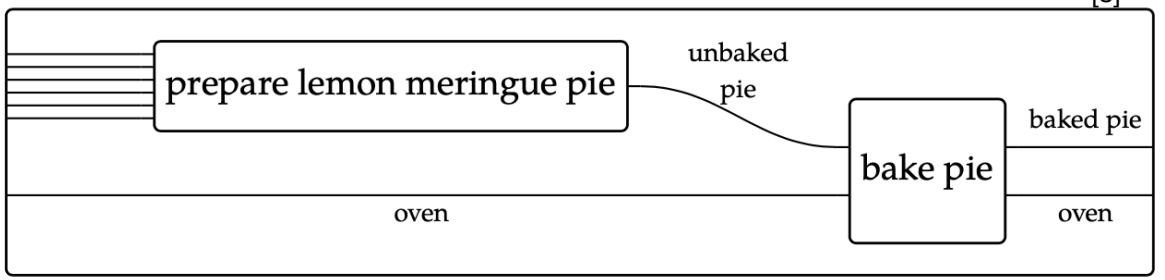
- May create more robust logic for doing transformations from SysML diagrams to reliability artifacts, resulting in fewer errors and more varied analyses
- Could enable the use SysML diagrams more frequently as a single source of truth
- Potentially save time (both in generating artifacts and checking their correctness) and increase the power of MBSE approaches

Category theory basics

- At its core, categories consist of only three elements:
  - A set of objects
  - Arrows between objects
  - Rules that these arrows have to follow
- With these rules, categories describing highly complex ideas can be built



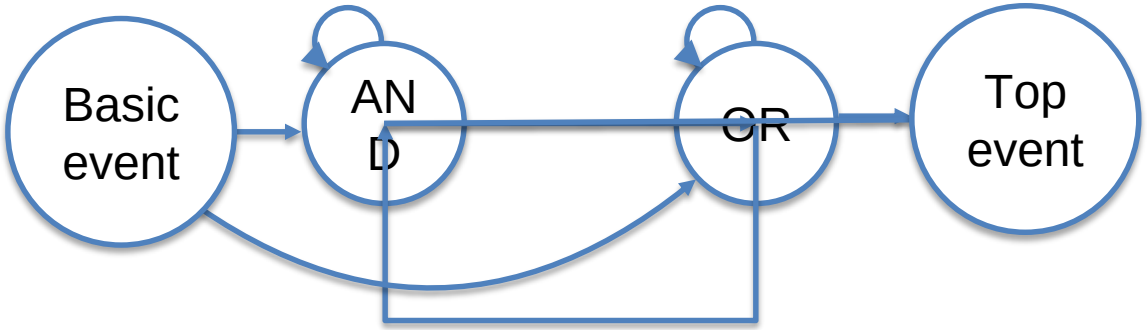
[3]



[3]

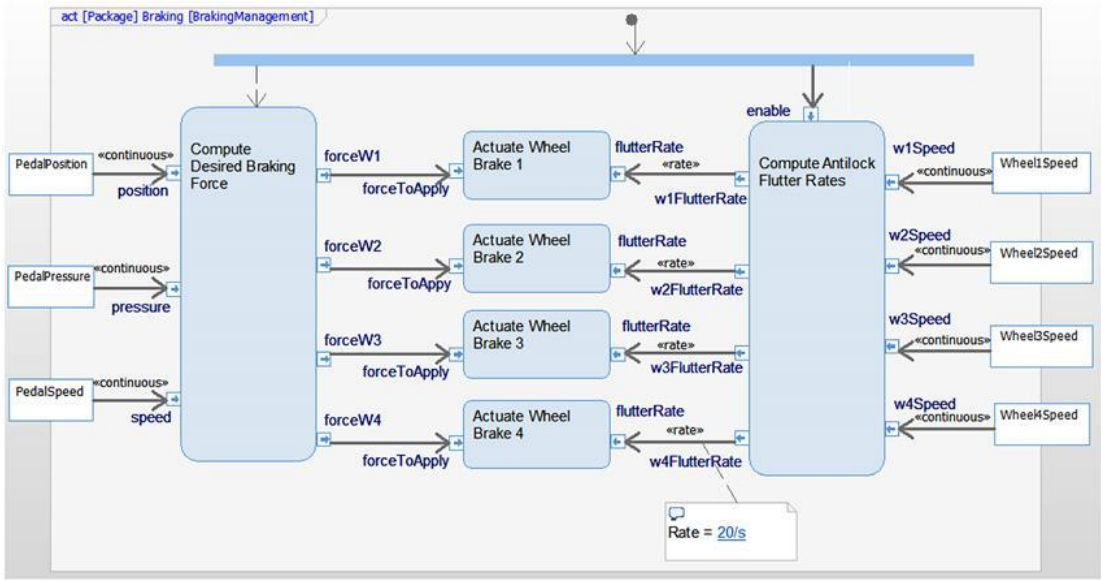
The category of (simplified) fault trees

- This category represents all the legal connections of a fault tree with only:
  - Basic events
  - AND gates
  - OR gates
  - A top event (system failure)



SysML activity diagrams

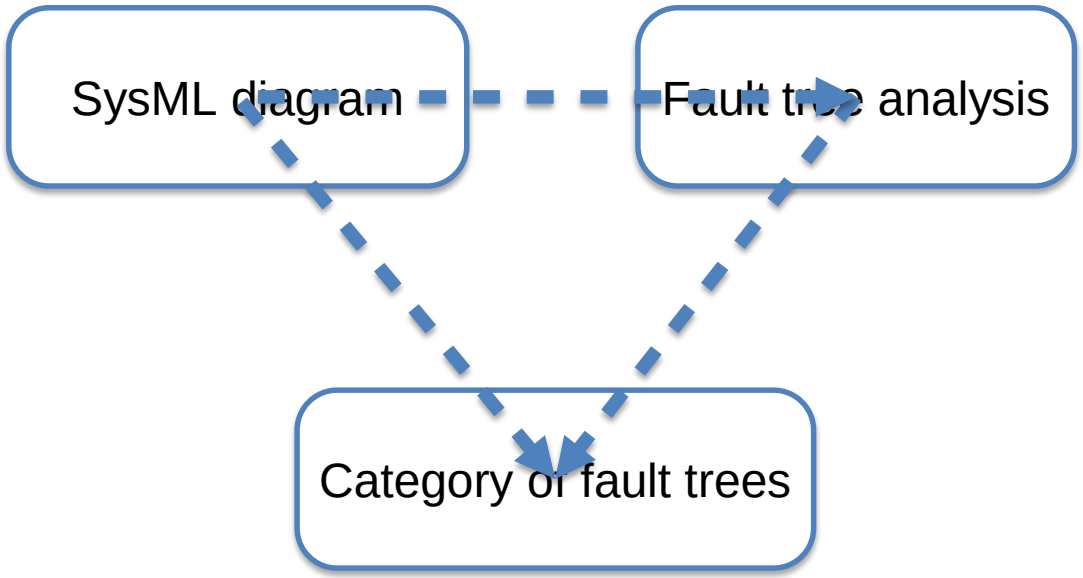
- For this example, an activity diagram representing an anti-lock brake system (ABS) is used
- Subsets of SysML, like activity diagrams, have categorical properties
- The categorical properties will be used to make connections



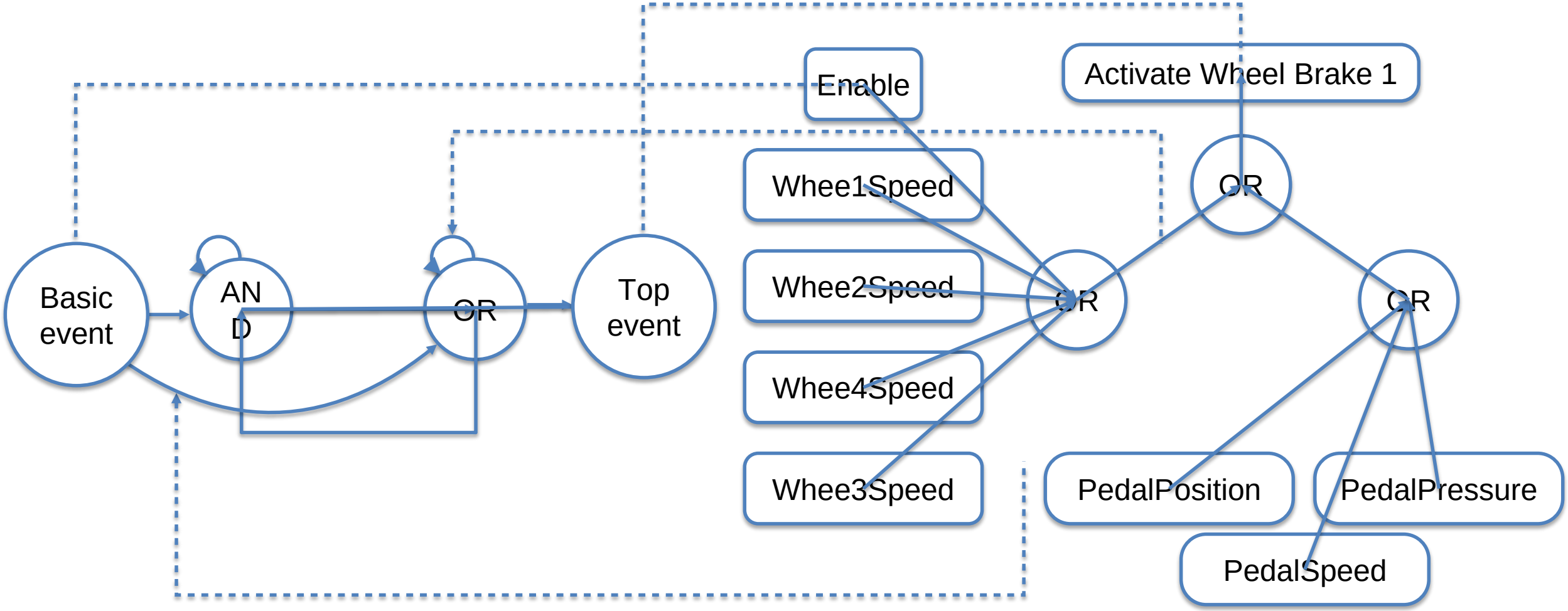
[2]

Connections between these categories

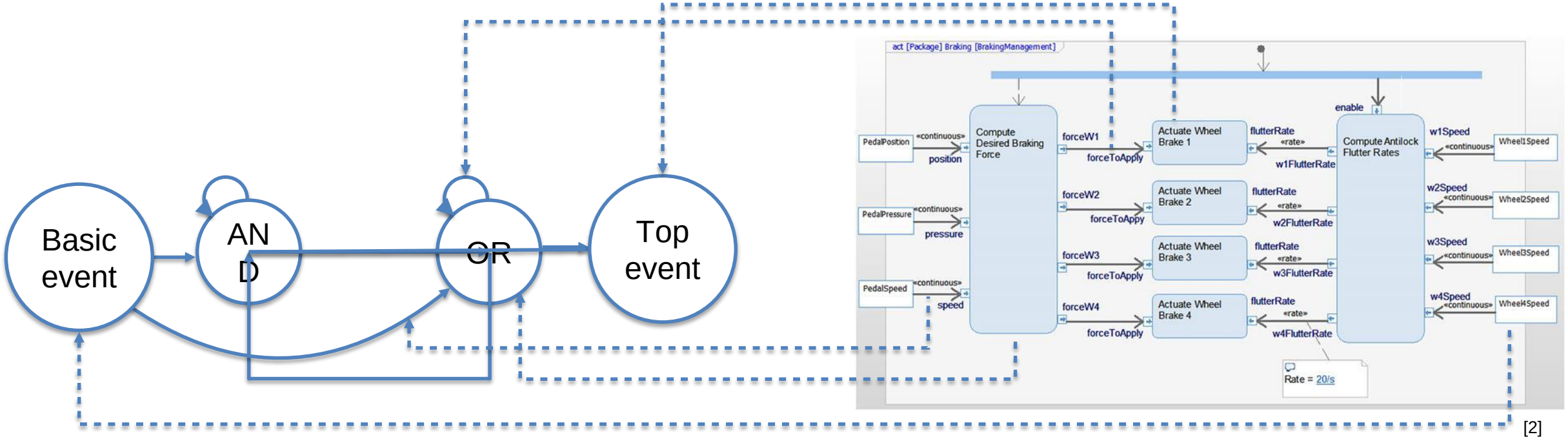
- The goal is to use category theoretic approaches to show logical consistency between each of these pieces
- The arrangement shown here is a co-cone in category theory terms



ABS Example

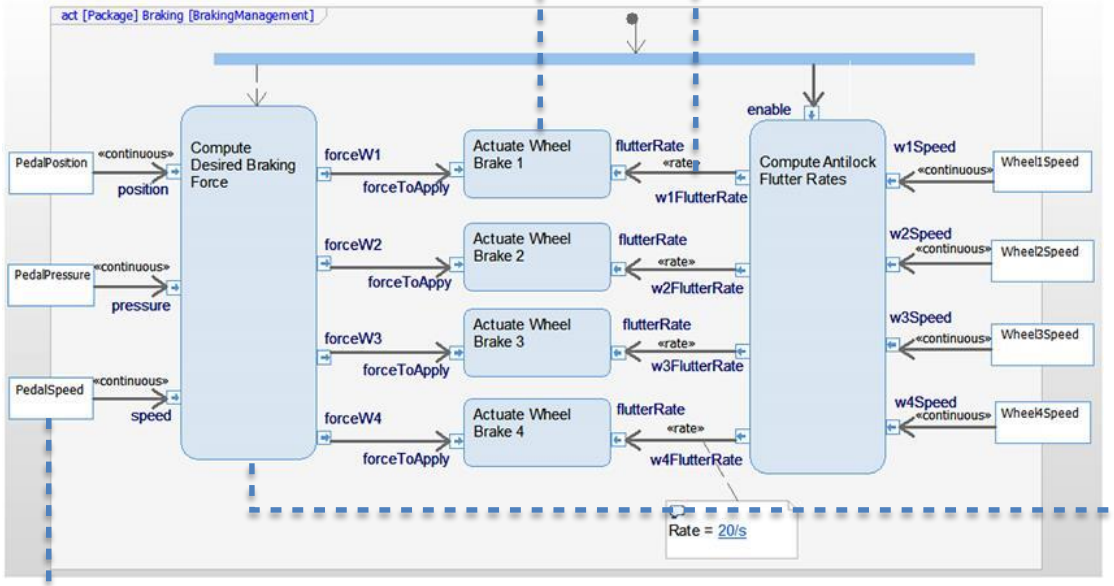


ABS Example (cont.)



[2]

ABS Example (cont.)



[2]

Conclusion and Future Work

- So far, category theory seems like a promising theoretical basis for deriving reliabilities analyses from representations such as SysML
- Examine SysML 2's formalisms
- Expand fault tree complexity and logical constraints
- Validate this approach using systems whose reliability has been analyzed by SMEs starting with a SysML model
- If the approach shows promise, it may be possible to develop an automated system for translations based on it

Questions?

References

1. Lindsey, Nancy J., Mahdi Alimardani, and Luis D. Gallo. 2020. “Reliability Analysis of Complex NASA Systems with Model-Based Engineering.” *2020 Annual Reliability and Maintainability Symposium (RAMS)*, January. https://doi.org/10.1109/rams48030.2020.9153633.
2. Bruce Powel Douglass. 2016. *Agile Systems Engineering*. Waltham, Ma: Morgan Kaufmann.
3. Fong, Brendan, and David I Spivak. 2019. *An Invitation to Applied Category Theory : Seven Sketches in Compositionality*. Cambridge ; New York, Ny: Cambridge University Press.