Intro to Hazard Analysis with the Functional Reasoning Design Language (FRDL)

Why Perform Hazard Analysis? - The Need for Safety

- Complex Safety-Critical Systems, like Aircraft, Nuclear Power Plants, and Human Spaceflight systems have a high expectations of safety and many potential points of failure
- To make the system safe, we first have to understand conditions (fault modes, disturbances, circumstances, scenarios, etc.) could make the system unsafe
- Hazard analysis helps us identify these conditions so we can mitigate them **in the design of the system**
    - When we can still add design mitigations (we aren't stuck operating an unsafe system)
    - Before the hazards are realized (we aren't surprised by hazardous events we could have mitigated)

How do you perform hazard analysis? Depends on the process or standard!

- Examples of Processes:
  - Failure Modes and Effects Analysis (FMEA)
  - Functional Hazard Analysis (FHA)
  - Hazard and Risk Analysis (HARA)
- Examples of Standards:
  - **Generic:** ARP-926 "Fault/Failure Analysis Procedure"
  - **Automotive:** ISO-26262 "Road vehicles — Functional safety"
  - **Aviation:** ARP-4761 "Guidelines And Methods For Conducting The Safety Assessment Process On Civil Airborne Systems And Equipment"

What a generic hazard assessment process looks like:

1. **Define the system:** What is the name of the system (function, component, assembly, etc.) and what is its scope and environment (inputs, outputs, connections, operators, etc.)?
2. **Identify hazards:** What things could go wrong in the system (e.g., faults, environmental conditions, misuses) that could lead to harm (e.g., loss of function, damage to property, harm to people, operators or the environment)?
3. **Analyzing/assessing hazards:** What are the effects of these hazards in the relevant times when the system is operating (e.g., phases of operation, configurations)?
    - May come with an assessment of risk (e.g., severity/cost, probability/rate)

Based on this, one may prescribe **mitigations** to reduce hazard risks

Constructing a hazard table (at its most basic)

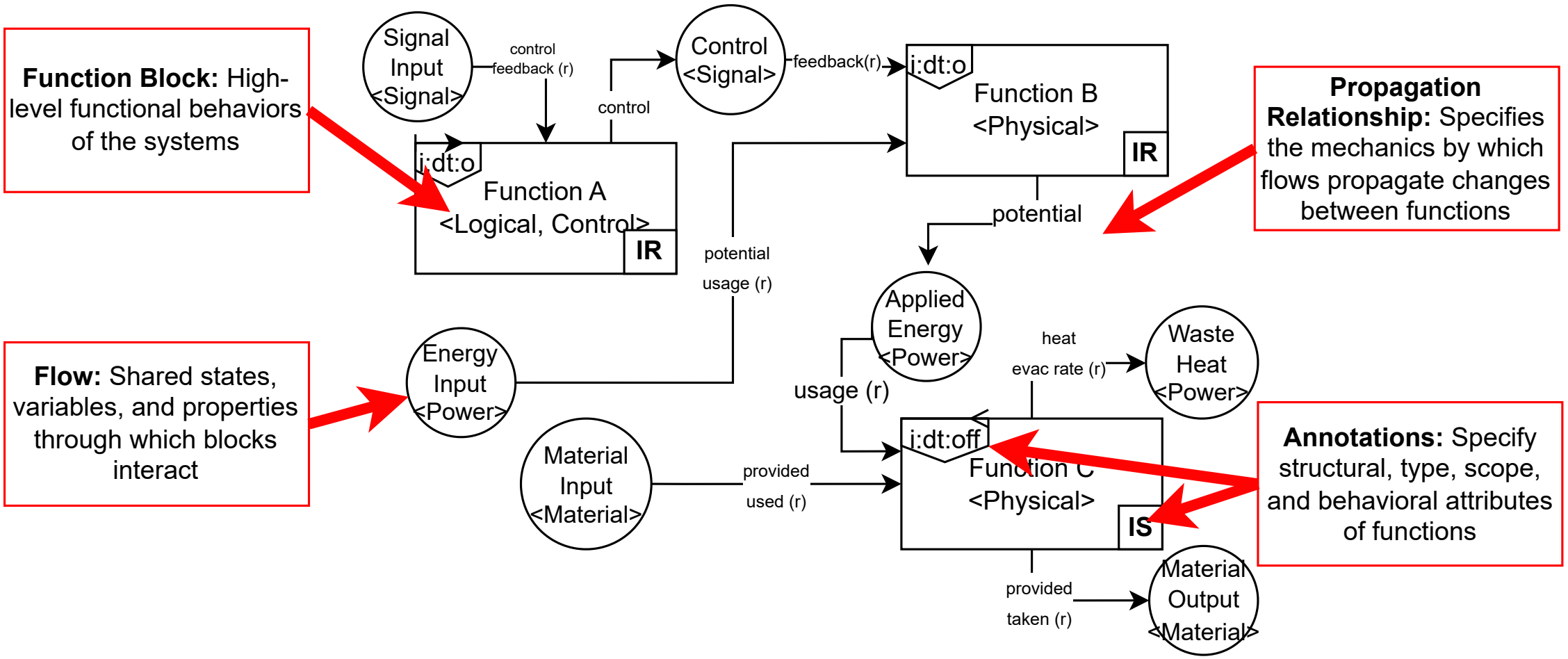
Function	Hazard	Causes	Effects
Perform Job	Incorrect Job Performed	Misunderstanding of work	Work incomplete
	Poor Job Performance	Stress, Distraction, etc.	Work late or incomplete
Travel to Job site	Late to job site	Traffic, oversleeping, poor planning	Unable to work full day

Exercise: Construct a hazard table for a system of your choice. It could be a physical product, a vehicle, software, a task/process, or anything else you can think of.

What is FRDL (and why use it for hazard analysis)?

- FRDL: Functional Reasoning Design Language
- Diagrams that you can use to represent the overall functions of a system and their *behavioral interactions*
    - Functions: Functionality that the system provides
    - Behavioral interaction: Ways that the functions interact with each other
- FRDL helps with hazard analysis by giving you a *model* of the system to base the assessment of causes and effects off of
    - Instead of just brain-storming possible causes/effects, you can use the model to see what parts of the system will be effected and how, giving you a more **complete** and **detailed** analysis

What does an FRDL diagram look like?



See fmdtools specification.

How do you analyze hazards with and FRDL diagram?

0.) Imagine how the system is supposed to work nominally

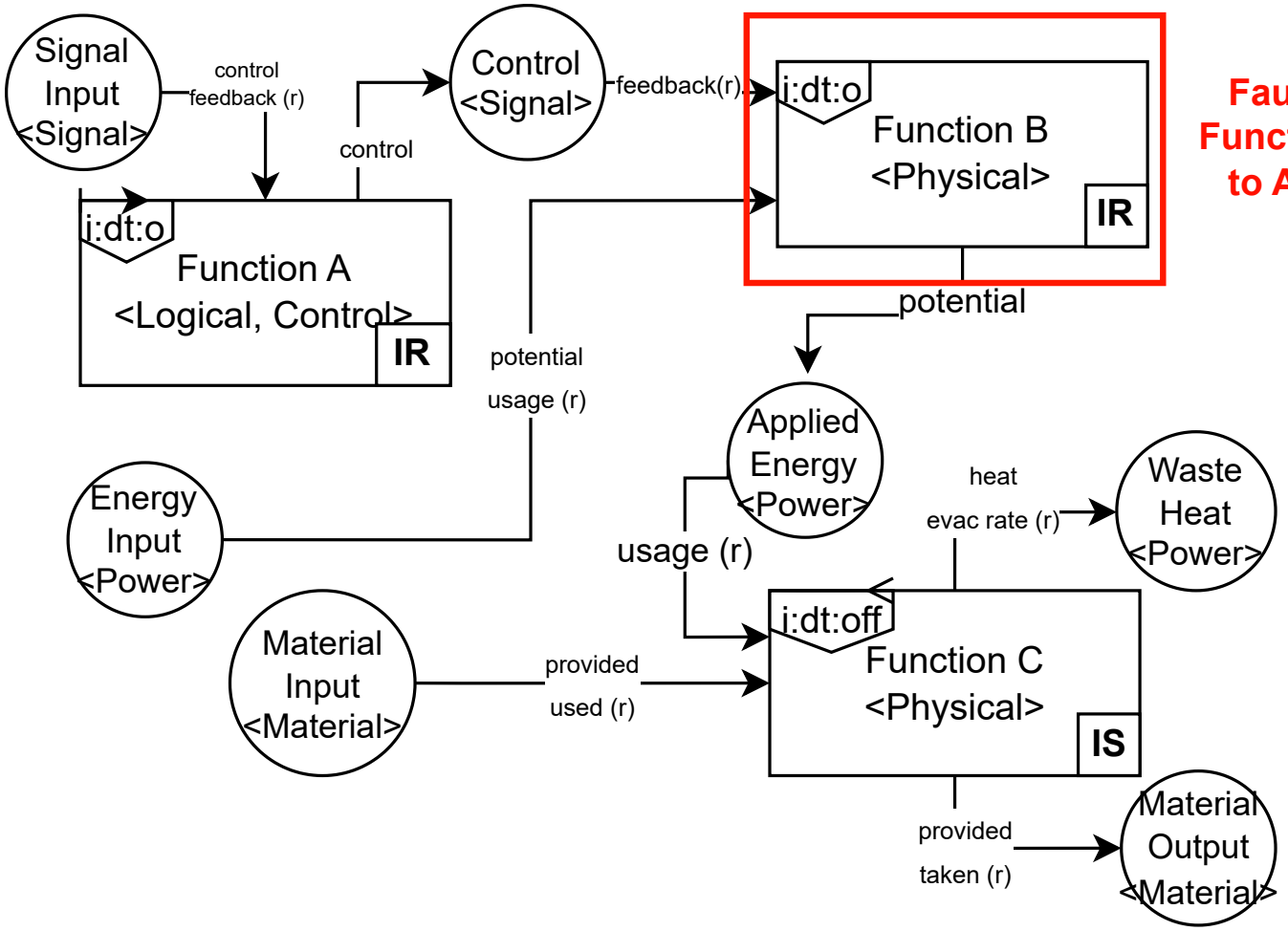
1.) Inject the hazardous condition(s) into the relevant function(s) and evaluate the effects on those functions

2.) Determine the impacts to each flow connected to the affected function(s) per the propagation arrows

3.) Repeat Step 1-2 for each function affected by the altered flow states until you've exhaustively elicited effects

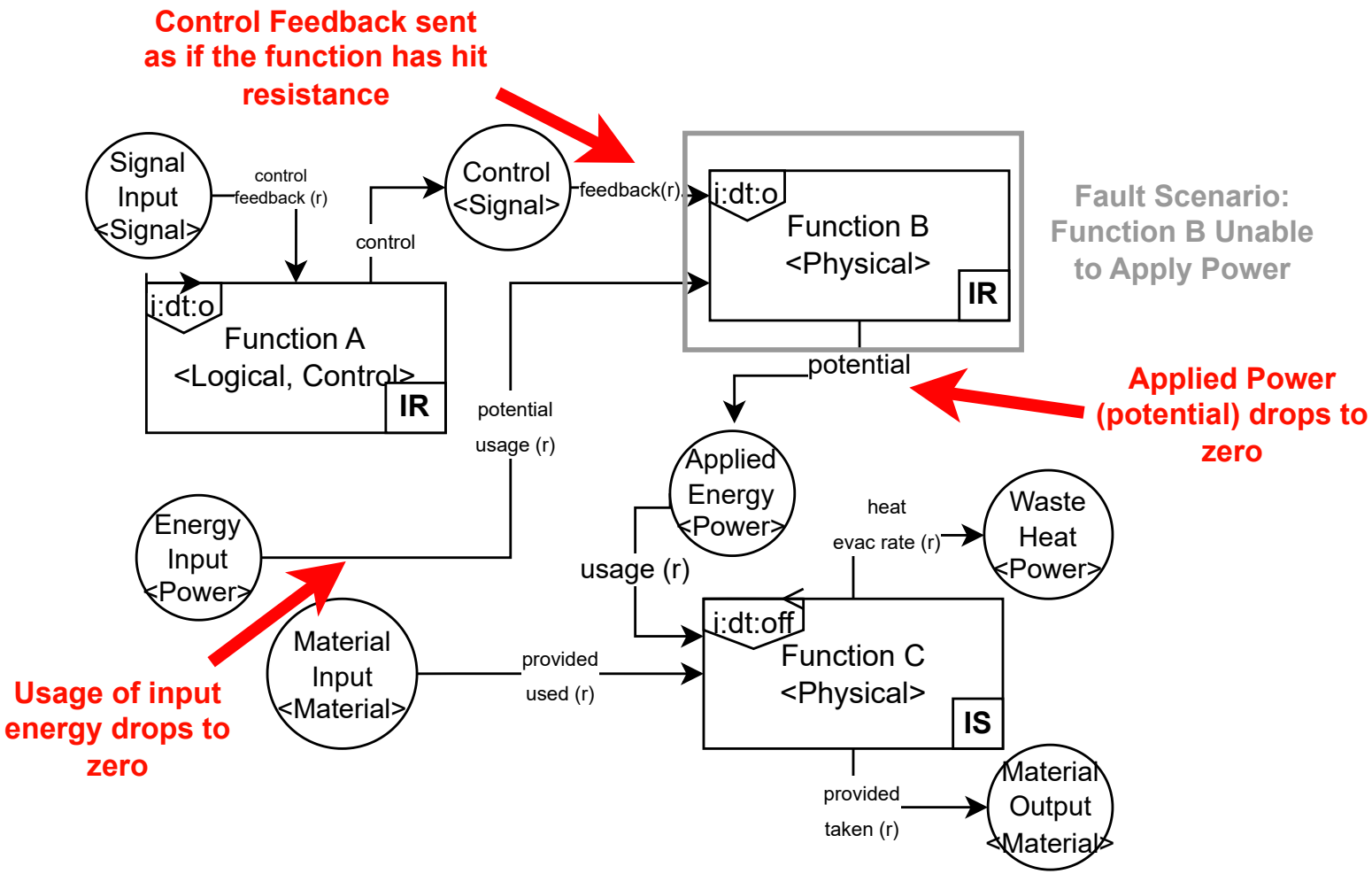
For causes, run through this process in reverse. See FRDL/Specification/Usage/Analysis for more details.

Example - Step 1

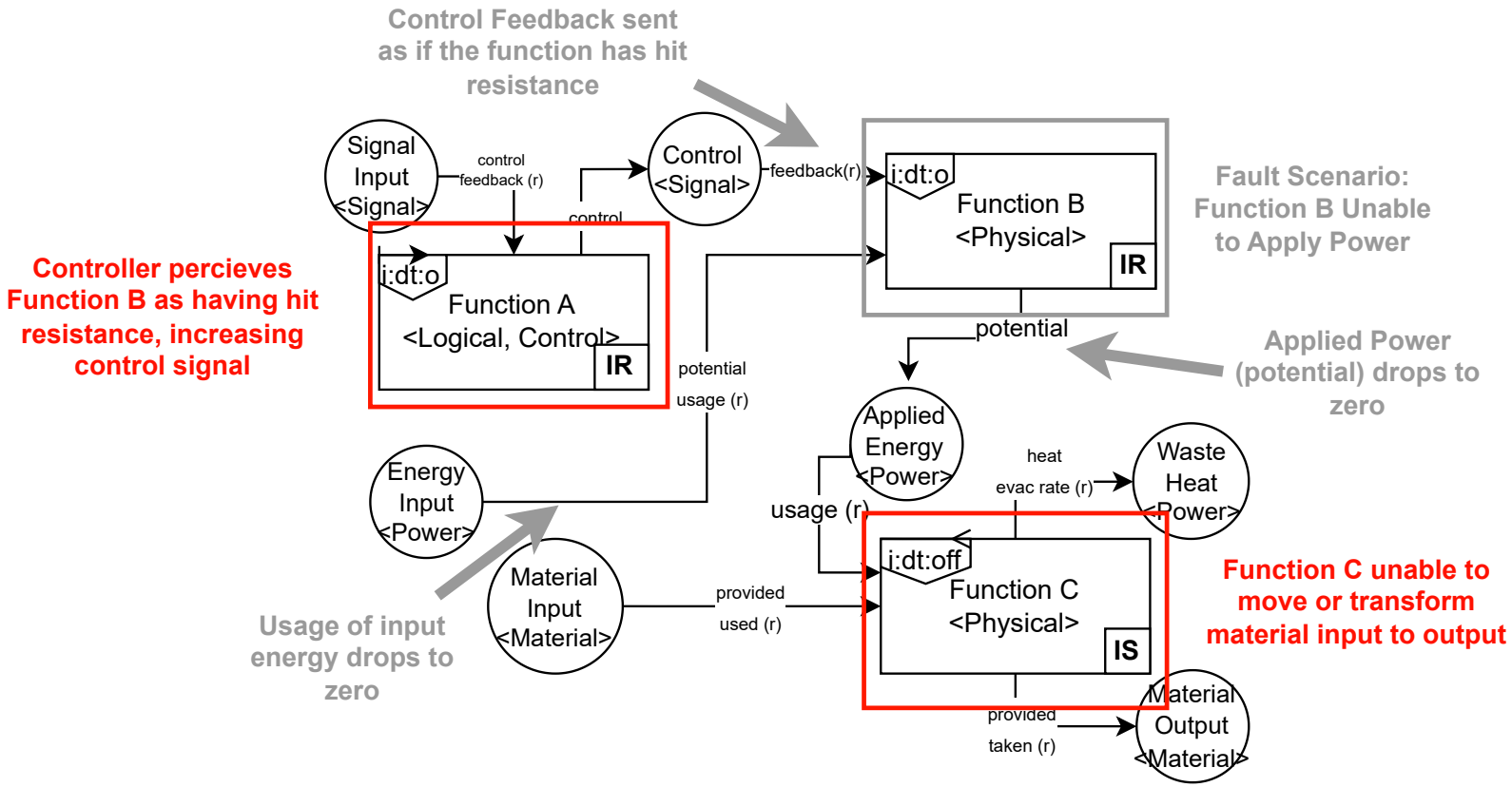


Fault Scenario: Function B Unable to Apply Power

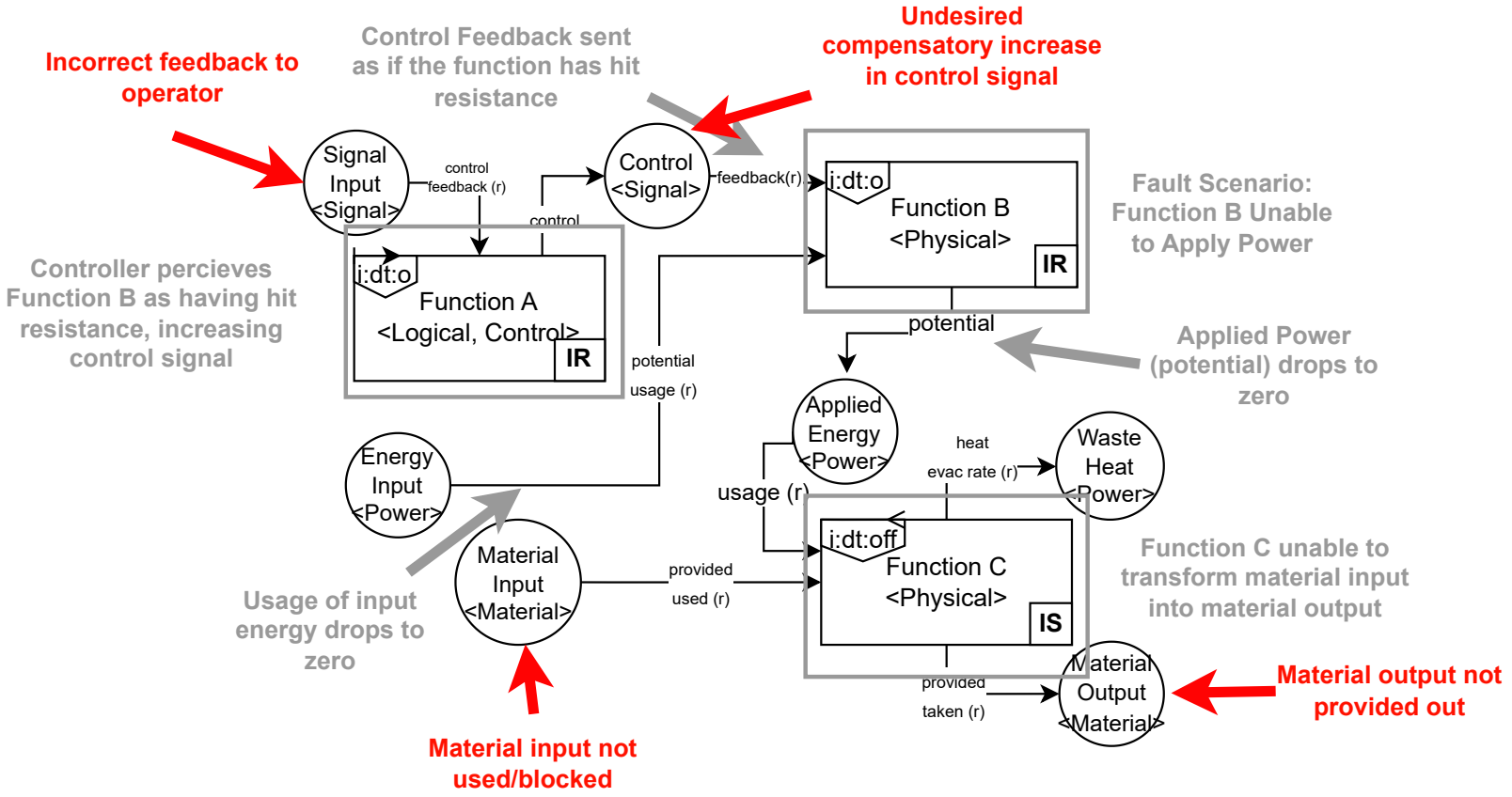
Example - Step 2



Example - Step 1 (again)



Example - Step 2 (again)

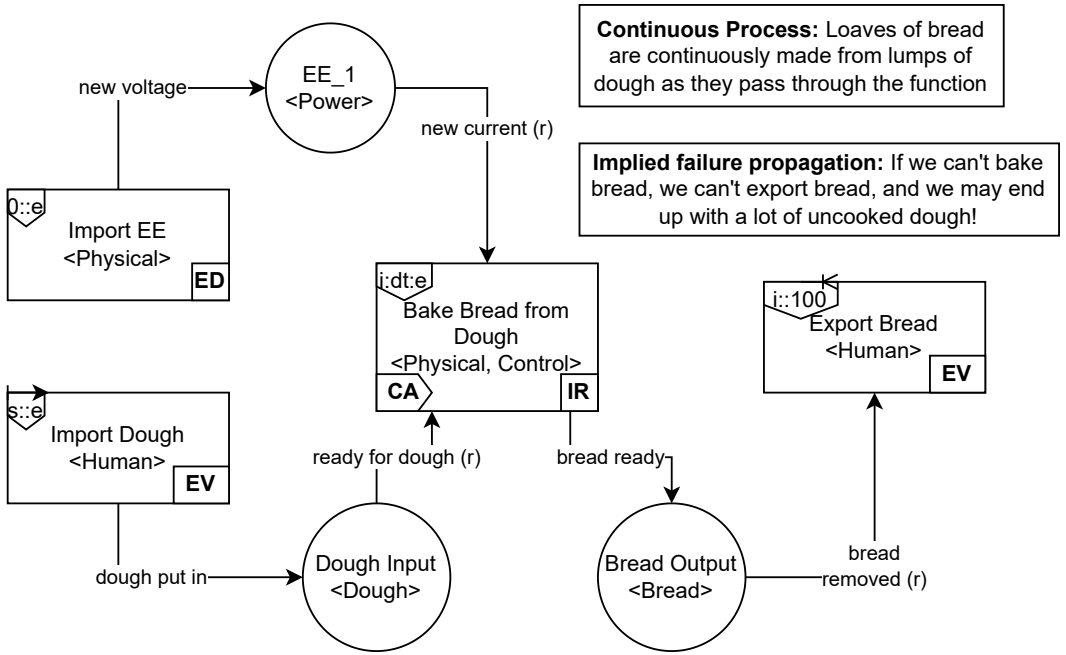


Some Takeaways

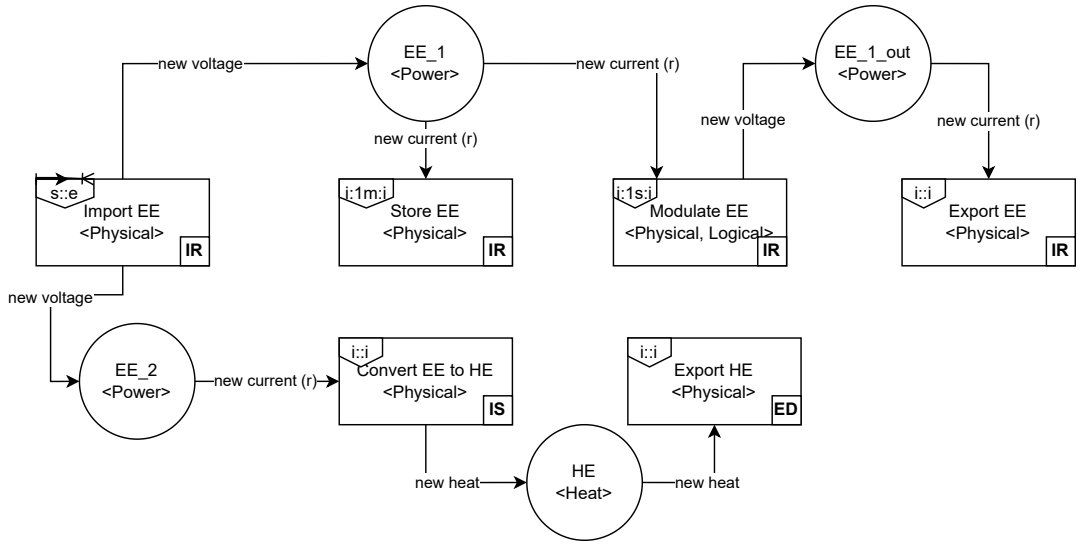
- Analyzing behavior in FRDL means working **directly with the diagram** to determine hazard effects, as opposed to just coming up with the effects out of your head
- However, there is also an analytical component in terms of figuring out what would happen to each function/flow
- However, sometimes the diagram may not have the flows needed to propagate the behavior, in which case you would need to update the diagram
- One also has to make analysis decisions such as:
    - How to represent the system in FRDL
    - What assumptions to use when propagating behavior
    - When to stop the analysis

More Examples

Baking Bread



Circuit



- Some explanation of these examples is provided in FRDL/Guide/Examples

More Helpful Information

- The FRDL Specification and Guide has a good overview of the details of developing FRDL models (as well as analyzing hazards)
- "Defining A Modelling Language to Support Functional Hazard Assessment" is the conference paper that initially defined the FRDL and describes some of the rationale for its development
    - Conference presentation here
    - A revised journal draft that is up-to-date with FRDL 0.7.1 (which is in review) may be provided upon request