1 Motivation and Objectives

- CPS are increasingly everywhere
- many CPS are safety-critical, and a fault can literally kill people
- cyber threats and vulnerabilities are increasingly everywhere
- **key assertion** traditional defense techniques are not only insufficient, they are at least in some cases unnecessary. This assertion is also true for the different paradigm of what we will call "cyber resilience" techniques; i.e. it is unclear whether they are necessary or sufficient
- **another key assertion** ★[1] security techniques for CPS are usually tailored for that specific application or system. There is no assurance when transitioning to other applications or techniques.
- therefore, we propose to understand the theory and science behind whether, when, and where different CPS security/resilience techniques are (in)effective and/or (un)necessary

bold statement about the current state of cyber and safety-critical CPS

Consider the example in Figure 2, where

catchy example with associated figure

Our focus is not on improving defenses against cyber attack, or even improving detection and adaptation techniques in the face of a cyber attack. Rather, our efforts aim to

understand the trade-offs and optimize decision-making about when, where, and how to apply design patterns...

Our approach is to develop models that can...

Figure 1: not sure what to put here.

2 Background and Related Approaches

A bit about traditional defense and its limitations, some of our work (and others') on resilience, etc ★[2] ★[3]

3 Research Goals and Approaches

We propose to focus on three research thrusts that aim to

1, 2, and 3...

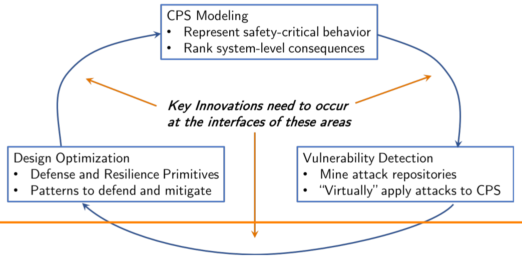
CPS Modeling
• Represent safety-critical behavior
• Rank system-level consequences
Key Innovations need to occur
at the interfaces of these areas
Design Optimization
• Defense and Resilience Primitives
• Patterns to defend and mitigate
Vulnerability Detection
• Mine attack repositories
• "Virtually" apply attacks to CPS

Figure 2: Overview this is just notional, needs a good figure

3.1 Thrust 1: ...

Goals and Challenges:

Approaches and Preliminary Work:

[1] ★NB: this is another reason why this research

[2] ★NB: I think we need to pick 1 or more techniques that have been well developed like my resilient state estimator or the resilient kalman filter and use those to both motivate the problem and use them to show how to transition to other applications and platforms

[3] ★NB: I can discuss about these techniques

Figure 4: Timeline of proposedwork, including technical development, evaluation ,and broader impact

★[4]
★[5]

Future Work: If successful, this project will extend our preliminary work by

by "future work" I mean the work we'll do if this is funded

3.2 Thrust 2: ...

Goals and Challenges:

Approaches and Preliminary Work:

Future Work:

3.3 Thrust 3: ...

Goals and Challenges:

Approaches and Preliminary Work:

Future Work:

4 Integration and Validation Plan

This multidisciplinary research requires expertise in a number of areas, a tight collaboration among its team members, and a close integration of all phases of the research. The primary expertise needed includes The team consists of experts in all of the areas and the rough team breakdown is shown in Figure 3. The PIs are all members of the Link Lab, whose mission is to enhance excellence of CPS research at the University of Virginia. They and all of their students will be sitting together on a daily basis in a 17,000 square foot collaborative lab. They will formally meet as a group once per week but subgroup meetings and impromptu meetings will take place on a daily basis.

controls, decision-making, modeling...

While significant research progress will occur in each subproject, we emphasize a rigorous plan for integration throughout the project. This includes a periodic interactive activity called the

something related to exercising our theory on a testbed, which we will describe below. Nicola, do you have boilerplate on the stuff in your lab?

Figure 3: Proposed experimental testbed will consist of one ground and two aerial ve-

Timeline and milestones:

[4] ★NB: Here I can talk about the work that I'm doing on safe reinforcement learning and supervised/unsupervised learning. Basically the library of known vulnerabilities and the previous observations of the attack effects on specific systems together with the resilient techniques results can be seen as training data for the new system or for the system operating in different conditions under attack

[5] ★NB: We can assume for now that this operation is done at pre-planning, offline but it would not be too hard to do th same online

5 Broader Impact, Education Plan, and Outreach Activites

Dissemination: The proposed research will enhance the ...

Integration into curriculum: The proposed research will be integrated into coursework

Undergraduate research:

K-12 outreach:

Contributions to diversity:

6 Relevant Prior Research Funded by NSF

Cody Fleming is Co-PI on NSF grant... . **Peter Beling** is ... . **Nicola Bezzo** ...