- **Storage and Control Module Architecture in PyCIGAR (Mike and Sy-Toan)**
    - Sean: We have the situation where one controller is controlling multiple storage systems. How often does this happen? Ideally, we would leverage distributed nature to our advantage. A single point of failure system like this is a big target. How common is this and what should we do about it?
        - Mike: Not sure how common it is, but we want to be able to model this. At different levels of the grid, these controllers could exist so we need to be as general as possible
        - David: this is a standard deployment architecture and we expect to see more of this. One co-op is providing Tesla power wall units and centrally controlling them a few times a month for peak shaving. The economics of this are beautiful.
    - Anna: the dependence on a single signal is a weakness and could be a mode of failure. Can we incorporate local measurements into the policy to add some robustness in the case that the input signal is spoofed (FDI attack)? Agents could be trained so that they know that if they respond to a signal where they believe there is a large inconsistency, then they should not act.
        - Mike: Noting that precludes us from doing this.
        - Sean: points out that there could also be a fail safe policy
    - Dan: This adds a new physical element to the types of attacks that can be carried out. The red team attacker could be cast in a battery control module and would need to interact with the battery physics (if the attack were to focus on using a battery to inject/consume power). So, some of the physical constraints of the battery would need to be taken into account by the attacker
- **Grid Forming/following & Active Load Stability Simulation (Ciaran)**
    - Ciaran: Important to note that pushing eigenvalues deeper into the RHP requires larger gains in the state feedback matrix, so these are more difficult for the attacker to execute
    - Dan: Can you compare the control effort required to execute attack 1 and attack 2?
        - Full control (attack 2) needs less control effort to destabilize the system
    - Dan: Do you have any preliminary thoughts on the types of supervisory control systems we should be thinking about for the second phase of this project?
        - Ciaran: Develop a local supervisory controller that sits on device and determines if gains need to be re-tuned

- Ciaran: Participation factor analysis of 2 attacks shows exactly what states are being destabilized. If we can map from unstable mode into states and we can change the parameters associated with these states.

    - Dan: How reasonable is it that an adversary would be able to execute the full control attack scenario? What is a reasonable attack between the setpoint attack and the full control attack?
        - Ciaran: Need enough information to build an observer to execute this attack. So it does need a good deal of information. But we should build our controller to deal with the worst case scenario.
        - Ciaran: From Sahoo paper, the full flexibility attack is due to the use of an adversary introducing a load in the system. Attack can be launched with only 2-3% of system load
    - Dan: in the hardening attack slide, why isn't the single blue eigenvalue near 0 a candidate for attack?
        - Ciaran: That eigenvalue is an artifact of the small signal stability analysis which is not physical, but shows up in the linearization
    - Anna: have you looked at the work for Tx voltage collapse (Ian Dobson)? It may be applicable to this work
        - Ciaran: my understanding of voltage collapse is that it occurs on a longer timescale, but it is worth exploring.

- **Open Modeling Framework (OMF) Updates. Use Case Analysis, Network Reduction (David and Lisa)**
    - Really want to know the settings that would destabilize the distribution systems
    - Storage going in at all levels
    - Dan: The presence of propriety control schemes from microgrid vendors is a problem. How do we address this from a cybersecurity perspective? That is, if we design a defensive strategy, how can we be sure it will be platform agnostic?
        - Ciaran: We're operating at a higher abstraction, as we're designing our controllers according to the standards.
        - Sean: ICSCERT is something we might want to consider. Maybe we would need some kind of certificate of reliability from certain vendors?
        - Ignacio: ICSCERT rates multiple devices and gives probabilities of being attacked (https://us-cert.cisa.gov/ics/advisories). Inside each device, under the executive summary - "Attention", they provide the "likelihood" of a known vulnerability being exploited. Labels are usually low/medium/high

    - David: There is some CEDS CESER work on storage firmware and trying to determine if its reliable
      - Dan: I think some of the folks at Idaho National Lab are working on this
      - Sean: I think Argonne too.
  - David: Our use cases stayed away from batteries providing bulk system stability services. It is likely that load control will dominate these markets once someone figures out how to do it well. It's so cheap on a cost per cycle basis
  - Sindhu: What's your opinion of the use of grid forming inverters for blackstart?
    - David: I've never seen a discussion of black start in the co-ops. This has been pushed out as a vendor problem. I'd have to think about situations where coops would need to black start, as ideally the co-ops would island when the distribution feed goes down, but if you run out of fuel then this could be an issue. This is beyond the kind of planning tools that utilities are presently using.
  - Dan: What are your greatest challenges looking out in the next year
    - David: we had thought that our biggest challenges would be related to OpenDSS, but Lisa has this under control
    - David: Showing utilities exciting results that they can use is the biggest challenge. We need to be focusing on realistic scenarios that utilities can see in the near term. More evangelism about the work we're doing
  - Dan: For the substation power factor, from the talk I gather that most distribution operators need to stay within 5% of unity, but over what time period? Can small perturbations be tolerated?
    - David: Events shorter than 1 minute, it wouldn't show up on SCADA. Utility will watch KVAR hours so one would need to keep the integral of the power factor excursions under control.
- **Red Team Planning/Methodology (Bruno)**
  - Dan: we should make a map of the attacks and associated impacts similar to your slide 11
  - Sean: maybe we should consider an attack tree (graph), allowing us to consider parallel attacks and multiple attacks working in coordinating. Identifying the level of access at each stage as well would
- **Log(V) 3LPF: A linearized solution to train reinforcement learning algorithms for unbalanced distribution systems (Ignacio)**

- Dan: at what stage do you envision testing this out in closed loop with RL training?
    - We’re close - we should see the solution to the IEEE 8500 within a month or so and after that we will start the process of integrating into the PyCIGAR/RL framework