# Center Overview

http://ncr.mae.ufl.edu/aacoe.php

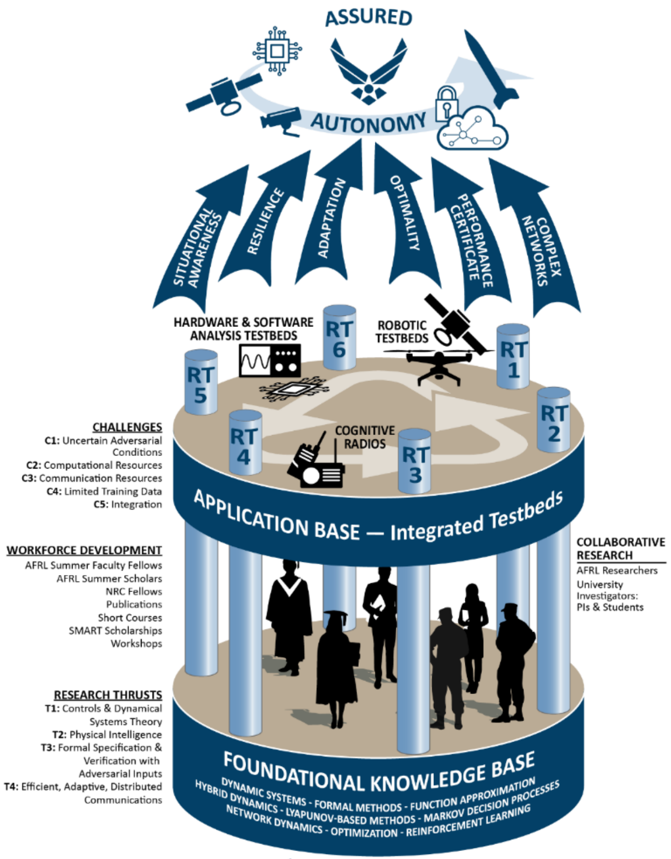
UF UNIVERSITY of FLORIDA

Duke UNIVERSITY

TEXAS The University of Texas at Austin

UC SANTA CRUZ

# Center Overview



ASSURED AUTONOMY

SITUATIONAL AWARENESS

RESILIENCE

ADAPTATION

OPTIMALITY

PERFORMANCE CERTIFICATE

COMPLEX NETWORKS

HARDWARE & SOFTWARE ANALYSIS TESTBEDS

ROBOTIC TESTBEDS

COGNITIVE RADIOS

RT 1

RT 2

RT 3

RT 4

RT 5

RT 6

APPLICATION BASE — Integrated Testbeds

**CHALLENGES**

**C1:** Uncertain Adversarial Conditions

**C2:** Computational Resources

**C3:** Communication Resources

**C4:** Limited Training Data

**C5:** Integration

**WORKFORCE DEVELOPMENT**

AFRL Summer Faculty Fellows

AFRL Summer Scholars

NRC Fellows

Publications

Short Courses

SMART Scholarships

Workshops

**COLLABORATIVE RESEARCH**

AFRL Researchers

University Investigators: PIs & Students

**RESEARCH THRUSTS**

**T1:** Controls & Dynamical Systems Theory

**T2:** Physical Intelligence

**T3:** Formal Specification & Verification with Adversarial Inputs

**T4:** Efficient, Adaptive, Distributed Communications

FOUNDATIONAL KNOWLEDGE BASE

DYNAMIC SYSTEMS - FORMAL METHODS - FUNCTION APPROXIMATION

HYBRID DYNAMICS - LYAPUNOV-BASED METHODS - MARKOV DECISION PROCESSES

NETWORK DYNAMICS - OPTIMIZATION - REINFORCEMENT LEARNING

**AFOSR Center of Excellence in Assured Autonomy in Contested Environments**

- >$6M over 6 years (3 x 2 year increments)
- 10 PIs @ 4 Universities:
  - R. Bevilacqua (UF: optimal, switching)
  - K. Butler (UF: cyber resiliency/privacy)
  - W. Dixon (UF: ADP, networks, hybrid)
  - N. Fitz-Coy (UF: optimal, games)
  - M. Hale (UF: networks, privacy)
  - M. Pajic (Duke: cyber resiliency/privacy)
  - R. Sanfelice (UCSC: hybrid, networks)
  - J. Shea (UF: networks, privacy)
  - U. Topcu (UT: formal, hybrid, optimal)
  - M. Zavlanos (Duke: ADP, networks, formal)
- AFOSR provides 50% of funding
- AFRL (RV, RW, RY) provide 50%

# Center Motivation

- Innovation & technology dominance and strong economy have allowed for exquisite systems that for decades have operated in largely uncontested environments.
  - Remote piloted vehicles (RPV) and monolithic satellites provide various strategic and tactical advantages.
  - Intelligence, surveillance, and reconnaissance (ISR) in close proximity with RPVs or from protected space assets, while simultaneously striking from distances and with speeds beyond the capability of countermeasures.
- These advantages are mitigated as the technology gap closes and as other world economies become near peers and risks to the warfighter and financial costs increase and tactical capabilities become stressed when military operations are in contested or denied environments (i.e., anti-access/area denial (A2AD) environments).
- Increased stand-off distance, persistence, and scaled projection of power have resulted in an urgency for development and fielding of human-in-the loop/semiautonomous systems.

# Center Motivation

- As these advantages are taken to the limit, coupled with the resultant need for rapid decision-making capabilities, emerging technology will move along a spectrum towards greater automation with less human intervention.
- In contested environments, autonomous systems are even further motivated by the potential desire to complete mission execution when communication with a human operator is unavailable.
- Autonomous systems must execute high level missions plans with verifiable assurances despite uncertain adversarial environments where the integrity and availability of sensor information and communications are challenged.
- Key innovations include analysis, design and synthesis tools that enable autonomous mission execution despite uncertainty within complex dynamics while accounting for the integrity and privacy of information on computationally constrained resources.

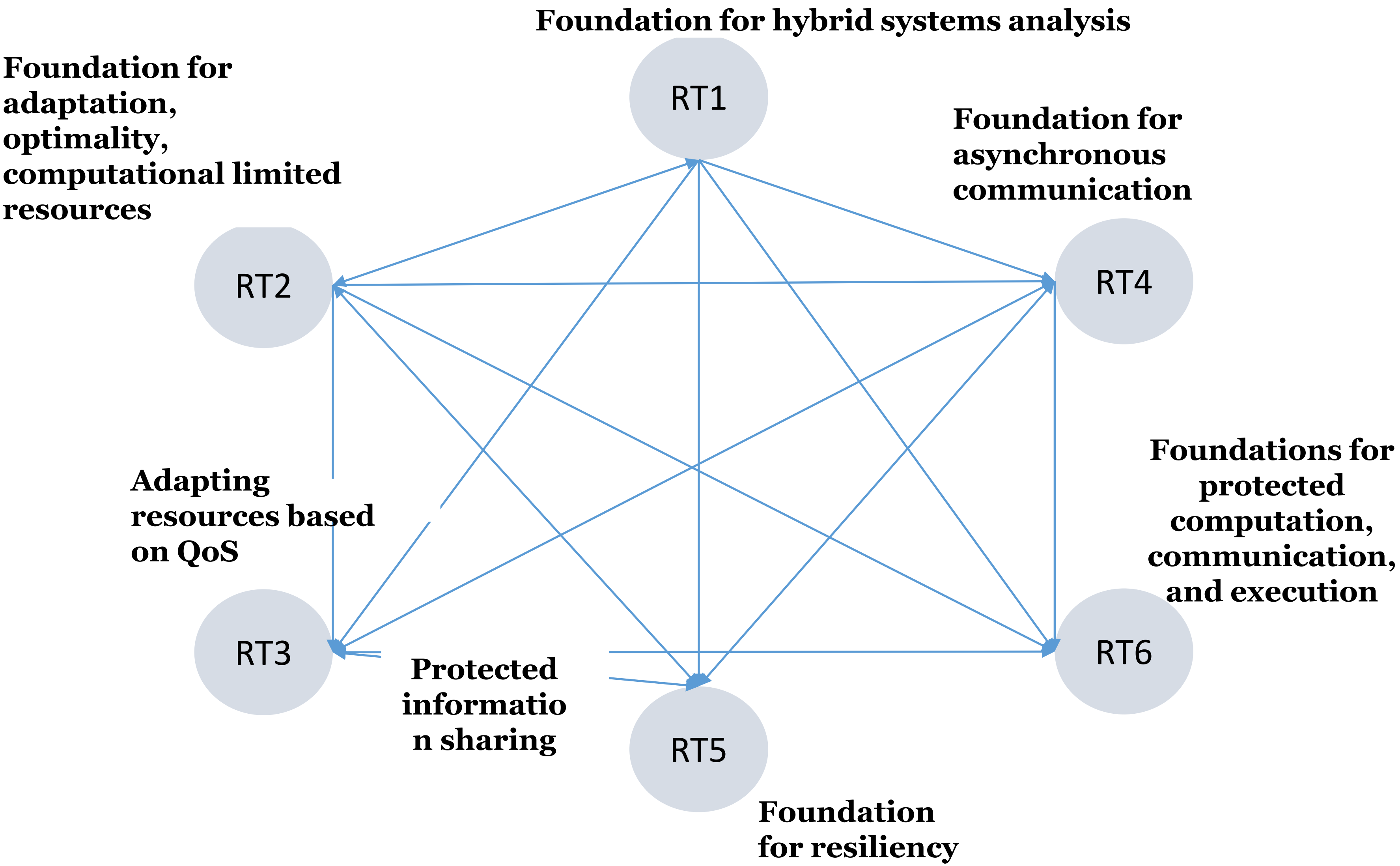
# Center Goals & Vision

- Networks of autonomous systems will require information exchanges of many data types, including high-level mission specifications and sensor feedback for navigation and control
- The goal of assuring autonomy is complicated by the interplay between dynamics of autonomous agents and the stochastic and intermittent dynamics of network traffic
- This challenge is further amplified by delays and asynchrony in information flows
- Information perturbations can also emanate from adversarial actors in unique and complex ways, requiring security-aware design and analysis methods
- For example, we will develop techniques to protect mission-critical information and prevent information disruption/corruption
- These challenges must be addressed considering resource limitations and quantitative tradeoffs.

**Research Topics**

- Nonsmooth Systems
- Adaptation, Optimality, and Synthesis
- Network Systems
- Asynchronous Information
- Attack-Resilient Design
- Protecting Information

# Tightly Coupled RTs



Foundation for hybrid systems analysis

Foundation for adaptation, optimality, computational limited resources

Foundation for asynchronous communication

Adapting resources based on QoS

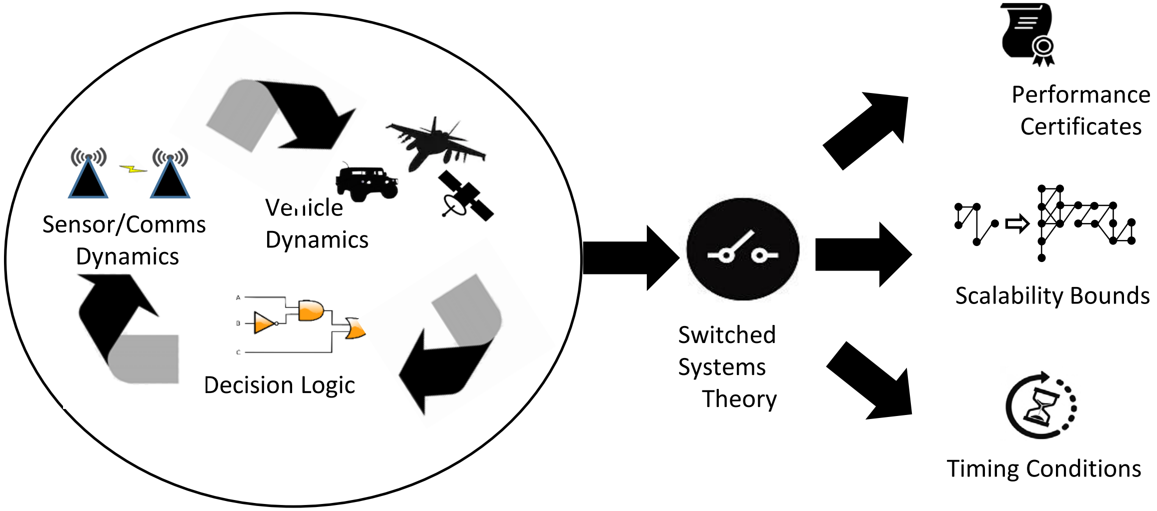
Foundations for protected computation, communication, and execution

Protected informatio n sharing

Foundation for resiliency

# Nonsmooth Systems

- Most of the results in the center involve complex systems that have multiple modes of operation, interaction with multiple agents, sequent of events that trigger different actions, decision logic that must be reasoned about, etc. – the fusion of information and dynamics
- This RT permeates most of the other RTs, but open questions remain regarding the development new nonsmooth analysis and design frameworks for safety, intermittency, asynchrony, uncertainty



# Nonsmooth Systems

- **Some Major Contributions**
  - Tools to verify the satisfaction of temporal logic (TL) specifications for hybrid dynamical systems, where conditional invariance and eventual conditional invariance are employed (Connection to RT2)
  - Methodology to design an observer with inter-sample injection to exponentially estimate, with a given decay rate, the state of a continuous-time Lipschitz nonlinear system in the presence of sporadically available measurements (Connection to RT3)
  - (AFRL co-authored) Data-based, exponentially converging observers for a monocular camera to estimate the Euclidean **structure** of viewed objects and camera **motion**, without requiring the typical positive depth constraint (Connection to RT2)
  - Single-agent indirect herding & relay-explorer problems: Development of (less conservative) dwell-time conditions and formal sequencing conditions (connections between Lyapunov methods, model-predictive control (MPC) and metric temporal logic (MTL)) (Connection to RT2, RT3)

# Adaptive, Optimal, Synthesis Methods

- Complex environments often exhibit uncertainty, yet, there is a desire for autonomous systems to make the best possible (optimal) decision despite the uncertainty, and in a timely manner e.g., to meet high-level specifications
- Further complexities emerge when the system is changing among different subsystems, or the uncertainty is time-varying

- **Some Major Contributions**
  - Use of reinforcement learning (RL)-based controllers to approximate multiple value functions of specific classes of subsystems while following a switching sequence (Connection to RT1)
  - (AFRL co-authored) Online approximate optimal control techniques using a combined framework of sparse, segmented BE extrapolation and barrier functions (BFs), to optimally regulate a dynamical system while providing formal safety guarantees (Connection to RT1, RT5)
  - (AFRL co-authored) An infinite horizon approximate dynamic programming (ADP) problem is addressed for a system with unknown drift parameters and control effectiveness faults (Connection to RT1, RT5)

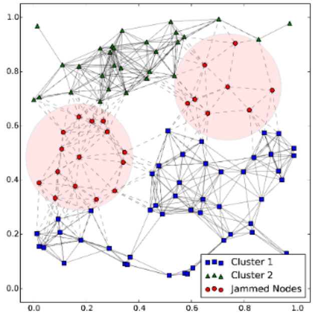
# Adaptive, Optimal, Synthesis Methods

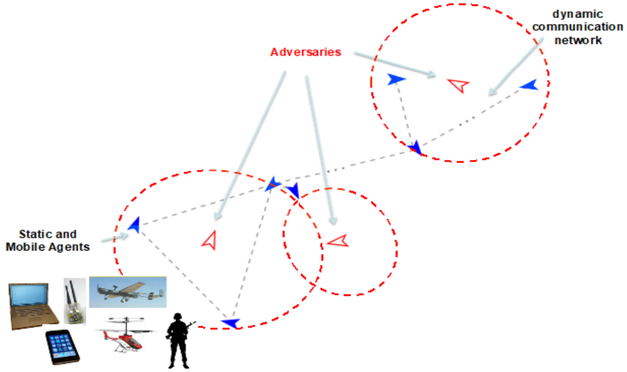
- **Some Major Contributions** (cont.)
  - Advancements and applications of integral concurrent learning: regolith excavation robot, marine vehicle where the rigid body and hydrodynamic parameters are unknown, and a network of low Earth orbiting spacecraft consisting of multiple chasers and a single cooperative or unknown target (Connection to RT1 & RT3)
  - A hybrid gradient descent algorithm for optimization for systems with hybrid dynamics, with applications to parameter estimation and model predictive control (Connection to RT1)
  - Accelerated optimization algorithms with no overshoot and oscillations nearby the set of minimizers of the optimization problem being solved, with a rate of convergence that is characterized mathematically
  - Model-free learning (+tool) for Markov Decision Processes (MDPs) and stochastic games with maximal probabilistic guarantees
  - Developed synthesis methods for uncertain partially observable MDP that offer orders of magnitude better scalability. Applied these methods in the context of spacecraft motion planning against stochastic uncertainties and potential adversaries (Connection to RT5)

# RT3 &4

## Network Systems & Asynchronous Information

- Ensuring the availability and integrity of information in complex contested environments presents a number of challenges for autonomous agents
- These challenges are exacerbated for large networks of agents operating in adversarial conditions (e.g., issues of scalability, computational resources, verifiability, collaboration strategies, and additional unique complexities)
- Since such networks are the union between the physical agent dynamics and the information dynamics, this research topic focuses on analysis, design and synthesis methods for agents *within a network and over a network*
- Moreover, sharing information across the network can lead to variable and unknown time-delays and asynchrony among agents in the network





# RT3 &4

## Network Systems & Asynchronous Information

- **Some Major Contributions**
  - Control scheme enabling a network control system to detect and mitigate false data injection (FDI) attacks (Connection with RT5)
  - A parallelized block-based primal-dual algorithm for solving constrained convex optimization problems, in presence of asynchrony
  - Results bounding the probability of connectivity for random graphs and unions thereof, applicable to multi-agent applications in both control and optimization, where some convergence rates explicitly depend upon the time needed to attain a connected union graph
  - Controller, estimator, and predictor framework for tracking a moving target using intermittent measurements by a network of mobile cameras, with non-overlapping fields-of-views and operating regions (Connection with RT1)
  - Results to estimate the maximum time that a control algorithm can wait to update the control input and still guarantee asymptotic stability and safety (Connection with RT1)

# RT3 &4

## Network Systems & Asynchronous Information

- **Some Major Contributions** (cont.)
  - (AFRL co-authored) Control scheme enabling clusters of agents to obtain consensus using intermittent and asynchronous state feedback over a connected union graph (Connection with RT1)
  - Developed the first constrained convex optimization algorithm that is fully parallelized and allows all delays to be arbitrarily long
  - Quantified the contribution of individual communications to attaining connected network topologies over time

# Attack Resilient Design

- The goal of this research topic is to address security challenges related to attacks against a multi-agent mission where the attacker can (1) take over a sensor and supply wrong or untimely sensor readings, (2) disrupt actuation, (3) affect communication between agents, or (4) even compromise some of the agents involved in the mission
- These attacks manifest themselves as malicious interference signals, and the defenses against them have to be introduced in the control/autonomy design
- Our key research results have focused on security-aware control design for systems with varying levels of autonomy, while guaranteeing the desired levels of system performance (i.e., Quality-of-Control) even when the system is under attack. Our goal has been to add resiliency at every level of the autonomy-stack (low-level control, switched controllers, planners)

# Attack Resilient Design

- **Some Major Contributions**
  - A method developed for modeling and detection of event insertion and removal attacks, in distributed sequential control, based on the supervisory control theory framework, and a method provided to identify communication links requiring protection to avoid catastrophic damage to the system
  - Statistical Model Checking (SMC) for hyperproperties
  - Mixed Integer Linear Program (MILP)-based framework for integrating security guarantees with end-to-end timeliness requirements for control transactions in resource-constrained cyber-physical systems
  - Development of trust and reputation model using redundant state information to detect and exclude Byzantine adversaries from the network composed of cooperative agents (Connection with RT3 &4)

## Protecting Safety- and Mission-Critical Information

- Agents' actions can be observed by adversaries and decisions to change modes, e.g., from surveying an area to pursuing a target, can reveal modes of operation and switching strategies to adversaries
- Agents' communications can also be intercepted, including communications within and between teams of agents, and these communications can contain sensitive information, such as the agents' intents and tactics
- While adversarial environments can impose a variety of disturbances from external sources, efforts in this research topic will also explore the strategic disruption of information as a means to safeguard agents' actions and communications

# Protecting Safety- and Mission-Critical Information

- **Some Major Contributions**
  - Differentially private formation control enabling agents to assemble formations while only sharing differentially private output data. Developed guidelines for calibrating privacy under different control-theoretic requirements (Connection with RT3)
  - Developed a privacy-preserving policy synthesis algorithm that protects the privacy of the transition probabilities of its input MDP, using a Dirichlet mechanism to privatize the transition probabilities (Connection with RT2)
  - Developed a new analysis of adversarial robustness demonstrating adversaries leveraging query-efficient techniques using zeroth-order optimization counter-intuitively discover more on-manifold examples
  - Developed the first differential privacy protections for information in the unit simplex
  - Applied that differential privacy mechanism to decision policies in MDPs to take actions that conceal their intent

# Workforce Dev.
# AFRL Collaborations
# Publications

UF UNIVERSITY of FLORIDA

Duke UNIVERSITY

TEXAS
The University of Texas at Austin

UC SANTA CRUZ

# Collaborative Interactions

- Project partially supports
  - 5 postdocs/research scientists, 46 (+11) PhD, 2 (-3) MS
- Now have Alumni
  - 3 postdocs – Univ. of Sherbrooke, Univ. of Arizona, Apple
  - 4 PhD – RW, Ford, Qualcomm, Univ. of the Bio
  - 2 MS – Lockheed Martin (Orlando), Walmart Labs
- SMART Fellowship application for RV (Sage Edwards)
- AFRL/Space Scholar/intern ~10 students summer 2020
- AFRL Summer Faculty Fellows program
  - Riccardo Bevilacqua (2019 & 2020 AFRL/RW)
  - Matthew Hale (2020 AFRL/RW)

- Publications
  - 119 total, 47 in 2020
  - Joint publications - 14 w/ PIs, 12 w/ AFRL
- Workshops
  - ~5 workshops, ~ 3-5 invited sessions (in-progress for webpage)
  - Starting bi-monthly seminar series (when?)

UF UNIVERSITY of FLORIDA Duke UNIVERSITY TEXAS The University of Texas at Austin UC SANTA CRUZ