Extending Flexible Contracts for Mission Assurance and Reliability Assessment

Sponsor: DASD(SE)

By
Dr. Azad M. Madni

9th Annual SERC Sponsor Research Review
November 8, 2017
FHI 360 CONFERENCE CENTER
1825 Connecticut Avenue NW, 8th Floor
Washington, DC 20009

www.sercuarc.org
Outline

- Mission Assurance
- Project Objective
- Approach
- Accomplishments To Date
- Follow-on Plans
Project Team

- Dr. Azad M. Madni, Principal Investigator
- Dr. Michael Sievers, Advisor, Mission Assurance Expert
• Mission Assurance (MA) defined in DOD Directive 3020.40:
  "a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the DoD to carry out the National Military Strategy."

• MA is an implied requirement for all systems

• Reliability Assessment (RA) is part of MA and therefore also a requirement for all systems
Current MA Approach

MA performed during design cannot reflect real-time situational awareness
Questionable Predictions

• Can’t always reliably predict system behavior
  — can’t fully control system’s environment and usage
  — can’t understand all states the system might be in

• So, don’t have good understanding of whether system is:
  — performing satisfactorily (i.e., within safe regime)
  — in trouble (e.g. in unsafe states)
  — heading into potential trouble (i.e., about to enter unsafe state)

• Online assessments can potentially help understand a system’s overall state and status, and guide system decisions
  — continually evaluate system belief state as we take actions
Develop Model-Based Approach for On-Line Mission Assurance and Reliability Assessment based on Extending Flexible Contracts Construct (SERC Incubator Project)
Accomplishments to Date

- Developed probabilistic model-based approach to MA
- Made presentation to SERC Advisory Board (May 23, 2017)
- Demonstrated building blocks for model-based MA
- Secured Transition Letter from The Aerospace Corporation
- Completing Incubator Report
- Paper submitted to 2018 INCOSE IS
Probabilistic Model-Based MA

• Driven by specific requirements
  — Verification and Testing
  — Real-time MA (includes RA)
  — Scale with increase in system size and interconnections

• Expected Benefits
  — continuity of operations and critical processes in the face of disruptions
  — protection of organization’s resources and functions from disruptions
Flexible Contracts (FCs) are trained during nominal and off-nominal operation. The State Estimator determines the probability distribution of a set of “belief states” from observations made and actions taken. MA is evaluated from the belief distribution. The Response Policy determines the optimal action to take as a function of the state estimation and MA evaluation. FCs are implemented by POMDP process models.

Online evaluation of system belief states enables real-time MA estimation.
Key Construct: Flexible Contract

- Hybrid modeling construct with learning capability
  - for stochastic/probabilistic systems
  - partial observability, noisy sensors, uncertain environment
  - key trade-off: degree of formality (V&V) vs level of flexibility (resilience)
  - developed at design time, trained during operational use ("learning")

- Comprises:
  - traditional contract
  - flexibility: relax assume-guarantee assertions in traditional contract
  - Partially Observable Markov Decision Process (uncertainty handling)
  - in-use learning (hidden states, transitions, emissions)
  - pattern recognition

- Applications
  - resilient multi-UAV swarm control
  - resilient autonomous vehicle SoS network
  - dynamic mission assurance
Flexible Contract (FC)

FC evaluates POMDP reward; typical responses:
- Keep going
- Stop
- Enforce trajectory to a safe state
- Notify support team
Use of FC for MA

- Compute probability associated with either being in a bad state, questionable state, or heading into a bad or questionable state.
- For example, if system is in state S1, and there are transitions to S2 which lead to S3 (a bad state), then we can compute the probability of getting into S3.
- We might also have a transition from S1 to S4 to S5 to S6 and compute that probability (which might be higher than $S1 \rightarrow S2 \rightarrow S3$).
- Reliability is the probability of not getting to S3.
- If we know transition rates and repair rates, we can predict availability, etc.
- This is a relatively straightforward Markov problem that happens to have hidden states.
Example

Suppose we have a simple system comprising prime (P) and redundant (R) computers cross-strapped to sensor and actuator interfaces:

\[ R_{sys} = R_{sens} \times R_{act} \times (2R_{comp} - R_{comp}^2) \]
• Analyze static block diagram
  —e.g., fault trees evaluate potential causes of mission failure (top-down)
Proposed Approach: Iterative MA Evaluation

— At every iteration of belief estimate and action choice, can also evaluate system reliability, safety, risk, etc.

— Analysis comprises computing probabilities associated with the states, e.g.:
  - \( P \text{ (system is sound)} = \sum \text{Prob (system is in a known “good” state)} \)
  - \( P \text{ (system has failed)} = \sum \text{Prob (system is in a known “failed” state)} \)
  - \( P \text{ (system is in a risky state)} = \sum \text{Prob (system is in an unknown or un-designed for state)} \)
How This Approach Works for Our Example

- An initial Markov Model for a repairable system derived from invariant contracts might look like this:

The initial transition rates are set by up-front reliability analyses and repair rates.
Adding Flexibility: Example

- We know there are many possible states between failed and working for computers, sensors and actuators, but we might not know what these are – for simplicity, we’ll add a single hidden state, H1:

![Diagram showing state transitions]

The transition rates to and from H1 are initialized to 0. As the system runs, we observe system outputs and update transition rates.
Proposed Approach: Exploits RT-166 Building Blocks

- Mission Planning Problem
- Modeling Construct
- Resilient Contract
- State Transition Model
- Control Architecture
- Iterative Belief Update
Mission Planning Problem: UAV-SoS

- Dynamic
- Unpredictable
- Actions (discrete, stochastic)
  - Discrete
  - Stochastic

- Observations (partial, noisy)

- Next action?

- Environment
  - Weather
  - Adversaries
  - Other UAVs
  - Dynamic
  - Unpredictable

- Actions (discrete, stochastic)
Inflexible Contracts: Examples

• Contract #1: At the next instant, if obstacle ahead, then turn left

• Contract #2: At the next instant, if no obstacle ahead, then continue path
Resilience Contract: Extending Inflexible Contracts

- Can extend previous inflexible contracts to include threats
  - threats can be to the left, right, or unsure
  - define concept of belief state and penalty function
  - evaluate belief state based on sensor inputs, and then optimize penalty function

- A simple penalty function:
  - \[ P(\text{leftThreat}) \times 10 + P(\text{rightThreat}) \times (-100) + (1 - (P(\text{rightThreat}) + P(\text{leftThreat})) \times (-1) \]

- If \( P(\text{leftThreat}) = 0.95 \), \( P(\text{rightThreat}) = 0.01 \), and \( P(\text{can't decide}) = 0.04 \), then:
  - penalty = \( 0.95(10) + 0.01(-100) + 0.04(-1) = 9.5 - 1 - 0.04 = 8.49 \), if turn left
  - penalty = \( 0.01(10) + 0.95(-100) + 0.04(-1) = 1 + 95 - 0.04 = -95.94 \), if turn right

- Want to turn right because penalty for turning right is negative (i.e., reward), but penalty for turning left is positive
State Transition Model

Quad Copter State

- Initialize / Spin Up
- Shut Down
- Normal Motors:
  - Do / Increase Motor Speed
- Degraded Motor
- Failed Motor
- Auto Plan Enabled:
  - Do / Process Plan
- Read Forward Sensors
- Evaluate Environment

- Ascend
- Descend
- Turn Right
- Turn Left
- Hover
Exemplar Swarm Control Architecture

Environment Sensors

Belief MDP Model

Agent

Policy

Belief Estimates

State Estimator

Actions

Observations

UAV Swarm
Iterative Belief Update

**Belief Vector**

**Action = observe**

\[ b_1(s_i) = \frac{P(o|s_i, a) \sum_{s_j \in S} P(s_i|s_j, a)b_0(s_j)}{P(o|a, b)} \]
Graphic shows **progression** of four belief states’ probabilities starting with all states being equally probable. When observation “a” arrives at the State Estimator, the belief estimates change making state S1 the most likely. When “d” is observed, the **belief evaluation** makes state S4 the most likely. Lastly, another “a” is observed and S1 is again the most likely. If S4 = “failed,” for example, then **reliability** = 1-Pr(S4).
• **MA (including RA) is required for all DOD systems**

• **Current MA approaches**
  — limited to only design time considerations
  — fail to exploit real-time operational data to adjust MA estimates

• **Proposed Approach**
  — flexible contracts (probabilistic formal model-based approach)
  — supports verification and testing
  — flexible assertions (environmental uncertainty, support behavior adaptation)
  — exploitation of real-time operational data in MA assessment

• **Key insights**
  — Inflexible contracts can be made flexible through inclusion of “belief states” and “reward/penalty functions”
  — Replace “assert-guarantee” with “belief-reward” in traditional contract
  — Bayesian Belief Networks to iteratively update beliefs with new data

• **Impact:** advance state-of-the-art in MA and RA
Follow-on Plans

- Finalize exemplar system of interest to DOD
- Build on our technology platform from RT-166
- Incorporate actionable visualization
- Explore how heuristics can dynamically modify POMDP policy
  —strictly formal/formulaic methods are insufficient to cope with real world complexity (Sievers and Madni, 2017)
- Pursue staged implementation
  —MDP on simple problem, POMDP on simple problem, online MA assessment on representative problem
- Transition prototype to SERC and transition partner(s)

Have team in place and identified transition opportunities


Thank You!