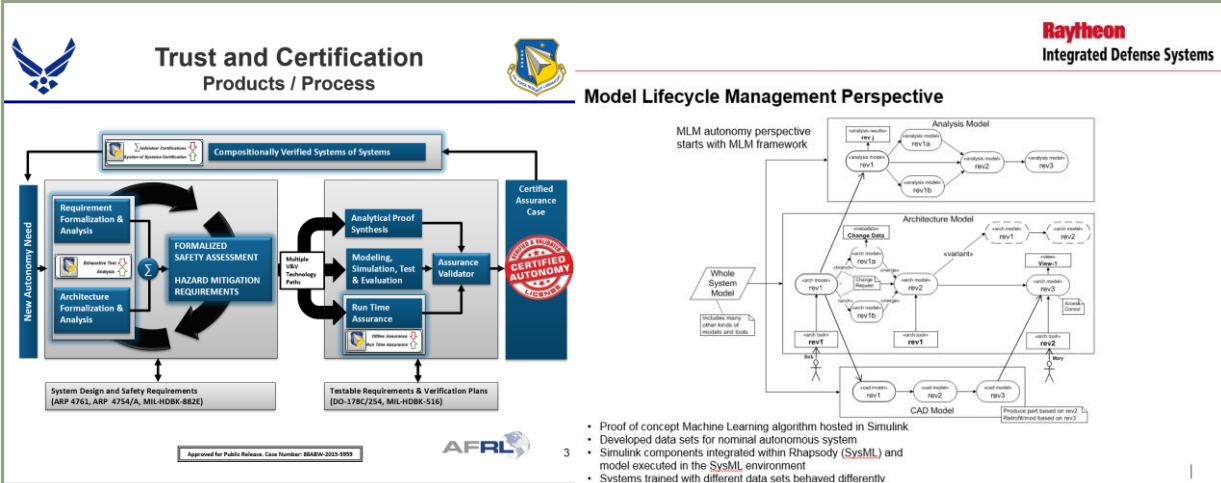
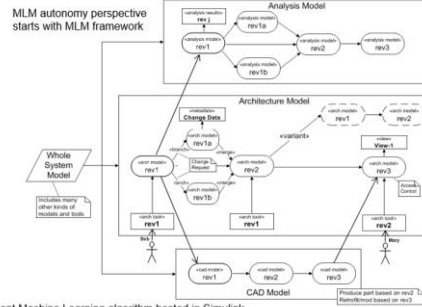


# IV&V of Autonomous Systems in a Model Based Engineering Context

AFRL, Raytheon collaboration



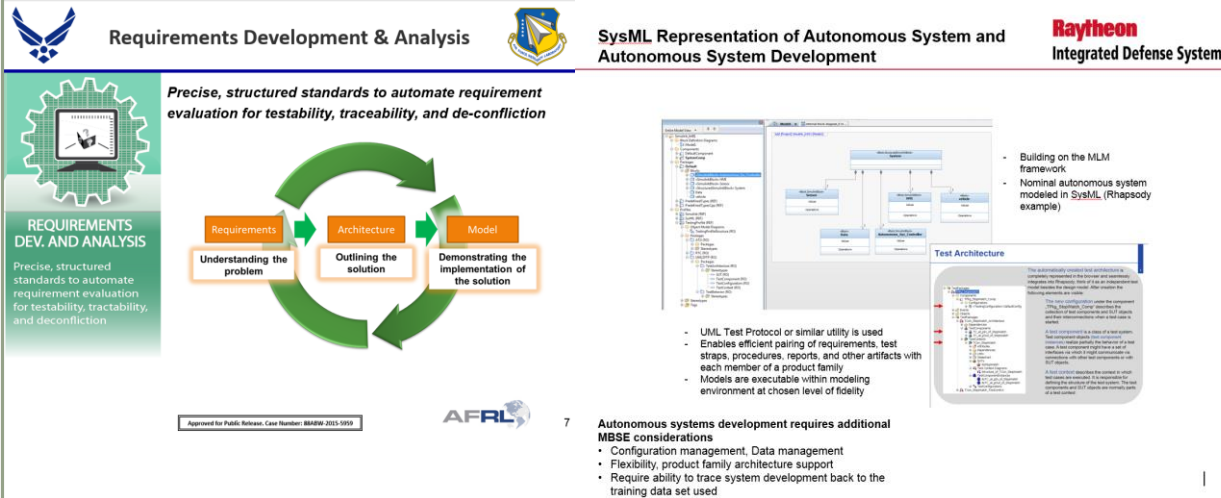
## Model Lifecycle Management Perspective



- Proof of concept Machine Learning algorithm hosted in Simulink
- Developed data sets for nominal autonomous system
- Simulink components integrated within Rhapsody (SysML) and model executed in the SysML environment
- Systems trained with different data sets behaved differently

Section	Rating	Red	Yellow	Green
System of Systems V&V	B	3	8	7
Uncertainty	D	6	6	5
Emergent Behavior	C	1	3	18
Defacto Standards Licensing vs Certification	A	14	2	1
Requirements	A	14	5	11
Modeling and Simulation	A	15	2	2
Trust	B	4	10	3
Human/Machine Interaction	B	2	12	4
Test	A	11	6	
Runtime Verification	B	2	11	5
Synthesis	C	1	4	15
Tool Verification	B	3	9	4
Security	D	4	9	8

Figure 2: Priority and Score for Each Technical Challenge (Red (A) = Near Term, Orange (B) = Mid Term, Green (C) = Far Term)



- Autonomous systems development requires additional MBSE considerations**
- Configuration management, Data management
  - Flexibility, product family architecture support
  - Require ability to trace system development back to the training data set used

## “Chatter” – notional interface

The interface shows 'Chatter Settings' with sections for 'Information by Time or Event', 'Unusual Values', and 'Save Data'. The log displays threat level transitions: '18:07:18 New Threat Level transition: Benign → Suspicious' and '18:05:16 New Threat Level transition: Suspicious → Threatening'. Logos for AFRL and Raytheon are present.

Applied to Fast Attack Craft / Fast Inshore Attack Craft (FAC/FIAC)

## MBE Development & Sustainment

IV&V Support ↔ Trust Ingrained

