Addressing Model Inadequacy during Design with Incremental Model Updates

NASA GSFC Systems Engineering Seminar

Mark Chodas

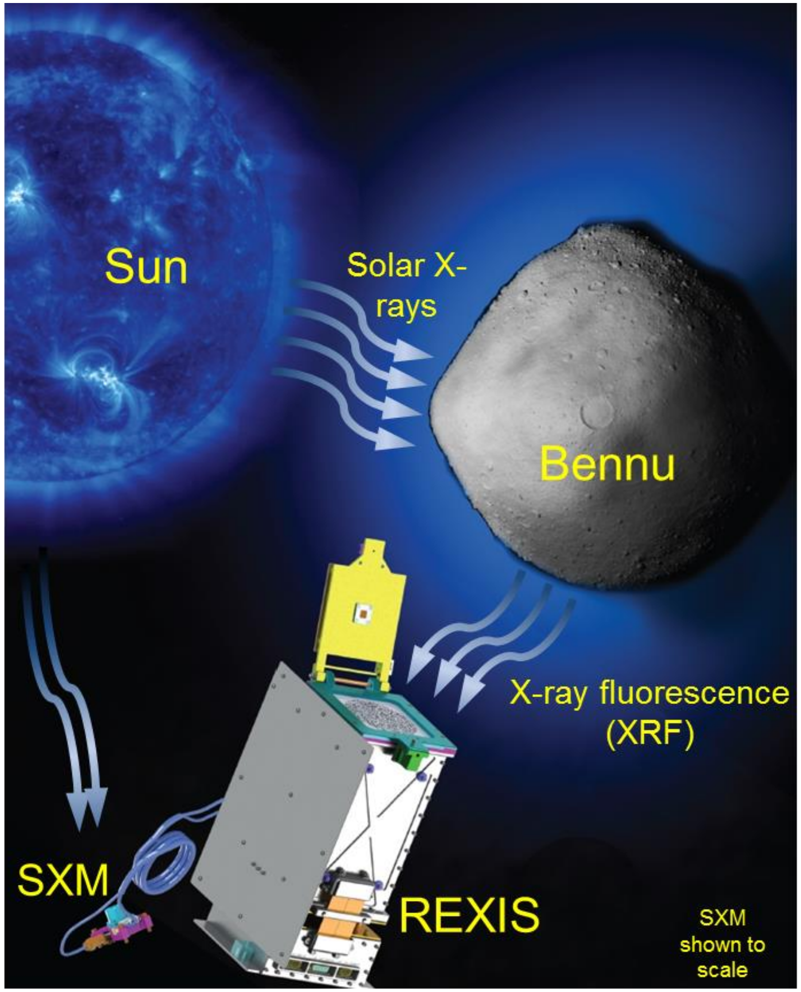
6/12/2017

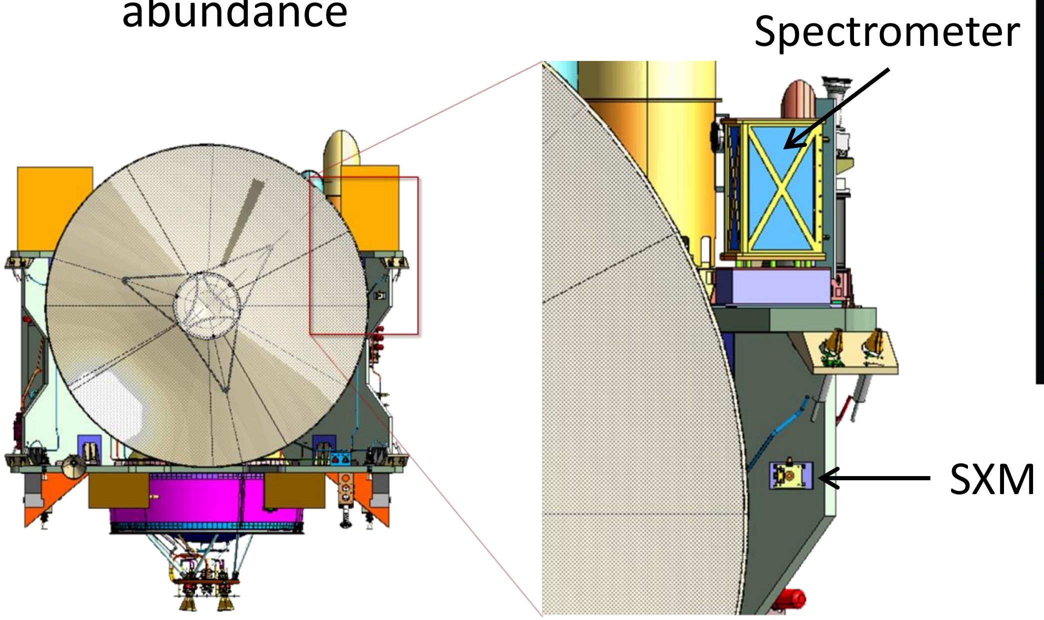
Outline

- Background
  - REXIS Overview
  - NASA Risk Management Process
  - Categories of Uncertainty
  - Model Based Systems Engineering
- Motivation
  - Risk Management Shortcomings
  - Programmatic & Technical Issues
- Problem Statement
- Approach
  - Design as decision making
  - Lifelong Planning A*
  - Incremental Model Update Algorithm
- Case Studies
  - REXIS
  - NASA GSFC MDL

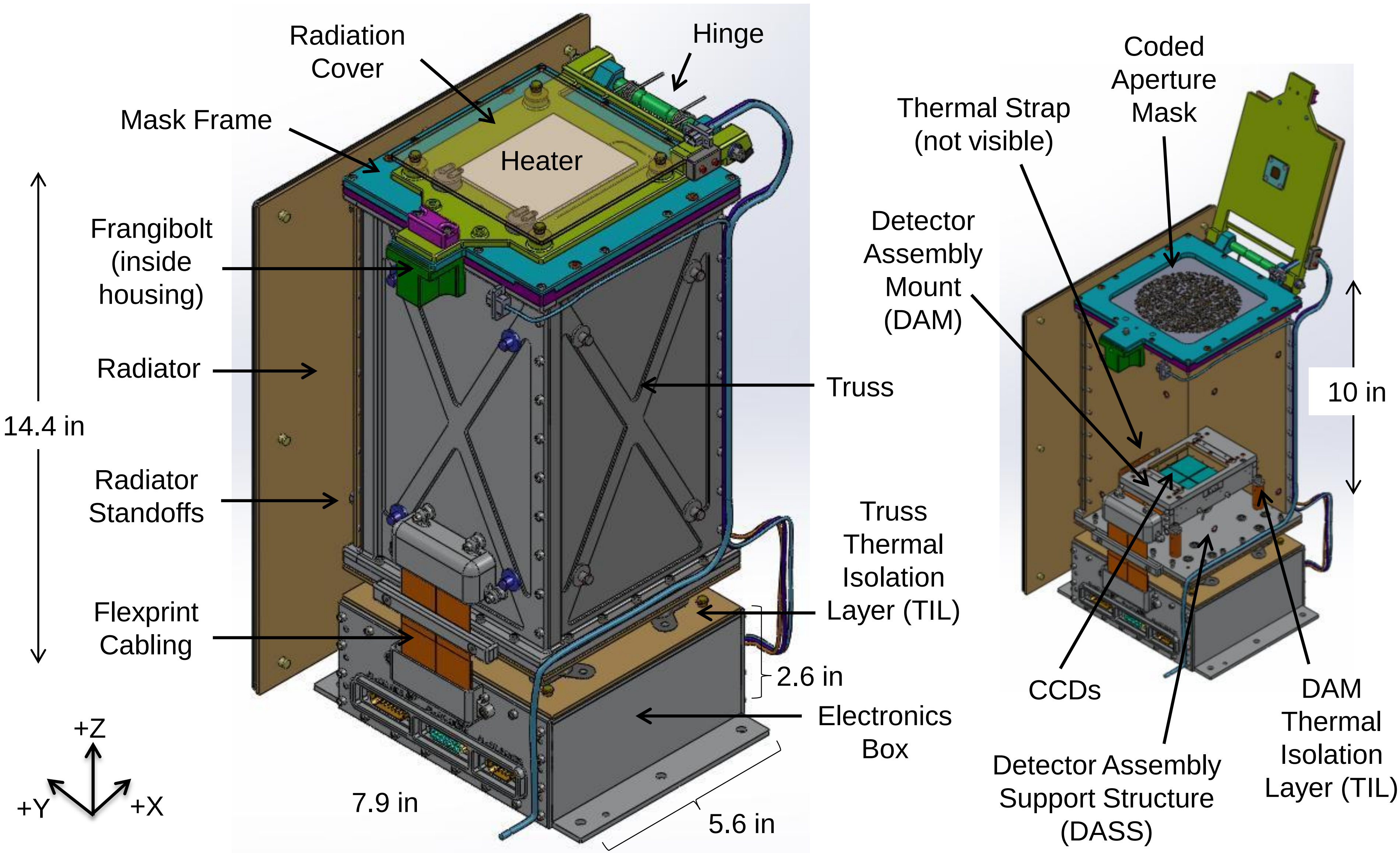
REXIS Science Goals

- One of five instrument on the OSIRIS-REx asteroid sample return mission scheduled for launch in 2016
- Measures X-rays that are fluoresced from Bennu
- Fluorescent line energies depend on the electronic structure of the matter
  - Provides a unique elemental signature
  - Line strengths reflect element abundance





REXIS Spectrometer Design

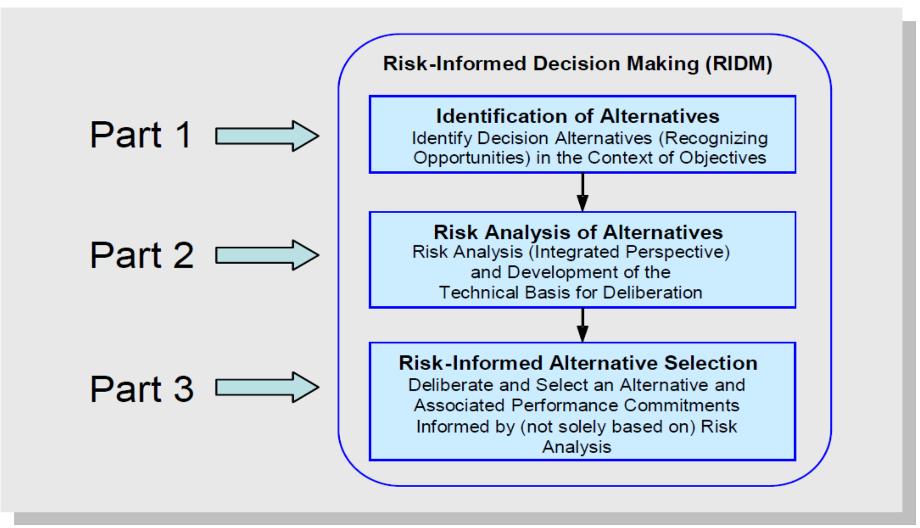


NASA Risk Management Process [1]

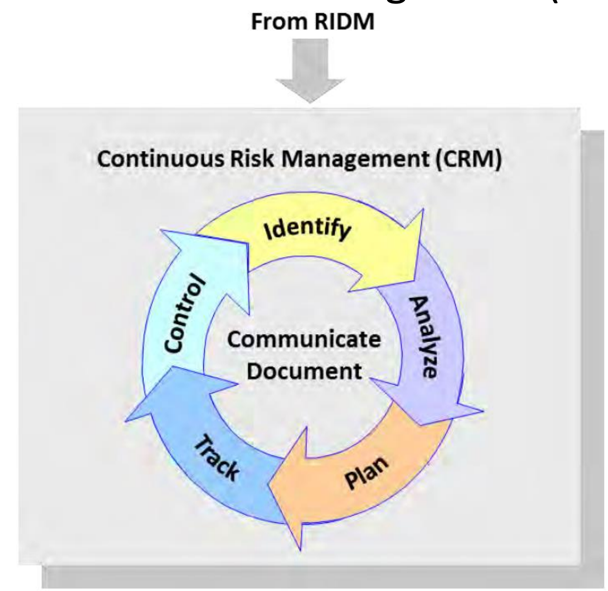
Risk management identifies and controls safety, technical, cost, and schedule issues that could impact mission success

RM = RIDM + CRM

Risk Informed Decision Making (RIDM)



Continuous Risk Management (CRM)



Models used extensively in risk management to identify risks, calculate the likelihood that a risk will manifest, analyze the consequence of a risk on the system, and to mitigate risks

[1] NASA Risk Management Handbook. NASA-SP-2011-3422. Version 1, Nov 2011.

Categories of Uncertainty

	Aleatory	**Epistemic**
Parametric	Material properties	Environmental properties
Nonparametric	New technologies	Design Uncertainty, Model Inadequacy

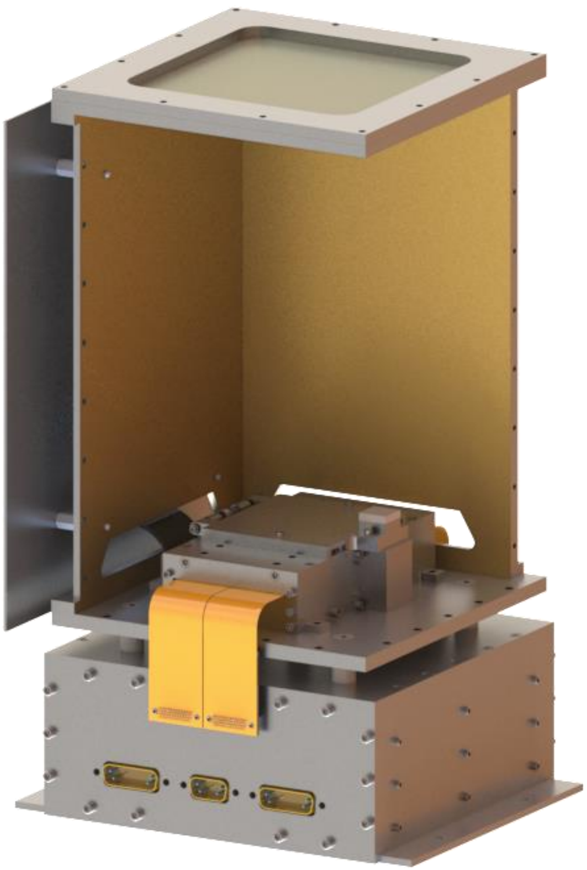
- This research focuses on design uncertainty and model inadequacy
  - Design Uncertainty: Uncertainty in which design option will be chosen out of a set of design options [19]
  - Model Inadequacy: The difference between a model output and the true behavior of the system [7]
- Design uncertainty and model inadequacy are always high at the beginning of a project and decrease over the lifecycle

[7] Brynjarsdóttir, J., & O'Hagan, A. (2014). Learning about physical parameters: The importance of model discrepancy. Inverse Problems, 30(11), 114007.
[19] Daniel Pierre Thunnissen. Propagating and mitigating uncertainty in the design of complex multidisciplinary systems. PhD thesis, California Institute of Technology, 2005.

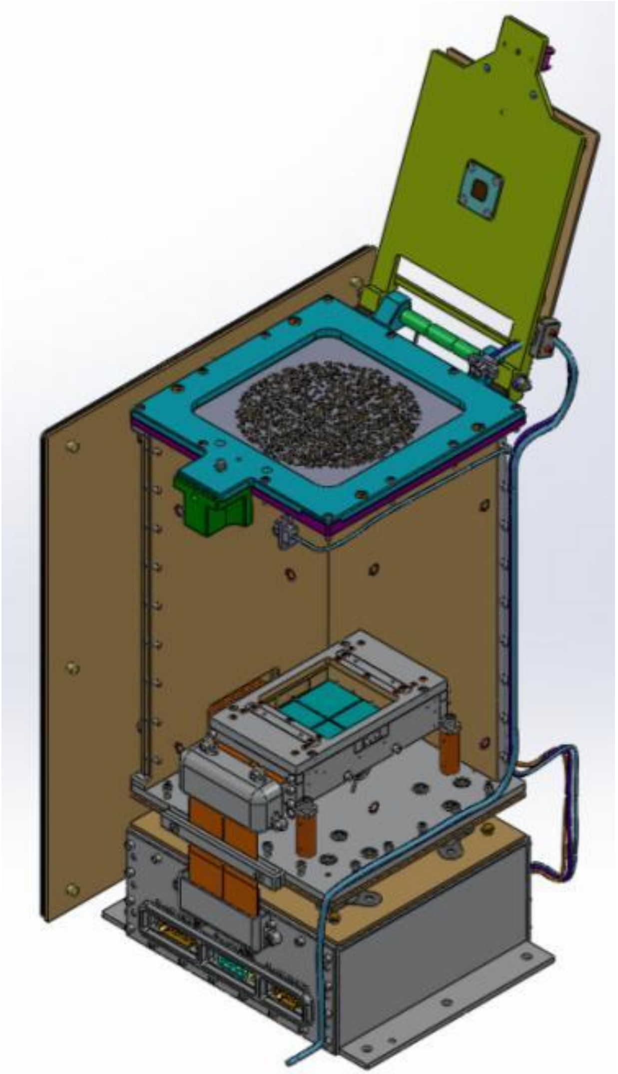
Examples of Design Uncertainty

CAD Model

PDR



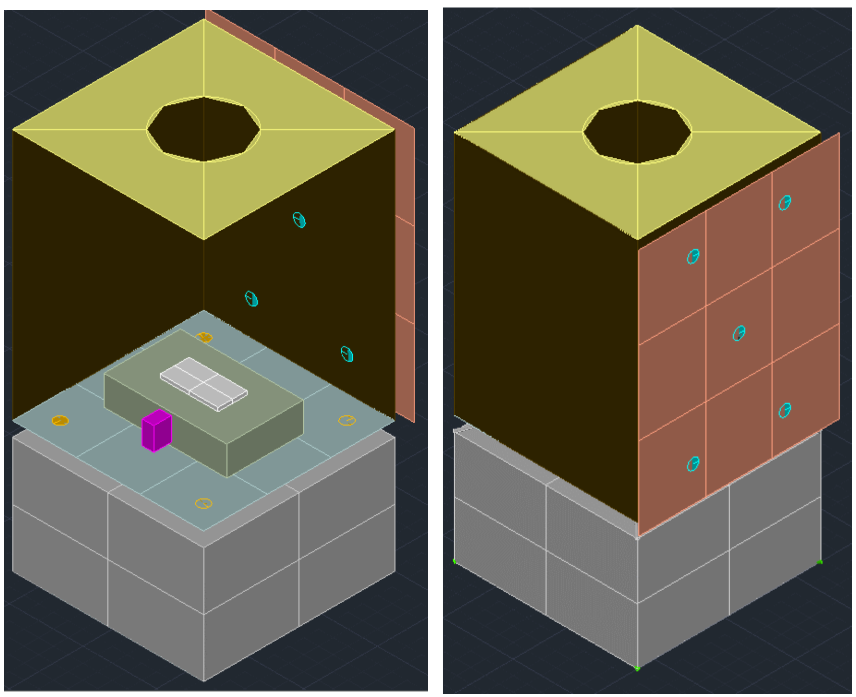
CDR



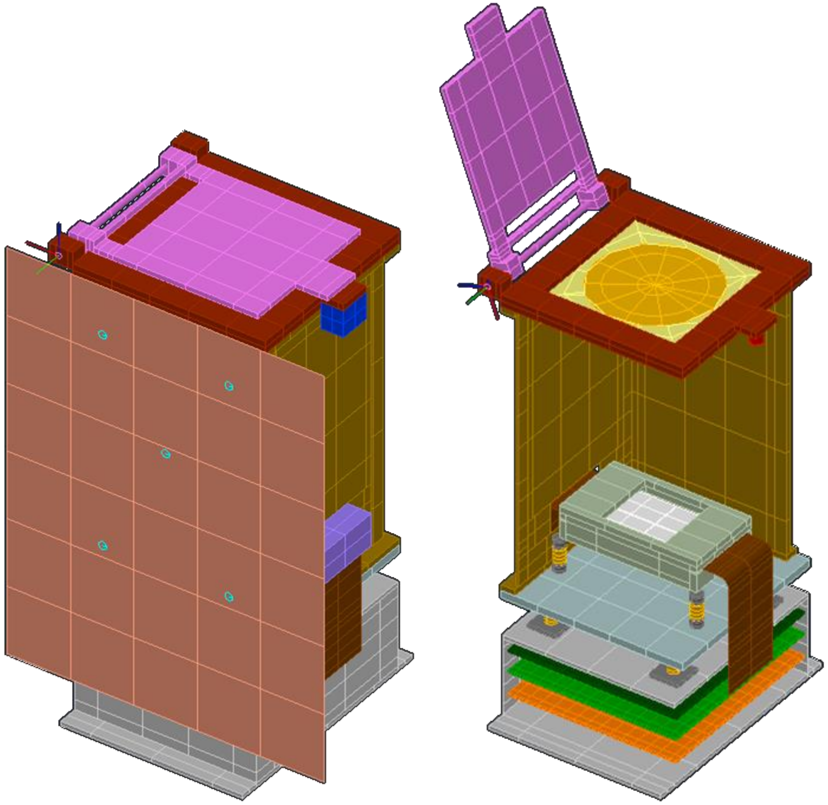
Examples of Model Inadequacy

Thermal Model

PDR

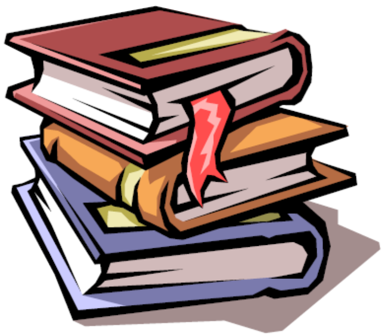


CDR



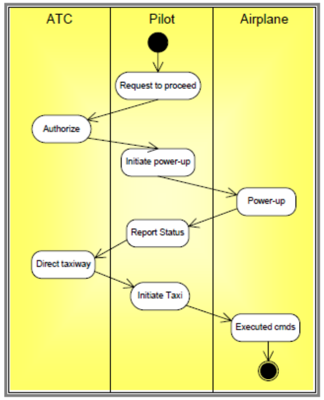
Model-Based Systems Engineering

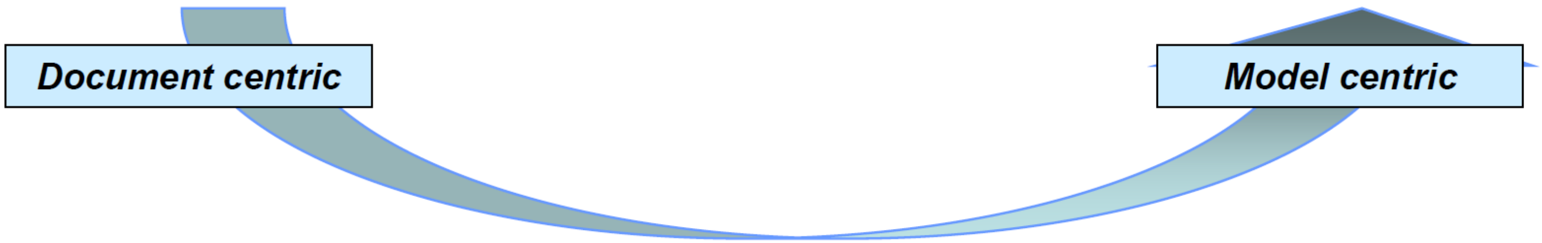
Past



SE Artifacts
- **Specifications**
- **Interface requirements**
- **System design**
- **Analysis & Trade-off**
- **Test Plans**

Future





INCOSE Model-Based Systems Engineering vision [15]

- Centralized, single-source-of-truth for system information
- Adds rigor and precision to the systems engineering process
- Similar to the introduction of CAD for mechanical design

[15] S. Friedenthal, R. Griego, and M. Sampson. INCOSE Model Based Systems Engineering (MBSE) Initiative. In INCOSE 2007 Symposium, 2007.

Risk Management with Model-Based Systems Engineering

Model-Based Systems Engineering (MBSE): the formalized application of modeling to support systems requirements, design, analysis, verification, validation, and operations

Applications of MBSE to Risk Management:

<u>Capture of System Information to Support Risk Analyses</u>
- Clear information capture to improve risk identification and analysis [9]
- Capturing component nominal and off-nominal behavior [6, 8]
- Tying component failures to requirement violations [6]

<u>Automated Risk Product Generation:</u>
- Fault tree generation [11]
- FMEA generation [10]
- FMECA generation [12]
- Probabilistic Risk Assessment [13]

MBSE expected to allow automated updating of risks when system model changes but no established process for:
- Determining what model changes necessitate risk updates
- Efficiently re-performing risk analyses

[6] Jean-Francois Castet, Magdy Bareh, Jeffery Nunes, Steven Jenkins, and Gene Lee. Fault management ontology and modeling patterns. In AIAA SPACE 2016, page 5544. 2016.
[8] Cressent, R., David, P., Idasiak, V., & Kratz, F. (2013). Designing the database for a reliability aware Model-Based System Engineering process. Reliability Engineering & System Safety, 111, 171-182.
[9] Evans, J., Cornford, S., & Feather, M. S. (2016, January). Model based mission assurance: NASA's assurance future. In Reliability and Maintainability Symposium (RAMS), 2016 Annual (pp. 1-7). IEEE.
[10] Hecht, M., Dimpfl, E., & Pinchak, J. (2014, November). Automated Generation of Failure Modes and Effects Analysis from SysML Models. In Software Reliability Engineering Workshops (ISSREW), 2014 IEEE International Symposium on (pp. 62-65). IEEE.
[11] Faida Mhenni, Nga Nguyen, and Jean-Yves Choley. Automatic fault tree generation from sysml system models. In Advanced Intelligent Mechatronics (AIM), 2014 IEEE/ASME International Conference on, pages 715–720. IEEE, 2014.
[12] Michel Izygon, Howard Wagner, Shira Okon, Lui Wang, Miriam Sargusingh, and John Evans. Facilitating r&m in spaceflight systems with mbse. In Reliability and Maintainability Symposium (RAMS), 2016 Annual, pages 1–6. IEEE, 2016.
[13] Sam Schreiner, Matthew L Rozek, Andy Kurum, Chester J Everline, Michel D Ingham, and Jeffery Nunes. Towards a methodology and tooling for Model-Based Probabilistic Risk Assessment (PRA). In AIAA SPACE 2016, page 5545. 2016.

Motivation - Overview

Are there areas for improvement in NASA's risk management process?

Does NASA's risk management process adequately address all categories of uncertainty?

1. Design change only performed in contingency
2. Risk mitigation re-planning only triggered on mitigation plan inadequacy
3. Risk re-analysis only triggered on inadequacy of mitigation plan built off of risk analysis model

Do space missions tend to experience programmatic and/or technical issues?

Evidence shows programmatic overruns are common and technical failures occasionally occur [2-5, 20]

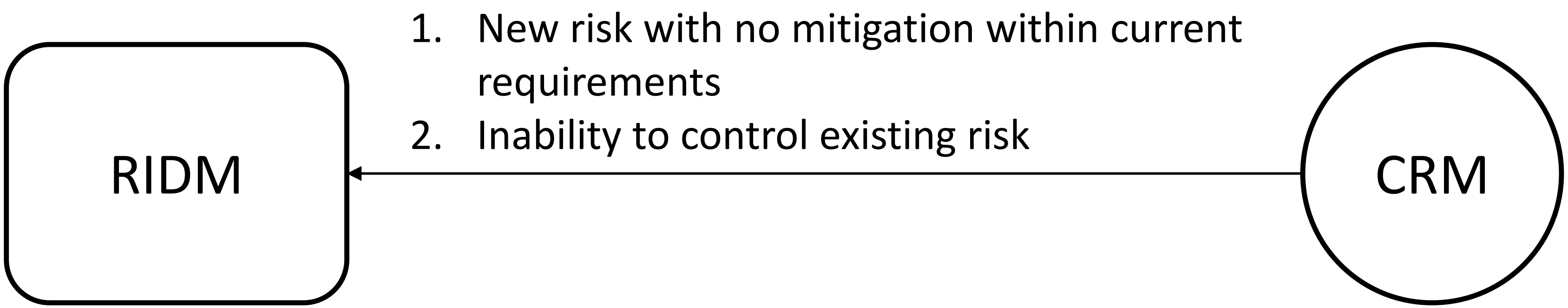
[2] D.L. Emmons, M. Lobbia, T. Radcliffe, and R.E. Bitten. Affordability Assessments to Support Strategic Planning and Decisions at NASA. In Aerospace Conference, 2010 IEEE, 2010.
[3] Report of the Columbia Accident Investigation Board Volume I. Technical report, 2003.
[4] A. Albee, S. Battel, R. Brace, G. Burdick, J. Casani, J. Lavell, C. Leising, D. MacPherson, P. Burr, and D. Dipprey. Report on the loss of the Mars Polar Lander and Deep Space 2 missions. 2000.
[5] Glenn Reeves and Tracy Neilson. The Mars Rover Spirit Flash Anomaly. In Aerospace Conference, 2005 IEEE, pages 4186–4199. IEEE, 2005.
[20] Robert E Levin and GAO Director. Space acquisitions: Stronger development practices and investment planning needed to address continuing problems. Statement to the House Armed Services Committee, Subcommittee on Strategic Forces, 2005.

Risk Management Shortcomings

- Design change only performed in contingency
- Risk mitigation re-planning only triggered on mitigation plan inadequacy
- Risk re-analysis only triggered on inadequacy of mitigation plan built off of risk analysis model

Risk Management Shortcomings

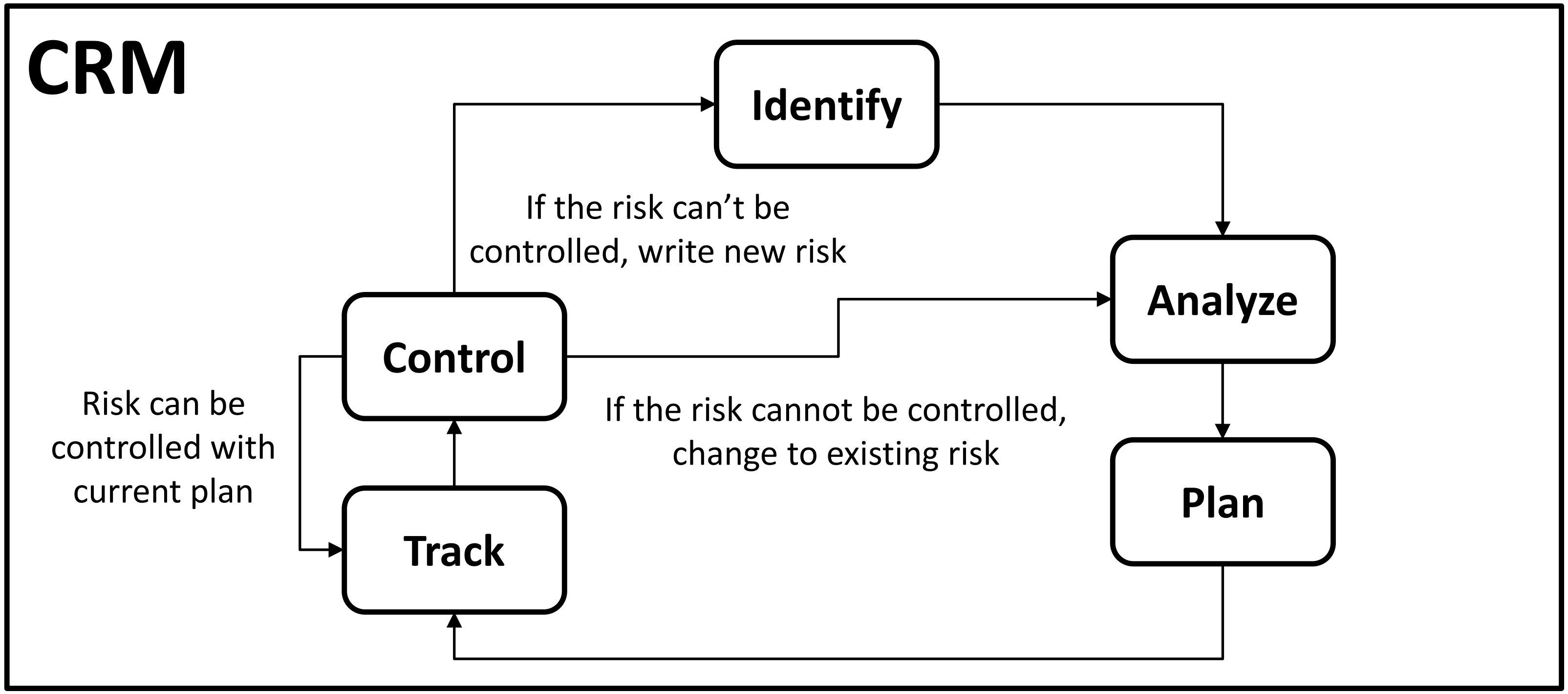
- Design change only performed in contingency



- Risk mitigation re-planning only triggered on mitigation plan inadequacy
- Omitting Risk Re-Analysis

Risk Management Shortcomings

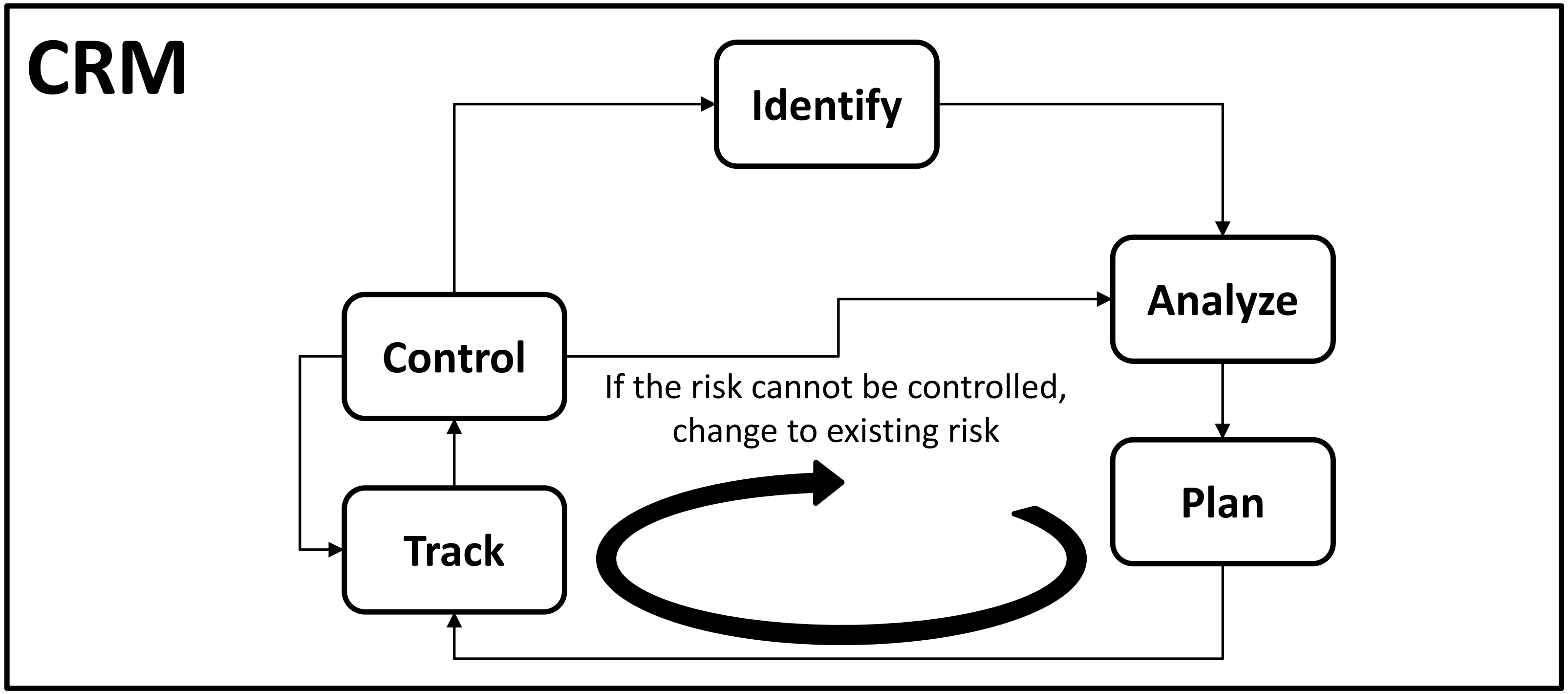
- Design change only performed in contingency
- Risk mitigation re-planning only triggered on mitigation plan inadequacy



- Risk re-analysis only triggered on inadequacy of mitigation plan built off of risk analysis model

Risk Management Shortcomings

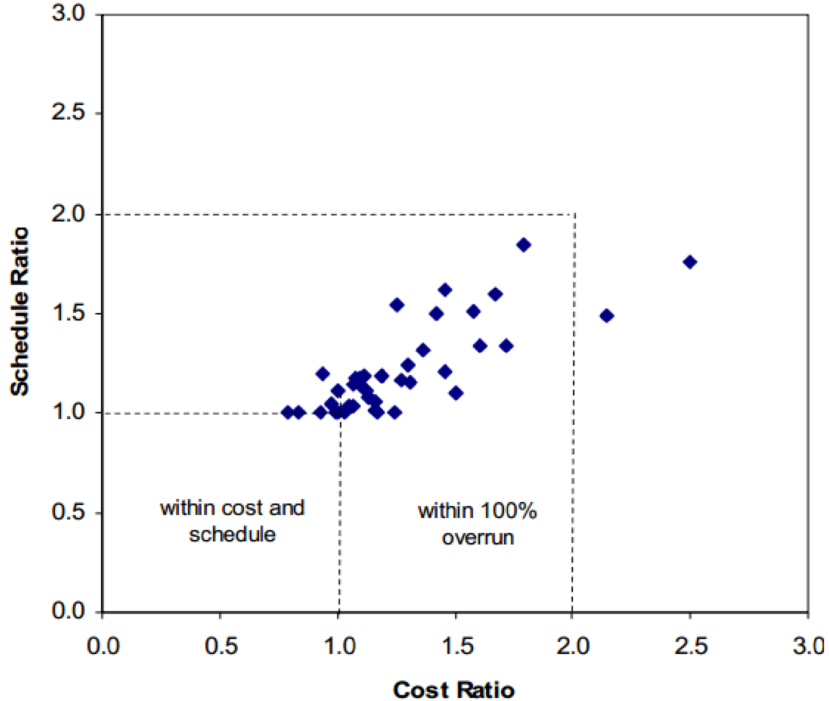
- Design change only performed in contingency
- Risk mitigation re-planning only triggered on mitigation plan inadequacy
- Risk re-analysis only triggered on inadequacy of mitigation plan built off of risk analysis model



Risk Management Shortcomings

- Design change only performed in contingency
  - Decisions made using RIDM are only revisited when risks cannot be adequately mitigated in the CRM process
    - No re-analysis mechanism inherent to the RIDM process
  - Design changes that improve on existing and adequate plans are not considered
- Risk mitigation re-planning only triggered on mitigation plan inadequacy
  - Risk mitigations only replanned when existing risk mitigation plan is inadequate
  - Risks mitigations plans do not necessarily evolve as the system changes
    - In real missions, risks are typically examined on a monthly basis and mitigation plans can be updated
- Risk re-analysis only triggered on inadequacy of mitigation plan built off of risk analysis model
  - Risk re-analysis relies on output of risk analysis model
  - If risk analysis model is insensitive to system changes, then it won't be updated to track those changes
- How to address these shortcomings?
  - Re-analyze all risks whenever new information is learned
    - Able to take advantage of new possibilities for improved risk mitigations
    - Decouples risk re-planning from risk analysis model output
    - Re-analysis must be done efficiently to avoid excessive wasted effort

Programmatic Overruns



Cost and schedule overruns for selected NASA projects between 1992 and 2007. The average cost overrun is 27% and the average schedule overrun is 22% with cost and schedule overruns being correlated [2].

DoD space systems also have experienced drastic programmatic overruns [20]

– AEHF: Cost ↑ 50%, Schedule → 3yrs
– NPOESS: Cost ↑ 10%
– SBIRS-High: Cost ↑ 150%, Schedule → 6yrs

[2] D.L. Emmons, M. Lobbia, T. Radcliffe, and R.E. Bitten. Affordability Assessments to Support Strategic Planning and Decisions at NASA. In Aerospace Conference, 2010 IEEE, 2010.
[20] Robert E Levin and GAO Director. Space acquisitions: Stronger development practices and investment planning needed to address continuing problems. Statement to the House Armed Services Committee, Subcommittee on Strategic Forces, 2005.

Technical Mishaps

- Space Shuttle Columbia [3]
  - Mishap: Loss of mission due to foam strike on left wing leading edge leading to orbiter burn up during reentry
  - Foams strikes were known to occur, but not regarded as safety issue
    - Seen on previous flights, but never caused clear threat to mission
  - **Risk Management Failure: Consequence of foam strike risk drastically underestimated**
    - **Model inadequacy in model for consequence of foam strike**
- Mars Polar Lander (MPL) [4]
  - Mishap: Loss of mission likely due to premature thruster cutoff due to errant touchdown signal
  - Incorrect touchdown logic missed in software and system testing due to requirements flowdown error and re-test configuration oversight
  - **Risk Management Failure: Unidentified risk due to gap in requirements flowdown and testing configuration**
    - **Design uncertainty in test sequence. Did not account for the changes made to the test sequence**
- Mars Exploration Rovers (MER) [5]
  - Mishap: Near loss of Spirit rover from battery depletion due to FLASH memory bug
  - Internal file system did not delete files correctly, eventually ran out of memory space to create new files in
  - Memory allocation service hung, causing the rover to continuously reset
  - Continuous resets gradually drained battery but were able to be stopped before loss of mission
  - **Risk Management Failure: Unknown software interactions and gap in ground verifications**
    - **Model inadequacy in model of the consequence of the internal file system bug**

[3] Report of the Columbia Accident Investigation Board Volume I. Technical report, 2003.
[4] A. Albee, S. Battel, R. Brace, G. Burdick, J. Casani, J. Lavell, C. Leising, D. MacPherson, P. Burr, and D. Dipprey. Report on the loss of the Mars Polar Lander and Deep Space 2 missions. 2000.
[5] Glenn Reeves and Tracy Neilson. The Mars Rover Spirit Flash Anomaly. In Aerospace Conference, 2005 IEEE, pages 4186–4199. IEEE, 2005.

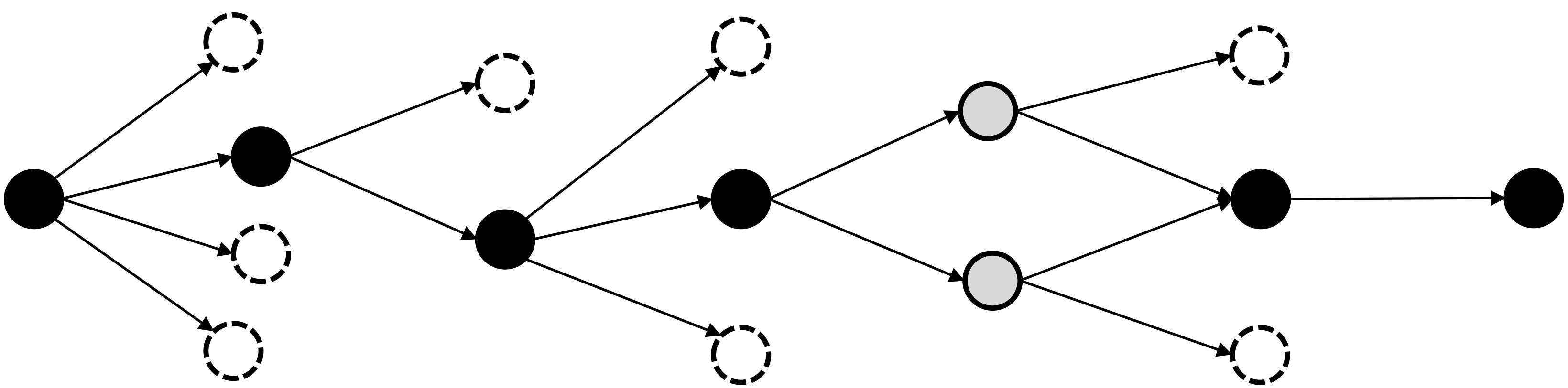
Problem Statement

Can risk management be improved to avoid the common occurrence of cost and schedule overruns or technical failures?

Hypothesis: By leveraging model-based systems engineering and algorithms from incremental planning, the risk management process can better identify the ramifications of new information as it is gained during the design process and can rigorously update risk estimates.

Decision-based Design Process

- Design as a series of decisions/trade studies that iteratively refine an initial design [14][21]
- Each decision is made under a state of knowledge (context)
- New information is learned during the design process as a result of testing, analysis, design decisions, etc.
- The new information may mean that previous decisions are no longer optimal/violate constraints

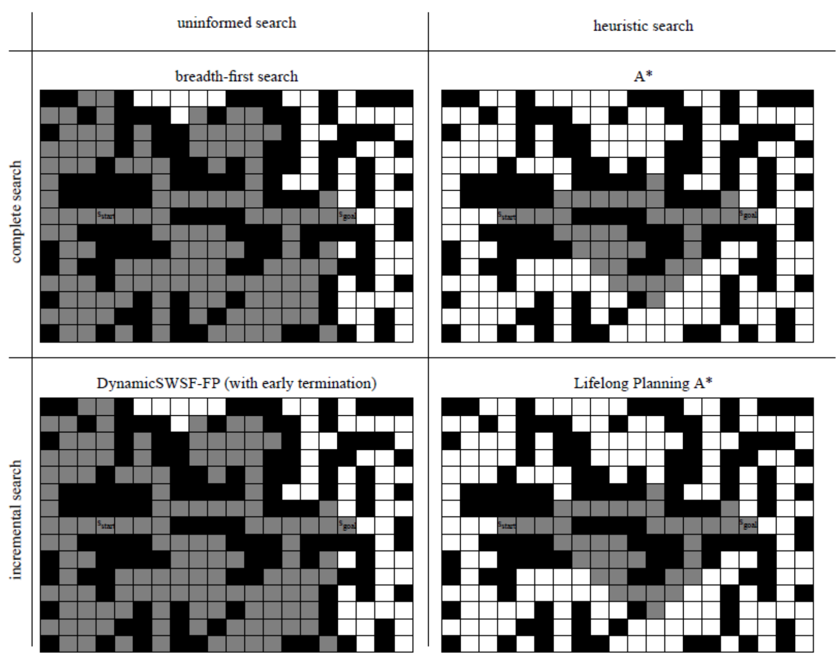


[14] Hazelrigg, G. A. A framework for decision-based engineering design. Transactions-American Society of Mechanical Engineers Journal of Mechanical Design, 120, 653-658., 1998.
[21] Steven R Hirshorn, Linda D Voss, and Linda K Bromley. NASA Systems Engineering Handbook. 2017.

Epistemic Uncertainty in Incremental Planning

- Similar to design process in that no truth data available
  - Plan based on best information available at the time
- Addresses epistemic uncertainty through efficient updates to incorporate new information
  - Leverage previous search results to speed up the search for a new solution
- Lifelong Planning A* algorithm (LPA*) [16]

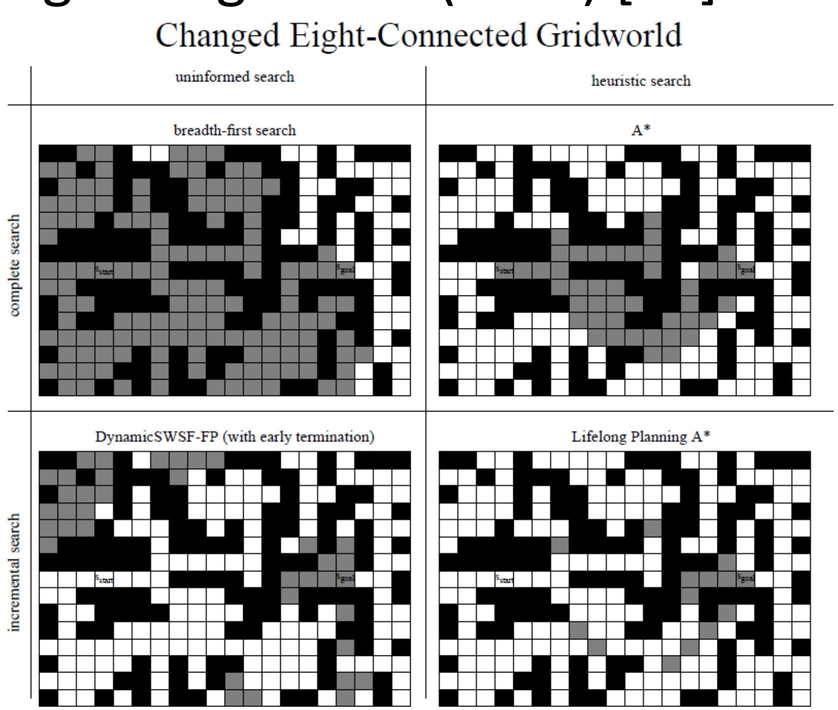
Original Eight-Connected Gridworld



[16] Koenig, S., Likhachev, M., & Furcy, D. (2004). Lifelong planning A∗. Artificial Intelligence, 155(1-2), 93-146.

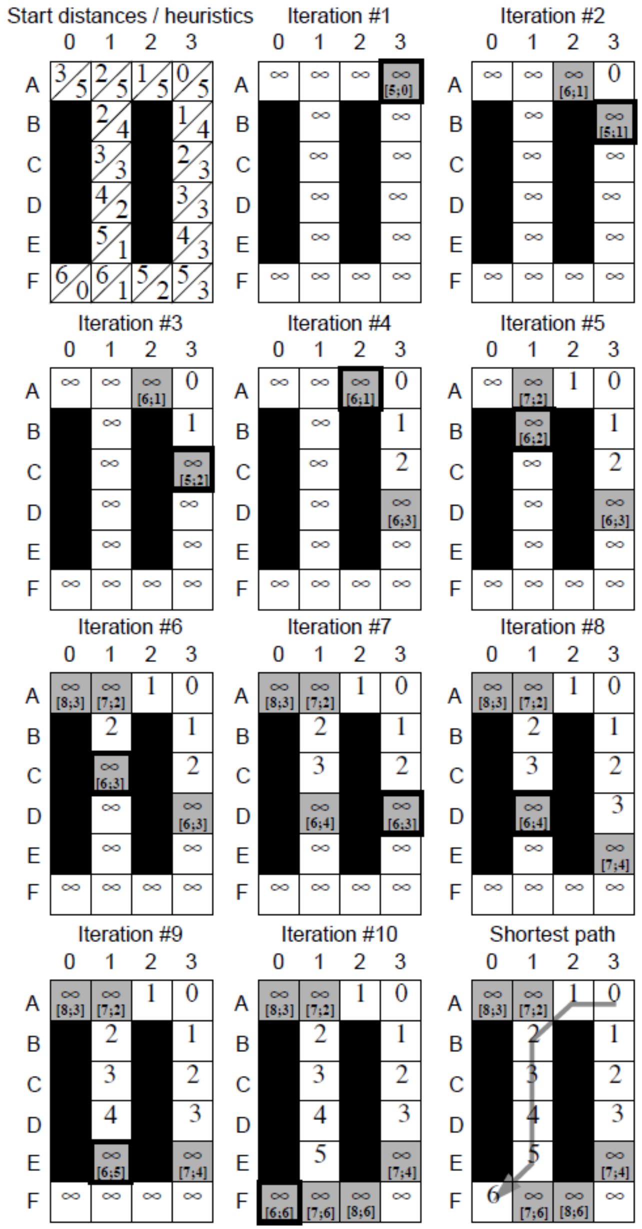
Model Inadequacy in Incremental Planning

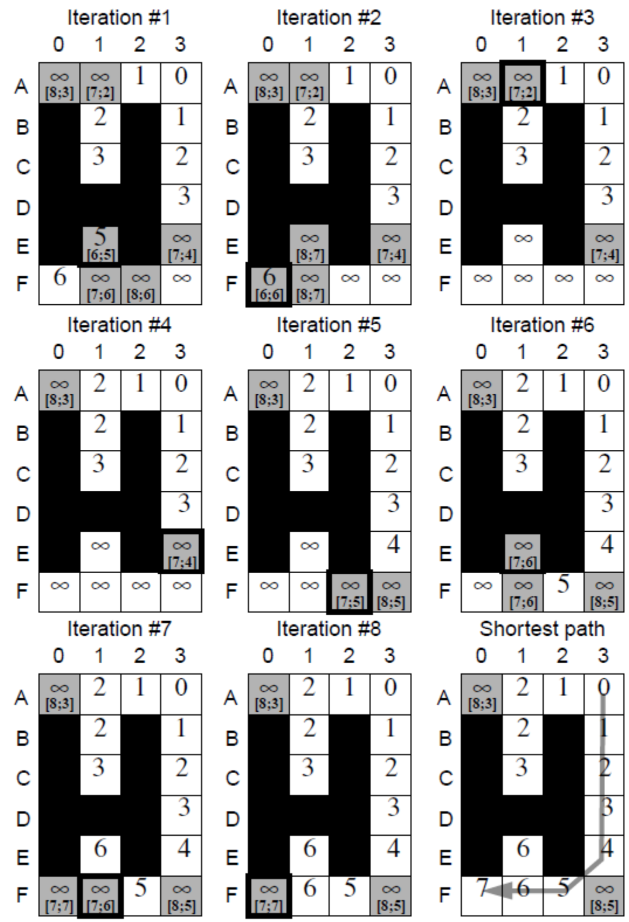
- Similar to design process in that no truth data available
  - Plan based on best information available at the time
- Addresses epistemic uncertainty through efficient updates to incorporate new information
  - Leverage previous search results to speed up the search for a new solution
- Lifelong Planning A* algorithm (LPA*) [16]



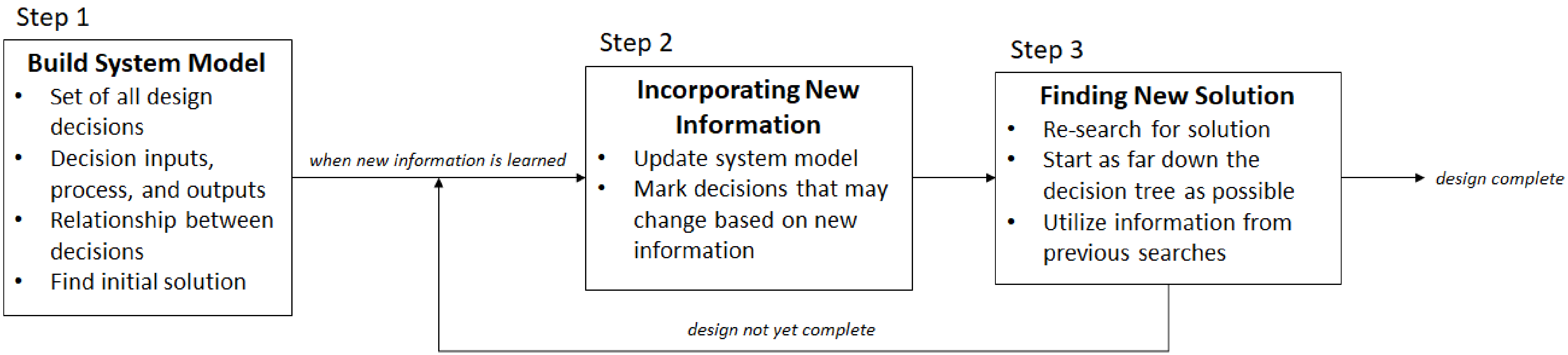
[16] Koenig, S., Likhachev, M., & Furcy, D. (2004). Lifelong planning A∗. Artificial Intelligence, 155(1-2), 93-146.

Lifelong Planning A* Algorithm





Methodology Overview



1. Build a system model that records all design decisions, the design decision making process, and design products (chosen point design, risks, etc.)
2. When new information is learned, identify which portions of the system may have to change
3. Efficiently find new design solution reusing knowledge where possible and update risk analyses

Methodology may be performed manually or automatically

Methodology – Build System Model

Step 1 → Step 2 → Step 3

- System model must include:
  - Design Decisions
    - Inputs
    - Options
    - Methodology
  - Decision Tree Structure
  - Chosen Point Design
  - Risks

Detector Heat Rejection Method

Inputs:
- Detector heat dissipation
- Detector temperature
- Detector location
- Presence of thermoelectric cooler
- S/C interface temperature

Options:
- Reject to deep space
- Reject to S/C

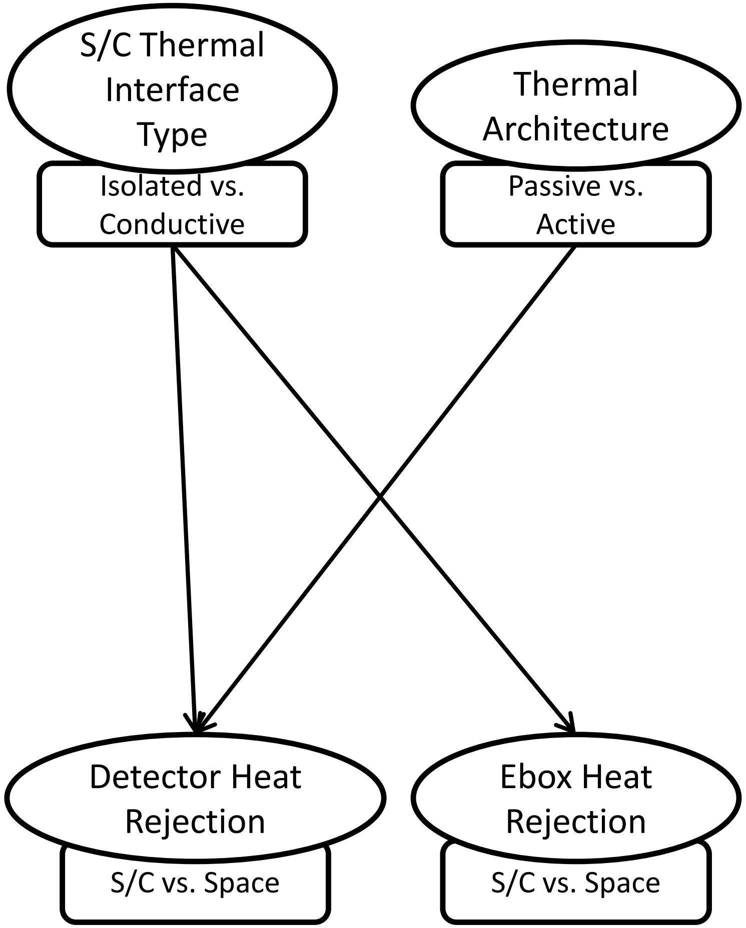
Methodology:
- Reject to S/C if possible, if not, reject to deep space

Output: System Model

Methodology – Build System Model

Step 1 → Step 2 → Step 3

- System model must include:
  - Design Decisions
    - Inputs
    - Options
    - Methodology
  - Decision Tree Structure
  - Chosen Point Design
  - Risks

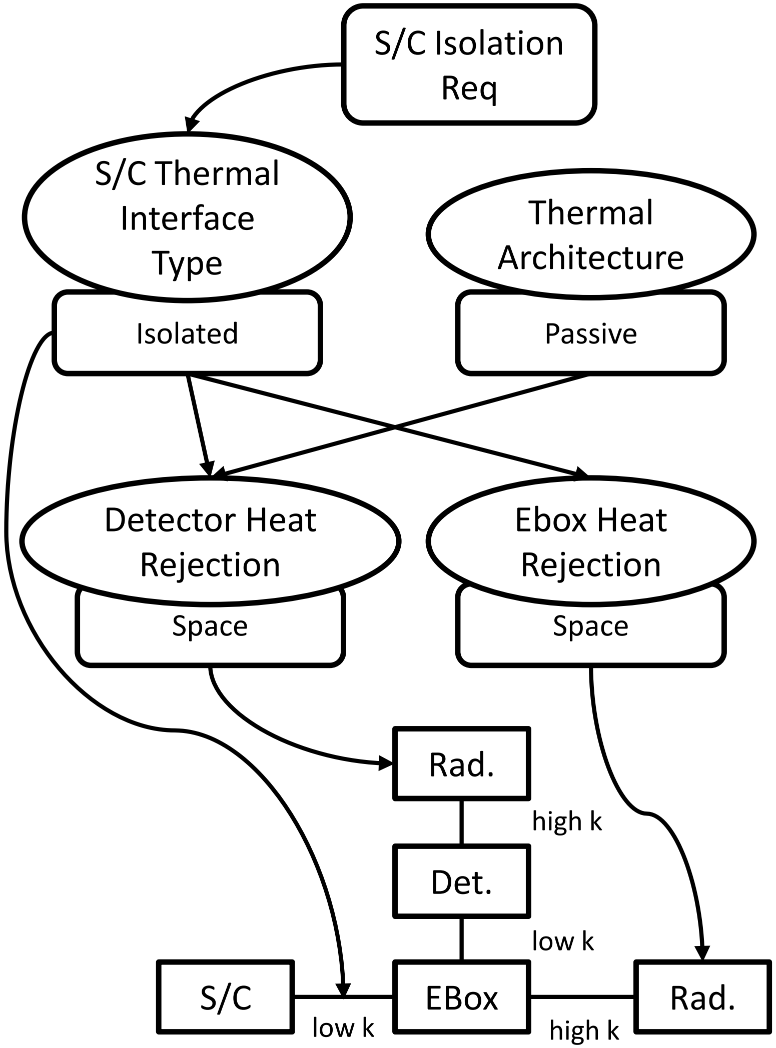


<u>Output</u>: System Model

Methodology – Build System Model

Step 1 → Step 2 → Step 3

- System model must include:
  - Design Decisions
    - Inputs
    - Options
    - Methodology
  - Decision Tree Structure
  - Chosen Point Design
  - Risks

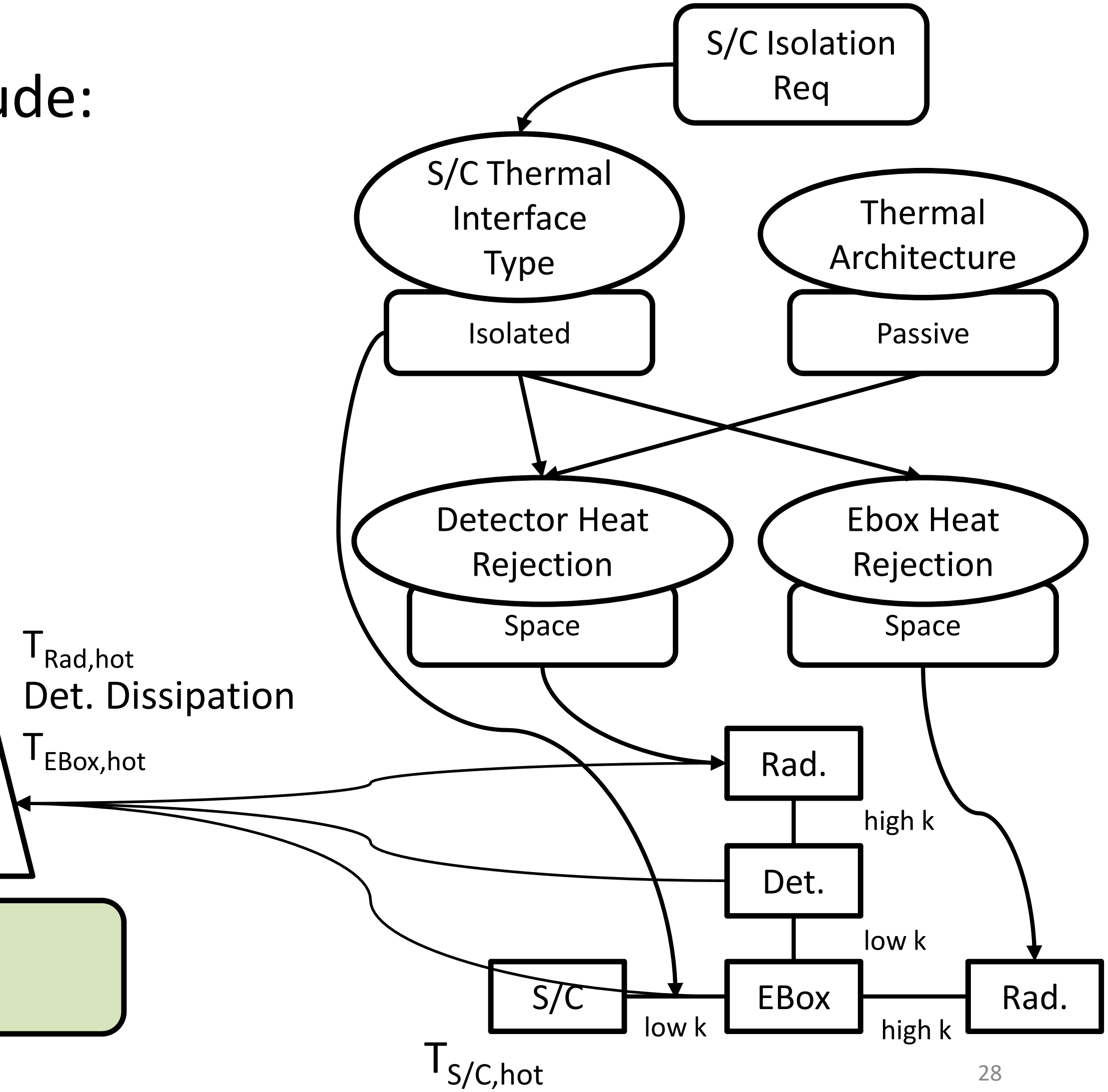


Output: System Model

Methodology – Build System Model

Step 1 → Step 2 → Step 3

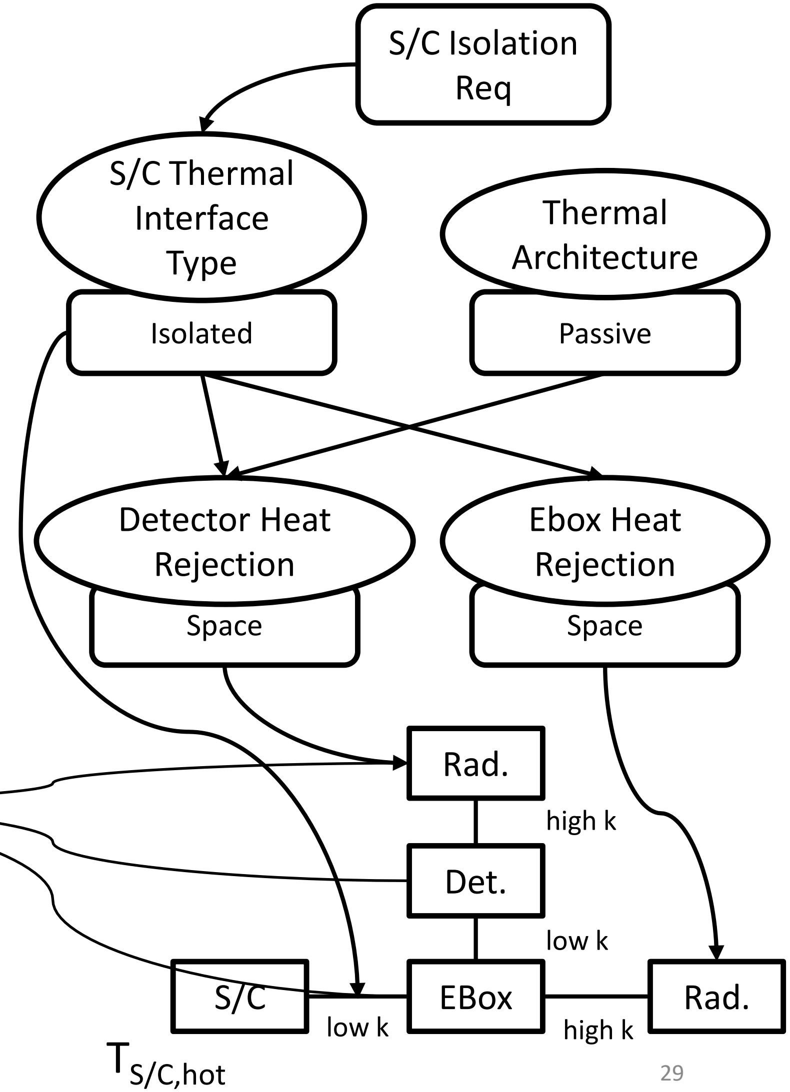
- System model must include:
  - Design Decisions
    - Inputs
    - Options
    - Methodology
  - Decision Tree Structure
  - Chosen Point Design
  - Risks

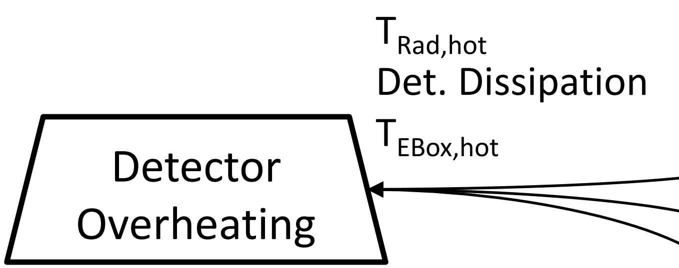


<u>Output</u>: System Model

Methodology – Incorporate new Information

- When new information is learned:
  - Identify which decisions are affected
    - Is the changed variable in any decision justifications?
  - All decisions downstream from changed decisions could change as well



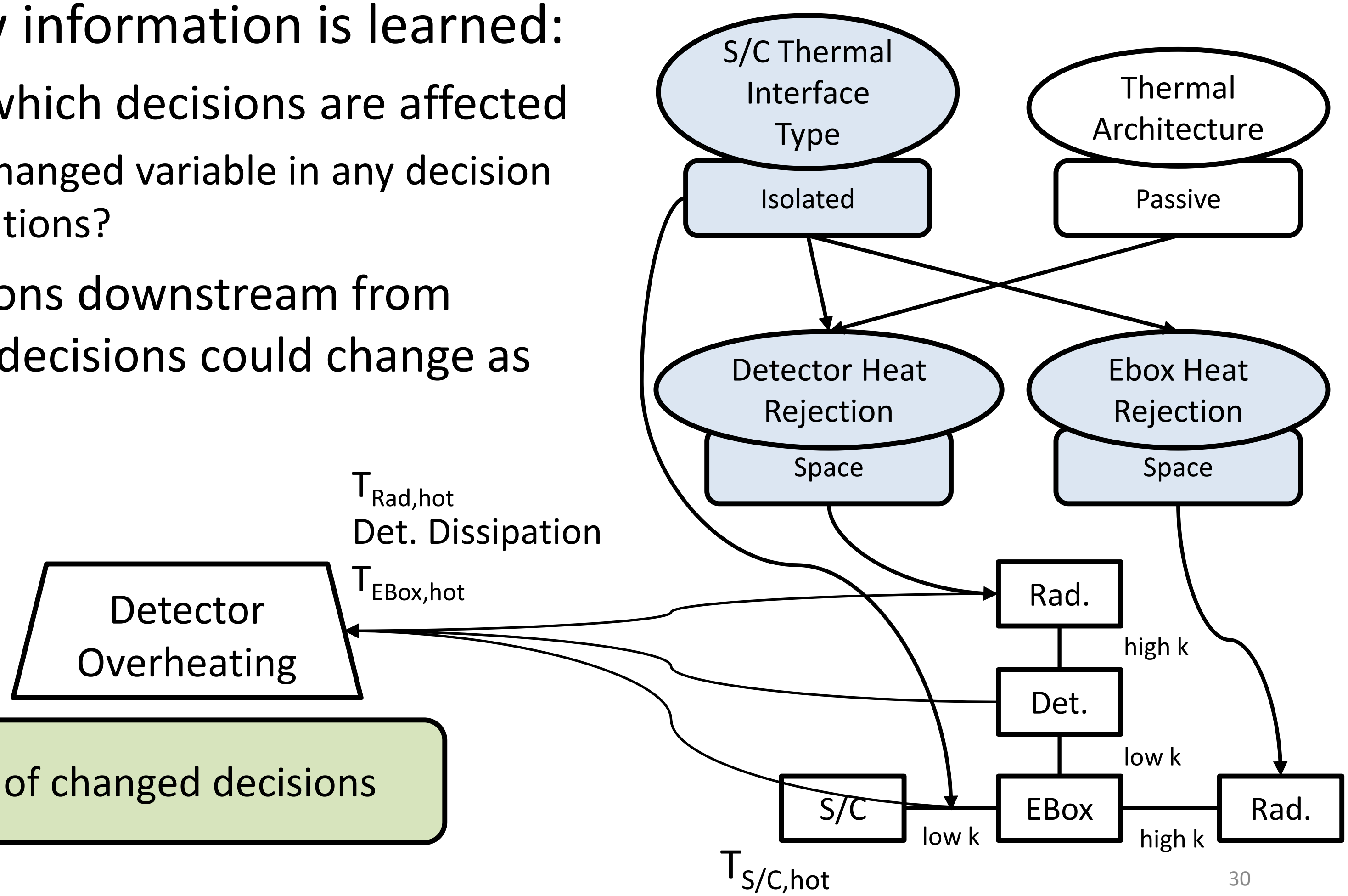


Output: List of changed decisions

Methodology – Incorporate new Information

Step 1 → **Step 2** → Step 3

- When new information is learned:
  - Identify which decisions are affected
    - Is the changed variable in any decision justifications?
  - All decisions downstream from changed decisions could change as well

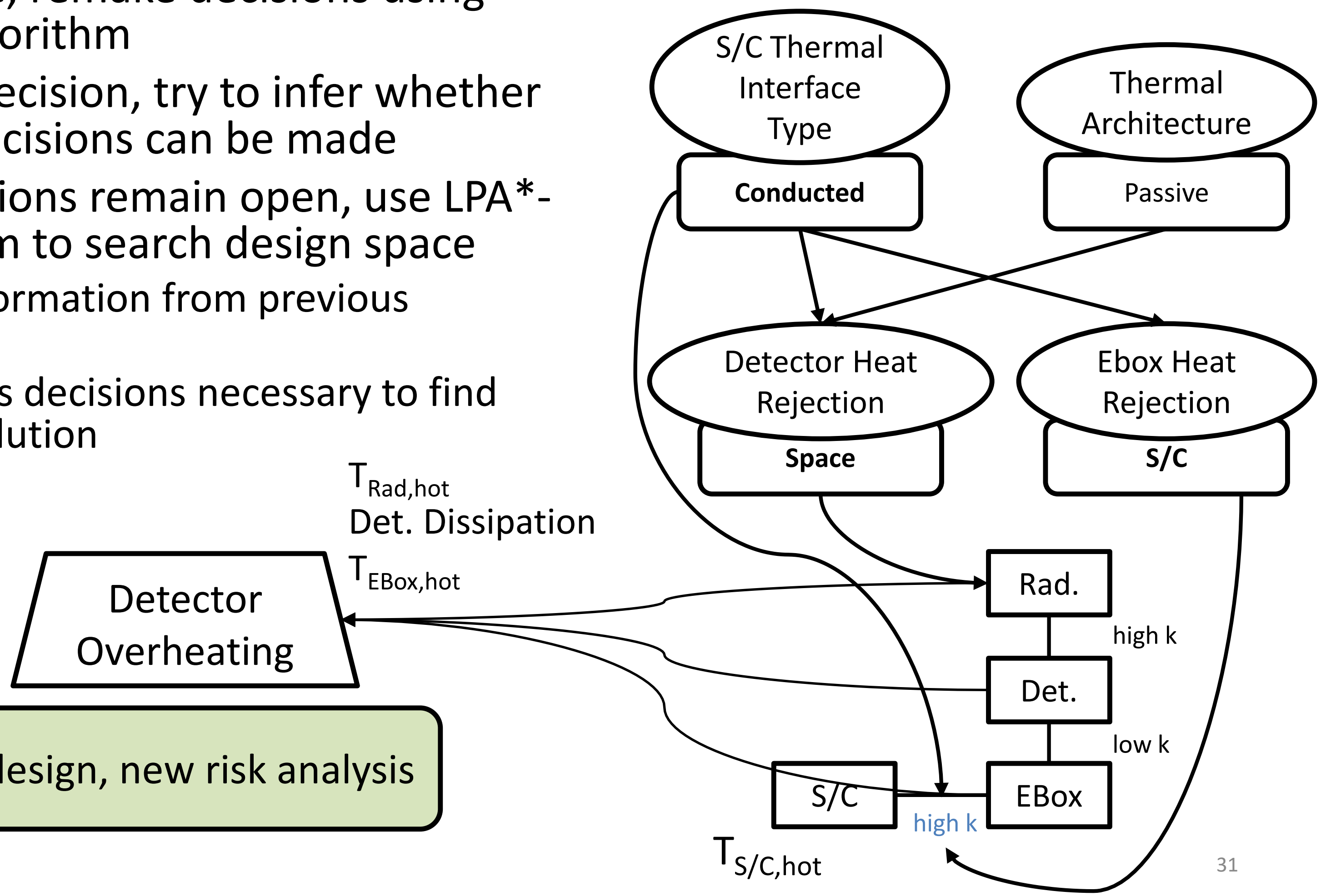


Output: List of changed decisions

Methodology – Find New Solution

Step 1 → Step 2 → **Step 3**

- Starting with decisions near root of decision tree, remake decisions using recorded algorithm
- After each decision, try to infer whether any other decisions can be made
- Where decisions remain open, use LPA*-like algorithm to search design space
  - Reuses information from previous searches
  - Only makes decisions necessary to find optimal solution

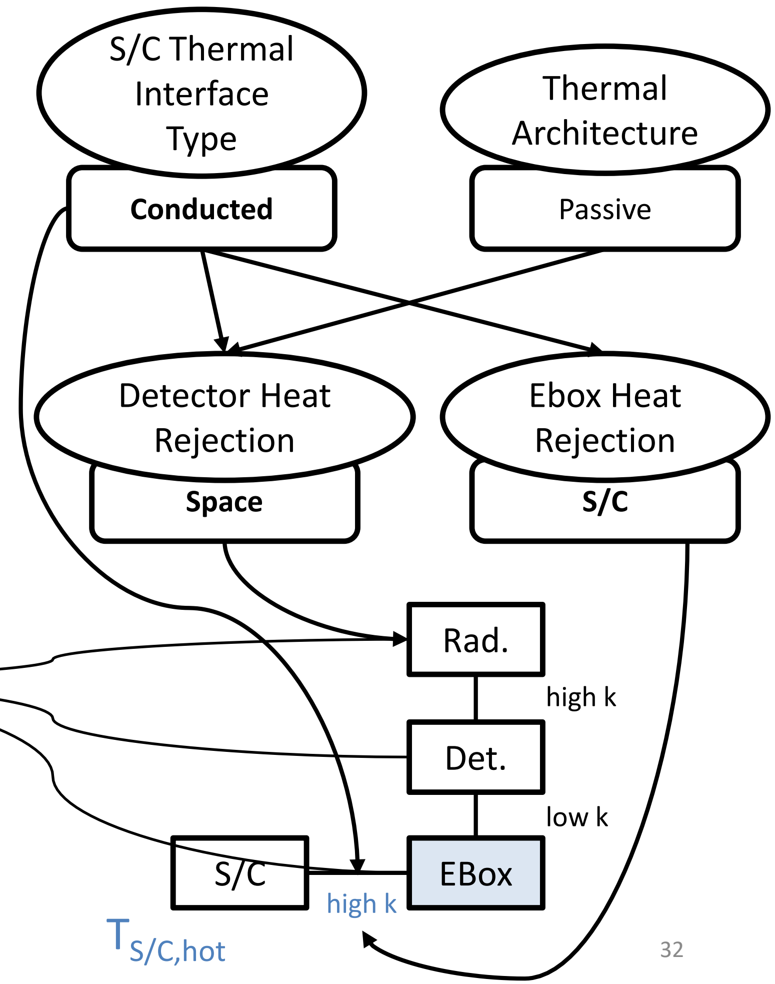


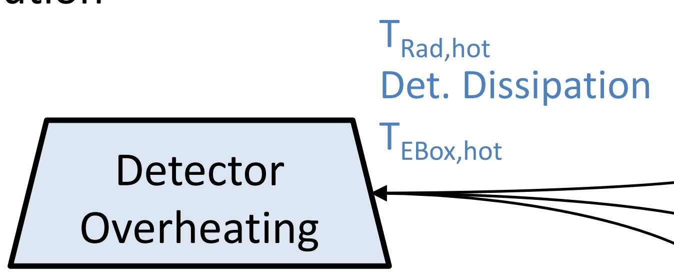
Output: New design, new risk analysis

Methodology – Find New Solution

Step 1 → Step 2 → **Step 3**

- Starting with decisions near root of decision tree, remake decisions using recorded algorithm
- After each decision, try to infer whether any other decisions can be made
- Where decisions remain open, use LPA*-like algorithm to search design space
  - Reuses information from previous searches
  - Only makes decisions necessary to find optimal solution





Output: New design, new risk analysis

Case Studies

- Regolith X-ray Imaging Spectrometer (REXIS)
  - X-ray instrument on NASA OSIRIS-REx mission
  - Can compare results with historical risk management methodology
  - Performance Metric: Number of risks found with my approach that were not found historically
- NASA GSFC Mission Design Lab (MDL) Study
  - Provides example of early lifecycle design challenges
  - Can do independent comparison with current NASA risk management methodology
  - Will hypothesize alternative design solutions to mitigate possible future risks
  - Performance Metric: Number of risks found with my approach post-study that were not identified during the study

Thank you!

Questions?

References

[1] NASA Risk Management Handbook. NASA-SP-2011-3422. Version 1, Nov 2011.

[2] D.L. Emmons, M. Lobbia, T. Radcliffe, and R.E. Bitten. Affordability Assessments to Support Strategic Planning and Decisions at NASA. In Aerospace Conference, 2010 IEEE, 2010.

[3] Report of the Columbia Accident Investigation Board Volume I. Technical report, 2003.

[4] A. Albee, S. Battel, R. Brace, G. Burdick, J. Casani, J. Lavell, C. Leising, D. MacPherson, P. Burr, and D. Dipprey. Report on the loss of the Mars Polar Lander and Deep Space 2 missions. 2000.

[5] Glenn Reeves and Tracy Neilson. The Mars Rover Spirit Flash Anomaly. In Aerospace Conference, 2005 IEEE, pages 4186–4199. IEEE, 2005.

[6] Jean-Francois Castet, Magdy Bareh, Jeffery Nunes, Steven Jenkins, and Gene Lee. Fault management ontology and modeling patterns. In AIAA SPACE 2016, page 5544. 2016.

[7] Brynjarsdóttir, J., & O'Hagan, A. (2014). Learning about physical parameters: The importance of model discrepancy. Inverse Problems, 30(11), 114007.

[8] Cressent, R., David, P., Idasiak, V., & Kratz, F. (2013). Designing the database for a reliability aware Model-Based System Engineering process. Reliability Engineering & System Safety, 111, 171-182.

[9] Evans, J., Cornford, S., & Feather, M. S. (2016, January). Model based mission assurance: NASA's assurance future. In Reliability and Maintainability Symposium (RAMS), 2016 Annual (pp. 1-7). IEEE.

[10] Hecht, M., Dimpfl, E., & Pinchak, J. (2014, November). Automated Generation of Failure Modes and Effects Analysis from SysML Models. In Software Reliability Engineering Workshops (ISSREW), 2014 IEEE International Symposium on (pp. 62-65). IEEE.

[11] Faida Mhenni, Nga Nguyen, and Jean-Yves Choley. Automatic fault tree generation from sysml system models. In Advanced Intelligent Mechatronics (AIM), 2014 IEEE/ASME International Conference on, pages 715–720. IEEE, 2014.

[12] Michel Izygon, Howard Wagner, Shira Okon, Lui Wang, Miriam Sargusingh, and John Evans. Facilitating r&m in spaceflight systems with mbse. In Reliability and Maintainability Symposium (RAMS), 2016 Annual, pages 1–6. IEEE, 2016.

[13] Sam Schreiner, Matthew L Rozek, Andy Kurum, Chester J Everline, Michel D Ingham, and Jeffery Nunes. Towards a methodology and tooling for Model-Based Probabilistic Risk Assessment (PRA). In AIAA SPACE 2016, page 5545. 2016.

[14] Hazelrigg, G. A. A framework for decision-based engineering design. Transactions-American Society of Mechanical Engineers Journal of Mechanical Design, 120, 653-658., 1998.

[15] S. Friedenthal, R. Griego, and M. Sampson. INCOSE Model Based Systems Engineering (MBSE) Initiative. In INCOSE 2007 Symposium, 2007.

[16] Koenig, S., Likhachev, M., & Furcy, D. (2004). Lifelong planning A∗. Artificial Intelligence, 155(1-2), 93-146.

[17] Armen Der Kiureghian and Ove Ditlevsen. Aleatory or epistemic? does it matter? Structural Safety, 31(2):105–112, 2009.

[18] Scott Uebelhart, David Miller, and Carl Blaurock. Uncertainty characterization in integrated modeling. In 46th AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference, page 2142, 2005.

[19] Daniel Pierre Thunnissen. Propagating and mitigating uncertainty in the design of complex multidisciplinary systems. PhD thesis, California Institute of Technology, 2005.

[20] Robert E Levin and GAO Director. Space acquisitions: Stronger development practices and investment planning needed to address continuing problems. Statement to the House Armed Services Committee, Subcommittee on Strategic Forces, 2005.

[21] Steven R Hirshorn, Linda D Voss, and Linda K Bromley. NASA Systems Engineering Handbook. 2017.

Backup

Background – Uncertainty Definitions

- Aleatory vs. Epistemic [17]
  - Aleatory Uncertainty: Randomness intrinsic to a phenomenon
  - Epistemic Uncertainty: Uncertainty from a lack of knowledge about a phenomenon
- Parametric vs. Nonparametric [18]
  - Parametric Uncertainty: Uncertainty associated with model parameters
  - Nonparametric Uncertainty: Uncertainty not dependent on the model parameters
- Design Uncertainty: Uncertainty in which design option will be chosen out of a set of design options [19]
- Model Inadequacy: The difference between a model output and the true behavior of the system [7]

[7] Brynjarsdóttir, J., & O'Hagan, A. (2014). Learning about physical parameters: The importance of model discrepancy. Inverse Problems, 30(11), 114007.
[17] Armen Der Kiureghian and Ove Ditlevsen. Aleatory or epistemic? does it matter? Structural Safety, 31(2):105–112, 2009.
[18] Scott Uebelhart, David Miller, and Carl Blaurock. Uncertainty characterization in integrated modeling. In 46th AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference, page 2142, 2005.
[19] Daniel Pierre Thunnissen. Propagating and mitigating uncertainty in the design of complex multidisciplinary systems. PhD thesis, California Institute of Technology, 2005.