Goal-Function Tree Modeling for Systems Engineering and Fault Management

Dr. Stephen B. Johnson
Jacobs ESSSA Group, Dependable System Technologies, LLC, and NASA Marshall Space Flight Center

Jonathan T. Breckenridge
Jacobs – ESSSA Group\ Ducommun Incorporated, Miltec Systems

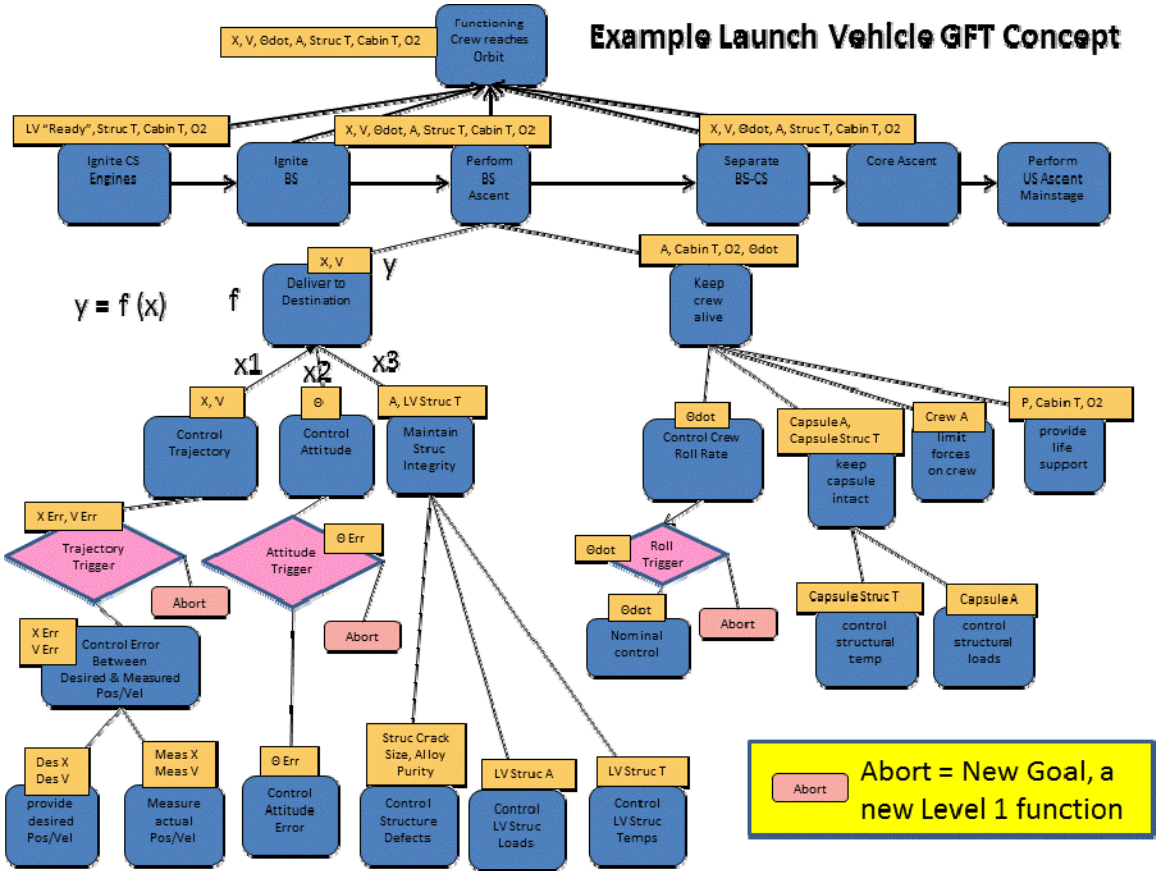
The draft NASA Fault Management (FM) Handbook (2012) states that Fault Management (FM) is a "part of systems engineering", and that it "demands a system-level perspective" (NASA-HDBK-1002, 7). What, exactly, is the relationship between systems engineering and FM? To NASA, systems engineering (SE) is "the art and science of developing an operable system capable of meeting requirements within often opposed constraints" (NASA/SP-2007-6105, 3). Systems engineering starts with the elucidation and development of requirements, which set the goals that the system is to achieve. To achieve these goals, the systems engineer typically defines functions, and the functions in turn are the basis for design trades to determine the best means to perform the functions. System Health Management (SHM), by contrast, defines "the capabilities of a system that preserve the system's ability to function as intended" (Johnson et al., 2011, 3). Fault Management, in turn, is the operational subset of SHM, which detects current or future failures, and takes operational measures to prevent or respond to these failures. Failure, in turn, is the "unacceptable performance of intended function." (Johnson 2011, 605) Thus the relationship of SE to FM is that SE defines the functions and the design to perform those functions to meet system goals and requirements, while FM detects the inability to perform those functions and takes action. SHM and FM are in essence "the dark side" of SE. For every function to be performed (SE), there is the possibility that it is not successfully performed (SHM); FM defines the means to operationally detect and respond to this lack of success. We can also describe this in terms of goals: for every goal to be achieved, there is the possibility that it is not achieved; FM defines the means to operationally detect and respond to this inability to achieve the goal.

This brief description of relationships between SE, SHM, and FM provide hints to a modeling approach to provide formal connectivity between the nominal (SE), and off-nominal (SHM and FM) aspects of functions and designs. This paper describes a formal modeling approach to the initial phases of the development process that integrates the nominal and off-nominal perspectives in a model that unites SE goals and functions of with the failure to achieve goals and functions (SHM/FM). This methodology and corresponding model, known as a Goal-Function Tree (GFT), provides a means to represent, decompose, and elaborate system goals and functions in a rigorous manner that connects directly to design through use of state variables that translate natural language requirements and goals into logical-physical state language. The state variable-based approach also provides the means to directly connect FM to the design, by specifying the range in which state variables must be controlled to achieve goals, and conversely, the failures that exist if system behavior go out-of-range. This in turn allows for the systems engineers and SHM/FM engineers to determine which state variables to monitor, and what action(s) to take should the system fail to achieve that goal. In sum, the GFT representation provides a unified approach to early-phase SE and FM development.

This representation and methodology has been successfully developed and implemented using Systems Modeling Language (SysML) on the NASA Space Launch System (SLS) Program. It enabled early design trade studies of failure detection coverage to ensure complete detection coverage of all crew-threatening failures. The representation maps directly both to FM algorithm designs, and to failure scenario definitions needed for design analysis and testing. The GFT

representation provided the basis for mapping of abort triggers into scenarios, both needed for initial, and successful quantitative analyses of abort effectiveness (detection and response to crew-threatening events).

A corresponding paper by Jonathan Breckenridge and Stephen B. Johnson titled “Implementation of a Goal-Based Systems Engineering and Fault Management Process Using the Systems Modeling Language (SysML)” describes the SysML modeling approach used to represent the SLS GFT. Ideally, this paper should be accepted and presented in the same session as this paper, if it is accepted. Figure 1 shows a non-SysML representation of a GFT for an SLS-like launch vehicle.



Statement of problem: Current SE and SHM/FM methods poorly integrate nominal and off-nominal perspectives, particularly in the feasibility and preliminary development phases. Nor do they provide sufficient physical/logical rigor to connect goals and functions to design, or to enable early, direct analysis and trade studies of needed FM functions and designs.

Proposed method of solution: Development and implementation of the GFT methodology and representation. This integrates goals, functions, and state variables to significantly improve nominal SE functional decomposition, and to enable off-nominal FM design trades and analyses.

Results expected and obtained: The GFT Model was successfully developed on the SLS Program in its Mission and Fault Management organization. This model successfully represented, and enabled integrated analysis of both nominal and off-nominal system goals and functions, tied

directly through state variables to designs. The methodology enabled direct analysis of FM detection coverage of various combinations of abort triggers, mapping of abort conditions and triggers to failure scenarios, and enabled early assessments of expected response effectiveness.

Significance of the contribution: This moves both SE and SHM/FM from ad hoc, natural-language based representation of goals and functions to a rigorous logical-physical representation right at the start of system development. This enables early FM design trade studies from the top down during feasibility studies and preliminary design phase, instead of design band-aids applied after completion of the nominal design. The FM design trades and requirements are thereby directly linked to the systems engineering design trades and requirements.

References

Breckenridge, 2013	Breckenridge, Jonathan, and Stephen B. Johnson, "Implementation of a Goal-Based Systems Engineering Process Using the Systems Modeling Language (SysML)", abstract submitted to AIAA Infotech@Aerospace 2013.
Johnson et al., 2011a	Johnson, Stephen B., Thomas J. Gormley, Seth S. Kessler, Charles D. Mott, Ann Patterson-Hine, Karl M. Reichard, Philip A. Scandura, Jr., *System Health Management: with Aerospace Applications*. Chichester, UK: John Wiley & Sons, 2011.
Johnson et al., 2011b	Johnson, Stephen B., and John C. Day, "System Health Management Theory and Design Strategies," for AIAA Infotech@Aerospace Conference 2011, 29-31 March 2011, St. Louis, Missouri. AIAA paper 977233.
NASA-HDBK-1002	NASA Fault Management Handbook, Draft 2, April 2012.
NASA/SP-2007-6105	NASA Systems Engineering Handbook, Revision 1, December 2007.