A Proposed Software Reliability Modeling Initiative

Robert W. Stoddard

Principal Researcher, SEI, CMU

ASQ Fellow

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM20-0022

Agenda

BLUF

Software Reliability Modeling Concepts

Traditional Reliability Modeling Approach

Recommended Reliability Modeling Approach

Software Reliability Initiative Recommendations

Questions

BLUF

1. We are concerned with reliability of a heavily software intensive system and SofS
2. Software is not perfect and must be allocated some of the system failure rate
3. To reasonably model software reliability, software behavior must be modeled in terms of states including failure states
4. Practical methods (Markov and Petri Net) and tooling (SHARPE and Mobius) are now available along with published books, papers, training and modeling coaches
5. The system can be decomposed into hardware, software and hybrid software/hardware components, each of which may be modeled differently based on the behavioral model and nature of available failure data
6. This reliability modeling approach is congruent with the planned STPA modeling for safety and security and can serve multiple purposes
7. This reliability modeling approach will more accurately drive the needed improvements to the software

Agenda

BLUF

Software Reliability Modeling Concepts

Traditional Reliability Modeling Approach

Recommended Reliability Modeling Approach

Software Reliability Initiative Recommendations

Questions

Software Reliability Concepts - 01

1. Just as software testing may be viewed as Black Box, Grey Box and White Box, software reliability modeling may be similarly viewed
2. Black Box approach:
   a) Software treated as a black box with only high level information available to model reliability
   b) One may take software system test results and estimate reliability
   c) Many assumptions must be made with such an approach such as usage profile, variation in inputs, environment and traversing infinite paths in the software which threatens credibility of the reliability estimate
   d) Makes it next to impossible to show reliability growth because of the physical limits of test time in calculating the reliability estimate
   e) Offers little guidance in how to improve the estimate of the software reliability
   f) Offers the least evidence to support NSCCA activities and assurance

Software Reliability Concepts - 02

3. Grey Box Approach:
   a) Could be an approach of measuring software failure at a CSCI level
   b) May be unknowledgeable of usage profile of the software
   c) Still makes many assumptions about how to combine failure and reliability information at the system level
   d) Offers only limited improvement in the other deficiencies of Black Box approach
4. White Box Approach:
   a) Takes advantage of all knowledge of software architecture, design and even code
   b) Attempts to characterize and model the actual behavior of the software
   c) Reasonably overcomes all of the limitations listed for Black and Grey Box approaches
   d) Involves more evidence to defend reliability estimates to external stakeholders including independent NSCCA teams

Agenda

BLUF

Software Reliability Modeling Concepts

Traditional Reliability Modeling Approach

Recommended Reliability Modeling Approach

Software Reliability Initiative Recommendations

Questions

Traditional Reliability Approach by Hardware Engineers

1. Generally assume software will be error-free and thus, entire allocated failure rate is reserved for hardware
2. Traditionally, hardware reliability engineers employ the weakest form of reliability modeling called “Reliability Block Diagrams (RBD)”
3. Using RBD models, an exponential failure distribution with constant failure rate is assumed to make calculations easier
4. The hardware may decomposed to any desirable level of components
5. The RBD contains some mix of series model fragments and parallel model fragments
6. Reliability of a series is simply the multiplication of the reliability of the components in the series
7. Reliability of a parallel model is 1 – [(1-R1)*(1-R2)*…(1-Rn)] of n components
8. All systems may be modeled as some nested combination of series and parallel models

BAE Reliability Approach for Hardware Reliability

1. Will model the system hardware as a hierarchal set of RBD models based on a decomposition of the hardware components
2. Will answer system reliability estimates as a single Probability of Failure or Reliability Probability
3. Many low level hardware components will be modeled with time to failure models based on historical and/or current testing results
4. The time to failure model results will then be transformed into Probability of Failure or Reliability Probability
5. In this fashion, a complete RBD model may be evaluated with probabilities assigned to each box in the RBD model

Agenda

BLUF

Software Reliability Modeling Concepts

Traditional Reliability Modeling Approach

Recommended Reliability Modeling Approach

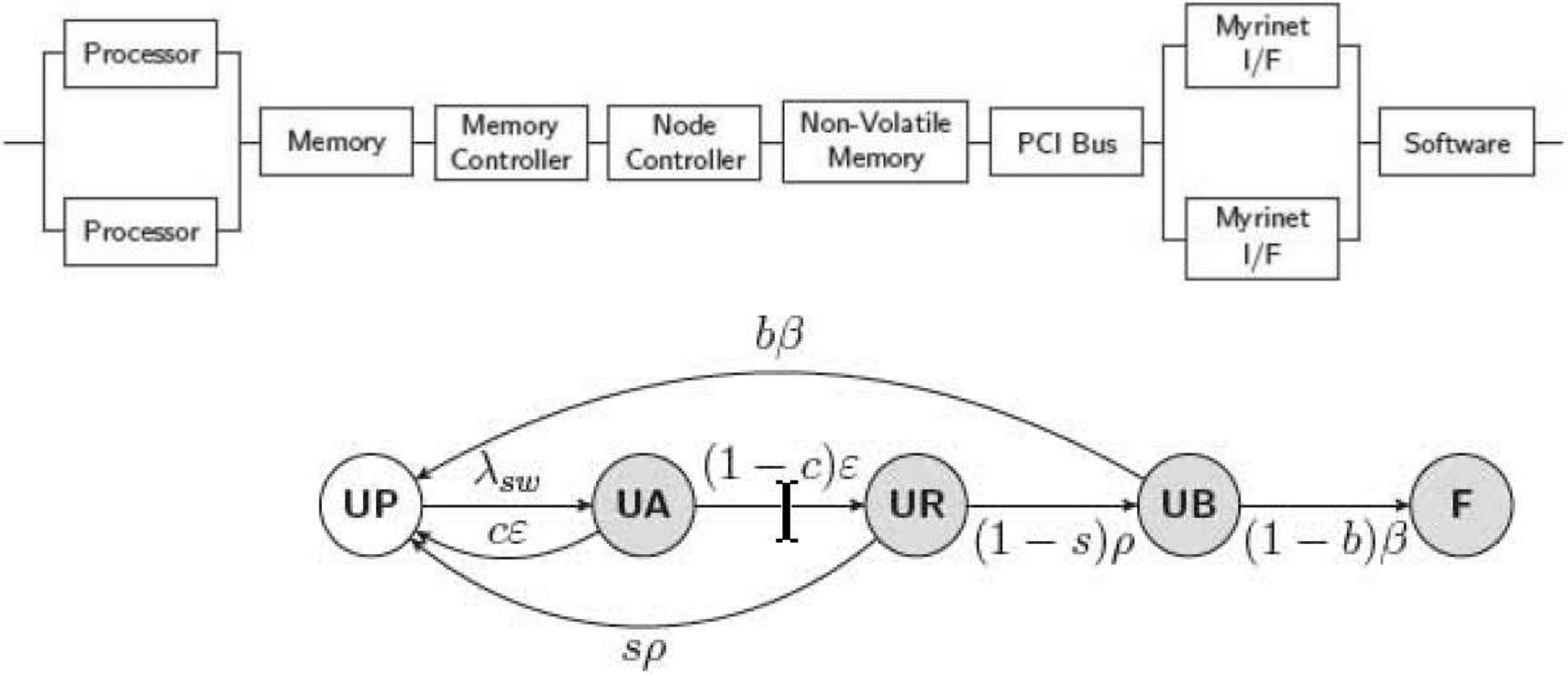
Software Reliability Initiative Recommendations

Questions

Recommended Reliability Approach - 01

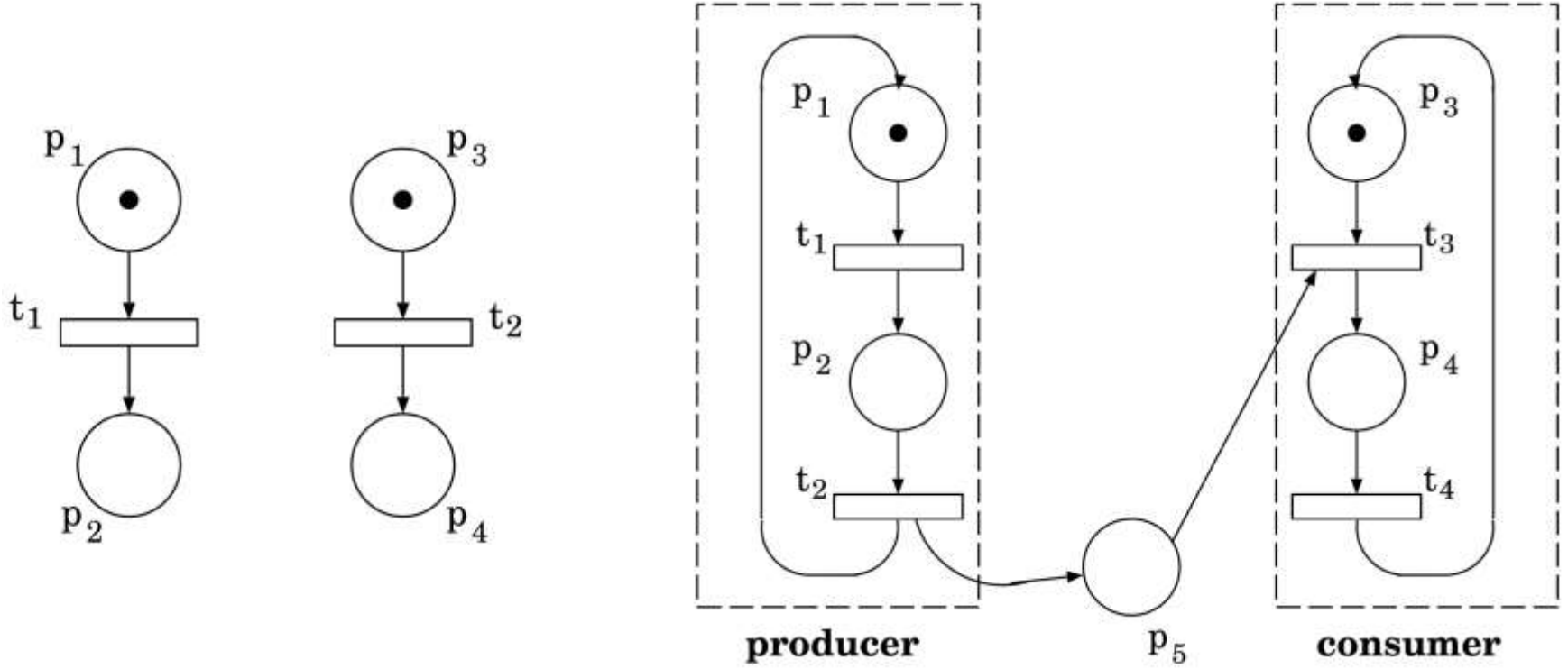
1. Accept that this program is a software intensive program in which software may not reasonably be assumed to be perfect, e.g. failure free
2. Pursue a “White Box” approach to modeling software reliability by modeling the behavior of the software
3. Modeling the behavior of software generally begins with Markov Modeling and, when faced with highly complex software in which the Markov Model explodes in complexity, pursue Petri Net Stochastic Activity Network models
4. Such modeling is mature, realistic and practical with tools such as SHARPE by Dr. Kishor Trivedi (Duke University) and Mobius by Dr. William Sanders (previously Univ of Illinois at Champaign Urbana and now Dean of Engineering at CMU)
5. See 2017 Guidebook https://www.amazon.com/Reliability-Availability-Engineering-Modeling-Applications-ebook/dp/B0744KXDTL/ref=sr_1_1?keywords=kishor+trivedi&qid=1578887065&s=books&sr=1-1

Example of Markov Reliability Models



From 2017 Guidebook https://www.amazon.com/Reliability-Availability-Engineering-Modeling-Applications-ebook/dp/B0744KXDTL/ref=sr_1_1?keywords=kishor+trivedi&qid=1578887065&s=books&sr=1-1

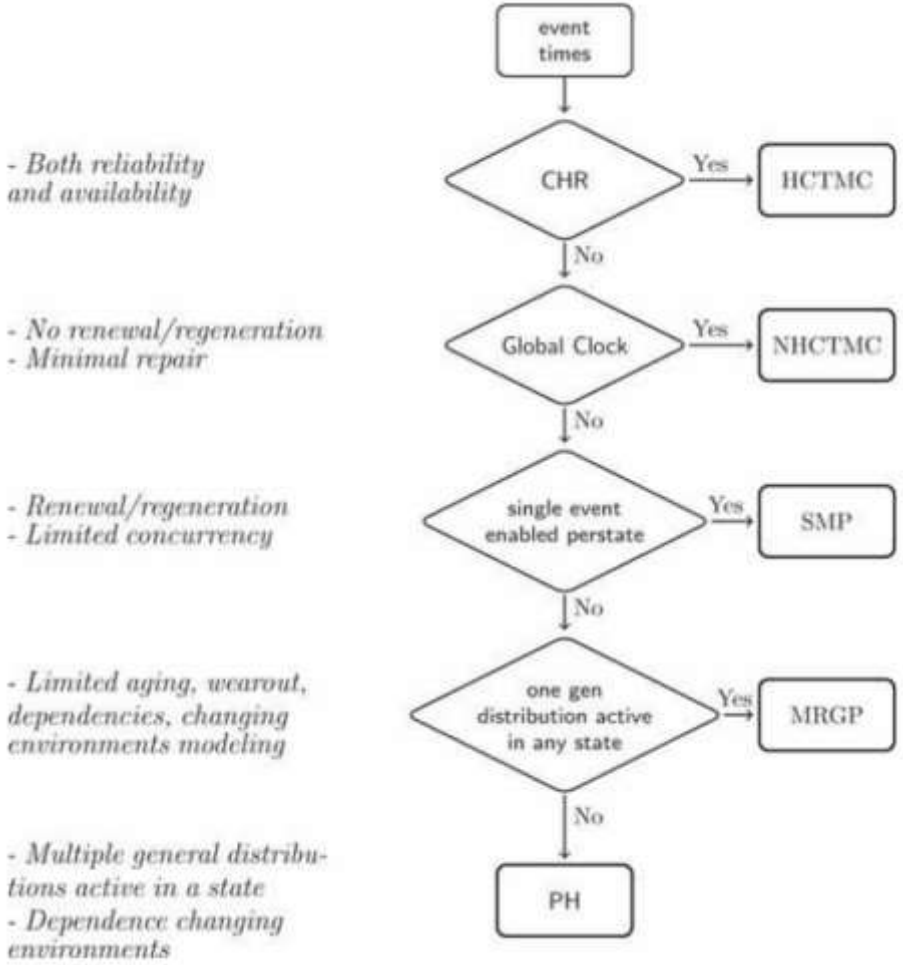
Example of Petri Net Reliability Models



Taken from System Modelling with Petri Nets,
https://www.cse.iitk.ac.in/users/cs698g/papers/miopetrinet.pdf

Guide to Model Type to Use

From 2017 Trivedi Guidebook
https://www.amazon.com/Reliability-Availability-Engineering-Modeling-Applications-ebook/dp/B0744KXDTL/ref=sr_1_1?keywords=kishor+trivedi&qid=1578887065&s=books&sr=1-1



Recommended Reliability Approach - 02

6. Begin with the system level RBD envisioned by the Hardware Reliability community
7. Identify a system decomposition of components as follows:
   a) Hardware components
   b) Software components
   c) Hybrid hardware and software components
8. Decide how to model each component:
   a) Probability of Failure based on test results
   b) Time to Failure based on test results
   c) Probability of Failure or Time to Failure based on Behavioral Models
9. Transform all Time to Failure results to a Probability of Failure
10. Evaluate the system level reliability estimate using the system RBD for a given system mission thread

Recommended Reliability Approach - 03

11. No single correct approach to modeling software intensive systems
12. Considerations influencing decision about what level and type of components should be in the reliability model:
    a) Nature of the planned failure data to be collected from testing and operation for both hardware and software,
    b) Nature of the system, hardware and software architecture to be modeled,
    c) Nature of expected failure distributions, e.g. exponential versus non-exponential),
    d) Nature of the desired hierarchy of the reliability models
13. CSCI's and CSC's may be treated differently based on the above considerations
14. The allocated system failure rate must be allocated downward to components and subcomponents whether they are hardware, software or hybrid
15. Consequently, a software reliability IPT must be formed to integrate with the existing system hardware reliability IPT

Agenda

BLUF

Software Reliability Modeling Concepts

Traditional Reliability Modeling Approach

Recommended Reliability Modeling Approach

Software Reliability Initiative Recommendations

Questions

Software Reliability Initiative Recommendations - 01

1. Organize and staff a software reliability IPT team to supplement existing Hardware/System reliability IPT
2. Identify a core team of full-time members and additional part time SMEs to help achieve coverage across all software
3. Work with the Hardware/System reliability IPT to define the pure hardware and software components as well as the hybrid hardware/software components
4. Revisit the reliability allocations for the complete program to adjust for allowing failure rate allocation to software components
5. Using Trivedi's guidance in 2017 text book, decide the modeling approach for each component
6. Reconfirm test failure data will be available for all components
7. Predict realism of reliability goal achievement and re-allocate reliability allocations as needed along with actions to cause reliability improvement

Software Reliability Initiative Recommendations - 02

8. Early planning of the Software Reliability IPT should include:
   a) Leveraging existing and planned Cameo architecture models
   b) Motivating creation and leverage of software architecture and design behavior charts
      i. State transition diagrams
      ii. Process flow diagrams
      iii. Message sequence charts
      iv. Timing charts
      v. Control flow and data flow charts
   c) Accomplishing Software Reliability IPT baseline training
      a) Markov and Petri Net modeling
      b) Tool training (SHARPE and Mobius)
      c) RBD, Fault Tree and FMECA training

Agenda

BLUF

Software Reliability Modeling Concepts

Traditional Reliability Modeling Approach

Recommended Reliability Modeling Approach

Software Reliability Initiative Recommendations

Questions

Contact Information

Robert Stoddard

Email:

rws@sei.cmu.edu

Telephone:

+1 412.268.1121 desk

+1 724.263.7113 cell