

Risk-Based Strategic Software Design: How Much COTS Evaluation is Enough?

EDSER Position Paper

Barry Boehm, Dan Port

Computer Science Department

University of Southern California

Henry Salvatori Computer Science Center

Los Angeles, CA 90089-0781

{boehm, dport}@usc.edu

ABSTRACT

Risk consideration is a valuable assessment aid when making strategic software design decisions. Expressing development considerations in terms of risk exposures over an independent variable (e.g. time, cumulative effort, etc.) enables the quantitative assessment of typically qualitative attributes. Assuming total risk exposure is additive over individual risk exposure functions, optimal levels for the individual considerations can be identified as function of loss-magnitude and loss-probability estimates for risk sources. Such levels provide strategic trade off considerations (with respect to risk) and have proven valuable in several previous applications such as “how much testing is enough” with respect to defect removal and market window strategic risk considerations. Here we consider a similar application for making strategic design decisions in determining how much effort (or time) should be spent evaluating COTS products with respect to project cost, market window, and a multitude of COTS assessment attributes such as availability, ease of use, maturity, and vendor support.

Keywords

COTS, COTS integration, software risk, software economics, COTS assessment

1 INTRODUCTION

Software design is largely an art. We tend to approach it though as if it were not, as if there are secret scrolls of software design that developers divine upon to create the ideal system. Yet in reality few solid universal principles or formulas exist. At best there are heuristics and guidelines abstracted from skilled developer experience. These tend to provide design strategies more than specific design techniques. However all design strategies involve *risk*.

Risks are situations or possible events that can cause a project to fail to meet its goals. They range in impact from trivial to fatal and in likelihood from certain to improbable. Since risk considerations dictate the path

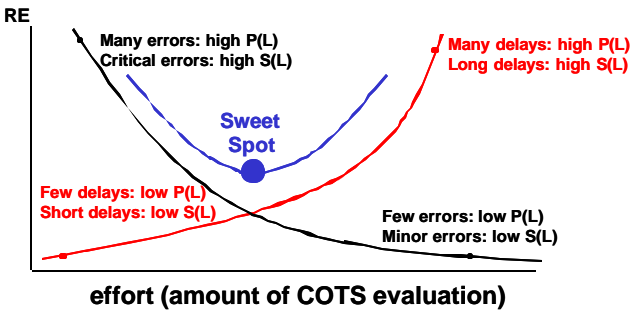
a development must take, it is important that those risks be cataloged candidly and completely. See the references for a taxonomy of risks [1] and a method for identifying them [2,3].

Indeed, the use of risk considerations within software development has proven to be a valuable tool to answer difficult strategic issues such as complex “how-much-is-enough of a given activity” questions. For example, how much is enough of domain engineering? prototyping? testing? configuration management? and so on. The recommended approach is to evaluate Risk Exposure (RE), which is computed as Probability (Loss) • Size (Loss) over some independent effort quantity such as time or cost. Typically specific RE functions are computed and the total RE is the sum of these functions. So long as the functions are computed within a particular project, this additive assumption is likely reasonable. Generally there is risk of project error (RE_{error}) from doing too little effort and project delay (RE_{delay}) from doing too much. We assume that a project starts out with a given amount of risk exposure due to potential “error” and that effort expended will identify and remedy these thus decreasing the risk exposure. If only technologically efficient risk reduction strategies are chosen, RE_{error} will a monotonically decreasing function. Using analogous assumptions, RE_{delay} will monotonically increase. This is reasonable since RE_{delay} represents the cumulative risk exposure due to delay. We assume that the project starts out with no risk of delay and that any effort expended contributes to the overall delay risk. Ideally, the effort expended will be that which minimizes the sum RE_{error} + RE_{delay}. This approach applies to most activities that are undertaken in an iterative development scenario.

2 COTS EVALUATION ERROR AND DELAY

Risk considerations can help determine “how much COTS evaluation is enough” before committing to a design. The more evaluation that is done, the lower becomes RE_{error} due to unforeseen or uncontrolled attributes, as assessed COTS attributes reduce both the size of loss due to “surprise” and the probability that surprises still remain. However, the more effort spent evaluating, the higher is RE_{delay} from losses due to increased project cost from extended evaluation activities and possible losses due to non-use of system, dissatisfied customers, or both competitors entering the market and decreased profitability on the remaining market share.

As shown in Figure 1, the sum of these risk exposures achieves a minimum at some intermediate level of evaluation. The location of this minimum-risk exposure point in time will vary by type of organization. For example, it will be considerably shorter for a “dot.com” company than it will for a safety-critical product such as a nuclear power plant. Calculating the risk exposures also requires an organization to accumulate a fair amount of calibrated experience on the probabilities and size of losses as



functions of evaluation duration and project delay.
 Figure 1: COTS Evaluation Risk Exposure

3 COTS EVALUATION ATTRIBUTES

When evaluating COTS products there are a large number of attributes that effect RE_{error} such as Correctness, Version Compatibility, and Vendor Support. What we want to know is the degree to which each of these attributes should be evaluated so as to provide an optimal investment strategy given a projects particular requirements and constraints. We would like to answer questions such as “it is better to buy or build?” and “should we choose a more reliable vendor or a product with more features?” Risk analysis can help answer such questions. Table 1 lists common COTS assessment attributes [4, p. 245] and

can be utilized to formulate a COTS evaluation strategy as will be described subsequently.

Correctness	Flexibility
Availability/Robustness	Installation/Upgrade Ease
Security	Portability
Product Performance	Functionality
Understandability	Price
Ease of Use	Maturity
Version Compatibility	Vendor Support
Inter-component Compatibility	Training
Vendor Concessions	

Table 1: COTS Evaluation Attributes

The degree to which each evaluation attribute is significant is relative to each COTS product, the project itself, and to the particular evaluation technique applied. For example, Ease of use tends to vary greatly from product to product. Security may not be relevant for some uses of a particular component within the system regardless of which COTS products used. Prototyping tends to provide more comprehensive results than product references (e.g. product testimonials). While Prototyping (as an evaluation technique) may reduce the risk of error more than testimonials, it also takes more time and thus increases risk of delay.

Also relative to the particular product and project is how attributes vary with respect to the amount of evaluation effort. For some COTS products a single evaluation is enough to resolve a risk attribute (as is typical with Price). For others, it may be a function of time outside project control such as with Upgrade Ease and Vendor Support. There may also be attributes whose risk attributes are resolved “stepwise” through repeated evaluation, as typical with Availability/Robustness, performance, and Ease of use. A COTS risk exposure assessment strategy should address the above issues. We will present one that does in the next section.

4 DEGREE OF EVALUATION DETAIL DRIVEN BY RISK CONSIDERATIONS

Up to this point we have only discussed how risk considerations relate to effort. We now consider the results of such effort. Risk considerations can also aid in determining the degree evaluation effort and

appropriate evaluation techniques. This means, for example, that the traditional ideal of a complete, consistent, formal evaluation may not always be a good idea for certain COTS components. A key in this is determining risk exposures for the COTS evaluation attributes listed in Table 1. For example in assessing the use of a well-known commercial web server for an e-commerce application, the Ease of Use risks are unlikely to incur large losses and is commonly relevant to a limited number of developers and hence has a low probability of occurrence. For this attribute, the risk exposure is low and a through evaluation is likely unwarranted. In contrast, Security risks may incur a large loss and may have a high probability of occurring and hence should be thoroughly evaluated.

The following guideline provides a means of avoiding over-evaluation and under-evaluation of COTS assessment attributes based on risk-considerations:

- ?? If it's risky to not evaluate extensively, DO evaluate extensively (e.g., scalability, safety)
- ?? If it's risky to evaluate extensively, DO NOT evaluate extensively (e.g., well-established, well-known, highly tested products)

Below we illustrate a stepwise COTS risk exposure assessment approach.

1. Identify the most significant COTS evaluation attributes from Table 1. Label them 1,..., n.
2. Estimate the relative Size(Loss)_i quantities for attributes i=1,...,n
3. Estimate the cost C_{ij} and the change in probability $\Delta \text{prob}(\text{Loss})_{ij}$ resulting from evaluating attribute i using technique j
4. Order the evaluation activities cost-benefit ratios $CB_{ij} = [\text{Size}(\text{Loss})_i * \Delta \text{prob}(\text{Loss})_{ij}] / C_{ij}$
5. Graph the cumulative cost-benefit ratios SCB_{ij} in decreasing order (see Figure 2) as a function of the cumulative cost SC_{ij}

This above process produces an optimal investment strategy of cumulative COTS evaluation risk exposure reduction versus cost.

CONCLUSION

COTS evaluation appears qualitatively intuitive for each individual aspect, however there are often many factors that must be considered. The impact of all considerations may be quite complex and counter intuitive. This complexity shows up in particular

when attempting to translate qualitative evaluations into quantitative results such as determining an optimal quantitative amount of evaluation effort to expend and level of evaluation detail. Risk exposure values are a tangible and accessible means of assessing individual aspects that effect COTS evaluation efforts. The total risk exposure is computed as the sum of the individual risk exposures (a linearity condition) and optimal total values will indicate optimal values for the individual risk contributions. In this way individual effort can be allocated in such a way to achieve minimum total risk exposure. Typically it is fairly straightforward to estimate individual risk exposures. COTS evaluation attributes such as those listed in Table 1 provide tangible guidance as to which areas to assess. Risk-based design can help answer difficult development questions before they become serious problems such as what COTS evaluation techniques are sufficient and how much evaluation is enough.

REFERENCES

1. Carr, M. J.; Konda, S. L.; Monarch, I; Ulrich, F. C. & Walker, C.F., "Taxonomy-Based Risk Identification", Software Engineering Institute, Carnegie Mellon University, Technical Report CMU/SEI-93-TR-6, ESC-TR-93-183, June, 1993.
<http://www.sei.cmu.edu/legacy/risk/kit/tr06.93.pdf>
2. [Hall 98]
3. [Boehm 91]
4. Boehm, B., Abts, C., Brown, A.W., Chulani, S., Clark, B., Horowitz, E., Madachy, R., Reifer, D. and Steece, B., *Software Cost Estimation with COCOMO II*, Prentice Hall, 2000.

