Abstract—Safety-critical systems certification is a complex endeavor. Regulating agencies are moving to goal-based standards in an effort to remedy significant problems of prescriptive standards. However, goal-based standards introduce new difficulties into the development and certification processes. In this work I introduce Certification-Based Development, or CBD. CBD is a process framework designed to mitigate these difficulties by meeting the needs of a specific certifying agency with regard to a specific system.

Keywords: certification; safety case; safety-critical systems; standards

I. INTRODUCTION

The goal of safety-critical systems certification is to protect the public interest: safety. Certifying agencies, including the US Food and Drug Administration (FDA) and the US Federal Aviation Administration (FAA), attempt to ensure that the residual risk of system operation has been reduced to a satisfactory level.

Certification agencies often use prescriptive standards to inform developers of best practices and to ensure that developers use appropriate means to create systems. Prescriptive standards have two significant problems:

- Prescriptive standards are unaccommodating of variation of technology, applications, and safety requirements across systems.
- Prescriptive standards prescribe processes to execute and artifacts to create, but not the specific qualities systems need. Prescriptive standards offer no assurance of adequate dependability.

Recently, certifiers have been moving away from prescriptive standards to goal-based standards. Goal-based standards set goals for the safety of a system. Developers are free to use any means they choose to fulfill the goals, as long as the developers can demonstrate that the safety goals have been met. Such a demonstration is typically recorded as a safety case, a special form of assurance case.

The safety case consists of two major parts:

- evidence that supports the claim that a system is safe, and
- an argument that shows how the evidence supports the claim.

These two elements must be present in all safety cases: an argument without evidence is not convincing, and evidence without an argument is unexplained, leaving the certifier to infer how the evidence shows that the system is safe.

Through the use of safety cases, goal-based standards deal with both disadvantages of using prescriptive standards. However, goal-based standards introduce two new disadvantages:

- There are no quality metrics for assurance cases. Thus, determining how convincing a safety case is difficult, despite standards calling for “compelling, comprehensive, and valid” safety cases [1].
- Significant variation in the various items comprising a safety case is possible. In order to make informed judgments, the certifier must be knowledgeable about all of the possible forms.

If the argument of a safety case is flawed, the top-level goal might not be fulfilled. The quality of a safety case is treated in UK Defence Standard 00-56 [1], which states:

“The Safety Case... provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment.”

The standard does not define “compelling, comprehensible and valid,” or provide any metrics for determining the extent to which a certain safety case meets these requirements. Because of the lack of quality metrics, developers are unsure of how to meet these requirements, and certifiers are unsure of how to determine if a safety case meets the requirements.

The high variability of safety cases also affects both the developer and the certifier. For a successful certification effort, the developer must know what the certifier expects as a quality submission, and the certifier must know what the developer could submit. These problems are not easily remedied simply by document specification, as certification experts work on a wide variety of devices. Thus, a solution to these problems would necessarily be applicable both across and within domains.
I propose the concept of Certification-Based Development (CBD). CBD is a domain-independent process framework, designed to align system development with the certifying agency’s responsibility for the public interest. By using CBD, both preparing for and conducting the certification process become predictable.

II. RELATED WORK

Prescriptive standards [2], [3], [4] are almost universally used by government agencies across the world to set functional and dependability requirements, affecting almost all industries. If practiced properly, safety standards limit certain classes of faults. However, the efficacy of prescriptive standards relies on the assumption that the process implies the goals; there is no evidence to support this assumption. Moreover, the standards are generalized by necessity; standards do not take into account the intricacies of individual systems.

An alternate approach is the idea of assurance cases, of which the safety case is a special instance. Safety case technology is well-established in the literature [5], [8], [10], [9], [11]. Several European government agencies mandate safety cases for their systems [12], [13]. Others recognize the importance of safety case development and documentation [14], [15]. Safety cases should be maintained throughout the lifetime of the system for which they are created; this approach is called “early and often” [13].

Assurance-Based Development (ABD) [7] is an approach to critical software system development that combines software creation with assurance case creation. The ABD process takes into account both dependability and functionality by combining them into “fitness for use,” or just fitness. ABD takes the “early and often” approach of assurance case construction to the extreme; the need to provide evidence of fitness drives development decisions.

Assurance-Based Certification (ABC), introduced by Graydon et al. [16], provides a definition of “compelling, comprehensive, and valid.” This definition is operational: a certifier examines the safety case for the presence of a specific set of properties. If the safety case possesses all the properties, then the safety case is “compelling, comprehensive, and valid.”

III. PROBLEM STATEMENT

The move to goal-based standards solves the problems that plague prescriptive standards, but introduces two new problems: lack of quality metrics and significant variability in safety cases. The requirements for CBD are derived from the need to solve these problems; these requirements are shown in the left side of Table I. The right side of Table I shows how CBD meets its requirements; the individual elements of the right side are discussed in more detail in Section VI.

IV. APPROACH

In order for CBD to succeed, I am developing a generic framework that can be instantiated to meet the needs of a given certifying agency and specific system. A given instance of this framework will need to instantiate:

1) Definition of certification: the criteria to be used for certification.
2) Process mechanism of CBD: the framework that integrates certification, safety case development, and system development.
3) Accessory artifacts: argument, document, and process patterns, and software tools to aid CBD practitioners. Patterns are used to encode expert knowledge and make it available to others.

The definition of certification will be an operational definition, as described in [16].

CBD patterns are inspired by classical software design patterns [17] and safety case patterns [5], [11]. In addition to argument patterns (described in detail in [5], [11]), CBD will have document templates and process patterns.

V. EXPECTED CONTRIBUTION

The proposed plan will sufficiently develop CBD for deployment in critical industries with minimal startup cost. The patterns and tools developed will serve as a bootstrap, enabling system developers and certification professionals to collaborate, using CBD, to ultimately build safer systems. Deployment will also serve as a large-scale, comprehensive evaluation of CBD, with opportunities for refinement and application to other system properties.

CBD will enable faster and more accurate certification, and less variability in the development and certification processes.

VI. PROGRESS TOWARDS SOLUTION

A. CBD Structure

The structure of CBD is shown in Figure 1. CBD has three major components:

- A set of domain-independent properties affecting all products in all domains for a given certifier applying CBD. The purpose of these properties is to ensure that important properties that are frequently required across domains are documented. One such property is called an Agency Domain-Independent Property, or DIP.
- A collection of certification assets, called the Certification Assets Package (CAP). A CAP sets the parameters of ABC to values derived from the domain of interest. A properly designed CAP also allows the certifiers to provide structure and reduce the variability of the development and certification processes.
- A device-specific instantiation of a development process for the device of interest.
The focus of CBD is the safety case that is produced by the developers and supplied to the certifiers. Through the safety case, the developers and certifiers can communicate, an essential part of a successful certification effort.

B. The Certification Assets Package

The safety case requirements and properties are conveyed by the certification assets. These entities describe all of the constraints that are needed to ensure that the variability of development and certification of a given device is as low as is reasonably practicable (ALARP).

These certification entities are put together into the Certification Assets Package, or CAP. Agencies create CAPs for each type of system they regulate. For example, the FDA will have a CAP for infusion pumps.

1) CAP Creation: Agencies create a CAP using a systematic process, illustrated in Figure 2.

To create a CAP, we start with the DIPs relevant to the CAP domain, which are determined by agency policy. For each DIP, we define domain-specific items in each of the following categories (a) notations, (b) templates for processes, evidence, and argumentation, (c) desired argument properties, and (d) challenges. These items are our certification assets. For each DIP, the assets pertain only to maintaining the particular DIP we are considering in the system development/certification effort.

The resulting CAP meets CBD requirements, as detailed in Table 1.

VII. METHODOLOGY

I will follow the below methodology to continue developing CBD.

1) Extend previous work on safety-case-based certification [16] to create a systematic process that generates operational definitions of desired system properties for any given certifying agency.

2) Develop the CBD framework, largely through leveraging the use of patterns for arguments, documents, and processes. Create CBD tools wherever necessary.

Table I

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Requirement is Met By...</th>
</tr>
</thead>
<tbody>
<tr>
<td>The safety case must be accessible by and familiar to the certifier. Artifacts must (a) use agreed-upon notations, (b) be structured in a prescribed form, and (c) be presented in a prescribed manner.</td>
<td>The definition of the Certification Assets Package (CAP) by the certifier. The certifier chooses or artifact patterns that fulfill their requirements of agreed-upon notations, prescribed structure, and prescribed presentation manner.</td>
</tr>
<tr>
<td>The safety case must be amenable to systematic and comprehensive technical review that allows the certifier to make an appropriate certification decision about the supplied safety case. The certification decision process must be objective and repeatable.</td>
<td>The use of Assurance-Based Certification in the CBD mechanism.</td>
</tr>
<tr>
<td>CBD must be objectively consistent across domains within the purview of a given regulating agency.</td>
<td>Met by defining the structure of CAPs at the organizational level, i.e., all FDA CAPs will have a set structure, all FAA CAPs will have a (possibly different) structure, etc. CAP structure will embody the different Agency Domain-Independent Properties, as in Figure 1.</td>
</tr>
<tr>
<td>CBD must be objectively consistent across devices in a given domain.</td>
<td>Having one CAP for each specific domain in a certifier’s purview, i.e., the FDA has one CAP for infusion pumps, one (likely different) CAP for artificial hearts, etc. CAP contents are defined by the Domain-Specific Entities shown in Figure 1.</td>
</tr>
</tbody>
</table>
3) Evaluate CBD by using it to develop a novel safety-critical system. Evaluation will focus on the Diabetes Advanced Information System (DAIS).

The Evaluation section explains DAIS and the CBD evaluation strategy in more detail.

VIII. EVALUATION

CBD evaluation will be in two parts: (a) a theoretical evaluation of variability and assessment difficulty reduction, and (b) a feasibility evaluation on a real safety-critical system.

The theoretical evaluation will measure how much variability is reduced by taking into account possible common methods of safety case construction and presentation, and comparing them with what CBD offers. The evaluation will show the assessment difficulty reduction by measuring the difference between the theoretical minimum time taken to assess a safety case without CBD provisions and with challenges and other CBD provisions.

DAIS is a software system that was designed to improve the safety of the living environment of a Type I diabetic using an insulin pump and continuous glucose monitor (CGM).

Instead of focusing on the interaction between patient and insulin pump, DAIS holds the patient and insulin pump as given and seeks to enhance the diabetics living environment, providing an organized view of supplies the patient needs as well as emergency response mechanisms. The initial DAIS concept is being used as a case study for the systematic application of safety engineering to medical systems in another student's research. I am working with two undergraduate students in the Computer Science department to implement DAIS.

DAIS will serve as a feasibility evaluation for the CAP creation process and CAP usage in the context of CBD.

IX. PUBLICATION LIST


ACKNOWLEDGMENTS

I would like to thank my research advisor, Dr. John C. Knight, for his guidance in my research and other endeavors.

REFERENCES


