Res Eng Design (2011) 22:245–261
DOI 10.1007/s00163-011-0109-6

ORIGINAL PAPER

The fundamentals of barriers to reverse engineering and their implementation into mechanical components

Shane K. Curtis · Stephen P. Harston · Christopher A. Mattson

Received: 1 June 2010 / Accepted: 21 March 2011 / Published online: 9 April 2011

Abstract Reverse engineering is a common design strategy in industry. It is a term that has come to encompass a large array of engineering and design activities in the literature; however, in its basic form, reverse engineering is simply the process of extracting information about a product from the product itself. Depending on its use, it may or may not be advantageous to utilize a reverse engineering strategy. As with any rational decision, reverse engineering is only favorable when the benefits from its use outweigh the investment. Therefore, a general understanding of the principles that increase the difficulty or investment required to reverse engineer mechanical products would be helpful for everyone affected by reverse engineering activities. In this paper, we articulate and explore these fundamental principles after reviewing examples from the literature and from our own experience. We then use the principles as a basis for the development of a methodology to build barriers to reverse engineering into new products.

Keywords Reverse engineering · Barrier to reverse engineering · Product imitation

A portion of this work was originally published in the 2010 ASME IDETC/CIE proceedings (DETC2010-28610).

S. K. Curtis · S. P. Harston · C. A. Mattson (✉)
Department of Mechanical Engineering,
Brigham Young University, Provo, UT, USA
e-mail: mattson@byu.edu

S. K. Curtis
e-mail: shanekcurtis@gmail.com

S. P. Harston
e-mail: sharston@gmail.com

1 Introduction

Reverse engineering carries various connotations in different industry settings. At one end of the spectrum, reverse engineering is associated with design theft and piracy with the intent to plagiarize and capitalize on the work of others (Naumovich and Memon 2003; Grimm 2004). On the other hand, reverse engineering can be as conventional as competitive benchmarking (Ulrich and Eppinger 2004) or as benign as the dissection of a popular product by a curious consumer (McLoughlin 2008). Regardless of the motivation behind its use, we adopt the following definition for this paper:

Reverse engineering is the process of extracting information about a product from the product itself (Harston and Mattson 2010b).

Notice that the definition of reverse engineering used here is different from *imitation*, which we define as the process of replicating the performance of an existing product in one or more of its performance areas (Knight et al. 2009). Reverse engineering often leads to imitation; however, the definition of reverse engineering as defined here limits the discussion to simply the information-extraction process.

There are many reasons to employ reverse engineering as a viable engineering design tactic. A few common reasons are listed below:

- To compare products through competitive benchmarking (Harrington 1991; Raja 2008)
- In preparation for imitating a product (Musker 1998)
- To obtain technical data that do not exist (Pal et al. 2006; Creehan and Bidanda 2006; Urbanic and ElMaraghy 2009)
- To obtain technical data that the original supplier is no longer willing or able to provide (Thompson et al. 1999; Raja 2008)

- To shorten market entry times (Raja 2008)
- To enhance existing data (Ingle 1994)
- To perform product verification (Ingle 1994)
- To aid in product design (Hsiao and Chuang 2003)
- To investigate patent law infringement (Ohly 2009)
- To assist in academia or other learning environments (Mowery et al. 2004; Ohly 2009)

While this list is not exhaustive, it illustrates how reverse engineering is used in a variety of settings. As such, it is important to know what factors affect reverse engineering difficulty. This knowledge is beneficial—both for original designers and those reverse engineering. It can potentially help original designers to design products that are more difficult to reverse engineer, thereby maintaining a market advantage over their competitors. On the other hand, those reverse engineering can use this knowledge to select projects that will be *successful*, meaning that the payoff is sufficiently greater than the reverse engineering cost.

This paper is devoted to investigating *barriers* in the reverse engineering process, which can be defined with the following:

A barrier to reverse engineering is anything that impedes the extraction of information about a product from the product itself (Harston and Mattson 2010b).

Some examples of barriers to reverse engineering include the complexity of turbine blade surfaces, inaccessibility of hidden or microscopic features of an embedded circuit, inadequate measurement equipment, or even an inexperienced engineer. Barriers for mechanical systems can be classified into *internal* and *external* barriers. Internal barriers are physical features of the product itself, or lack thereof, that hinder reverse engineering, while external barriers are extrinsic to the product. The *total* barrier is affected by all barriers whether internal, external, or a combination of the two.

The existence of barriers to reverse engineering has been discussed in the literature from multiple perspectives including hardware (McLoughlin 2008), software (Naumovich and Memon 2003; Nelson 1996), CAD modeling (Várady et al. 1997) material microstructures (Harston and Mattson 2010a), and adoption of reverse engineering at the strategic and managerial level in manufacturing companies (Fernandes 2008). These perspectives offer valuable insight into many of the challenges of reverse engineering and in some instances are directly applicable to mechanical systems; however, the nature of barriers to reverse engineer mechanical components has yet to be articulated in the literature. Moreover, a design methodology to strategically implement barriers into a product would be a valuable contribution to the literature, as no such method exists in published form, so far as the authors perceive. When barriers are effectively implemented, competitors are forced to spend additional time and resources in developing their own competing technology, or, at a minimum, spend additional resources on extracting the information (Grand 2004). Consequently, the original product is likely to maintain larger portion of the market share for a longer period of time.

Not all products benefit from incorporating barriers to reverse engineering. Some products may be so simple, or sold at low margins, so that incorporating barriers to reverse engineering is not practical. Deciding which products are suitable for barrier implementation is a critical question that can be answered by the methodology presented in this paper.

In this paper, we characterize the fundamental types of barriers to reverse engineer mechanical components. We provide examples and theories from related fields to illustrate how these barriers can potentially stymie reverse engineering efforts. In so doing, we provide valuable insight into how one can either increase or decrease the magnitude of a barrier to reverse engineering. Our tenet is that the difficulty to reverse engineer a product can (i) be controlled and (ii) designed in a strategic manner. Further, the methods presented in this paper facilitate the implementation of our tenet.

The remainder of this paper is organized as follows: In Sect. 2, we define and explain the fundamental types of barriers to reverse engineering. Section 3 presents two metrics that may be used to analyze barriers to reverse engineer a product. In Sect. 4, we introduce a barrier implementation methodology to assist original designers in creating products that are more difficult to reverse engineer. Finally, in Sec. 6, we provide concluding remarks.

2 Barriers in the reverse engineering process

The general procedure of reverse engineering has been defined and examined in detail by both Ingle (1994) and Otto and Wood (2001). Additional techniques for digitizing physical objects for CAD applications have been presented by Várady (2001), Sarkar and Menq (1991), and Raja (2008). Though there exist multiple descriptions of the reverse engineering process, they can all be distilled to three simple steps as seen in Fig. 1. The three basic reverse engineering steps are: (i) planning, (ii) data collection, and (iii) data processing. As Fig. 1 suggests, the process can be iterative in nature. During data processing, for example, the reverse engineering team must validate extracted information, so as to know when the process is complete. If errors are discovered, due to missing or low quality data, the reverse engineering team must extract more information from the product. When barriers to reverse engineering

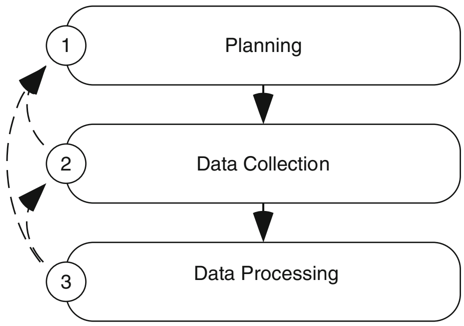

Fig. 1 Steps of the reverse engineering process

are strategically implemented, the process would ideally have to be repeated several times.

Before presenting the methodology that impedes competitors from gaining valuable information from a product we classify barriers into the following three categories, which will facilitate the presentation of the said methodology:

- Technical complexity of the product or feature
- Availability of the necessary resources (Summers and Shah 2010)
- Skill of the reverse engineering team (Summers and Shah 2010)

Barriers associated with the technical complexity of the product or feature are internal barriers to reverse engineering, while the remaining types of barriers are external. The skill of the reverse engineering team could be considered a necessary resource, i.e., a human resource; however, as skill is an intangible asset with unique characteristics, we consider it separately in the discussion of the barrier types presented in this section. While the original designer has direct control over internal barriers, it will be shown that he or she can also indirectly affect the external barriers as well.

When a simple product is evaluated by someone with the necessary resources and adequate skill, then the total barrier to reverse engineer that product is small. The opposite is also true—the total barrier is high if the product is technically complex and the reverse engineering team lacks necessary resources and skills. It follows that the magnitude of the total barrier is directly proportional to the technical complexity of the product, while inversely proportional to both the availability of the necessary resources and the skill of the person or team reverse engineering the product.

We note here that while legal barriers can and do exist to prevent the commercialization of copied products, there are few laws to prevent the reverse engineering of hardware (Samuelson and Scotchmer 2002). Current laws state that reverse engineering is an acceptable method of obtaining trade secrets as long as the product acquisition was done legitimately (Samuelson and Scotchmer 2002; McLoughlin 2008). These laws are justified by many, since the time and effort required to reverse engineer a product is often viewed as substantial enough to allow the original designer to maintain a large market share (Samuelson and Scotchmer 2002). Interestingly, patents facilitate reverse engineering as they disclose critical product information and key technologies. In some cases, laws are outright violated and products are continually built directly from patent information even though the patent owners have claimed patent infringement and seek compensation (Maskus et al. 1998). Thus, it may not be wise for an original designer to rely solely on legal barriers to mitigate reverse engineering attempts of their product.

The remainder of this section investigates in greater detail how these three barrier categories interact to create information-extraction difficulties during the reverse engineering process.

2.1 Technical complexity of the product

Perhaps the most apparent barrier to reverse engineering is the technical complexity of the product. We decompose technical complexity into the quantity of information, the information type (e.g. geometric dimensions, material composition), and the extent to which different information types interact. If a product is more technically complex, it will be more difficult to reverse engineer. As this is an internal barrier, the original designer can literally build physical features into the product to increase the difficulty to reverse engineer the product. Therefore, the original designer has a direct influence on this type of barrier.

A product can contain many disparate types of information, such as geometric, material, chemical, electrical, or even esthetic information. Certain types of information are inherently more difficult to extract than others (Harston and Mattson 2010b). Von Hippel articulates this in (1998) by defining the "stickiness" of a unit of information as the *incremental expenditure required to transfer that unit of information to a specified locus in a form useable by a given information seeker*. In other words, stickiness is a measure of the rate at which usable information may be extracted from a product while reverse engineering. When systems containing sticky information interact with other systems in a product, the result is a powerful barrier to reverse engineering. For example, when material properties that are difficult to reverse engineer are heterogeneously placed at critical geometric locations, the barrier to reverse engineer is larger than when the same microstructure is homogeneously distributed.

Information stickiness varies for different information types, even within the geometric domain. Free form surfaces are not easily measured with traditional measurement devices such as micrometers or calipers (Campbell and Flynn 2001); therefore, their complexity could be potentially difficult to capture during the data-collection step, as they require more expensive, and user intensive, measurement equipment. This is exemplified by Soo et al. in (2005) where the difficulties of digitally capturing the complicated and arbitrary curves of a Chinese bamboo-net handicraft are discussed in detail. Additionally, the physical size of the measurement can have a large impact on the information stickiness. For instance, as computer chips have decreased in size, they have become increasingly more difficult to reverse engineer (James 2006).

Products can contain a large amount of information. One challenge for the reverse engineering team lies in distinguishing between information that is *superfluous* and information that is *pertinent* to product performance (Harston and Mattson 2010b). This distinction can be difficult to make, especially when products contain a plethora of nonessential information or when essential information is disguised to appear trivial (McLoughlin 2008). Extracting superfluous information will decrease the return on reverse engineering investment, as resources are wasted on information that does not provide significant benefits. Therefore, it is important for the reverse engineering team to make this distinction, if possible in the planning step (see Fig. 1), before collecting data from the product.

Additionally, one must ensure that all pertinent information is extracted from the product. This is typically done during the data-processing step. McEvily (2005) presents a case study of reverse engineering failure, where a butterfly valve in an aircraft engine caused the plane to crash. He states that the *original alloy and part dimensions [of the butterfly valve] were accurately duplicated*; however, the firm reverse engineering the valve failed to extract the heat treating process required to properly reconstruct the valve. As a result, the valve was inadequately manufactured and failed in use.

Another aspect of product complexity is the accessibility of pertinent information. Products can be difficult to dissect; essential components of the product can be enclosed in the product in such a way that nondestructive disassembly is nearly impossible (Pooley and Graves 2008). This is the case with many computer chips, where the coating on the chip is designed so that when the coating is removed, one or more layers of the chip are also destroyed, thereby making the rest of the chip difficult, if not impossible, to reverse engineer (Dam and Lin 1996). Another way to limit accessibility of pertinent information is to add locks to a product. For mechanical products, this may be in the form of custom made fasteners (Campbell and Flynn 2001; Grand 2004). In general, the harder it is to access the information, the stickier the information becomes.

The fundamental principles to understand about the technical complexity of barriers to reverse engineering can be summarized with the following:

- The technical complexity of a product or feature is an internal barrier to reverse engineering—the original designer has a direct influence over the magnitude of this barrier.
- When sticky information interacts with other sticky information in a product, the result is a powerful barrier to reverse engineering.
- The stickiness of pertinent information can be increased by reducing its accessibility or including more superfluous information in the product to disguise pertinent features.

We note that in Sect. 4, a list of specific actions to increase product complexity is provided.

2.2 Availability of the necessary resources

We now turn our attention to external barriers to reverse engineering; specifically, the barriers associated with the availability of necessary resources. By necessary resources, we mean required tools (including tools for disassembly, performance analysis, data synthesis, measurement etc.), samples of the product, and any other object or software that is required to successfully extract information from the product itself. Unlike internal barriers, the original designer can only indirectly influence the magnitude of external barriers as they may not be able to control the resources extrinsic to the product. However, by strategically designing the product, original designers can require those reverse engineering to use resources that are expensive or not readily available in order to be successful at reverse engineering. While there may be more than one approach to extract information from a product, some information can only be acquired with the correct tools such as the material microstructure of a custom made material that is critical for proper performance of the product. On the other hand, a reverse engineering team can overcome many barriers by acquiring essential resources.

First and foremost, the product or system being analyzed needs to be accessible. Even if a product is readily available on the market, it may be expensive or may only be available in limited quantities, thereby discouraging others from attempting to reverse engineer the product as the required investment increases. Often times, it is of interest to those reverse engineering to know how the original product fails, possibly to prevent or improve the conditions of failure. Clearly, when only a few sample parts are available, extracting this type of information can be difficult (Ingle 1994).

Second, equipment used during the data-collection step (see step two of Fig. 1) needs to be available. Often, a high level of precision and accuracy is needed when collecting information from a product. This is much easier to accomplish with appropriate equipment, which for geometric information could include micrometers, gages, coordinate measuring machines, and optical scanning equipment (Thompson et al. 1999) or for material microstructure information could include a scanning electron microscope (Adams et al. 2005). At the same time, a significant amount of skill and experience, see Sect. 2.3, may be needed to operate these measuring tools, as well as to understand their limitations and shortcomings (Várady et al. 1997, 2005; Ali et al. 2008; Grimm 2006b).

Third, converting collected data into a usable form during the data-processing step (see step three of Fig. 1) can also be challenging. For geometric information, this form is often digital, meaning in the form of a CAD model or drawing. This, of course, requires CAD or CAE software. Much care is needed during this process to ensure that minimal error is introduced when processing the data (Bradley and Currie 2005; Creehan and Bidanda 2006). For material microstructure information, the data collected through scanning electron microscopy needs to be analyzed with orientation image microscopy (OIM) software (Adams et al. 2005). Clearly, if this equipment is unavailable, the magnitude of the barrier to reverse engineering will be large.

Finally, proper testing and validation of extracted data are vital to the success of a reverse engineering project. Assumptions made in the planning step in Fig. 1, such as decisions regarding information relevance, need to be verified as the data collected may or may not actually be pertinent. Additionally, some information may still be needed to adequately reverse engineer the product. Verification can take on many different forms, each requiring specific resources. CAD systems can help verify that all the needed geometric dimensions have been extracted. CAE systems can further aid in this process by analyzing motion, stress, heat transfer, and failure modes. If the necessary equipment is available, prototypes can be built and subsequently tested for the purpose of verification.

For example, the non-circular brass gears in Fig. 2a were originally part of a photocopy machine. As part of this study, we reverse engineered the gears to illustrate the verification process. The gears were measured using an optical comparator, and the data were manually entered into a CAD system. The resulting CAD model appears in Fig. 2b. A motion analysis was done using CAE software to verify that the gears properly meshed. Acrylic prototypes were then manufactured using a laser cutter and are shown in Fig. 2c. The acrylic prototype was made five times larger, to accommodate for the resolution of the laser cutter. Finally, brass gears were cut in true scale using wire electric discharge machining (EDM), as shown in Fig. 2d. Multiple tools were needed to verify that we extracted the correct information about the non-circular gears. In fact, the prototypes revealed some flaws in our extracted data, as the reconstructed brass gears did not perform as well as the original gears. If the necessary resources were not readily available (optical comparator, CAD and CAE software, laser cutter, wire EDM), then this process would have taken a different path characterized by its own difficulty. Therefore, we can see that the resources available to the

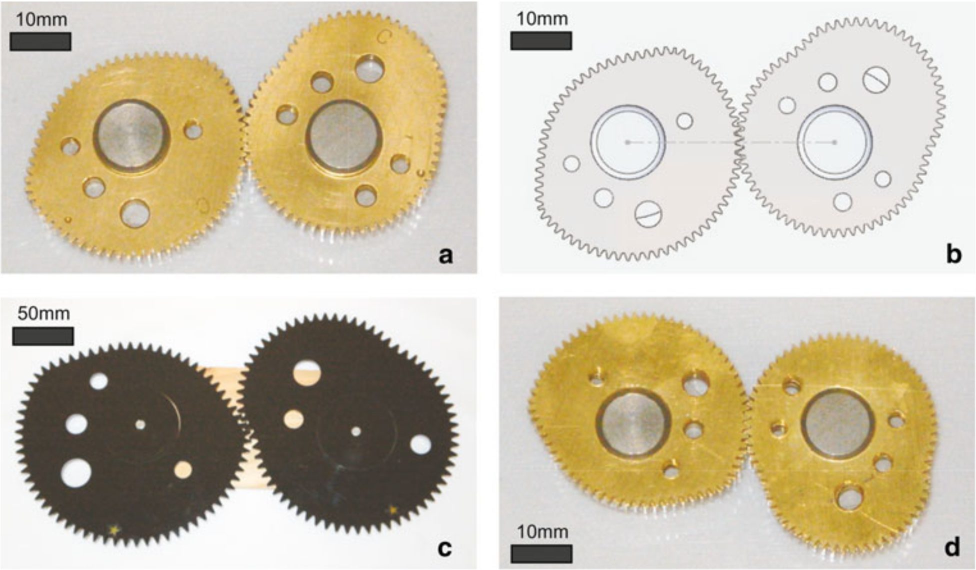

Fig. 2 Reverse engineering example of non-circular gears. **a** Original brass gears, **b** CAD model, **c** Acrylic prototypes, **d** Reconstructed brass gears

reverse engineering team influence the difficulty to reverse engineer the product.

The fundamental principles to understand about the resource-availability category of barriers can be summarized with the following:

- The availability of the necessary resources is an external barrier to reverse engineering—the original designer typically has an indirect influence on this barrier.
- When few or no samples of the product are available, the magnitude of this barrier increases dramatically.
- Proper equipment is often required for efficient product dissection, information extraction, and data processing. The absence of this equipment could severely reduce the quality of collected data. The barrier can be made larger by embedding information that requires specialized and/or unavailable tools to extract.

Section 4 provides specific actions that can be taken to increase the magnitude of this type of barriers.

2.3 Skill of the reverse engineering team

The third and last category of barriers to reverse engineering is the skill of the reverse engineering team. Clearly, when required skills are absent, the barrier to reverse engineering is larger. Skill can be considered from two perspectives. First, a familiarity or basic understanding of the science governing the system being analyzed is often essential for effective reverse engineering. For instance, a working knowledge of chemistry is necessary to extract chemical information from a battery. Second, expertise and experience with the reverse engineering process and its associated tools is also extremely important. More than likely, a successful reverse engineering project will require the synergy and collaboration of a group of professionals with different skill sets—economists, market analysts, accountants, engineers, managers, etc. Thus, skills in multidisciplinary design and project management are valuable.

The reverse engineering team must begin by considering the purpose for reverse engineering in the planning step of Fig. 1. This will determine whether or not there is a need to capture *as-built* information from the product or *design intent* information (Grimm 2006a). In its extreme form, the as-built approach aims to copy every bit of information from a product to the best ability of the team. Even though the as-built approach focuses on copying all information, it is likely that some assumptions will be made, i.e. assuming that bolts in a system are consistent sizes therefore not requiring a detailed analysis of each bolt of a similar shape and size. Some deviation from the original product may also occur due to manufacturing tolerances and errors made during the reverse engineering process. On the other hand, design intent attempts to determine the nominal performance and understand the desired relationship between components. For simple features, recovering design intent may be straight forward; however, with more complex features such as a turbine blade (Mohaghegh et al. 2007), distinguishing between manufacturing variations and design intent becomes significantly more difficult, or in other words, the likelihood of making an invalid assumption increases. Although methodologies do exist for extracting design intent when reverse engineering (Barbero 2009), recovering design intent is likely to require more resources and time (Grimm 2006a) when compared to the as-built approach. Therefore, experience with reverse engineering would help in selecting an appropriate extraction strategy.

A well-known historical example that illustrates this type of barrier to reverse engineering occurred during World War II. After a forced landing in the former Soviet Union, an American B-29 bomber, pictured in Fig. 3a, was reverse engineered by the Soviets to yield the Tupolev Tu-4 bomber, shown in Fig. 3b. Josef Stalin ordered that the downed B-29 (eventually, a total of four such aircraft came under Soviet control) be copied *exactly* (Boyne 2009; Suvorov 1981), so as to ensure that all the separate components would assemble correctly. It has even been rumored that existing damage on the B-29 fuselage (Danelek 2008) and manufacturing defects such as a small, misplaced rivet hole on the B-29 left wing (Suvorov 1981) were incorporated into the original Tu-4 design. This would indicate that the Soviets took more of an as-built approach to reverse engineering the B-29. As a result, the Tu-4 is nearly an exact replica of the B-29, with the exception of some subsystems such as the Soviet manufactured engines and cannons (Boyne 2009).

Additionally, the Soviet's thought it beneficial to extract information in the native units of the design (English units). Therefore, the Soviets needed to buy measuring equipment in Canada, England, and the United States and retrain thousands of engineers and technicians to work with the new measurement system (Suvorov 1981). Although the magnitude of the total barrier to reverse engineer the B-29 was large, the Soviets were able to utilize nearly unlimited resources in conjunction with enough skill to successfully reverse engineer the B-29.

The fundamental principles to understand about the barriers associated with the skill of the reverse engineering team can be summarized with the following:

- A reverse engineering team is more likely to succeed if they have a basic understanding of the science being analyzed *and* a familiarity with the process and tools of reverse engineering.

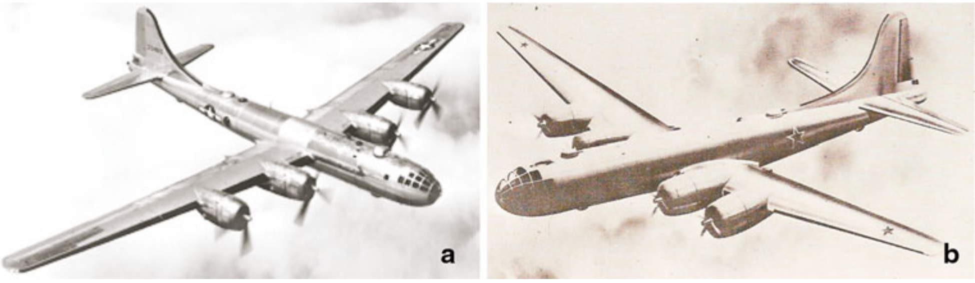

Fig. 3 Example of reverse engineering from WWII; The Tu-4 is a reverse-engineered copy of the B-29. **a** United States Air Force B-29 bomber [USAF (1944), Boyne (2009)], **b** Soviet Union Tupolev Tu-4 bomber [Norby (1978)]

- Knowing which approach is needed—as-built, design intent, or a combination of both—will help maximize the return on reverse engineering investment.

Similar to technical complexity and availability of resources previously discussed, in Sect. 4, we provide a list of ways to make a product more difficult to reverse engineer.

In this section, Sect. 2, we have explored the fundamentals of barriers that can stymie reverse engineering efforts during any step of the reverse engineering process. We have demonstrated that by increasing the complexity of a product—such as making information inaccessible and introducing complicated information interactions—we can increase the reverse engineering barrier. An example of a reverse-engineered butterfly valve that failed demonstrated the difficulty of extracting information that interacts with other information, and to extract information that is difficult to access. We next demonstrated how reverse engineering can be made more difficult when competitors lack necessary resources. Although original designers may not have direct control over the resources available to competitors, when a product design requires special tools or materials that the competitors are likely not to have, the barrier to reverse engineering is increased. An example of non-circular gears was given which shows that resources available influence the reverse engineering difficulty. Finally, we demonstrated how the skills of the reverse engineering team also affect the reverse engineering barrier. Similar to resources available, the original designers can only indirectly affect what skills are required, since they cannot control what skills the reverse engineering team will have. The example of the Soviet replicate of an American B-29 bomber demonstrates that even technically complex products can be adequately reverse engineered when the team has the proper skill set. In the next section, we add to this anecdotal understanding of what affects barriers to reverse engineering and present metrics that have been developed to systematically characterize the reverse engineering barrier. This systematic barrier characterization enables designers to quantify what barriers are most effective and efficient in specific design applications. This can even be done in conjunction with numerical optimization which is the topic of a separate paper by the authors.

3 Summary of metrics for barriers to reverse engineering

In this section, we briefly present two metrics that have been published in the literature that are used for characterizing the barrier to reverse engineer any product. The purpose of this section is not to present the full development of the metrics, but to give a brief summary for convenience to the reader and to facilitate the discussion in Sect. 4.

Qualitative as well as *quantitative* metrics exist for characterizing reverse engineering difficulty. One qualitative measure has been termed the *attack difficulty* (Weingart et al. 1990) and is summarized in Table 1. This classification system ranges from 1 to 6 based on the tools and skills required to reverse engineer a product. Similar qualitative classifications have been presented by Christiansen (2006) and Abraham et al. (1991). An advantage of these measures is that they are intuitive, and can be easily evaluated in the early stages of the product development process.

Quantitative metrics may be less intuitive, but can be used with numerical optimization techniques to literally maximize the time and barrier to reverse engineer a product (Harston and Mattson 2010b) and its tolerances (Curtis et al. 2009). We provide a brief overview here of the fundamental metrics presented by Harston and Mattson in (2010b), and we refer the reader to their work for a more detailed explanation of the equations and variables in the metrics. Harston and Mattson adapted Ohm's law (Ohm 1827) to meaningfully (with an average error of 12.2%) quantify the time and barrier to reverse engineer products. They observed that the rate at which information can be extracted from a product is dependent upon the ratio of known information to the total information contained by a product. This is similar to how the discharge rate of a

Table 1 Qualitative attack difficulty classifications (Weingart et al. 1990)

Level	Name	Description
1	None	The attack can succeed "by accident," without the attacker necessarily being aware that a defense was intended to exist. No tools or skills are needed
2	Intent	The attacker must have a clear intent in order to succeed. Universally available tools (e.g., screwdriver, hobby knife) and minimal skills may be used
3	Common tools	Commonly available tools and skills may be used (e.g., those tools available from retail department or computer stores, such as a soldering iron or security driver bit set)
4	Unusual tools	Uncommon tools and skills may be used, but they must be available to a substantial population (e.g., multimeter, oscilloscope, logic analyzer, hardware debugging skills, electronic design and construction skills.) Typical engineers will have access to these tools and skills
5	Special tools	Highly specialized tools and expertise may be used, as might be found in the laboratories of universities, private companies, or governmental facilities. The attack requires a significant expenditure of time and effort
6	In laboratory	A successful attack would require a major expenditure of time and effort on the part of a number of highly qualified experts, and the resources available only in a few facilities in the world

capacitor in a simple resistor-capacitor circuit is dependent upon the voltage difference across the resistor. In both scenarios, there exists an exponential decaying relationship—for reverse engineering, between unextracted information and time, and for the capacitor, between electrical charge remaining in a capacitor and time. The mathematical relationships developed with Ohm's law adequately describe both cases.

From Harston and Mattson (2010b) the quantitative barrier, B, to reverse engineering is defined as

$$B = \frac{P}{F^2} \tag{1}$$

where P is the power—effort per time exerted to extract information—and F is the rate at which information is extracted from a product. The value of F is heavily dependent on (i) product complexity, (ii) skills of the team, and (iii) available resources. The value of P is constrained by

$$0 < P \leq 1 \tag{2}$$

where zero represents no effort being put forth to reverse engineer a product and one signifies full effort at maximum efficiency. Returning to Eq. 1, we see that when the flow of information from a product is low, then the barrier is large. Additionally, if the flow rate of information is held constant, and the power is free to vary according to Eq. 2, then a higher P will result in a larger B. In other words, if a reverse engineering team needs to put forth more effort to achieve the same flow of information from a product, then this is due to a larger barrier.

The storage capacity, S, of a product is defined as

$$S = \frac{KF}{P} \tag{3}$$

where K is the amount of unextracted information remaining in a product. Using these definitions, the time, T, required to reverse engineer a product can be accurately predicted using the following exponential decay relationship

$$T = -BS \ln\left(\frac{K}{K_0}\right) \tag{4}$$

where K_0 is the amount of information initially stored by the product. Thus, it follows that K is constrained to

$$0 < K \leq K_0 \tag{5}$$

which ensures that Eq. 4 yields a finite quantity of time. In summary, if K, F, and P are known for a particular information type, then S, B and T can be calculated for that information type.

Products generally contain more than one type of information that is pertinent to product performance; therefore, the total time, T^*, to reverse engineer a product is calculated as the sum of all the times to reverse engineer each information type, as calculated above. Likewise, the total information, K^*, and storage ability, S^*, of a product are also simple summations. The overall flow rate of information extraction for the entire product can be calculated by

$$F^* = \frac{K^*}{T^*} \tag{6}$$

which allows for the calculation of the effective power applied to reverse engineer the entire product

$$P^* = \frac{K^* F^*}{S^*} \tag{7}$$

With F^* and P^* defined, the total quantitative barrier, B^* can be calculated using Eq. 1. It is beneficial to consider both B^* and T^* as reverse engineering measures, as they are related, yet distinctly different. It is possible for a product to have a small B^*, but a large T^* due to the amount of information contained by the product. For example, consider a large flat plate with numerous holes of various sizes throughout. There is a small barrier to measure the diameter of any single hole (indicating a small B^*), yet the number of unique measurements required makes the total reverse engineering time relatively large.

The qualitative and quantitative metrics are related in that when the tool complexity and skill required increase, then the metric also increases. However, there is not a direct correlation between the two measures, i.e., a level 3 attack difficulty does not directly correlate with a specified range of B^*. This is because the quantitative metrics are also influenced by the relative amounts of each information type contained by a product, while the qualitative metrics are not.

Ultimately, these metrics can be used to quantify and compare the effectiveness of multiple types of barriers and help designers select which barriers will be efficient and effective for the desired application. Due to the numerical nature of the metrics, numerical optimization may be used to facilitate the search for the ideal barrier. Along with B^* and T^*, the optimization objective function can also include barrier implementation cost, return on investment, barrier development time, and any other relevant objectives.

4 How to plan for, select, and implement barriers to reverse engineering

Often the market advantage achieved when a firm successfully develops an innovative product acts as the driving force for technological progress. However, if a competing firm can successfully reverse engineer the innovative product, then the market advantage of the original firm is quickly lost (Macmillan et al. 1985). When this occurs, the incentive for innovation is reduced (Shapiro 1985). Therefore, it is in the best interest of original designers to design products that are difficult to reverse engineer. A product can be made difficult to reverse engineer simply by making one critical component difficult to reverse engineer. For example, consider how the performance of an entire aircraft system was influenced by a single critical component, namely the butterfly valve described in Sect. 2.1. While critical component selection is the subject of another paper by the authors, in the current paper, we assume that the critical components for receiving barriers to reverse engineering have been previously determined. As a note, components that are heavily constrained are often the best candidates for implementing barriers. The more a component is constrained by specifications or interactions with other components, the less likely competitors will be able to design around the barriers, thus requiring competitors to overcome the barriers. Other guidelines have been presented in Table 2 to facilitate implementation of barriers into products. For the remainder of this section, we will take the perspective of the original designer, as we present a methodology to implement barriers to reverse engineering.

Table 2 Guidelines for implementing effective barriers to reverse engineering

Guideline
The barrier to reverse engineering may be increased by increasing the technical complexity, increasing the resources needed, and/or increasing the skills required to reverse engineer a product or feature
The barrier produces a benefit greater than the cost of its development, implementation, and manufacture
The barrier requires competitors to use more resources or time to reverse engineer a product/feature than to independently develop their own
The barrier protects a product/feature that is at risk of being reverse engineered
The barrier's effectiveness increases when it protects a product/feature with few alternative feasible designs
The barrier does not degrade product performance past a tolerable point determined by the designer

A five step process is used to implement barriers to reverse engineering as illustrated in the flow chart in Fig. 4. The first step is to gather information (what is the barrier trying to protect, what are the time and budget constraints, how many barriers are required, etc.) and specify target values (target B, T, attack difficulty level, etc.). It is important to understand what information the barrier is trying to protect, as well as understand the competitor's ability to extract that information.

Different barriers are more effective in different scenarios. If the goal is to impede consumers from discovering what components are used in an electrical circuit, some have found an effective barrier to be encoding labels for resistors and capacitors in the electronics (McLoughlin 2008). If the goal is to protect proprietary information, creating a product that cannot be opened without destruction of critical components may be a sufficient barrier. If the goal is to increase the required skills and resources of competitors, one may use material microstructures that are anisotropic, heterogeneous, and are difficult to detect or reproduce. By understanding what information needs to be protected, the design team can determine if multiple small barriers will be more effective or a single large barrier. Multiple small barriers are beneficial as they require competitors to solve several problems that may be completely independent. A careful review of the metrics in Sect. 3 shows that the difficulty of overcoming multiple independent barriers is more than the sum of those same barriers. If only a single barrier is implemented, and competitors are able to efficiently overcome the barrier, the information may not be adequately protected. However, a

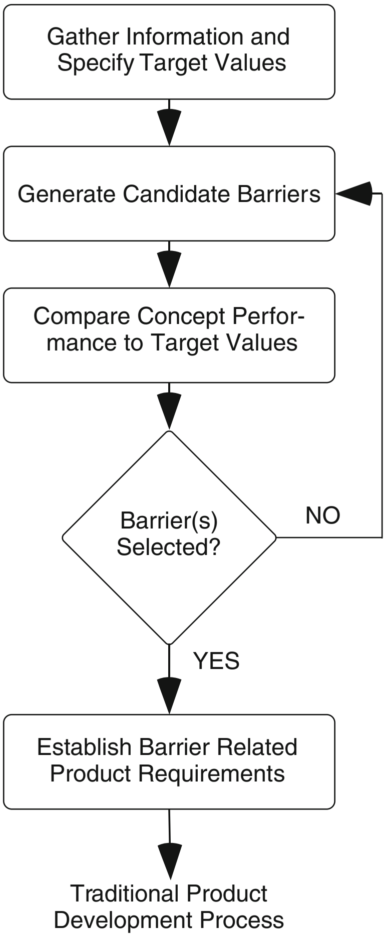
Gather Information and Specify Target Values
Generate Candidate Barriers
Compare Concept Performance to Target Values
Barrier(s) Selected?
NO
YES
Establish Barrier Related Product Requirements
Traditional Product Development Process

Fig. 4 Barrier implementation methodology

single large barrier, if sufficiently difficult to overcome, may be the best protection. Some questions to be answered during this step might include:

- What information is the barrier trying to protect?
- Are the resources available to implement the barrier? If not, are we willing to acquire the resources?
- What resources are available to competitors?
- A cost-efficient barrier may be to implement a barrier in an area that we are experienced in and competitors are not. Does such an area exist?
- When is the barrier going to be implemented into the product? Now? 2 years?
- Does there exist barriers from other products that can be directly implemented?

These types of questions help define the nature of the required barriers. Discovering this information is a critical first step to strategic barrier creation.

In the first step, we also specify target values. By target values, we mean target development cost of the barrier, length of development time, and importantly, target values of B and T and/or level of attack difficulty. In Sect. 3, we reviewed qualitative and quantitative metrics that can be used to systematically characterize the barrier to reverse engineer any product. While both the qualitative and quantitative metrics can quantify B, only the quantitative metrics estimate T. In general, both of the metrics are simply methods for comparing one product with another in a systematic and standardized manner. An effective way to determine a target barrier is to select a benchmark product, use the metrics to determine the barrier of the benchmark product and then decide how much of an improvement over the benchmark product is desired.

The second step toward implementing barriers to reverse engineering into a product is to generate candidate barriers. As we discussed in Sec. 2, barriers to reverse engineering generally exist in three forms (product complexity, resource availability, and reverse engineering skill); however, the original designer only has a direct influence over the product complexity. This is consistent with the quantitative metrics, in that the original designer can directly affect the amount or type of K, and can only indirectly affect F or P. In general, the most efficient barriers are those that decrease the rate at which information can be extracted. Therefore, the designer can use this influence to increase the required skill and necessary resources to successfully reverse engineer their product. Candidate barriers will vary from industry to industry, and generating effective candidate barriers will come with experience, however, here we list a few generic barriers that might serve as a catalyst for concept generation in specific applications:

- Design components that are difficult to access (Grand 2004)
- Require unique tools to extract information (Campbell and Flynn 2001; Grand 2004)
- Require unique skills to extract information (Reed and DeFillippi 1990)
- Avoid explicitly disclosing information such as labels on electrical components (McLoughlin 2008; Grand 2004; Naumovich and Memon 2003)
- Obfuscate information (McLoughlin 2008)
- Avoid standard sizes (Suvorov 1981)
- Increase or decrease geometric scale (Musker 1998; James 2006)
- Couple component functions (von Hippel 1998)
- Design components that self destruct when tampered with Pooley and Graves (2008), Dam and Lin (1996), Grand (2004)
- Remove evidence of manufacturing processes (Harston and Mattson 2010a)
- Create anti-robust designs—components only work at within a small tolerance (McLoughlin 2008)
- Design components that require multiple disciplines that are typically not coupled (Reed and DeFillippi 1990)

- Design a component to appear, or have the performance, of another component (Livingston 2007)
- Design a critical component to look like an insignificant component (Livingston 2007) or vice versa (McLoughlin 2008)
- Design components that look different but have the same function (Harston and Mattson 2010a) or vice versa (Naumovich and Memon 2003)
- Design and implement multiple functionally-equivalent configurations of the same product (Dube et al. 2008)

While not all of these candidate barriers may always be practical to implement, the goal is to make the competitors spend time and resources on gathering information that is either not needed or require them to extract information that is expensive (either in time and/or resources). Ideally, any barrier introduced would require multiple iterations through the reverse engineering process (seen in Fig. 1). It is important to note that a barrier does not need to be impossible to overcome. Some believe that a barrier is sufficient when competitors spend as much time and resources as was spent in developing the original product, (Dam and Lin 1996; Grand 2004) while others believe that a barrier is sufficient if it can keep competitors out of the market until market saturation (Knight et al. 2009).

Following the flow chart in Fig. 4, the third step is to compare the performance of the candidate barriers to the target values of *B* and *T*. This is done by utilizing the metrics presented in Sect. 3. Candidate barriers that do not meet the specified requirements are removed.

For the fourth step, the designer must either choose one (or more) of the remaining barriers or generate additional candidates with more favorable characteristics. While some implementable barriers may simultaneously increase product performance (Harston and Mattson 2010a), other barriers may have adverse effects in other performance areas of the product (Christiansen et al. 2006). In the case of the latter, the designer must balance the benefits of increased security against potentially increased implementation costs, decreased system performance, and increased maintenance costs (Christiansen et al. 2006). This selection process can be facilitated with any multi-objective optimization routine, a weighted algorithm, or a scoring matrix similar to those used in a product development process (Ulrich and Eppinger 2004).

The final box in Fig. 4 is to establish barrier related requirements. In a typical product development process, product requirements are derived from customer specifications. The barrier related product requirements are additional product requirements that must be met to effectively implement the desired barrier(s) into the product. Contingent upon a successful product development process with the new requirements, the added/improved feature(s) will increase the difficulty to reverse engineer the product without greatly degrading the performance of other product features, and in some cases improve product performance.

5 Simple case study: cantilever L-beam

The purpose of this case study is to illustrate how to strategically make a simple device more difficult to reverse engineer, using the principles of the barrier implementation methodology presented in Sec. 4. We begin with a simple cantilever L-beam of pure copper, as shown by the benchmark L-beam in Fig. 5. One end of the beam is rigidly attached while a force is applied to the free end to make the end of the beam undergo a deflection, δ. A similar beam is actually located in some cell phones as part of an electrical connector assembly (Knight et al. 2009), and it plays an important role in keeping consistent electrical contact in the circuitry of a phone. Thus, it would be reasonable to need to protect this device against comparable cell phone manufacturers, who may attempt to reverse engineer the L-beam for numerous reasons (see Sect. 1).

The first step of the barrier implementation methodology, as discussed in Sect. 4, is to gather information and specify target values. For the design of the L-beam, we determined what skills and resources are available and what skills and resources are likely unavailable to competitors. We have the ability to analyze and design for both geometry *and* material microstructures. Microstructure analysis and design requires uncommon skills and tools (scanning electron microscope, orientation imaging software, etc.). It is likely that the entities that are interested in reverse engineering the L-beam electrical connector will not have access to these resources. Therefore, we sought to incorporate barriers that utilize microstructure design. Ideally, we would design and implement a reverse engineering barrier into the L-beam that is practically impossible to overcome. However, that large of a barrier may require a significant amount of time and resources to develop and implement. A more reasonable barrier is one that requires competitors to spend at least as much time reverse engineering the L-beam as we spent developing the original product. With this perspective in mind, we specified target values for *B* and *T*.

The reverse engineering barrier, *B*, can be specified with either qualitative or quantitative measures—both of which are presented in Sect. 3—and the time to reverse engineer a product, *T*, can be specified with the quantitative metrics. Performance standards in other areas may also be set here. As a reference, using the qualitative metrics, we classify the benchmark L-beam as a level 3, and using the qualitative metrics, the benchmark has a barrier of 2.36 * 10^3

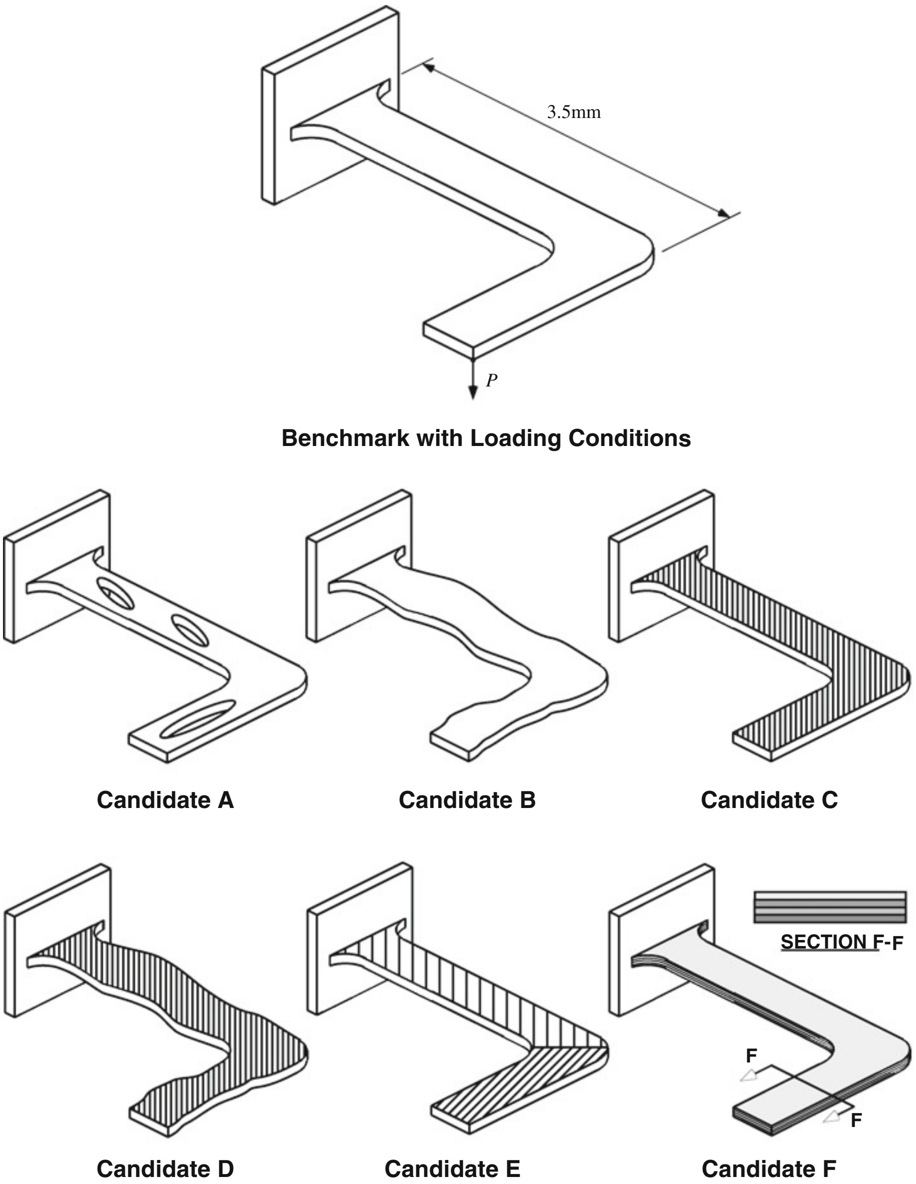

Fig. 5 L-beam designs incorporating candidate barriers

and is expected to take 2.73 * 10^3 s to reverse engineer. For this case study, we want to increase the qualitative difficulty of the L-beam to be greater than a level 5 (signifying the need for *highly specialized tools and expertise*), increase the total quantitative barrier, B^*, to be greater than 5.00 * 10^4, and increase the total time to reverse engineer the L-beam, T^*, to be greater than 1.00 * 10^5 s, or roughly greater than one day—which is greater than the time spent to develop the L-beam benchmark. While there are many different performance qualities of the beam that could be considered (heat transfer characteristics, electrical conductivity, weight, etc.) we have chosen to limit the discussion to a prescribed deflection under a static load. Additionally, we have chosen to make each candidate design undergo the same deflection under the same load. This is to illustrate how devices with the same functional performance can vary widely with respect to how difficult they are to reverse engineer.

The second step of the barrier implementation methodology is to generate candidate barriers. A few candidate barriers generated for the L-beam include the following: increasing geometric complexity by adding holes or curved features, strategically orienting anisotropic material microstructures to benefit mechanical performance, using heterogeneous materials to benefit mechanical performance, or any combination of the candidate barriers.

The third step of the barrier implementation methodology is to compare concept performance to target values. To do this, it is important that the barriers generated in the previous step are embodied into a preliminary design. This enables a direct comparison between the benchmark designs and the candidate barrier designs. Based upon the benchmark product, we have generated six L-beam designs incorporating a combination of the barriers generated above. The designs are shown as Candidates A through F in Fig. 5. In each case, we alter the geometry and/or material microstructure of the L-beam in an attempt to increase product complexity, and require uncommon tools and/or skills (see Sect. 2), thereby increasing the reverse engineering time and barrier. We now describe each L-beam candidate design shown in Fig. 5 in greater detail:

- *Benchmark* The L-beam is made out of pure, homogeneous, isotropic copper. The L-beam can be reverse engineered with common tools such as vernier calipers and radius gages.
- *Candidate A* This candidate takes the benchmark design and subtracts three elliptical holes, thereby adding more geometric information to the L-beam. While there is more information to extract, the same extraction tools that can be used to reverse engineer the benchmark can be used to reverse engineer this candidate.
- *Candidate B* This candidate adds curves to the exterior of the benchmark L-beam. These curves require uncommon measurement tools to be reverse engineered easily, such as an optical comparator or a coordinate measuring machine.
- *Candidate C* This candidate couples the geometry of the benchmark L-beam with a single, strategically oriented, anisotropic copper layer. The material microstructure now plays an integral part in the L-beam's performance, thereby requiring this information to be extracted from the product. This requires highly specialized skills and tools such as a scanning electron microscope and OIM software.
- *Candidate D* This candidate combines the geometry of Candidate B with the material anisotropy of Candidate C.
- *Candidate E* This candidate is composed of a heterogeneous copper material, created by a process called friction stir welding (Owen 2006). This L-beam can be reverse engineered with the same tools as candidates C and D; however, there are two material microstructures that need to be identified and analyzed.
- *Candidate F* This candidate utilizes ultrasonic consolidation (Harston and Mattson 2010a) to create an L-beam with four, thin, anisotropic, copper layers, each independently oriented, to achieve the desired performance. This results in four different material microstructures, each of which needs to be identified and analyzed. Furthermore, ultrasonic consolidation can be virtually undetectable to the naked eye, potentially disguising the layers as one single layer to anyone reverse engineering the L-beam.

We first analyzed each L-beam with the finite element analysis software ANSYS to ensure that (i) the L-beam achieved the desired deflection of $-1.50 * 10^{-4}$ m under a load of about 0.60 N and (ii) the L-beam did not plastically deform. We also determined, qualitatively and quantitatively, the reverse engineering barrier and time for each L-beam candidate. As discussed in Sect. 3, we need to first identify the quantity of information, K, the rate at which that information can be extracted, F, and the effort, P, put into extracting the information contained by the L-beams (i.e., geometry, material, and material microstructure).

The method used to quantify K, F, and P, does not matter so long as accuracy is ensured. The accuracy of the reverse engineering estimations of T, and B, are dependent upon the accuracy of K, F, and P. Numerous papers from the literature discuss how to reverse engineer geometric features utilizing CAD systems (Várady and Facello 2005; Stamati and Fudos 2007; Li et al. 2010. Toledo et al. (2008) present an efficient method by which geometric information may be determined, even from complicated systems, in an effort to determine original geometric data. Várady et al. (2007) present an automated approach to create CAD representations of structures that are accurate, capture design intent, and require little or no user assistance. Many of these methods may be used directly to estimate the quantity of geometric information, K_g, contained by a product. By recording the length of time to extract the geometric information, an estimation of the rate at which geometric information is extracted, F_g, can also be determined.

While the information-extraction methods presented above may be effective for large systems, for simple parts, such as the cantilever L-beam, it may be better to simply count the quantity of geometric information. The method that we use to quantify the geometric features of simple parts is based upon the degrees-of-freedom analysis often found in many CAD systems where algorithms determine when a sketch is over, or under, constrained. With this approach, the minimum number of independent geometric dimensions, K_g, required to fully constrain the geometric features in a global 2-D reference frame is

$$K_g = D - C \tag{8}$$

where D is the degrees of freedom, and C is the number of active constraints. For the current examples, we are only interested the degrees of freedom in 2-D. It follows that

$$D = 4N_L + 5N_A + 5N_E \tag{9}$$

and

$$C = 2N_C + N_T \tag{10}$$

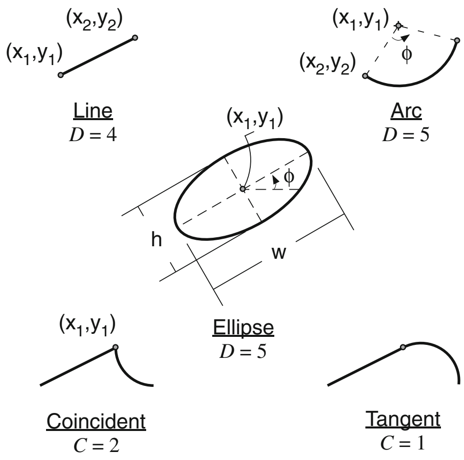

Fig. 6 Degrees of freedom for a line, arc, & ellipse. Constraints for coincident and tangent features

where N_L, N_A, and N_E are the number of lines, arcs, and ellipses, respectively, and N_C, and N_T are, respectively, the number of coincident and tangent constraints. The numbers in front of N_L, N_A, and N_E denote the degrees of freedom for each feature. Also notice that N_C is multiplied by 2. This is because when a point is coincident with another point, two degrees of freedom are removed—one in the x-direction and one in the y-direction when a cartesian coordinate system is used. A summary of the degrees of freedom and constraints for the features used in this paper may be seen in Fig. 6. Note that Eq. 8 defines the absolute position of a geometric feature. If desired, Eq. 8 can be modified to only consider degrees of freedom required to constrain geometric features in a relative manner. Inserting Eqs. 9 and 10 into Eq. 8 results in

$$K_g = 4N_L + 5N_A + 5N_E - 2N_C - N_T \tag{11}$$

which is the equation that is used for the L-beam candidates in determining the quantity of geometric information. To account for the thickness dimension of each L-beam, we add one (1) to the K_g obtained with Eq. 11. Note that we did not assume that lines are parallel or perpendicular, and we also did not assume that the arcs have the same radii. If desired, Eq. 11 can be modified to represent additional constraints. While this method of determining geometric information may be used for any product or feature, the automated CAD approaches (de Toledo et al. 2008; Várady et al. 2007) are likely to be more efficient when analyzing complicated products and systems.

While understanding geometric information is critical to developing (or overcoming) barriers to reverse engineering, arguably the most efficient barriers will be material related.(Harston and Mattson 2010a). As such, we also analyze the L-beams from the material perspective. The amount of material information, K_m is determined by how many different materials (without regard to material microstructure) each L-beam candidate includes. Likewise, the amount of material microstructure information, K_{mm}, contained by each L-beam is based on the number of unique microstructures present.

The flow rate, F, for each information type was determined from the authors' experience and with information-extraction tests similar to those described in Harston and Mattson (2010b). Additionally, We took a conservative approach by assuming P to be equal to one (1) for all information types in each candidate, implying that a competitor would exert a full effort in their reverse engineering attempts. These parameters are listed in Table 3. With K, F, and P defined, we used Eqs. 1, 3, 4, 6 and 7 to determine the B^* and T^* of each candidate L-beam. The results of this analysis are listed in Table 4.

Using these results, the barrier selection process—the fourth step of the barrier implementation methodology—becomes significantly easier to perform. Candidates A and B do not meet the reverse engineering time requirement (T^* greater than 1.00 * 10^5 s), while Candidate D does not meet the barrier requirement (B^* greater than 5.00 * 10^4). Therefore, they are removed from the candidate pool. An interesting result is that Candidate C has a larger barrier than Candidate D, although Candidate D would appear to be more complex. This phenomena is explained by examining the meaning of B^*, which is a measure of the difficulty to extract *any* pertinent information from the device. We see that since Candidate D contains more geometric information, which comparatively is easier to extract than material or microstructure information, it has a lower barrier than Candidate C. In other words, the average difficulty to extract a unit of pertinent information from Candidate D is less than the average difficulty to extract a unit of pertinent information from Candidate C. In this case, the time required to reverse engineer Candidate D is larger, simply because there is more information to extract. This exemplifies the distinct nature of B^* and T^*.

As all the remaining candidates meet the established reverse engineering requirements, additional criteria are

Table 3 Parameters for calculating the quantitative barrier and time to reverse engineer each L-beam candidate

L-Beam	Geometry (F = 6.10E-02) (P = 1)	Material (F = 1.67E-03) (P = 1)	Material microstructure (F = 2.78E-05) (P = 1)
Benchmark	$K = 19$	$K = 1$	$K = 0$
Candidate A	$K = 34$	$K = 1$	$K = 0$
Candidate B	$K = 49$	$K = 1$	$K = 0$
Candidate C	$K = 19$	$K = 1$	$K = 1$
Candidate D	$K = 49$	$K = 1$	$K = 1$
Candidate E	$K = 19$	$K = 1$	$K = 2$
Candidate F	$K = 19$	$K = 1$	$K = 4$

Table 4 Barrier performance results for the L-beam benchmark and barrier candidates

L-beam	δ (m)	Force (N)	Beam thickness (m)	Attack classification	$B^* * 10^3$	$T^* * 10^3$ (s)
Benchmark	−1.50E-04	−0.602	2.90E-04	3	2.36	2.73
Candidate A	−1.50E-04	−0.601	3.08E-04	3	1.67	3.47
Candidate B	−1.50E-04	−0.599	2.73E-04	4	1.41	4.21
Candidate C	−1.50E-04	−0.601	3.38E-04	5	95.4	111
Candidate D	−1.50E-04	−0.604	3.18E-04	5	37.5	112
Candidate E	−1.50E-04	−0.600	3.53E-04	5	188	219
Candidate F	−1.50E-04	−0.601	3.25E-04	5	374	435

needed to distinguish the candidates from one another. If manufacturing cost is the most important objective, than Candidate C may be optimal, as it only requires the material to be strategically oriented during the manufacturing process with no need for expensive welding equipment.

The fifth and final step of the barrier implementation methodology is to establish barrier related product requirements. Assuming Candidate C was selected to be implemented, some additional product requirements might include: material properties must be homogeneous, L-beam must be manufactured in a single plane, and material thickness is constrained since it is difficult to obtain thick sheets of strongly anisotropic materials.

It is clear from the results of this case study that the barrier and time to reverse engineer a mechanical component can be manipulated in a strategic manner. For instance, the predicted time to reverse engineer Candidate F is about 160 times greater than the benchmark. This is a significant increase, especially considering that a conservative approach was used. Conservative because we assumed that a reverse engineering team would immediately discern the existence of four disparate material microstructures without iteratively performing the reverse engineering process. In reality, the team reverse engineering the L-beams would likely initially miss this information, as layers that are welded together with ultrasonic consolidation are difficult to detect without the proper skills and equipment. Even if the team has the required skills and equipment, it is still likely to require multiple iterations before the microstructure is reverse engineered. Additionally, we note that the L-beam is a simple device. If this methodology were applied to a more technically complex product—which may include multiple component interactions—then the methodology can aid in potentially creating powerful, if not insurmountable, barriers to reverse engineering.

6 Concluding remarks

In this paper, we have presented several fundamental principles behind the difficulties to reverse engineering. Barriers can be present at any step in the reverse engineering process and come in a variety of forms. The magnitude of a barrier to reverse engineer a product is directly proportional to the technical complexity of the product, while inversely proportional to the skill of the reverse engineering team and the availability of the necessary resources. Original designers can influence the magnitude of internal barriers to reverse engineering, while those reverse engineering can affect external barriers. Additionally, we have presented a methodology—which is used in conjunction with the traditional product development process—that enables designers to strategically design products with built-in barriers to reverse engineering. When implemented, these barriers to reverse engineering impede competitors from extracting critical information from innovative products, thus enabling the innovative product to maintain its competitive advantage.

Acknowledgments This research was supported by National Science Foundation Grant CMMI-0800904 for Christopher A. Mattson and Brent L. Adams.

References

Abraham DG, Dolan GM, Double GP, Stevens JV (1991) Transaction security system. IBM Syst J 30(2):206–229

Adams BL, Kalidindi SR, Fullwood DT (2005) Microstructure sensitive design for performance optimization. BYU Academic Publishing, Provo

Ali F, Chowdary B, Imbert C (2008) Part design and evaluation through reverse engineering approach. In: The 2008 IAJC-IJME international conference

Barbero BR (2009) The recovery of design intent in reverse engineering problems. Comput Ind Eng 56(4):1265–1275

Boyne WJ (2009) Carbon copy bomber. Air Force Mag 92(6):52–56

Bradley C, Currie B (2005) Advances in the field of reverse engineering. Comput Aided Des Appl 2(5):697–706

Campbell RJ, Flynn PJ (2001) A survey of free-form object representation and recognition techniques. Comput Vis Image Underst 81:166–210

Christiansen BD (2006) Active FPGA security through decoy circuits. Master's thesis, Air Force Institute of Technology

Christiansen BD, Kim YC, Bennington RW, Ristich CJ (2006) Decoy circuits for FPGA design protection. In: IEEE international conference on field programmable technology. pp 373–376

Creehan KD, Bidanda B (2006) Rapid prototyping: theory and practice, Springer US, chap reverse engineering: a review & evaluation of non-contact based systems. pp 87–106

Curtis SK, Harston SP, Mattson CA (2009) A generic formulaic characterization of the time to reverse engineer the tolerances of a product. In: ASME IMECE 2009, Lake Buena Vista, Florida, USA, IMECE2009-13123

Dam KW, Lin HS (1996) Cryptography's role in securing the information society. National Academy Press, Washington, D.C.

Danelek JA (2008) UFOs: the great debate. Llewellyn Publications, Woodbury

Dube TE, Birrer BD, Raines RA, Baldwin RO, Mullins BE, Bennington RW, Reuter CE (2008) Hindering reverse engineering: thinking outside the box. IEEE Secur Priv 6:58–64

Fernandes KJ (2008) Reverse engineering: an industrial perspective, chap 11. Springer, London, pp 207–218

Grand J (2004) Practical secure hardware design for embedded systems. In: Proceedings of the 2004 embedded systems conference

Grimm T (2004) Reverse engineering is criminal. Tech. rep., Time Compression Technologies

Grimm T (2006a) A guide to reverse engineering. Tech. rep., Time Compression Technologies

Grimm T (2006b) Reverse engineering—3D scanning selection guide. Tech. rep., Time Compression Technologies

Harrington HJ (1991) Business process improvement: the breakthrough strategy for total quality, productivity, and competitiveness. McGraw-Hill Professional

Harston SP, Mattson CA (2010a) Capitalizing on heterogeneity and anisotropy to design desirable hardware that is diffcult to reverse engineer. J Mech Des 132:081001

Harston SP, Mattson CA (2010b) Metrics for evaluating the barrier and time to reverse engineer a product. J Mech Des 132:041,009 (p 9)

von Hippel E (1998) Economics of product development by users: the impact of "sticky" local information. Manag Sci 44:629–644

Hsiao SW, Chuang JC (2003) A reverse engineering based approach for product form design. Des Stud 24(2):155–171

Ingle KA (1994) Reverse engineering. McGraw-Hill, New York, NY

James D (2006) Reverse engineering delivers product knowledge, aids technology spread. Tech. Rep. ED Online ID #11966, Electronic Design, http://electronicdesign.com/Articles/ArticleID/11966/11966.html

Knight DC, Mattson CA, Adams BL (2009) Maximizing return on investment by constructing optimal barriers against competitors' market entry. In: 50th AIAA/ASME/ASCE/AHS/ASC structures, structural dynamics, and materials conference. AIAA, Palm Springs, pp 2009–2224

Li M, Langbein FC, Martin RR (2010) Detecting design intent in approximate cad models using symmetry. Comput Aid Des 42:183–201

Livingston H (2007) Avoiding counterfeit electronic components. IEEE Trans Compon Packag Technol 30:187–189

Macmillan I, McCaffery ML, van Wijk G (1985) Competitors' responses to easily imitated new products-exploring commercial banking product introductions. Strateg Manag J 6(1):75–86

Maskus KE, Dougherty SM, Mertha A (1998) Intellectual property rights and economic development in China. In: Conference on intellectual property rights and economic development

McEvily AJ (2005) Reverse engineering gone wrong: a case study. Eng Fail Anal 12:834–838

McLoughlin I (2008) Secure embedded systems: the threat of reverse engineering. In: ICPADS '08: proceedings of the 2008 14th IEEE international conference on parallel and distributed systems. IEEE Computer Society, pp 729–736

Mohaghegh K, Sadeghi MH, Abdullah A (2007) Reverse engineering of turbine blades based on design intent. Int J Adv Manuf Technol 32:1009–1020

Mowery KA, Blanchard DE, Smith S, Betts TA (2004) Investigation of imposter perfumes using GC-MS. J Chem Educ 81:87–89

Musker DC (1998) Reverse engineering. In: Protecting and exploiting intellectual property in electronics, IBC conferences, 10 June 1998

Naumovich G, Memon N (2003) Preventing piracy, reverse engineering, and tampering. IEEE Comput Soc 36:64–71

Nelson ML (1996) A survey of reverse engineering and program comprehension. In: In ODU CS 551—Software Engineering Survey

Norby MO (1978) Soviet aerospace handbook. Department of the US Air Force

Ohly A (2009) Patents and technological progress in a globalized worlda, 6th edn, Springer-Verlag, chap reverse engineering: unfair competition or catalyst for innovation?, pp 535–552

Ohm GS (1827) Die galvanische Kette, mathematisch bearbeitet. T. H. Riemann, Berlin

Otto K, Wood K (2001) Product design. Prentice Hall, Upper Saddle River

Owen CB (2006) Two dimensional friction stir welding model with experimental validation. Master's thesis, Brigham Young University

Pal DK, Ravi B, Bhargava LS, Chandrasekhar U (2006) Computer-aided reverse engineering for replacement parts: a case study. Def Sci J 56(2):225–238

Pooley J, Graves CT (2008) Trade secrets. Law Journal Press, New York

Raja V (2008) Reverse engineering: an industrial perspective, chap 1. Springer, London, pp 1–9

Reed R, DeFillippi RJ (1990) Casual ambiguity, barriers to imitation, and sustainable competitive advantage. Acad Manag Rev 15:88

Samuelson P, Scotchmer S (2002) The law and economics of reverse engineering. Yale Law J 111(7):1575–1663

Sarkar B, Menq CH (1991) Smooth-surface approximation and reverse engineering. Comput Aided Des 23(9):623–628

Shapiro C (1985) Patent licensing and r & d rivalry. Am Econ Rev 75:25–30

Soo SMK, Yuen EMW, Yu KM (2005) Reverse engineering of a bamboo-net handicraft. In: IEEE ninth international conference on computer aided design and computer graphics

Stamati V, Fudos I (2007) A feature based approach to re-engineering objects of freeform design by exploiting point cloud morphology. In: Proceedings of the 2007 ACM symposium on solid and physical modeling, vol 2. pp 1–9

Summers JD, Shah JJ (2010) Mechanical engineering design complexity metrics: size, coupling, and solvability. J Mech Des 132:021,004 (p 11)

Suvorov V (1981) The liberators: inside the Soviet army. New English Library, London

Thompson WB, Owen JC, de St Germain HJ, Stark SR, Henderson TC (1999) Feature-based reverse engineering of mechanical parts. IEEE Trans Robot Autom 15(1):57–66

de Toledo R, Levy B, Paul JC (2008) Reverse engineering for industrial-plant cad models. In: Tools and methods for competitive engineering, Izmir, Turkey. pp 1021–1034

Ulrich KT, Eppinger SD (2004) Product design and development, 3rd edn. McGraw-Hill/Irwin, Boston

Urbanic RJ, ElMaraghy WH (2009) Using a modified failure modes and effects analysis within the structured design recovery framework. J Mech Des 131:111,005 (13 pages)

USAF (1944) Boeing b-29. http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=2527

Várady T (2001) Reverse engineering shapes. ERCIM News 44:19–20

Várady T, Facello MA (2005) New trends in digital shape reconstruction. Math Surf XI 3604:395–412

Várady T, Martin RR, Cox J (1997) Reverse engineering of geometric models: an introduction. Comput Aided Des 29:255–268

Várady T, Facello MA, Terék Z (2007) Automatic extraction of surface structures in digital shape reconstruction. Comput Aided Des 39:379–388

Weingart SH, White SR, Arnold WC, Double GP (1990) An evaluation system for the physical security of computing systems. In: The sixth annual computer security applications conference. pp 232–243