**1. Introduction:**

The world has witnessed three digital convergences during the past three decades. Each time new technologies break down the barrier between physical and digital forms, new products and new markets has been created. The 1970s ushered in digitized sound using signal processing (1D), which made analog and digital conversion part of a common language in the telecom industry. The 1980s brought digitized fonts and pictures using image processing (2D). The convenience of switching between electronic and paper documents changed the publishing industry and the way to store and share information. The third convergence, beginning in the 1990s, focus on digitizing the physical world using geometry processing (3D). The convergence of physical and digital worlds enabled by reverse and forward engineering technologies should fundamentally change the way products are designed, manufactured, and marketed. By create a digital duplicate of world as easily as taking a digital picture, the biggest breakthrough of the twenty-first century will be in manufacturing industry.

Reverse engineering can be applied to re-create either the high-value commercial parts for business profits or the valueless legacy parts for historical restoration. To accomplish this task, the engineer needs an understanding of the functionality of the original part and the skills to replicate its characteristic details. In the fields of mechanical engineering and industrial manufacturing, reverse engineering refers to the method of creating engineering design and documentation data from existing parts and their assemblies. While in conventional engineering process, transforms engineering concepts and models into real parts, in the reverse engineering approach real parts are transformed into engineering models and concepts. Reverse engineering has a very common a broad range area such as mechanical engineering, software engineering, animation/entertainment industry, microchips, chemicals, electronics, pharmaceutical products etc. Focusing on the mechanical engineering domain, through the application of reverse engineering techniques an existing part is recreated by acquiring its’ surface or geometrical features data using contact or non contact digitizing or measuring devices. By using reverse engineering, creation of product takes advantage of the extensive use of CAD/CAM/CAE systems. And apparently provides enormous gains in improving in quality, materials properties, efficiency of re-design, manufacture and analysis. Therefore, reverse engineering is going with substantial business benefits in shortening the product development cycle.

Reverse engineering has been used to produce many mechanical parts, such as seals, O-rings, bolts and nuts, gaskets, and engine parts, and is widely used in many industries (Tut, 2010). The Society of Manufacturing Engineers (SME) states that the practice of reverse engineering “starting with a finished product or process and working backward in logical fashion to discover the underlying new technology” (Francis, 1988). Manufacturers all over the world have practiced reverse engineering in their product development. The new analytical technologies, such as three dimensional (3D) laser scanning and high-resolution microscopy, have made reverse engineering easier, but there is still much more to be learned. Several professional organizations have provided the definitions of reverse engineering from their perspectives. It has been incorporates in appropriate mechanical design and manufacturing engineering standards and multiple realistic product constraints with broad knowledge in multiple disciplines such as:

The part produced through reverse engineering should be in compliance with the requirements contained in applicable program criteria. To achieve a successful reverse engineering process requires. Though it roots back to ancient times in history, the recent advancement in reverse engineering has elevated this technology to one of the primary methodologies utilized in many industries, including aerospace, automotive, consumer electronics, medical device, sports equipment, toy, and jeweller. It is also applied in forensic science and accident investigations.

**1.1 Literature Review:**

Reverse engineering was often used during the Second World War and the Cold War. It is often used by military in order to copy other nation’s technology, devices or information, or parts of which, have been obtained by regular troops in the fields or by intelligence operations. In the last few years, increased computational power, more computer memory, and high-speed contact or non-contact scanning devices, discrete geometry has gained increasing importance in automotive design, manufacturing, and quality assurance. In recent year, the impact of reverse engineering in manufacturing industry is increase day per day and it also plays a significant role in promoting industrial evolution by just introducing the expensive products and stimulating additional competition. However, the average life cycle of modern inventions is much shorter. To accommodate this rapid rate of reinvention of modern machinery and instruments, reverse engineering provides a high-tech tool to speed up the reinvention process for future industrial evolution. Reverse engineering plays a significant role in the aviation industry primarily because of the following reasons: maturity of the industry, advancement of modern technologies, and market demands. From the dawn of the aviation industry in the early 1900s to its hardware maturity with the development of jet aircraft in the 1950s, the aviation industry revolutionized the modes of transportation in about 50 years.[1]

**1.2. What is Reverse Engineering?[2]**

Engineering is the process of designing, manufacturing, assembling, and maintaining products and systems. There are two types of engineering, forward engineering and reverse engineering. Forward engineering is the traditional process of moving from high-level abstractions and logical designs to the physical implementation of a system. In some situations, there may be a physical part/ product without any technical details, such as drawings, bills-of-material, or without engineering data. The process of duplicating an existing part, subassembly, or product, without drawings, documentation, or a computer model is known as reverse engineering. Reverse engineering is also defined as the process of obtaining a geometric CAD model from 3-D points acquired by scanning/ digitizing existing parts/products. The process of digitally capturing the physical entities of a component, referred to as reverse engineering (RE), is often defined by researchers with respect to their specific task (Motavalli & Shamsaasef 1996). Abella et al. (1994) described RE as, “the basic concept of producing a part based on an original or physical model without the use of an engineering drawing”. Yau et al.(1993) define RE, as the “process of retrieving new geometry from a manufactured part by digitizing and modifying an existing CAD model”. According to business dictionary “Legally sanctioned method of copying a technology which (as opposed to starting from scratch) begins with an existing product and works backward to figure out how it does what it does. When the product's basic principle or core concept is determined, the next step is to reproduce the same results by employing different mechanisms to avoid any (legally forbidden) patent infringement.

Reverse engineering is now widely used in numerous applications, such as manufacturing, industrial design, and jewelry design and reproduction For example, when a new car is launched on the market, competing manufacturers may buy one and disassemble it to learn how it was built and how it works. In software engineering, good source code is often a variation of other good source code. In some situations, such as automotive styling, designers give shape to their ideas by using clay, plaster, wood, or foam rubber, but a CAD model is needed to manufacture the part. As products become more organic in shape, designing in CAD becomes more challenging and there is no guarantee that the CAD representation will replicate the sculpted model exactly. Reverse engineering provides a solution to this problem because the physical model is the source of information for the CAD model. This is also referred to as the physical-to-digital process depicted in Figure 1.1 Another reason for reverse engineering is to compress product development cycle times. In the intensely competitive global market, manufacturers are constantly seeking new ways to shorten lead times to market a new product. Rapid product development (RPD) refers to recently developed technologies and techniques that assist manufacturers and designers in meeting the demands of shortened product development time.



**Figure 1.1:** Physical-to-digital process

For example, injection-molding companies need to shorten tool and die development time drastically. By using reverse engineering, a three-dimensional physical product or clay mock-up can be quickly captured in the digital form, remodeled, and exported for rapid prototyping/tooling or rapid manufacturing using multi-axis CNC machining techniques.

**1.3 Why Use Reverse Engineering?**

Reverse engineering is a multidisciplinary approach and virtually can be applied to industrial field universally. The prime applications of reverse engineering are either to re-create a copy of part of the original part or retrace the events of what happened. It is widely used in software and information technology industries, from software code development to Internet network security. Thousands of parts are reinvented every year using reverse engineering to satisfy the aftermarket demands that are worth billions of dollars. The invention of digital technology has fundamentally revolutionized it. Compared to the aviation and automobile industries, the applications of digitalized reverse engineering in the life science and medical device industries have faced more challenges and advanced at a more moderate pace. However, some briefly description has been presented with reverse engineering applications as follows:

Following are some of the reasons for using reverse engineering:

* 1. The original manufacturer no longer exists, but a customer needs the product, e.g., aircraft spares required typically after an aircraft has been in service for several years.
  2. The original manufacturer of a product no longer produces the product, e.g., the original product has become obsolete.
  3. The original product design documentation has been lost or never existed.
  4. Creating data to refurbish or manufacture a part for which there are no CAD data, or for which the data have become obsolete or lost.
  5. Inspection and/or Quality Control–Comparing a fabricated part to its CAD description or to a standard item.
  6. Some bad features of a product need to be eliminated e.g., excessive wear might indicate where a product should be improved.
  7. Strengthening the good features of a product based on long-term usage. • Analyzing the good and bad features of competitors’ products.
  8. Exploring new avenues to improve product performance and features.
  9. Creating 3-D data from a model or sculpture for animation in games and movies.
  10. Creating 3-D data from an individual, model or sculpture to create, scale, or reproduce artwork.
  11. Architectural and construction documentation and measurement.
  12. Fitting clothing or footwear to individuals and determining the anthropometry of a population.

**1.4 Stages of Reverse Engineering:[3]**

**1.4.1 Implementation recovery:** Quickly learn about the application and prepare an initial model. The first task is to browse existing documentation and learn about an application. The resulting context clarifies the developer's intent and makes it easier to communicate with application experts

The next step is to enter the database structure into a modeling tool by typing or automation. Some tools can read the system tables of an RDBMS and seed a model. Using these tools will make easier to least skim the database structure to get a feel for the development style. There are four steps to converting database structures into a model.

1. **Create tentative entity types**: Represent each physical data unit (COBOL record, IMS segment, CODASYL record type, or RDBMS table) as an entity type7. Give each entity type the same name as its corresponding physical data unit.
2. **Create tentative relationship types:** For a CODASYL application, represent the set types as relationship types. Otherwise, defer relationship types until design.
3. **Create tentative attributes:** The data elements in the legacy system become attributes of the entity types. Indicate not-null restrictions, data types, and lengths if the information is available.
4. **Note keys and indexes:** Note primary keys, candidate keys, and foreign keys if they happen to be defined. Otherwise, unique and secondary indexes has to be noted.

**1.4.2** **Design recovery:** Undo the mechanics of the database structure and resolve foreign key references. This stage deals with these three main issues are as follows

1. **Identity:** Most often, unique indexes will be defined for the candidate keys of the entity types. Otherwise, look for unique combinations of data; such data can suggest, but do not prove, a candidate key. One can also infer candidate keys by considering names and conventions of style. A suspected foreign key may imply a corresponding candidate key.
2. **Foreign keys:** Foreign key (references from one table to another) determination is usually the most difficult aspect of design recovery. Matching names and data types can suggest foreign keys. Some DBMSs, such as RDBMSs, let developers declare foreign keys and their referent, but (unfortunately) most legacy applications do not use this capability.
3. **Queries:** When queries are available, one can use them to refine their understanding of identity and foreign keys.

The final product of design recovery still reflects the DBMS paradigm and may include optimizations and errors. In practice, the model will seldom be complete. Portions of the structure may be confusing.

**1.4.3 Analysis recovery:** Remove design artifacts and eliminate any errors in the model.

1. **Clarification:** Removes any remaining artifacts of design. For example, an analysis model need not include file and database access keys; they are merely design decisions and contain no essential information.
2. **Redundancy**: Normally remove derived data that optimize the database design or that were included for misguided reasons. One may need to examine data before determining that a data structure is a duplicate.
3. **Errors:** Eliminate any remaining database errors. This step is included during analysis recovery because one must thoroughly understand the database before concluding that the developer erred. In the earlier stages, an apparent error could instead have been a reasonable practice or the result of incompletely understanding the database.
4. **Model integration:** Multiple information sources can lead to multiple models. For example, it is common to have a reverse-engineered model from study of the structure and data. A forward-engineered model might be prepared from a user manual. The final analysis model must fuse any separate models.

**1.4.4 Iteration:** The reverse engineering process is, of course, somewhat idealistic and not quite as neatly divided as the three stages imply. In practice, there is much iteration and backtracking. Portions of a model may proceed more rapidly than others. One should also need to backtrack to correct occasional mistakes and oversights. Nevertheless, the process provides a useful starting point, even for complex problems.

**1.5 Reverse Engineering Principles[4]**

Several broad principles govern the reverse engineering process.

* **Don't mistake hypotheses for conclusions.** Reverse engineering yields hypotheses. One must thoroughly understand the application before reaching firm conclusions.
* **Expect multiple interpretations.** There is no single answer as in forward engineering. Alternative interpretations of the database structure and data can yield different models. The more information that is available, the less judgments should vary among reverse engineers.
* **Shouldn’t be discouraged by approximate results.** It is worth a modest amount of time to extract 80 percent of an existing database's meaning. One can use the typical forward engineering techniques (such as interviewing knowledgeable users) to obtain the remaining 20 percent. Many people find this lack of perfection uncomfortable because it is a paradigm shift from forward engineering.
* **Expect odd constructs.** Database designers, even the experts, occasionally use uncommon constructs. In some cases, one won't be able to produce a complete, accurate model of the database because that model never existed.
* **Watch for a consistent style.** Databases are typically designed using a consistent strategy, including consistent violations of good design practice. One should be able to deduce the underlying strategy.

**2. Types of reverse Engineering**

**2.1 Reverse engineering of Mechanical Equipments[5]**

As computer-aided design has become more popular, reverse engineering has become a viable method to create a 3D virtual model of an existing physical part for use in 3D CAD, CAM, CAE and other software.[1] The reverse engineering process involves measuring an object and then reconstructing it as a 3D model. The physical object can be measured using 3D scanning technologies like CMMs, laser scanners, structured light digitizers, or computed tomography. The measured data alone, usually represented as a point cloud, lacks topological information and is therefore often processed and modeled into a more usable format such as a triangular faced mesh, a set of NURBS surfaces or a CAD model. Applications like Imageware, PolyWorks, Rapidform, or Geomagic are used to process the point clouds themselves into formats usable in other applications such as 3D CAD, CAM, CAE or visualization.

Reverse engineering is also used by businesses to bring existing physical geometry into digital product development environments, to make a digital 3D record of their own products or assess competitors' products. It is used to analyze, for instance, how a product works, what it does, what components it consists of, estimate costs, identify potential patent infringement, etc. Value engineering is a related activity also used by business. It involves deconstructing and analyzing products, but the objective is to find opportunities for cost cutting.

In today’s intensely competitive global market, product enterprises are constantly seeking new ways to shorten lead times for new product developments that meet all customer expectations. In general, product enterprise has



**Figure 1.2:** Product development cycle

in CADCAM, rapid prototyping, and a range of new technologies that provide business benefits. Reverse engineering (RE) is now considered one of the technologies that provide business benefits in shortening the product development cycle. Figure 1.2 depicts how RE allows the possibilities of closing the loop between what is “as designed” and what is “actually manufactured”.

**2.1.1 Computer Aided Reverse Engineering**

Reverse Engineering originally emerged as the answer to provide spares for replacing broken or worn out parts for which no technical data was available. This can be the case if the part was originally imported (without drawings) or the drawings being misplaced or lost. Reengineering or reverse engineering such parts can be a less expensive option compared to re-importing, not only for immediate replacement, but also to create additional spares to maintain the product over a longer period. Computer-based surface models are indispensable in several fields of science and engineering. For example, the design and manufacturing of vehicles, such as cars and aircrafts, would not be possible without sophisticated CAD and simulation tools predicting the behaviour of the product. The point cloud acquisition generally is performed by stationary scanning devices, like laser-range or computer-tomography scanners. After taking multiple scans from various sides or by rotating the object, the sampled points are combined into a single point cloud, from which the surface needs to be reconstructed. The resulting adaptive reconstruction method is based upon the repetitive application of the following steps (Pal et al., 2005):

* Starting from an initial bounding point enclosing the original point cloud the hierarchical space partitioning creates a point set by recursively subdividing each individual point into sub-point
* The resulting mesh is obtained by subdividing the coarser mesh and adapting its topology at locations where point have been removed
* The final data mapping locally constrains the mesh toward the point cloud. All vertices are projected onto local tangent planes defined by the individual points.

Reverse Engineering has been defined as a process for obtaining the technical data of a critical spare component. Computer-aided reverse engineering relies on the use of computer-aided tools for obtaining the part geometry, identifying its material, improving the design, tooling fabrication, manufacturing planning and physical realization. A solid model of the part is backbone for computer-aided reverse engineering. The model data can be exported or imported into CAD/CAE/CAM systems using standard formats such as IGES, STL, VDA and STEP.

**2.1.2 Feature Based Reverse Engineering**

Feature-based models have been suitable for manufacturing the mechanical parts with reverse engineering. Also, feature-based models are ideal for industrial design and manufacturing since the model produced can be easily modified. Feature-based and constraint-based methods can be characterized as knowledge-based methods. As researchers, it is useful to exploit design intent and feature relationships that exist in models created for industrial use, because they justify some of the attributes of the object that are obsolete. Such information can be expressed by geometric constraints (Thompson et al. 1999).

**2.2 Mechanical Reverse Engineering–The Generic Process:**

The generic process of reverse engineering is a three-phase process as depicted in Figure 1.3. The three phases are scanning, point processing, and application specific geometric model development. Reverse engineering strategy must consider the following:



**Fig 1.3: Mechanical Reverse Engineering – The Generic Process**

* + Reason for reverse engineering a part
  + Number of parts to be scanned–single or multiple
  + Part size–large or small
  + Part complexity–simple or complex
  + Part material–hard or soft
  + Part finish–shiny or dull
  + Part geometry–organic or prismatic and internal or external
  + Accuracy required–linear or volumetric

**2.2.1 Phase 1–Scanning**

This phase is involved with the scanning strategy–selecting the correct scanning technique, preparing the part to be scanned, and performing the actual scanning to capture information that describes all geometric features of the part such as steps, slots, pockets, and holes. Three-dimensional scanners are employed to scan the part geometry, producing clouds of points, which define the surface geometry. These scanning devices are available as dedicated tools or as add-ons to the existing computer numerically controlled (CNC) machine tools. There are two distinct types of scanners, contact and noncontact.

**I. Contact Scanners**

These devices employ contact probes that automatically follow the contours of a physical surface (Figure 1.4). In Ithe current marketplace, contact probe scanning devices are based on



**Figure 1.4:** Contact scanning touch probe.

on CMM technologies, with a tolerance range of +0.01 to 0.02 mm. However, depending on the size of the part scanned, contact methods can be slow because each point is generated sequentially at the tip of the probe. Tactile device probes must deflect to register a point; hence, a degree of contact pressure is maintained during the scanning process. This contact pressure limits the use of contact devices because soft, tactile materials such as rubber cannot be easily or accurately scanned.

**II. Non-Contact Scanners:**

A variety of noncontact scanning technologies available on the market capture data with no physical part contact. Noncontact devices use lasers, optics, and charge-coupled device (CCD) sensors to capture point data, as shown in Figure 1.5. Although these devices capture large amounts of data in a relatively short space of time, there are a number of issues related to this scanning technology.



**Fig 1.5:** Optical scanning device

* The typical tolerance of noncontact scanning is within ±0.025 to 0.2 mm.
* Some noncontact systems have problems generating data describing surfaces, which are parallel to the axis of the laser (Figure 1.5).
* Noncontact devices employ light within the data capture process. This creates problems when the light impinges on shiny surfaces, and hence some surfaces must be prepared with a temporary coating of fine powder before scanning.

These issues restrict the use of remote sensing devices to areas in engineering, where the accuracy of the information generated is secondary to the speed of data capture. However, as research and laser development in optical technology continue, the accuracy of the commercially available noncontact scanning device is beginning to improve.

The output of the scanning phase is point cloud data sets in the most convenient format. Typically, the RE software provides a variety of output formats such as raw (X, Y, Z values separated by space or commas).

**2.2.2 Phase 2–Point Processing**

This phase involves importing the point cloud data, reducing the noise in the data collected, and reducing the number of points. These tasks are performed using a range of predefined filters. It is extremely important that the users have very good understanding of the filter algorithms so that they know which filter is the most appropriate for each task. This phase also allows us to merge multiple scan data sets. Sometimes, it is necessary to take multiple scans of the part to ensure that all required features have been scanned. This involves rotating the part; hence each scan datum becomes very crucial. Multiple scan planning has direct impact on the point processing phase. Good datum planning for multiple scanning will reduce the effort required in the point processing phase and also avoid introduction of errors from merging multiple scan data. A wide range of commercial software is available for point processing.

The output of the point processing phase is a clean, merged, point cloud data set in the most convenient format. This phase also supports most of the proprietary formats mentioned above in the scanning phase.

**2.2.3 Phase 3–Application Geometric Model Development**

In the same way that developments in rapid prototyping and tooling technologies are helping to shorten dramatically the time taken to generate physical representations from CAD models, current RE technologies are helping to reduce the time to create electronic CAD models from existing physical representations. The need to generate CAD information from physical components will arise frequently throughout any product introduction process.

The generation of CAD models from point data is probably the most complex activity within RE because potent surface fitting algorithms are required to generate surfaces that accurately represent the three-dimensional information described within the point cloud data sets. Most CAD systems are not designed to display and process large amounts of point data; as a result new RE modules or discrete software packages are generally needed for point processing. Generating surface data from point cloud data sets is still a very subjective process, although feature-based algorithms are beginning to emerge that will enable engineers to interact with the point cloud data to produce complete solid models for current CAD environments.

The applications of RE for generating CAD data are equally as important as the technology which supports it. A manager’s decision to employ RE technologies should be based on specific business needs.

This phase depends very much on the real purpose for reverse engineering. For example, if we scanned a broken injection molding tool to produce a new tool, we would be interested in the geometric model and also in the ISO G code data that can be used to produce a replacement tool in the shortest possible time using a multi-axis CNC machine. One can also use reverse engineering to analyze as designed” to “as manufactured. This involves importing the as designed CAD model and superimposing the scanned point cloud data set of the manufactured part. The RE software allows the user to compare the two data Sets (as designed to as manufactured). This process is also used for inspecting manufactured parts. Reverse engineering can also be used to scan existing hip joints and to design new artificial hips joint around patient- specific pelvic data. This creates the opportunity for customized artificial joints for each patient.

The output of this phase is geometric model in one of the proprietary formats such as IGES, VDA, STL, DXF, OBJ, VRML, ISO G Code, etc.

**2.3 Reverse engineering of Software:**

The term "reverse engineering" as applied to software means different things to different people, prompting Chikofsky and Cross to write a paper researching the various uses and defining taxonomy. According to them, Reverse engineering is the process of analyzing a subject system to create representations of the system at a higher level of abstraction. It can also be seen as "going backwards through the development cycle".In this model, the output of the implementation phase (in source code form) is reverse engineered back to the analysis phase, in an inversion of the traditional waterfall model. Reverse engineering is a process of examination only: the software system under consideration is not modified (which would make it reengineering). Software anti-tamper technology is used to deter both reverse engineering and reengineering of proprietary software and software-powered systems. In practice, two main types of reverse engineering emerge. In the first case, source code is already available for the software, but higher level aspects of the program, perhaps poorly documented or documented but no longer valid, are discovered. In the second case, there is no source code available for the software, and any efforts towards discovering one possible source code for the software are regarded as reverse engineering. This second usage of the term is the one most people are familiar with. Reverse engineering of software can make use of the clean room design technique to avoid infringing copyrights.

On a related note, black box testing in software engineering has a lot in common with reverse-engineering. The tester usually has the API, but their goals are to find bugs and undocumented features by bashing the product from outside.

Other purposes of reverse engineering include security auditing, removal of copy protection ("cracking"), circumvention of access restrictions often present in consumer electronics, customization of embedded systems (such as engine management systems), in-house repairs or retrofits, enabling of additional features on low-cost "crippled" hardware (such as some graphics card chipsets), or even mere satisfaction of curiosity.

**2.3.1 Binary software**

This process is sometimes termed Reverse Code Engineering or RCE.As an example, decompilation(the result of decompiling) of binaries for the Java platform can be accomplished using Jad. One famous case of reverse engineering was the first non-IBM implementation of the PC BIOS which launched the historic IBM PC compatible industry that has been the overwhelmingly dominant computer hardware platform for many years. An example of a group that reverse engineers software for enjoyment is CORE, which stands for "Challenge Of Reverse Engineering." In the United States, the Digital Millennium Copyright Act exempts from the circumvention ban some acts of reverse engineering aimed at interoperability of file formats and protocols, but judges in key cases have ignored this law, since it is acceptable to circumvent restrictions for use, but not for access. Aside from restrictions on circumvention, reverse engineering of software is protected in the U.S. by the fair use exception in copyright law.

The Samba software, which allows systems that are not running Microsoft Windows systems to share files with systems that are, is a classic example of software reverse engineering, since the Samba project had to reverse-engineer unpublished information about how Windows file sharing worked, so that non-Windows computers could emulate it. The Wine project does the same thing for the Windows API, and OpenOffice.org is one party doing this for the Microsoft Office file formats. The React OS project is even more ambitious in its goals as it strives to provide binary (ABI and API) compatibility with the current Windows OSes of the NT branch, allowing software and drivers written for Windows to run on a clean room reverse engineered GPL open source counterpart. [ [6](https://en.wikipedia.org/wiki/Fair_use)]

**2.3.2 Binary software techniques**

Reverse engineering of software can be accomplished by various methods. The three main groups of software reverse engineering are

* Analysis through observation of information exchange, most prevalent in protocol reverse engineering, which involves using bus analyzers and packet sniffers, for example, for accessing a computer bus or computer network connection and revealing the traffic data thereon. Bus or network behavior can then be analyzed to produce a stand-alone implementation that mimics that behavior. This is especially useful for reverse engineering device drivers. Sometimes reverse-engineering on embedded systems is greatly assisted by tools deliberately introduced by the manufacturer, such as JTAG ports or other debugging means. In Microsoft Windows, low-level debuggers such as SoftICE are popular.
* Disassembly using a disassembler, meaning the raw machine language of the program is read and understood in its own terms, only with the aid of machine language mnemonics. This works on any computer program but can take quite some time, especially for someone not used to machine code. The Interactive Disassembler is a particularly popular tool.
* Decompilation using a decompiler, a process that tries, with varying results, to recreate the source code (A number of UML tools refer to the process of importing source code in order to generate UML diagrams, as "reverse engineering.") in some high level language for a program only available in machine code or byte code.

**2.3.3 Reverse Engineering process of Software[7]**

Reverse engineering, also called as back engineering, is the process of extracting knowledge from anything man-made & reproducing something based on that information. The process often involves disassembling something (a mechanical device, electronic components, computer program, or biological, chemical or organic matter) & analyzing its components & working in detail. Reverse engineering does not mean copying or changing the artifacts. It is only an analysis to deduce the design features.

**Tools for Reverse Engineering:**

* **Disassembler:**to convert binary code into assembly code, to extract strings, imported & exported functions, libraries, etc.
* **Debuggers:**debuggers allow the reverser to step through the code by running 1 line at a time to investigate the results.
* **Hex editors:**These allow the binary to be viewed in the editor & change it as per requirements.
* **PE & Resource viewer:**All the programs that run on windows should have a Portable Executable that supports the DLLs the program needs to borrow from.

**2.3.4 Issues in Software Reverse Engineering**:

**1. Abstraction Level**

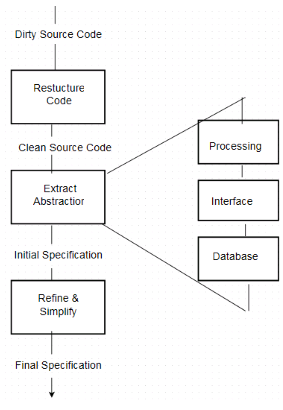
* This level helps in obtaining the design information from the source code.
* Ideally, abstraction level should be as high as possible.
* It is expected that abstraction level should be high in reverse engineering, so High abstraction level helps the software engineer to understand the program.
* Reverse Engineering process should be capable of deriving procedural design representation (a low-level abstraction), program and data structure information (a high-level abstraction), and UML class, state and deployment diagram (high level of abstraction).
* As the abstraction level increases, the software engineer provided with information that will allow easier understanding of the program.

**2. Completeness level**

* The completeness of reverse engineering process refers to the level of details that is provided at an abstraction level.
* The completeness decreases abstraction level increases. For example –From a given source code listing one can easily develop a complete procedural design representation. But it is very difficult to develop complete set of data flow diagram or entity relationship diagram. The completeness in reverse engineering process develops the interactivity. The term interactivity means the degree to which human “integrated” with automated tools to create effective reverse engineering process. As the abstraction level increases the interactivity must increase to bring the completeness.

**3. Directionality level**

* Directionality means extracting the information from source code and gives it to software engineer.
* The directionality can be one way or two way.
* The one way directionality means extracting all information from source code and gives it to software engineer.
* The two ways directionality means the information taken from source code is fed to a re-engineering tool that attempts to restructure or regenerate old program.
* Following fig shows process of reverse engineering.



**Fig1.6:** Software Reverse Engineering

* Initially the dirty source code or unstructured source code is taken and processed and code is restructured.
* After restructuring process the source code becomes clean source code.
* The core to reverse engineering is an activity called extract abstractions.
* In abstraction activity, the engineer must evaluate older program and extract information about procedures, interface, data structure or database used.
* The output of reverse engineering process is a clear, unambiguous final specification obtained from unstructured source code.
* The final specification helps in easy understanding of source code.

**2.4 Reverse-engineering of integrated circuits/smart cards[8]**

Reverse Engineering is an invasive and destructive form of analyzing a smart card. The attacker grinds away layer by layer of the smart card and takes pictures with an electron-microscope. With this technique it is possible to reveal the complete hardware and software part of the smart card. The major problem for the attacker is to bring everything into the right order to find out how everything works. Engineers try to hide keys and operations by mixing up memory positions, for example bus-scrambling

In some cases it is even possible to attach a probe to direct measure voltages while the smart card is still operational. Engineers employ sensors to detect and prevent this attack.[8] It takes very high effort to break a smart card used for payment, for example, and the technical equipment is only available to large chip-producers. Additionally the gain is low due to other security mechanisms like shadow accounts.

**2.4.1 Blob selection method [9]**

This is a simpler and faster of two proposed via detection methods. It is based on simple threshold filter and binary image blob feature analysis. After noise reduction, threshold filter is applied to the image. Threshold value is constant, defined by highest intensity pixel values in via regions of image. Such approach assumes that pixels in via areas are always of higher intensity compared to their surrounding areas. Vias have lower intensity edges which separate them from other areas. This is generally true for via photographs because insulating oxide layer between two metal layers has lower light reflectivity than via regions. After threshold filtering, resulting binary image is processed with simple blob reject filter. This step requires predefined approximate dimensions of via objects in pixels. Via size must be calculated in advance and provided to this method as input parameter. Size-based blob filtering removes binary objects which size does not fall into size range specified by filter parameter. Remaining objects are identified as vias.

**2.4.2 Cross correlation method**

Second method is based on statistical similarity search principle. Image regions which correlate with a provided via sample image are marked as via locations. After noise reduction, reference via search pattern is selected from the image. This pattern must be an image of single, very good quality generic via sample taken from original image. The search pattern must contain via and it must include some surrounding background edge pixels. Correct pattern selection is very important step for this algorithm. Best quality via pattern image can be derived by averaging a few well formed via image samples. Fundamental idea of this algorithm is to calculate correlation of search pattern at every point in test image [13]. This produces cross correlation map which is stored as image with equal dimensions as input. Fig. 4 shows cross correlation result of sample image in Fig. 3d. Correlation peak points are denoted by white ovals. Cross correlation image is threshold-filtered to isolate correlation peak points. Peak points form blobs in binary image. These blobs indicate via locations in the original image. If via size is unknown prior to detecting via locations, it is calculated afterwards. After identifying via locations, a part of original image (after noise filtering) is selected for further analysis. The selected part is threshold filtered and feature sizes at previously found via locations are measured. Collected via dimension set is used to calculate median value. Calculated value is the most accurate measurement of the actual via diameter.

**2.4.3 Extracted data processing**

After extracting via location and size data using two described methods, it is processed to confirm with via design rules. They define restrictions for via size and spacing. Design rules are input parameters for this processing stage. Usually via size must be rounded to 0.1µm precision and via shape must be square. Spacing design rule processing is used to discard some of recognition false positive matches. This is possible because they define the minimum distance between two vias. False positive via match can be identified by analyzing location data. It’s indicated when location does not fall into spacing grid of nearby vias.

Two methods suitable for extraction of integrated circuit metal layer interconnect data from microscope images were proposed and experimentally verified. Custom software application was developed to verify and tune proposed method algorithms. Test results show that in most cases blob selection method is the most suitable method for via identification in image. However both proposed methods are highly dependent on the quality of input image data. Cross correlation search method is highly preferable to blob selection when input image data quality degrades.

**2.5 Reverse-engineering for military applications:**

Reverse engineering is often used by military in order to copy other nations' technology, devices or information, or parts of which, have been obtained by regular troops in the fields or by intelligence operations. It was often used during the Second World War and the Cold War. Well-known examples from World War II and later include:

1. Jerry can: British and American forces noticed that the Germans had gasoline cans with an excellent design. They reverse engineered copies of those cans. The cans were popularly known as "Jerry cans."
2. Tupolev Tu-4: Three American B-29 bombers on missions over Japan were forced to land in the USSR. The Soviets, who did not have a similar strategic bomber, decided to copy the B-29. Within a few years they had developed the Tu-4, a near perfect copy.[ 10]
3. V2 Rocket: Technical documents for the V2 and related technologies were captured by the Western Allies at the end of the war. Soviet and captured German engineers had to reproduce technical documents and plans, working from captured hardware, in order to make their clone of the rocket, the R-1, which began the postwar Soviet rocket program that led to the R-7 and the beginning of the space race. [11]
4. K-13/R-3S missile (NATO reporting name AA-2 Atoll), a Soviet reverse-engineered copy of the AIM-9 Sidewinder, made possible after a Taiwanese AIM-9B hit a Chinese MiG-17 without exploding; amazingly, the missile became lodged within the airframe, the pilot returning to base with what Russian scientists would describe as a university course in missile development.[12]
5. BGM-71\_TOW Missile: In May 1975, negotiations between Iran and Hughes Missile Systems on co-production of the TOW and Maverick missiles stalled over disagreements in the pricing structure. The subsequent 1979 revolution ended all plans for such co-production. Iran was successful in reverse engineering the missile, and are currently producing their own copy: The Toophan.[1[3](https://en.wikipedia.org/wiki/BGM-71_TOW)]
6. China has [reversed engineered many examples](https://en.wikipedia.org/wiki/Intellectual_property_in_the_People%27s_Republic_of_China) of Western and Russian hardware, from fighter aircraft to missiles and [HMMWV](https://en.wikipedia.org/wiki/HMMWV) cars, such as the MiG-15 (which became the J-7) and the Su-33 (which became the J-15). More recent analyses of China's military growth have pointed to the inherent limitations of reverse engineering for advanced weapon systems.[[14]](https://en.wikipedia.org/wiki/Reverse_engineering#cite_note-33)
7. During the Second World War, Polish and British cryptographers studied captured German ["Enigma"](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma) message encryption machines for weaknesses. Their operation was then simulated on electro-mechanical devices called "[Bombes](https://en.wikipedia.org/wiki/Bombe)" that tried all the possible scrambler settings of the "Enigma" machines to help break the coded messages sent by the Germans.
8. Also during the Second World War, British scientists analyzed and defeated a [series of increasingly sophisticated radio navigation systems](https://en.wikipedia.org/wiki/Battle_of_the_Beams) being used by the German Luftwaffe to perform guided bombing missions at night. The British countermeasures to this system were so effective that in some cases German aircraft were led by signals to land at RAF bases, believing they were back in German territory.

**2.6 Medical Reverse Engineering**

Understanding, controlling and manipulation of patient data as well as shape, geometry and structure of the biomedical objects are important for developing Biomedical Engineering (BME) applications. Medical Reverse Engineering (MRE) is aimed to use the Reverse Engineering (RE) technology to reconstruct 3D models of the anatomical structures and biomedical objects for design and manufacturing of medical products as well as BME research and development.

The engineering originality of the human body has put reverse engineering in a unique place in the life science and medical device industries, particularly in implementing artificial parts into the human body. Applying scanned images with finite element analysis in reverse engineering helps engineers in precisely modeling customized parts that best fit individual patients. The baseline requirements for reverse engineering is in life science and medical devices for physiological characteristic of living cells, human organs, and the communications among them. Engineers and scientists often work in the reverse direction can be help by observed body behaviors and the biological elements there must underlie the mechanisms that can reproduce these biological functions.

Under reverse engineer environment the engineers, first have to identify the materials that are used for this part and characteristics medical device, then the part geometric form has to be accurately digitized, and the manufacturing process has to be verified. Reverse engineering is used in several medical fields: dentistry, hearing aids, artificial knees, and heart (Fu, 2008).

Based on requirement, advanced computer-aided manufacturing processes can build customized orthodontic devices for individual patients. The growth of reverse engineering applications is mostly dependent on technology evolution to make the wireless hearing aid smaller, more sophisticated, and more efficient at lower cost. The applications of reverse engineering to orthopedics, such as the knee, hip, or spine implantation, are very challenging, partially due to the complex motions of the knees, hips, or spine. A proper function of these implants manufactured by reverse engineering requires them to sustain multiaxial statistic stresses and various modes of dynamic loads.

It is also used to reconstruct the events just before and immediately after accidents in the aviation, automobile, and other transportation industries. Other fields, such as in fashion Design, in chemical industry, architecture and civil engineering, and art galleries, also find a lot of reverse engineering applications.

**2.7 Reverse Engineering in Modern Industries**

The distinction between an original equipment manufacturer and a supplier has been blurred in recent years in today’s dynamic and competitive global market. The application of reverse engineering, engine spare parts reproduced for the repair and replacement of worn-out components will have significant economic impact on the aviation industry and its customers. In the 1970s, to reverse engineer application for high pressure turbine blade was a challenge due to the need to decode highly guarded industry proprietary information. In the 2000s, have technical innovations changed the reverse engineering process, also the practice itself is also more widely accepted. The production of quality reverse engineered parts does require the full reinvention of engineering design and manufacturing process. To obtain precise geometric information for the aftermarket automobile parts, many companies also resort to the technology of digital scanning and reverse engineering. It provides a variety of auto parts, including spoilers, running boards, fenders, and wheel covers. The companies are not always able to take advantage of equipment manufacturer original CAD data, partially because the as-built parts are often slightly different from the CAD data. The U.S. federal government, the reverse engineered automotive parts are certified by the industry itself. Automotive Parts Association encourages price and quality competition in the marketplace so that customer expenses are reduced but till maintaining part quality. One of the widely cited reverse engineering examples in the military is the Soviet Tupolve Tu-4 (Bull) bomber. During World War II, three battle damaged U.S. B-29 Super fortress bombers made emergency landings in the Soviet Union territory after missions to Japan. Reverse engineered projects are not successful very time. For example, a reproduction of the 1903 Wright Flyer fell into a puddle after attempting flight on December 15, 2003.This ill-fated flight attempt brought out another risk factor in reverse engineering. Even though, might have produced a seemingly identical replica of the original part, the operability of the reverse engineered part also depends on the operating environment (Wego, 2011). A successful reverse engineering program requires great attention to the miniature details and accuracy of all measurements, in addition to a thorough understanding of the functionality of the original part.

**2.8 In Aerospace and Ship Hull Craft**

Reverse engineering approach has been used by Boeing and other aerospace companies to create digital inventories of spare parts or to convert legacy data into today’s CAD environments. Reverse engineering method is a key to the future of aerospace manufacturing as CAD tool. The modern aerospace industry uses reverse engineering for these key reasons (Ping, 2008):

To create legacy parts that does not have CAD models To overcome obstacles in data exchange To short out problems arising from discrepancies between the CAD master model and the actual tooling or as-built part To confirm the quality and performance by computer-aided inspection and engineering analysis

An industrial application of CAD is presented, which concerns the measurement and reengineering of the shape of a complete ship hull and of ship's parts, which is a frequently recurring task in the shipbuilding and ship repair sector. In order to choose the most appropriate measurement method, several typical aspects of our object of measurement, such as its size, possible obstructions and poor accessibility, have to be taken into consideration (Koelman, 2010).

**3.** **Legality**

**3.1 United States**

In the United States even if an artifact or process is protected by trade secrets, reverse-engineering the artifact or process is often lawful as long as it has been legitimately obtained. Reverse engineering of computer software in the US often falls under both contract law as a breach of contract as well as any other relevant laws. This is because most end user license agreements specifically prohibit it, and U.S. courts have ruled that if such terms are present, they override the copyright law which expressly permits it (see Bowers v. Baystate Technologies. Sec. 103(f) of the DMCA (17 U.S.C. § 1201 (f)) says that a person who is in legal possession of a program, is permitted to reverse-engineer and circumvent its protection if this is necessary in order to achieve "interoperability" — a term broadly covering other devices and programs being able to interact with it, make use of it, and to use and transfer data to and from it, in useful ways. A limited exemption exists that allows the knowledge thus gained to be shared and used for interoperability purposes.

**3.2 Overlap with patent law**

Reverse engineering applies primarily to gaining understanding of a process or artifact, where the manner of its construction, use, or internal processes is not made clear by its creator. Patented items do not of themselves have to be reverse-engineered to be studied, since the essence of a patent is that the inventor provides detailed public disclosure themselves, and in return receives legal protection of the invention involved. However, an item produced under one or more patents could also include other technology that is not patented and not disclosed. Indeed, one common motivation of reverse engineering is to determine whether a competitor's product contains patent infringements or copyright infringements.

**3.3 Ethical Angles [15]**

Reverse-engineering can also expose security flaws and questionable privacy practices. For instance, reverse-engineering of Dallas-based Digital: Convergence Corp.'s CueCat scanning device revealed that each reader has a unique serial number that allows the device's maker to marry scanned codes with user registration data and thus track each user's habits in great detail—a previously unpublicized feature.

Recent legal moves backed by many large software and hardware makers, as well as the entertainment industry, are eroding companies' ability to do reverse-engineering."Reverse-engineering is legal, but there are two main areas in which we're seeing threats to reverse-engineering," says Jennifer Granick, director of the law and technology clinic at Stanford Law School in Palo Alto, Calif. One threat, as yet untested in the courts, comes from shrink-wrap licenses that explicitly prohibit anyone who opens or uses the software from reverse-engineering it, she says.

The other threat is from the Digital Millennium Copyright Act (DMCA), which prohibits the creation or dissemination of tools or information that could be used to break technological safeguards that protect software from being copied. Last July, on the basis of this law, San Jose-based Adobe Systems Inc. asked the FBI to arrest Dmitry Sklyarov, a Russian programmer, when he was in the U.S. for a conference. Sklyarov had worked on software that cracked Adobe's e-book file encryption.

The fact is, even above-board reverse-engineering often requires breaking such safeguards, and the DMCA does allow reverse-engineering for compatibility purposes. "But you're not allowed to see if the software does what it's supposed to do," says Granick, nor can you look at it for purposes of scientific inquiry. She offers an analogy: "You have a car, but you're not allowed to open the hood."

**4. Conclusion:**

The fundamental principles and basic limitations of reverse engineering are similar in most industries. The general practice of reverse engineering, such as data collection, detailed analysis at a micro scale, modeling, prototyping, performance evaluation, and regulation compliance, are the same in principle for all industries. The success of this endeavor is usually subject to the general limitations of modern technologies. However, the specific methodologies used in different fields can be vastly different.

Whether it's rebuilding a car engine or diagramming a sentence, people can learn about many things simply by taking them apart and putting them back together again. That, in a nutshell, is the concept behind reverse-engineering—breaking something down in order to understand it, build a copy or improve it.

A process that was originally applied only to hardware, reverse-engineering is now applied to software, databases and even human DNA. Reverse-engineering is especially important with computer hardware and software. Programs are written in a language, say C++ or Java, that's understandable by other programmers. But to run on a computer, they have to be translated by another program, called a compiler, into the ones and zeros of machine language. Compiled code is incomprehensible to most programmers, but there are ways to convert machine code back to a more human-friendly format, including a software tool called a decompiler.

Reverse-engineering is used for many purposes: as a learning tool; as a way to make new, compatible products that are cheaper than what's currently on the market; for making software interoperate more effectively or to bridge data between different operating systems or databases; and to uncover the undocumented features of commercial products.

**5. References:**

1. Kumar, A[tul]; Jain, P[ramod] K[umar] & Pathak, P[ushparaj] M[ani] (2013) Reverse Engineering in Product Manufacturing: An Overview , Chapter 39 in DAAAM International Scientific Book 2013, pp. 665-678, B. Katalinic & Z. Tekic (Eds.), Published by DAAAM International, ISBN 978-3-901509-94-0, ISSN 1726-9687, Vienna, Austria
2. https://www.researchgate.net/publication/226320946\_Introduction\_to\_Reverse\_Engineering?enrichId=rgreq-d2682234cf928ffad6709fc7d69d9eb2-XXX&enrichSource=Y292ZXJQYWdlOzIyNjMyMDk0NjtBUzoxMDIyNTIxMDI1NTM2MDhAMTQwMTM5MDIwOTU0MA%3D%3D&el=1\_x\_3&\_esc=publicationCoverPdf
3. http://www.informit.com/articles/article.aspx?p=23692&seqNum=6
4. http://www.informit.com/articles/article.aspx?p=23692&seqNum=6
5. https://www.researchgate.net/publication/226320946\_Introduction\_to\_Reverse\_Engineering?enrichId=rgreq-d2682234cf928ffad6709fc7d69d9eb2-XXX&enrichSource=Y292ZXJQYWdlOzIyNjMyMDk0NjtBUzoxMDIyNTIxMDI1NTM2MDhAMTQwMTM5MDIwOTU0MA%3D%3D&el=1\_x\_3&\_esc=publicationCoverPdf
6. https://en.wikipedia.org/wiki/Fair\_use
7. https://www.quora.com/What-is-the-difference-between-re-engineering-and-reverse-engineering
8. https://en.wikipedia.org/wiki/Reverse\_engineering
9. Reverse Engineering of CMOS Integrated Circuits G. Masalskis, R. NavickasVilnius Gediminas Technical University, Department of Computer Engineering,Naugarduko str. 41, LT-03227, Vilnius
10. https://en.wikipedia.org/wiki/Tupolev\_Tu-4
11. https://en.wikipedia.org/wiki/V-2\_rocket
12. https://en.wikipedia.org/wiki/K-13\_(missile)
13. https://en.wikipedia.org/wiki/BGM-71\_TOW
14. Andrea Gilli and Mauro Gilli, "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage, International Security 43:3 (2019 141-189, https://doi.org/10.1162/isec\_a\_00337.
15. https://www.computerworld.com/article/2585652/reverse-engineering.html