วิศวกรรมย้อนกลับ ความก้าวหน้าของอุสาหกรรมโลก

สิปาง ดิเรกคุณากร
มหาวิทยาลัยศรีปทุม

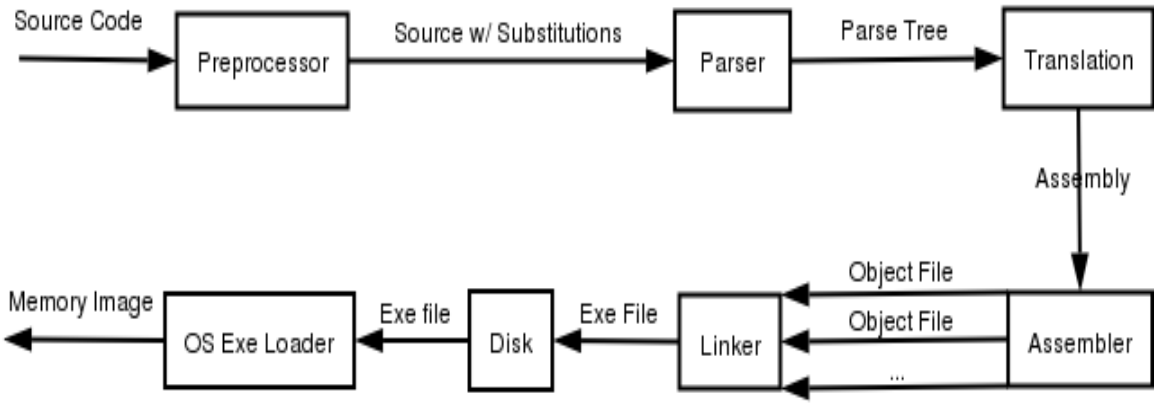
วิศวกรรมย้อนกลับ หรือ **Reverse Engineering** เป็นคนละคำกับคำว่า Reengineering ที่หมายถึงการจัดการองค์กรใหม่ โดยอาจมีเรื่องการลดจำนวนพนักงานเข้ามาเกี่ยวข้อง แต่คำว่าวิศวกรรมย้อนกลับเป็นขบวนการค้นหาหลักการหรือวิธีการทำงานของอุปกรณ์หรือระบบหรือซอฟแวร์ โดยการวิเคราะห์โครงสร้าง หน้าที่การทำงาน, วิธีการใช้งานหรือโปรแกรม ส่วนใหญ่จะเป็นการค้นหาที่เกี่ยวข้องกับอุปกรณ์อิเลกทรอนิกส์หรืออุปกรณ์จักรกลหรือโปรแกรม จากการวิเคราะห์ขั้นตอนการทำงานแล้วนำมาสร้างเป็นอุปกรณ์หรือระบบใหม่ที่ทำหน้าที่ได้เหมือนกับระบบที่ถูกวิเคราะห์โดยไม่ต้องมีทำการลอกแบบหรือทราบวิธีการทำงานจริง ๆ ของระบบที่ถูกทำการวิเคราะห์

ในสหรัฐและอีกหลาย ๆ ประเทศขบวนการผลิตและวิธีการประดิษฐ์สิ่งของทางการค้าจะปิดเป็นความลับทางการค้า วิธีการทำวิศวกรรมย้อนกลับกับสิ่งประดิษฐ์หรือขบวนการเป็นวิธีการที่ถูกกฎหมายตราบเท่าที่ขั้นตอนวิธีการที่ทำให้ได้มาซึ่งขั้นตอนยังถูกต้องตามกฎหมาย สำหรับสิ่งของที่มีสิทธิบัตร (Patent) ต้องมีการแสดงวิธีการหรือขั้นตอนการประดิษฐ์ก่อนที่จะทำการจดทะเบียน ดังนั้นไม่มีความจำเป็นต้องทำวิศวกรรมย้อนกลับเพื่อให้ได้มาซึ่งขั้นตอนวิธีการทำสำหรับสิ่งของที่มีการจดสิทธิบัตร แต่ส่วนหนึ่งที่เป็นแรงจูงใจให้มีการทำการวิเคราะห์โดยวิศวกรรมย้อนกลับคือการหารายละเอียดในผลิตภัณฑ์ของคู่แข่งว่ามีการละเมิดลิขสิทธิ์ (Copyright Infringements) หรือละเมิดสิทธิ์บัตรหรือไม่ (Patent Infringements)

ตัวอย่างของซอฟแวร์แซมบ้า (Samba) เป็นตัวอย่างที่น่าสนใจตัวอย่างหนึ่งของการทำวิศวกรรมย้อนกลับ โดยการที่ระบบซอฟแวร์จะสามารถทำให้มีการแชร์หรือการให้เครื่องคอมพิวเตอร์ที่อยู่ต่างเครื่องกันใช้แฟ้มข้อมูลเดียวกันได้กับระบบแฟ้มข้อมูลของไมโครซอฟท์วินโดส์ โดยตัวซอฟแวร์เองจะมีการทำงานอยู่บนระบบปฏิบัติการลีนุกซ์ (Linux) ซอฟแวร์มีการทำงานที่เป็นการเลียนแบบการทำงานของระบบปฏิบัติการวินโดส์โดยมีฟังก์ชั่นการทำงานที่สามารถทำได้เหมือนกัน ซอฟแวร์มีการอนุญาตให้เครื่องต่างระบบหรือเครื่องคอมพิวเตอร์ที่เป็นคนละประเภทสามารถทำการแชร์แฟ้มข้อมูลกับระบบวินโดส์ได้

การทำวิศวกรรมย้อนกลับสำหรับซอฟแวร์บางครั้งจะเรียกว่า การทำวิศวกรรมย้อนกลับของรหัส Reverse Code Engineering หรือ RCE ตัวอย่างเช่น ในการใช้งานซอฟแวร์หรือโปรแกรมที่เราใช้งานทุกวันนี้นั้นจะอยู่ในรูปที่เป็นรหัสไบนารี่หรืออยู่ในรูปของภาษาเครื่องแล้ว แต่ก่อนที่จะอยู่ในรูปนี้ได้จะต้องผ่านขั้น ตอนการที่เรียกว่า การคอมไพล์ (Compile) ซึ่งเป็นการแปลงโปรแกรม

ภาษาให้อยู่ในรูปรหัสไบนารี่ ตัวอย่างของซอฟแวร์ที่ทำวิศวกรรมย้อนกลับกับรหัสไบนารี่ของภาษาจาว่าได้แก่ซอฟแวร์ที่ชื่อ Jade ซอฟแวร์จะทำขั้นตอนที่เป็นการย้อนกลับหรือที่เรียกว่า Decompile โดยจะเป็นการแปลงให้รหัสไบนารี่หรือรหัสภาษาเครื่องให้กลับมาอยู่ในรูปโปรแกรมภาษาที่สามารถอ่านเข้าใจได้

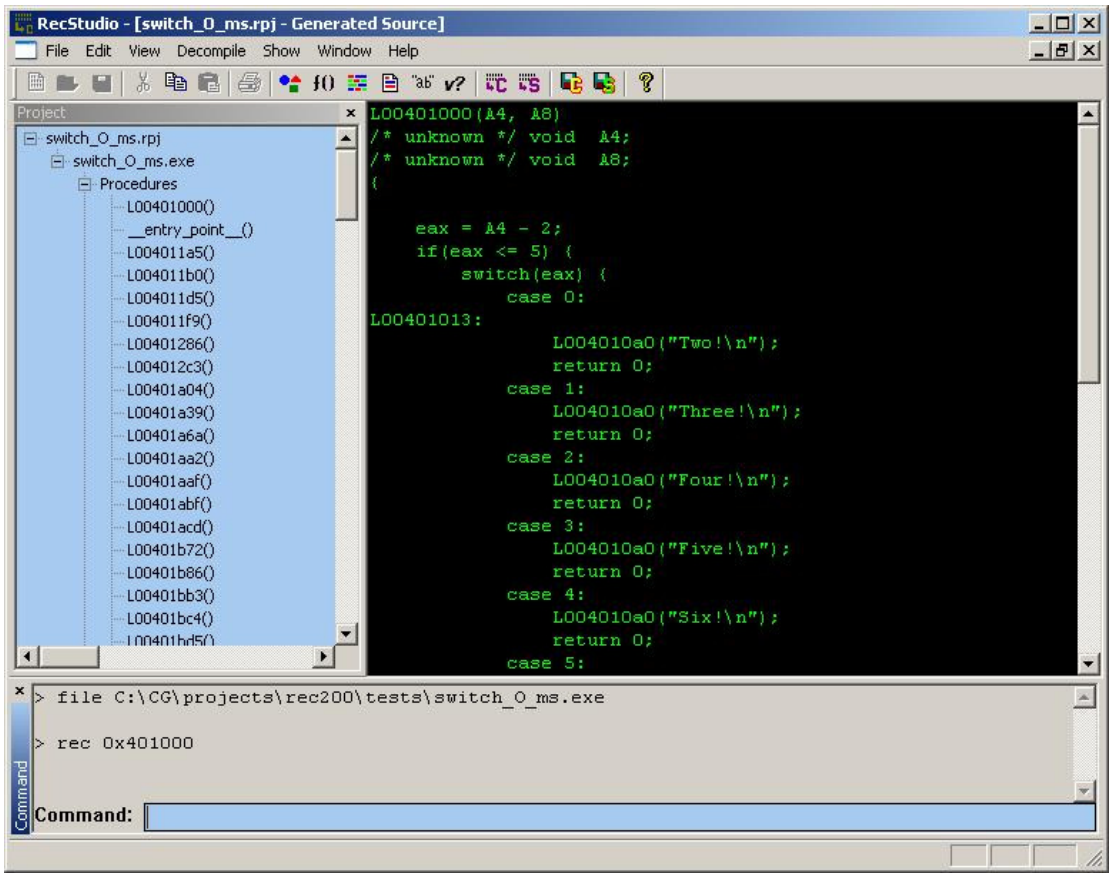


รูปแสดงขั้นตอนการคอมไพล์โปรแกรมจะประกอบด้วยขั้นตอนย่อย ๆ ได้แก่ Parser, Linker, Assembler

<u>เทคนิคในการจัดการกับรหัสไบนารี่ในขบวนการวิศวกรรมย้อนกลับ</u>

ในการพัฒนาโปรแกรมนั้นจะต้องใช้ขั้นตอนหรือวิธีการซึ่งในภาษาคอมพิวเตอร์เรียกว่าอัลกอริทึม (Algorithms) ซึ่งจะเป็นส่วนสำคัญที่ทำให้โปรแกรมที่ออกแบบมานั้นสามารถทำงานได้ตามที่ต้องการ หรือมีความรวดเร็วต่างกันก็จะมาจากส่วนนี้ วิศวกรรมย้อนกลับจะเป็นเสมือนการทดสอบกล่องดำเพื่อดูว่าขั้นตอนของการทำงานของซอฟแวร์นั้นๆ เป็นอย่างไร เพื่อที่จะได้ทราบถึงวิธีการทำงานของโปรแกรมหรือซอฟแวร์นั้นขั้นตอนการทำวิศวกรรมย้อนกลับของซอฟแวร์สามารถวิเคราะห์ได้คร่าวๆ มีดังนี้

1. วิเคราะห์โดยสังเกตข้อมูลที่เปลี่ยนแปลง โดยขั้นตอนนี้จะมีการวิเคราะห์ข้อมูลที่วิ่งอยู่ในสายซึ่งอาจเป็นการวิเคราะห์บัสหรือสายข้อมูลที่เชื่อมต่อซึ่งอาจใช้ Protocol Analyzer หรือ packet sniffer ในการวิเคราะห์ตรวจจับข้อมูล โดยข้อมูลที่วิ่งไปมาในสายจะบอกให้ทราบถึงรายละเอียดของสิ่งที่ต้องการซึ่งบางครั้งไม่จำเป็น ต้องมีการเชื่อมต่อเป็นเน็ตเวิร์ดจริง ๆ อาจเป็นเพียงการใช้งานเครื่องเดียว (Stand-Alone) แล้วดูพฤติกรรมในสายสัญญาณ บางครั้งการทำวิศวกรรมย้อนกลับในระบบที่เป็นแบบผนวกรวมหรือที่เรียกว่า Embedded System ก็สามารถวิเคราะห์ได้ง่ายโดยเครื่องมือที่ผู้ผลิตผลิตภัณฑ์ให้มา เช่น โปรแกรมที่ใช้ตรวจหาที่ผิด (Debugger) อย่าง JTAG ตัวอย่างของการทำวิศวกรรมย้อนกลับในระบบไมโครซอฟท์วินโดส์สำหรับการหาที่ผิด (Debug) ที่ระดับไบนารี่ได้แก่ซอฟแวร์ที่ชื่อ SoftICE



รูปแสดงตัวอย่างโปรแกรมที่มีการทำงานแบบวิศวกรรมย้อนกลับ
โปรแกรมจะมีการแปลงแฟ้มข้อมูลที่ใช้ทำงาน หรือ Executable file ให้อยู่ในรูปของภาษา C

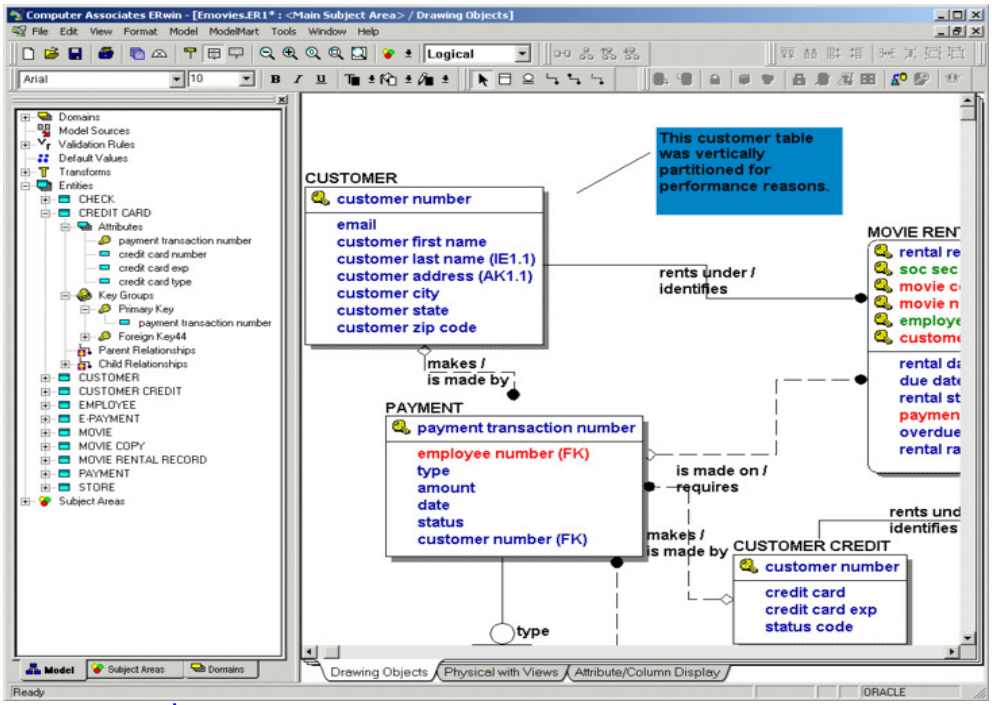
2. การวิเคราะห์โดยการทำให้อยู่ในรูปโค้ดของภาษาแอสแซมบลี หรือภาษาเครื่องที่โปรแกรมอ่านแล้วสามารถทำงานได้โดยตรง การทำให้อยู่ในรูปของภาษาแอสแซมบลี แล้วดูวิธีการทำงานของโปรแกรมจากการทำงานในแต่ละขั้นตอนก็จะสามารถทำให้ทราบวิธีการทำงานของซอฟแวร์ที่ต้องการทำวิศวกรรมย้อนกลับได้

3. การทำการแปลงรหัสกลับไปเป็นซอสโปรแกรมหรือการดีคอมไพล์ (Decompile) เป็นขั้นตอนที่เป็นเหมือนการลองผิดลองถูกซึ่งจะได้ผลลัพธ์ที่แตกต่างกันไปในแต่ละครั้ง เพื่อที่จะให้ได้รหัสซอสโค้ดของภาษาชั้นสูงหรือโปรแกรมภาษาจากขั้นตอนการแปลง ในกรณีที่มีเพียงแค่รหัสไบนารี่สำหรับทำการวิเคราะห์

นอกจากนี้การทำวิศวกรรมย้อนกลับของซอฟแวร์ยังเกี่ยวข้องกับการตรวจสอบระบบรักษาความปลอดภัย (Security audit) หรือแม้นกระทั่งการพยายามกันส่วนที่ป้องกันการแก้ไขในซอฟแวร์ (Cracking)

ตัวอย่างของการทำวิศวกรรมย้อนกลับในอุปกรณ์อิเลกทรอนิกส์อย่างเครื่องเล่น DVD ในเครื่องเล่นจะมีระบบที่ควบคุมการใช้สื่อดิจิตอลได้แก่ Content Scrambling System หรือที่เรียกว่า CSS ซึ่งใช้งานโดย DVD Forum กับภาพยนตร์ที่มาในรูปแผ่น DVD ตั้งแต่ปี 1996 โดยวิธีการจะใช้การเข้ารหัสแบบง่าย และอาศัยอุปกรณ์ที่ผู้ผลิตกำหนดข้อตกลงในเรื่องลิขสิทธิ์ การใช้งานจะจำเพาะว่าดิจิตอลเอ้าพุทต้องอยู่ในรูปที่เป็นความคมชัดสูงหรือสามารถเล่นได้เฉพาะกับเครื่องเล่นเท่านั้น ดังนั้นเวลานำไปใช้กับอุปกรณ์หรือเครื่องเล่นประเภทอื่นจะไม่สามารถใช้งานได้ การทำวิศวกรรมย้อนกลับในกรณีนี้ก็เพื่อที่หาวิธีแก้ตัวป้องกันไม่ให้จำกัดการใช้งานอยู่แต่เฉพาะกับเครื่องเล่น DVD เท่านั้น สำหรับระบบ CSS นั้นก็มีมือดีมาแก้ โดยในปี 1999 นาย Jon Lech Johansen ได้พัฒนาโปรแกรมที่เป็นการขัดการทำงานของ CSS โดยเป็นโปรแกรมที่มีชื่อว่า DeCSS ซึ่งทำให้มีการอนุญาติให้มีการเข้ารหัสเพื่อให้แผ่น DVD นั้นสามารถเล่นได้บนเครื่องคอมพิวเตอร์ที่เป็นระบบปฏิบัติการแบบ Linux ได้

นอกจากนี้ตัวอย่างของการทำวิศวกรรมย้อนกลับได้แก่ การย้อนรอยวิธีการผลิตโดยที่ไม่ต้องทราบขั้นตอนการผลิต บางครั้งก็สามารถใช้หลักการวิศวกรรมย้อนกลับผลิตขึ้นมาได้เพียงแต่ทราบส่วนประกอบเท่านั้น เช่น ขบวนการผลิตยา ในบางประเทศมีการใช้วิศวกรรมย้อนกลับเพื่อให้ทราบขั้นตอนการผลิตยา ทำให้สามารถผลิตยาบางประเภทได้ในราคาถูก นอกจากตัวอย่างที่ใกล้ตัวแล้วยังมีตัวอย่างการทำวิศวกรรมย้อนกลับในสมัยสงครามโลกครั้งที่ 2 ที่รายละเอียดของจรวจ V2 ซึ่งเป็นขีปนาวุธที่ออกแบบโดยเยอรมัน สำหรับต่อต้านฝ่านสัมพันธมิตรในสมัยสงครามโลก ก็ถูกทำวิศวกรรมย้อนกลับโดยฝ่ายสัมพันธมิตรได้เป็นจรวจ R-1 ซึ่งผลิตขึ้นในรัสเซียจนกระทั่งพัฒนาต่อจนเป็น R-7 และยุคของการท่องอวกาศก็เริ่มขึ้น



รูปแสดงโปรแกรมที่ช่วยในการพัฒนาระบบงานฐานข้อมูลโดยการเขียนแผนภาพแสดงความสัมพันธ์

ในการพัฒนางานระบบฐานข้อมูลก็มีวิธีการทำที่จัดว่าเป็นวิศวกรรมย้อนกลับได้เช่นกัน โดยปกติการพัฒนาระบบงานฐานข้อมูลที่ทำกันอยู่ในทุกวันนี้จะต้องมีการออกแบบระบบโดยการเขียนเป็นแผนภาพที่แสดงความสัมพันธ์ของแต่ละส่วนของข้อมูลที่ต้องการจัดเก็บก่อน เมื่อเขียนแผนภาพแสดงความสัมพันธ์เสร็จเรียบร้อยแล้วก็สามารถทำการแปลงจากแผนภาพให้อยู่ในรูปแบบภาษาสำหรับฐานข้อมูล ขั้นตอนของวิศวกรรมย้อนกลับสำหรับงานฐานข้อมูลก็จะเป็นการที่ซอฟแวร์บางประเภทวิ่งเข้ามาอ่านรายการที่เป็นภาษาฐานข้อมูลแล้วแปลงกลับให้อยู่ในรูปของแผนภาพที่แสดงความสัมพันธ์ ซึ่งการที่จะสามารถทำได้ในลักษณะดังกล่าวนี้จะเป็นหลักการที่ในวิชาวิศวกรรมซอฟแวร์เรียกว่า การทำต้นแบบอย่างรวดเร็ว Rapid Prototyping ซึ่งเหมาะกับการที่ต้องพัฒนาระบบงานที่ต้องการมีการปรับเปลี่ยนแก้ไข ซอฟแวร์ที่สามารถทำงานได้ในลักษณะดังกล่าวจะเรียก ว่า CASE Tools หรือ Computer-Aided Software Engineering แต่ไม่ใช่ซอฟแวร์ที่เป็น CASE Tools ทุกตัวที่มีความสามารถในการทำวิศวกรรมย้อนกลับ จะเห็นว่าหลักการวิศวกรรมย้อนกลับเป็นเรื่องที่สามารถประยุกต์ใช้ได้ในงานหลาย ๆ ประเภทไม่เฉพาะกับงานทางด้าน IT เท่านั้น ถ้าจะพิจารณาว่าหลักการต่าง ๆ หรือขั้นตอนการทำเป็นการเรียนรู้เพื่อผูกวิศวกรรมย้อนกลับก็จะจัดเป็นการเรียนรู้เพื่อแก้

The End