

# نظرة تعليمية عامة إلى الهندسة العكسية

علي محمد علي رشدي

قسم الهندسة الكهربائية وهندسة الحاسبات، جامعة الملك عبد العزيز،

ص. ب. 80204 ، جدة 21589،

arushdi@kau.edu.sa

**المستخلص.** تقدم ورقة البحث هذه مراجعة تعليمية لأدبيات الهندسة العكسية، كما تتضمن وصفا موسعا لأهم ملامحها، وتناقش أهميتها وأدواتها وأغراضها. تشرح الورقة مفهوم الهندسة العكسية وتتناول قضية مشروعيتها بشيء من التفصيل. وتستطرد الورقة في توضيح مفهوم الهندسة العكسية من خلال إجراء مقارنة بين الهندستين العكسية والأمامية (التقليدية). أحد أبرز إسهامات الورقة هو محاولة تجلية موقع الهندسة العكسية على الخريطة الهندسية من خلال سرد العديد من الأنشطة العلمية والعملية وثيقة الصلة بالهندسة العكسية، مع إيضاح أوجه تشابهها واختلافها معها. وتشمل هذه الأنشطة الهندسة القيمية (هندسة القيمة)، وإعادة الهندسة (الهندرة)، وهندسة الذهاب والإياب، والبحث العلمي، واختبارات الصندوق الأسود، وتعرف الدوائر (الدارات) الكهربائية، وإعادة هيكلة البرمجيات، واستخراج المعنى (فك الشفرة)، والتشخيص الطبي والهندسي، وحل الألغاز البوليسية، والاستدلال بنوعيه المنطقي والاختزالي. وتختتم الورقة بالتأكيد على الحاجة الملحة لاستخلاص الفائدة القصوى من الهندسة العكسية.

## 1. مقدمة

يمكن وصف الهندسة بأنها عملية تحويل مجموعة من المواصفات أو المتطلبات الوظيفية والتشغيلية إلى منتج أو نظام يفي بهذه المواصفات والمتطلبات. ومن ثم فإن الهندسة تقيم علاقة رياضية من واحد إلى متعدد، لأن المواصفات والمتطلبات الأصلية تأخذ شكلا مفردا بينما يتسنى تنفيذها في أشكال عديدة. وحينما يستقر تنفيذ المنتج أو النظام إلى شكل محدد فإن العلاقة الرياضية التي تنشأها الهندسة تصبح علاقة من واحد إلى واحد. ثمة عملية تأخذ الصورة العكسية للعملية سألقة الذكر، وقد اصطلح على تسميتها بالهندسة العكسية (reverse engineering) ونجم عن ظهورها أن صارت الهندسة في صورتها العادية أو التقليدية تحتاج أحيانا إلى تمييزها باسم الهندسة الأمامية (forward engineering). مهمة الهندسة العكسية هو محاولة استرجاع المواصفات والمتطلبات عند توفر شكل محدد للمنتج أو النظام، ولذلك فهي تسعى لإنشاء علاقة رياضية من واحد إلى واحد يكون معكوسها مقاربا أو مماثلا قدر الإمكان للعلاقة التي أقامتها الهندسة الأمامية.

نقدم في ورقة البحث هذه وصفا تفصيليا لأهم ملامح الهندسة العكسية، كما نتحدث عن أهميتها وأدواتها وأغراضها وعلاقتها بالأنشطة الشبيهة بها. تشمل هذه الورقة على ستة فصول تلي

فصل المقدمة الحالي. يشرح الفصل الثاني مفهوم الهندسة العكسية ويتناول قضية مشروعيتها بشيء من التفصيل، بينما يجري الفصل الثالث مقارنة بين الهندستين العكسية والأمامية (التقليدية). ويتبع ذلك الفصل الرابع بسرد أنشطة علمية وعملية وثيقة الصلة بالهندسة العكسية، مع إيضاح أوجه تشابهها واختلافها مع الهندسة العكسية. يبين الفصل الخامس بعض أدوات وأساليب الهندسة العكسية، بينما يتحدث الفصل السادس عن أغراضها. وختاما يضيف الفصل السابع بعض التعليقات الإضافية متضمنة الحديث عن الحاجة الملحة لاستخلاص الفائدة القصوى من الهندسة العكسية.

## 2. معنى الهندسة العكسية ومشروعيتها

تعرف الهندسة العكسية بأنها عملية استنتاج مجموعة من المواصفات لمنتج أو نظام هندسي بواسطة الفحص المنظم لعينة أو عينات من هذا المنتج [1, 2]. وتفصيلا، نقول إن الهندسة العكسية هي القيام بفحص منتج معين (جهاز أو نظام كهربائي ميكانيكي، نبيطة إلكترونية، حزمة برمجية، ... إلخ) بهدف فهم التقانة والمواد والعمليات المستخدمة في تصميمه وتصنيعه وتشغيله، وغالبا ما يستلزم ذلك تفكيك وتدمير أو إتلاف ذلك المنتج، وغالبا أيضا ما يتم ذلك في إطار تنافسي يستهدف بناء وبيع منتج منافس يماثل المنتج الأصلي في وظيفته، ويتفادى قدر الإمكان أن يبدو استنساخا من المنتج الأصلي في كافة تفاصيله. وتمثل الهندسة العكسية بذلك استخلاصا للمعلومات والمهارات والأساليب التي سبق لأخرين اكتشافها من المنتجات التي صنعوها، أي أن الهندسة العكسية ترفع شعار "عدم إعادة اختراع العجلة" (not reinventing the wheel) [3]. وما يغري بممارسة الهندسة العكسية أنها تتعرف أسرار المنتج بأن تنفق وقتا وجهدا ومالا أقل بكثير مما بذلته الهندسة الأمامية في إبداعه وتطويره.

وفي حالة كون المنتج الأصلي نظاما برمجيا، يمكن تعريف الهندسة العكسية بأنها تحليل النظام البرمجي بهدف استحداث تمثيلات له عند مستويات أعلى من التجريد، كما يمكن النظر إلى الهندسة العكسية بوصفها اقتفاء للاتجاه العكسي في دورة تطوير النظام البرمجي، أي الاتجاه من طور التنفيذ إلى طور التحليل. ويلاحظ في تعريف الهندسة العكسية للبرمجيات أن يشتمل استخراج المعلومات من البرنامج الأصلي على معلومات التوثيق (documentation) [4].

وثمة من يرون أن الهندسة العكسية ليست إلا عملا من أعمال القرصنة (piracy)، والرأي السائد والراجح أنها ليست كذلك وأنها لا بأس بها ولا ضير منها [5, 6]. والواقع يقول إنها إحدى الممارسات الشائعة والمقبولة والمتوقعة في عالمنا اليوم. وعندما تقوم مؤسسة بعرض أحد منتجاتها في السوق المفتوحة، فإن عليها أن تفترض أنه سوف يهندس عكسيا من قبل الآخرين وبصفة خاصة من قبل منافسيها. وبمعنى آخر، عليها أن تدرك أن أغلب الأسرار الصناعية (trade secrets) التي أودعتها هذا المنتج قد صارت مكشوفة تماما أمام الآخرين، اللهم إلا النزر اليسير من بعض أسرار العمليات الصناعية التي استخدمتها لتصنيع المنتج. ولذلك تعتبر عملية بيع منتج في السوق المفتوحة شبيهة نظريا ومكافئة قانونيا لعملية نشر وإعلان وإذاعة الإبداعات والمعلومات والأسرار المضمنة في هذا المنتج [6].

ومن المقبول قانونيا وأخلاقيا أن تقوم أية مؤسسة بشراء أي منتج متاح تجاريا أو تحصل عليه بأية طريقة مشروعة أخرى، ثم تصمم وتطور منتجا مماثلا منافسا من خلال ابتكارها لطريقة تصنيع معينة، شريطة ألا يمثل المنتج الجديد أو طريقة تصنيعه انتهاكا لبراءات اختراع مملوكة لآخرين. وبعبارة أخرى، لا يوجد خلاف على كون الهندسة العكسية وسيلة مشروعة لاكتشاف الأسرار الصناعية غير المحمية ببراءات اختراع، طالما تم الاستحواذ على المنتج المطلوب هندسته عكسيا بوسيلة مشروعة [6]. ونظريا لا توجد حاجة للهندسة العكسية لمنتج مبني على اختراع محمي ببراءة اختراع لأن بيانات البراءة يفترض فيها أن توضح عمل هذا الاختراع وبأفضل السبل [6].

ولا تمثل الهندسة العكسية تهديدا جائرا أو خطيرا للصانع الرائد المبدع الذي يحقق سبق إلى توفير منتج معين بأساليب الهندسة الأمامية [7, 6]، وذلك لسببين: أولهما عنصر زمن السبق (lead time) الذي يتمتع به إزاء منافسيه الذين يهندسون منتجه عكسيا، ويستأثر خلاله بالسوق استثنائا يمكنه من جني الأرباح المستحقة له، وثانيهما أن الهندسة العكسية ليست مجانية رغم رخصها، فهي بدورها لها تكلفتها في الجهد والمال، مما قد يثني الكثيرين عن القيام بها.

وقد أجريت دراسة [6] على مدى تأثير رفاهية المجتمع بخياري السماح وعدم السماح بالهندسة العكسية كنشاط مشروع. إن السماح بالهندسة العكسية كنشاط مشروع قد يقلل حافز الرواد إلى الإبداع، ولكنه لا ينزل بهذا الحافز إلى مستويات غير مقبولة، كما أنه يزيد الحافز لديهم إلى متابعة الإبداع والمثابرة عليه وعدم الركون إلى ما أسلفوا من إنجاز. كذلك فإن هذا السماح يصب في مصلحة المستهلكين بما يوفره من منافسة محمودة تؤدي إلى تقليل الأسعار. وإذا كانت نفقات الهندسة العكسية تعد خسارة وتبيدا للمجتمع ككل، فمن الميسور تجنبها باللجوء إلى بديل أكثر اقتصادا هو الترخيص (licensing)، حيث يرخص الصانع الرائد للمنتجين المقلدين بإنتاج منتجه مقبل تعويض مادي يقل بوضوح عن التكاليف المحتملة للهندسة العكسية، وهنا يكون الصانعان الرائد والمقلد قد اقتسما العائد المتوفر من تفادي نفقات الهندسة العكسية.

### 3. مقارنة بين الهندستين العكسية والأمامية

نستطرد في توضيح مفهوم الهندسة العكسية من خلال مقارنتها بمقابلتها الهندسة الأمامية، وذلك عملا بالمثل السائر "وبضدها تتمايز الأشياء." يمكننا أن نلخص أهم الفروق بين الهندستين العكسية والأمامية فيما يلي:

- الهندسة الأمامية تنطلق من المواصفات والمتطلبات إلى المنتج، أما الهندسة العكسية فتبدأ من منتج موجود فعلا لتنتهي إلى صورة مبدئية مؤقتة للمواصفات والمتطلبات [8].
- عنصر التيقن أو التأكد (certainty) أكثر ظهورا لدى الهندسة الأمامية التي تستوجب الإتيان بمنتج يفي بالمواصفات والمتطلبات، بينما قد تختلف تفسيرات الهندسة العكسية لطابع المنتج الذي تفحصه، ومن ثم فقد تتفاوت المواصفات والمتطلبات التي تعزوها

إلى ذلك المنتج. وتتسم مشاريع الهندسة العكسية بدرجة أكبر من عدم التيقن، ولذلك فهي أوج إلى ضبط ذلك باستخدام أساليب إدارة المخاطر (risk management).

- لما كانت الهندسة الأمامية هي الهندسة التقليدية فإنها أكثر نضجا وانتشارا، كما أن جمهور المهندسين العاملين هم من المتخصصين الماهرين فيها، أما الهندسة العكسية فلا زالت وليدا ناشئا في مراحل التشكل الأولى، وثمة ندرة واضحة في المختصين الذين يمتلكون المهارات اللازمة لها.

- كلتا الهندستين الأمامية والعكسية مزيج من العلم والفن، ولكن الهندسة الأمامية إلى العلم أقرب، وكلتا الهندستين تستعمل الأساليب القياسية والخوارزمية فضلا عن الأساليب التنقيبية والتجريبية والاستكشافية، ولكن جرعة الأساليب التنقيبية والتجريبية والاستكشافية لدى الهندسة العكسية أكبر.

- تمثل الهندسة الأمامية عملية خلق وإبداع بالضرورة، وهي توفر وصفا صريحا لخطواتها بحيث يعرف المهندس ما هو مطلوب عمله سلفا، أما الهندسة العكسية فهي عملية فحص لا تستوجب ولا تستدعي بالضرورة تغييرا فيما هو قائم. وبينما تتسم الهندسة الأمامية بطابع إرشادي توجيهي (prescriptive)، فإن الهندسة العكسية تفتقر إلى مثل هذا الطابع، وتتمتع بدلا من ذلك بطابع تكييفي تهايوي (adaptive) حيث يتعين على المهندس أن يتكيف ويتواءم مع ما يجده من آثار عمل الآخرين [8]. وما ذكرناه لايفي كون الهندسة العكسية عنصرا من عناصر الإبداع، وذلك من ناحية أنها تؤدي إلى تنوع وتعدد مواصفات المنتج الواحد.

- النموذج الذي تبنيه الهندسة الأمامية يجب أن يكون صحيحا وكاملا، أما النموذج عند الهندسة العكسية فقد يكون ناقصا معيبا غير مكتمل ولكنه دائما أفضل من لا شيء.

- تتفاوت الهندستان بوضوح من ناحية استهلاكهما للوقت، فالهندسة العكسية عادة أسرع كثيرا من الهندسة الأمامية، وقد يصل عامل تفوقها في السرعة إلى زهاء عشر مرات وأحيانا إلى مائة مرة.

وهذه الاختلافات والفروق بين الهندستين العكسية والأمامية تمثل فرصة للتكامل والتعاون والتقارب أكثر بكثير من أن تشكل عائقا للتنافس والتباعد [2].

#### 4. أنشطة قريبة من الهندسة العكسية

نحاول هنا التأمل في الهندسة العكسية من زوايا عدة، من خلال النظر إلى بعض الأنشطة العلمية والعملية وثيقة الصلة بها مع إيضاح أوجه تشابهها واختلافها معها. ومن هذه الأنشطة:

- **الهندسة القيمية (هندسة القيمة) (value engineering):** وهي تشبه الهندسة العكسية في كونها تفككان وتحلان المنتجات والنظم، ولكن الهندسة القيمية تتميز بكون الهدف منها إيجاد فرص لتخفيض التكاليف.
- **إعادة الهندسة (الهندرة) (reengineering):** وهي تشبه الهندسة العكسية في كونها تعنيان بفحص نظم قائمة فعلا، ولكن الهندرة تتدخل بالتعديل في بنية وخصائص هذه النظم نفسها ومن ثم تقوم بتحويلها وتطويرها إلى نظم جديدة ذات خصائص أفضل. ولذلك تعرف الهندرة بالتجديد أو الإحياء (renovation) كما تعرف بالإصلاح أو الاستصلاح (reclamation) [2]. ويمكن وصف الهندرة بأنها عملية هندسة عكسية تعقبها تأسيسا عليها عملية هندسة أمامية.
- **هندسة الذهاب والإياب (round-trip engineering):** ووظيفتها التحديث المتزامن (synchronized updating) للكينونات البرمجية المرتبطة لتفادي وجود تناقض فيما تحويه من معلومات. لا تعني هندسة الذهاب والإياب مجرد الجمع بين الهندستين الأمامية والعكسية، بل يبرز فيها فضلا عنهما تحقيق عنصر التزامن.
- **البحث العلمي (scientific research):** الذي يستقصي القوانين الطبيعية ويستكشف أحوال المخلوقات، فهو أشبه ما يكون بمثابة هندسة عكسية لبعض مكونات هذا الكون، غير أن ثمة فروقا عديدة هامة بين البحث العلمي والهندسة العكسية أهمها أن البحث العلمي بمعناه المذكور يدرس على الأغلب كينونات من صنع الله عز وجل بينما الهندسة العكسية تتناول على الأغلب كينونات من صنع الإنسان.
- **اختبارات الصندوق الأسود (black-box tests):** وهي اختبارات تستعمل في التعرف على معالم النظم الهندسية بمعرفة مداخلها ومخارجها ووظيفتها العامة فقط [4] حيث يتعذر الوصول إلى أو التحكم في أو ملاحظة ما يوجد بداخلها، وهذه الاختبارات تشبه الهندسة العكسية في قيام كل منهما بفحص نظم معينة، ولكن هذه الاختبارات لا تفكك النظم الأصلية ولا تتلفها.
- **تعرف الدوائر (الدارات) الكهربائية (electric-circuit identification):** وهي حالة خاصة من اختبارات الصندوق الأسود، يعرف فيها أن ما بداخل الصندوق هو دائرة كهربائية ذات هيئة (topology) معلومة وعناصر معروفة النوع مجهولة القيم حيث يراد تحديد هذه القيم. وهذه المسألة أدق صياغة وأوضح غاية من المسألة العامة للهندسة العكسية، ولذلك تناولتها الأبحاث العلمية الرصينة بالفحص والتمحيص وتضم أدبياتها خوارزميات عديدة للحل. وربما شكلت هذه الأدبيات نواة صلبة تتمحور حولها أدبيات رصينة للهندسة العكسية.

- **إعادة الهيكلة (restructuring):** وهي تمثل في مجال البرمجيات تحويلًا من تمثيل معين إلى تمثيل آخر عند نفس مستوى التجريد مع المحافظة على السلوك الخارجي للنظام من ناحية الوظيفة والمفهوم. ولذلك فهي تماثل الهندسة العكسية في كونها تقعان تحت مظلة صيانة البرمجيات (software maintenance) [4].

- **استخراج المعنى (فك الشفرة) (cryptanalysis):** وهو تحويل نص معي غير مفهوم (تم توليده بخوارزمية ترميز (cryptography)) إلى نص واضح مفهوم. عملية استخراج المعنى فيها شبه واضح من الهندسة العكسية، وبخاصة تلك المتعلقة بالبرامج المعتمنة (obfuscated) [9] وهي برامج جرى تعميمها وتعقيدها عمداً ليتعذر فهم خطواتها. غير أن استخراج المعنى يمثل استكشافاً مقصوداً لذاته، بينما الهندسة العكسية عادة استكشاف ممد عمل إنتاجي تال.

- **التشخيص (diagnosis):** تشابه الهندسة العكسية عملية التشخيص بمعناها الطبي (تحديد الأمراض بمعرفة الأعراض وإجراء تحاليل وقياسات) وبمعناها الهندسي (تحديد الخلل بمعرفة نوع العطب وإجراء اختبارات وقياسات). ولكن التشخيص هو خطوة نحو علاج مرض أو إصلاح خلل في نظام قائم، بينما الهندسة العكسية تسعى لاستحداث نظام جديد.

- **حل الألغاز البوليسية (mystery solution):** وهو استخلاص خبايا وأسرار الجرائم الخفية، وهذا أمر يختلف ظاهرياً عن الهندسة العكسية ويبدو لأول وهلة مغايراً لها بالكلية، ولكنهما يتشابهان في كونهما يعولان على معلومات ناقصة أو متناقضة أو غير متيقنة، ويحاولان جبر النقص ومعالجة التناقض وتحديد ما يمكن الوثوق به، أملاً في استنتاج معلومات إضافية يمكن بها رسم صورة متكاملة متنسقة لفهم الموضوع برمته.

- **التفكير الاستدلالي (inferential thinking) أو الاستدلال (reasoning):** ويشمل ذلك الاستدلال المنطقي (logical reasoning) المبني على الاستنباط (deduction) وهو التوصل من مقدمات إلى نتائج كانت مبطنة وكامنة فيها، وهو ما يكافئ الانتقال من العام إلى الخاص، كما يشمل الاستدلال الاختزالي (reductive reasoning) الذي يحتاج إلى منهجية حصيفة تعصمه من الانزلاق إلى مغالطات منطقية (logical fallacies). وينقسم الاستدلال الاختزالي إلى (أ) الاستقراء (induction) وهو التوصل من مقدمات إلى نتائج خارجة عنها ولكنها بمثابة امتداد واستكمال لها على الأرجح، وهو ما يكافئ الانتقال من الخاص إلى العام، و(ب) الاستمثال الشارح (explanatory abduction) وهو الانتقال من الخاص إلى الخاص، و(ج) الاستمثال المبدع (innovative abduction) وهو الانتقال من العام إلى العام [10]. والاستدلال في أي منحى من مناحي الحياة وأي تخصص من تخصصات العلم لا يتأتى إلا أن يكون

توليفة من جميع أساليب الاستدلال الأربعة، ولكن نجاحه يتطلب أن يكون أقرب إلى (وإن كان غير مقتصر على) نوع معين من أنواع الاستدلال تمليه طبيعة التخصص محل الدراسة (انظر شكل 1). والهندسة العكسية تعد توليفة من جميع أساليب الاستدلال، ولكن نجاحها يتطلب أن تكون أقرب إلى نوعي الاستمثال اللذين يعرفان معا بالاستدلال التناظري أو التمثيلي (analogical reasoning) [11].

## 5. أدوات وأساليب الهندسة العكسية

تطورت أدوات وأساليب الهندسة العكسية تطورا كبيرا خلال الأعوام القليلة الماضية، إذ يوجد:

- برمجيات تحليل المكونات والوظائف للنظم المادية العتادية (الميكانيكية والكهربائية) والنظم المعرفية (نظم البرمجيات).
- برمجيات توظف أساليب الذكاء الصناعي (الاصطناعي) (artificial intelligence) وخوارزميات الرؤية الحاسوبية (computer vision) في خدمة الهندسة العكسية.
- برمجيات تتعرف على المنتج البرمجي، وتعيد كتابته بدلالة لغة عالية المستوى.
- قواعد البيانات المستمدة من و/أو الخادمة لجهود الهندسة العكسية.
- تقانات المسح الضوئي التي تستخدم حزم الليزر لمسح المنتج الأصلي، ومن ثم رسم صورة دقيقة له.
- آلات قياس دقيقة يمكن بواسطتها خلق نموذج ثلاثي الأبعاد للمنتج الأصلي، ومن ثم عمل نمذجة معضدة بالمحاسب للمنتج المطلوب.

## 6. أغراض الهندسة العكسية

أسلفنا القول إن الغرض الأهم للهندسة العكسية هو بناء وبيع منتج منافس يماثل المنتج الأصلي في وظيفته، ويتفادى قدر الإمكان أن يبدو استنساخا من المنتج الأصلي في كافة تفاصيله. وفي ذلك تلعب الهندسة العكسية دور البديل المشروع (غالبا) لعمليات التجسس الصناعي. توجد أغراض أخرى للهندسة العكسية نذكر منها:

- تقوم الشركات الصناعية بفحص منتجات المنافسين للتأكد من أنهم لم يقوموا بتطويرها من خلال انتهاك حقوق الملكية الفكرية (براءات الاختراع) العائدة لها.
- تتم الهندسة العكسية لمنتج معين أحيانا لأن التوثيق المكتوب لأعمال التصميم الخاصة به قد فقد (أو لم يتم أصلا)، أو لأن الأشخاص المسؤولين عن هذا التصميم قد تركوا العمل بالمؤسسة صاحبة المنتج، أو (في حالة المنشآت المعمارية الأثرية) لوجود فجوة تاريخية هائلة قد تصل إلى آلاف السنين تفصل المصممين والبناء الأصليين عن أولئك المنوط بهم الصيانة والترميم.

- تعتبر الهندسة العكسية ذلك الجزء من عملية الصيانة الذي يوفر للقائمين بها فهم النظام المطلوب صيانتة إلى الحد الذي يسمح لهم بتعديل النظام وتصحيح أخطائه وإصلاح أعطابه وتحسين أدائه وتفعيل وسائل الأمان به وضمان تكيفه مع البيئة المتغيرة [2]. ويبرز هذا الدور في صيانة البرمجيات خاصة تلك المتعلقة بقواعد البيانات أو المواقع على الشبكة العنكبوتية [14-12]، وأيضا تلك المسماة بالبرمجيات التراثية ( legacy software)، وهي برامج ذات أهمية استراتيجية بالغة للمؤسسات التي تستعملها، ولكنها تضخمت وفقدت مرونتها ومقدرتها على التجاوب مع احتياجات المستخدمين، ولم يعد ثم بديل لهندستها عكسيا سوى التخلص منها والبداية من الصفر. كذلك تعتبر الهندسة العكسية من الوسائل الفعالة لحماية البرمجيات ضد الفيروسات وغيرها من الجوارح البرمجية الخبيثة التي قد تخترقها أو تدمرها [15].

- تمثل الهندسة العكسية خطوة هامة في نقل وتوطين واستيعاب ثم توليد التقانة (التقنية) في البلدان النامية، فعن طريقها يتسنى للمهندسين المحليين فهم خصائص المنتجات العالمية وعمليات إنتاجها والمواد المستخدمة في تصنيعها، ويكتسبون القدرة على تطوير منتجات منافسة تستطيع مجاراة التطور التقني المستمر في المواد والعمليات الإنتاجية.

- تساعد الهندسة العكسية في المحافظة على بعض الحرف التراثية التي يتهددها عدم استمرارية الخلف في التلقي شفاهة عن السلف، لأسباب متعلقة بصعوبة الحرفة وطول الزمان اللازم لتعلمها وعدم وجود أي توثيق مكتوب لها [16].

- تمثل الهندسة العكسية وسيلة قوية للتعلم الفعال (الذاتي أو النشط) (active learning) للتصميم الهندسي [17]، وقد صح لدى كثير من الخبراء العالميين في تعليم التصميم الهندسي أن الأفضل تكليف طالب الهندسة بعدد من مشاريع الهندسة العكسية قبل انتقاله إلى دراسة موضوعات وأساليب التصميم الهندسي طبقا لرؤية الهندسة الأمامية. ويشجع على هذا التوجه أن الهندسة العكسية لا تكتفي الآن باستعادة النموذج الكامل للمنتج، وإنما تسعى أيضا لمعرفة نوايا وأهداف التصميم الأصلي [18].

- تقوم المؤسسات العسكرية في جميع الدول تقريبا بالهندسة العكسية للمنتجات الحربية للدول الأخرى، سواء كانت عدوة أم حليفة، وذلك للتعرف على أسرار التقانة الحربية المملوكة لها. وهنا تؤدي الهندسة العكسية دورا مكملا وربما بديلا لأعمال التجسس التي تقوم بها الاستخبارات. وفي خلال الحرب العالمية الثانية (1939ج-1945ج) اضطرت بعض الطائرات الأمريكية من طراز بي-29 (عند عودتها بعد ضربها للأراضي اليابانية) إلى الهبوط في أراضي الاتحاد السوفييتي السابق. وكان الاتحاد السوفييتي آنذاك حليفا مؤقتا لأمريكا، ولكنه لم يكن يملك طائرة قاذفة استراتيجية على غرار الطائرة الأمريكية بي-29 ولذلك حرص على أن يهندس هذه الطائرة عكسيا مستنسا إياها إلى طراز سوفييتي جديد. أما خلال الحرب الباردة (1945ج-1991ج) فقد وقع العكس، حيث رصدت الاستخبارات الأمريكية جائزة مليون دولار أمريكي لمن يأتيها



بطائرة مقاتلة سوفيينية سليمة من طراز ميغ، وقد حصلت بالفعل على طائرة من طراز ميغ-17، وأفادت من فحصها في تصميم وتصنيع المقاتلات الأمريكية إف-15 وإف-16 بحيث تمتعت هذه المقاتلات بمزايا تكتيكية واضحة على منافساتها السوفيينية.

- تلتقي الهندسة العكسية مع علوم الأحياء في عدة مجالات. فثمة مشروع يستهدف الهندسة العكسية لمخ ذبابة الفاكهة (ذبابة الدروسوفيلا) ومن ثم رسم مخطط الدوائر ( circuit diagram) لهذا المخ خلال عشرين عاما. وإذا نجح هذا المشروع، فإن ذلك سوف يعني قطع حوالي خمس الطريق نحو فهم مخ الإنسان فهما يبسر معالجة كثير من الاعتلالات العصبية مثل الاكتئاب والصرع وربما الخرف [19].

- المجال التقليدي للهندسة العكسية هو النظم غير الحيوية، ولكن طموحاتها بدأت تتجه إلى وتتداخل جزئيا مع النظم الحيوية. ويأخذ ذلك مسارين مختلفان كثيرا في طبيعتهما ومخرجاتهما وفي مدى شبههما بالهندسة العكسية. أما المسار الأول فيعني بتطوير الإنسان الآلي (الإنسالي أو الرابوط (robot))، وهذا يعني نوعا من الهندسة العكسية لكيونات حيوية (تشمل البشر) باستخدام تقانات غير حيوية لتوليد كينونات غير حيوية. بينما يهتم المسار الثاني باستنساخ أو تهجين الكائنات الحية على المستوى الجيني، ويقتصر شبه هذا المسار بالهندسة العكسية في كونه يدرس الكينونات الحيوية الموجودة ليحاكيها بكائنات حيوية، ولكنه لا يقوم بمحاكاتها من المبادئ الأولية بل يبدأ بعناصر تتوفر فيها صفة الحياة.

- يمكن أن يكون هدف الهندسة العكسية هو مجرد إشباع حب الاستطلاع (curiosity) عند كثير من الهواة، وفي هذا الإطار يرى البعض أن قيام الطفل بتحطيم لعبة جديدة لا يعبر عن نزعة تخريبية بقدر ما يبشر بنشاط بدائي مبكر للهندسة العكسية.

## 7. خاتمة

قدمنا في هذه الورقة وصفا سريعا لأهم ملامح وفوائد الهندسة العكسية. لقد لاحظ كثير من المختصين ما للهندسة العكسية من أهمية بالغة في مجالات عدة، وصدرت دعوات كثيرة إلى استخلاص الفائدة القصوى منها، وإلى دعم وتطوير البحث العلمي في موضوعاتها المختلفة. ولقد أسلفنا القول إن الهندسة العكسية تمثل خطوة هامة في نقل وتوطين واستيعاب ثم توليد التقانة (التقنية) في البلدان النامية. ولكن ممارسات الهندسة العكسية في هذه البلدان لا زالت بدائية وبعيدة عن أي تخصص علمي. ولذلك فالحاجة ماسة لتنمية تخصص الهندسة العكسية ليصبح تخصصا رصينا مرتبطا بغيره من التخصصات العلمية وخادما لكافة فروع الهندسة.

## المراجع

- [1] **Rekoff Jr., M. G.**, On Reverse Engineering, *IEEE Transactions on Systems, Man, And Cybernetics*, VOL. **SMC-15**, No. 2, pp. 244-252, 1985.
- [2] **Chikofsky, E. J.**, and **J. H. Cross II**, Reverse Engineering and Design Recovery: A Taxonomy, *IEEE Software*, Vol. 7, No. 1, pp. 13-17, 1990.
- [3] **Fogler, H. S.**, and **S. E. LeBlanc**, *Strategies for Creative Problem Solving*, 2<sup>nd</sup> Edition, Prentice-Hall, Upper Saddle River, NJ, USA, 2008.
- [4] **Radatz, J.** (Committee Chair), *The IEEE Standard Dictionary of Electrical and Electronics Terms*, 6<sup>th</sup> Ed., The IEEE Press, New York, NY, USA, 1997.
- [5] **Cifuentes, C.**, and **A. Fitzgerald**, Is Reverse Engineering Always Legal? *IT Professional*, Vol. 1, No. 2, pp. 42-48, 1999.
- [6] **Samuelson, P.**, and **S. Scotchmer**, The Law and Economics of Reverse Engineering, *The Yale Law Journal*, Vol. 111, pp. 1576-1663, 2002.
- [7] **McLoughlin, I.**, Secure Embedded Systems: The Threat of Reverse Engineering, *Proceedings of the 14th IEEE International Conference on Parallel and Distributed Systems 2008, ICPADS '08*, pp. 729-736, 2008.
- [8] **Blaha, M. R.**, The Case for Reverse Engineering, *IT Professional*, Vol. 1, No. 2, pp. 35-41, 1999.
- [9] **Udupa, S. K.**, **S. K. Debray**, and **M. Madou**, Deobfuscation: Reverse Engineering Obfuscated Code, *Proceedings of the 12th Working Conference on Reverse Engineering*, 10 pp., 2005.
- [10] **Eekels, J.**, On the Logic and Methodology of Engineering Design, *IChemE Transactions*, Vol. 80, Part A, pp. 615-624, 2002.
- [11] **Ball, L. J.**, **T. C. Ormerod**, and **N. J. Morley**, Spontaneous Analogizing in Engineering Design: A Comparative Analysis of Experts and Novices, *Design Studies*, Vol. 25, No. 5, pp. 495-508, 2004.
- [12] **McAllister, A.**, Reverse Engineering a Medical Database, *Proceedings of the Third Working Conference on Reverse Engineering 1996*, pp. 121-130, 1996.
- [13] **Lammari, N.**, **I. Comyn-Wattiau**, and **J. Akoka**, Extracting Generalization Hierarchies from Relational Databases: A Reverse Engineering Approach, *Data & Knowledge Engineering*, Vol. 63, No. 2, pp. 568-589, 2007.
- [14] **Boldyreff, C.**, and **R. Kewish**, Reverse Engineering to Achieve Maintainable WWW Sites, *Proceedings of the Eighth Working Conference on Reverse Engineering 2001*, pp. 249-257, 2001.
- [15] **Soo, S. M. K.**, **E. M. W. Yuen**, and **K. M. Yu**, Reverse Engineering of a Bamboo-Net Handicraft, *Ninth International Conference on Computer Aided Design and Computer Graphics, 2005*, 6 pp., 2005.
- [16] **Cipresso, T.**, and **M. Stamp**, Software Reverse Engineering, Chapter 31 in: P. Stavroulakis, and M. Stamp (Editors), *Handbook of Information and Communication Security*, Springer, Berlin, Germany, 2010.
- [17] **Wood, K. L.**, **D. Jensen**, **J. Bezdek**, and **K. N. Otto**, Reverse Engineering and Redesign: Courses to Incrementally and Systematically Teach Design, *Journal of Engineering Education*, Vol. 90, pp. 363-374, 2001.
- [18] **Barbero, B. R.**, The Recovery of Design Intent in Reverse Engineering Problems, *Computers & Industrial Engineering*, Vol. 56, No. 4, pp. 1265-1275, 2009.
- [19] **Adee, S.**, Reverse Engineering the Brain, *IEEE Spectrum*, Vol. 45, No. 6, pp. 51-53, 2008.

# **A Tutorial Overview of Reverse Engineering**

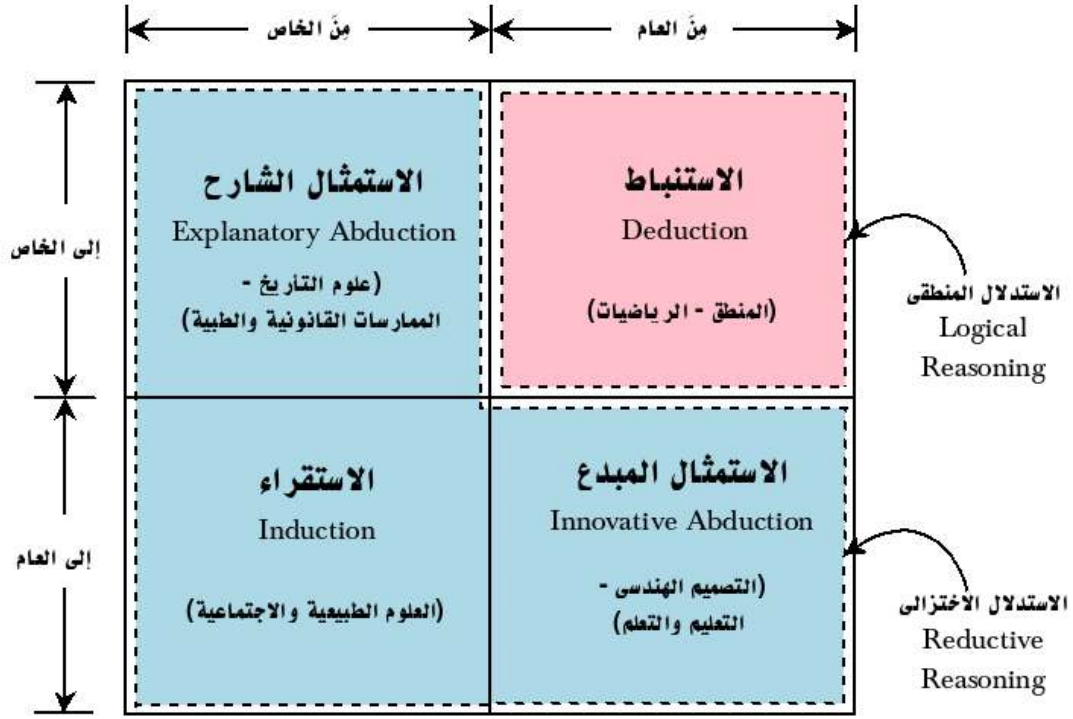
Ali Muhammad Ali Rushdi

Department of Electrical and Computer Engineering,

King Abdulaziz University,

P. O. Box 80204, Jeddah 21589, Saudi Arabia, arushdi@kau.edu.sa

**ABSTRACT.** This paper is a tutorial overview of the literature on reverse engineering. The paper includes an expanded description of the main features of reverse engineering, discusses its importance, tools, and goals, and addresses the issue of its legality in considerable detail. The paper elaborates its explanation of the concept of reverse engineering by offering a comparison between reverse engineering and forward (traditional) engineering. One of the most important contributions of the paper is its attempt to accurately locate reverse engineering on the engineering map through an extensive enumeration of scientific and practical activities closely related to reverse engineering, and through the identification of the similarities and dissimilarities which these activities have with reverse engineering. These activities include: value engineering, reengineering, round-trip engineering, scientific research, black-box tests, electric-circuit identification, software restructuring, cryptanalysis, medical and engineering diagnosis, mystery solution, and logical and reductive reasoning. The paper concludes by emphasizing the urgent need to make the most of reverse engineering.



شكل 1: تصنيف أساليب الاستدلال طبقاً لطبائع مقدماتها واستنتاجاتها من حيث الخصوصية والعمومية، مع بيان مجالات بروز وتخصص كل أسلوب.