

Building a Software System Using a Spiral Model to Evaluate the Overall Risk of Projects Using Fuzzy Number Theory

Jamal Salah Al-Din Sayed Majeed

Ro'a Amer Hussain

College of Computer Science and Mathematics

University of Mosul, Mosul, Iraq

Received on: 18/10/2012

Accepted on: 30/01/2013

ABSTRACT

This research aims presented a practical application for the process of assessing the overall risk of the projects following the risk management in software engineering steps, the life cycle is the most famous in this area is a (Spiral Model), this model represented by the core of the process to building a system based on customers information taken from them in the form of hearings conversations. This research depended on EA tool (Enterprise Architect) that building by a company (Sparex Systems) for represent the processes of stages to analysis because it is the basis currently used in the world and the most prevalent and most recently the base idea for this work is found the rate of aggregative risk in project by used fuzzy model for fuzzy number by follow Lee's algorithm. This system has been applied a practical in bank / public administration / northern region of the data / analysis and risk assessment of bank credit / short-term and long-term.

Keywords: Spiral Model, Enterprise Architect, Fuzzy Number, Lee Algorithm,

بناء نظام برمجي يتابع النموذج اللولبي لتقييم الخطر الإجمالي للمشاريع باستخدام نظرية التضييب الرقمي

رؤى عامر حسين

جمال صلاح الدين سيد مجيد

كلية علوم الحاسوب والرياضيات، جامعة الموصل

تاريخ قبول البحث: 2013/01/30

تاريخ استلام البحث: 2012/10/18

المخلص

يهدف البحث إلى تقديم تطبيق عملي لعملية تقييم المخاطر الكلية للمشاريع بإتباع خطوات إدارة المخاطر في هندسة البرمجيات، دورة حياة التي تعد الأشهر في هذا المجال وهو النموذج الحلزوني (Spiral Model) الذي يشكل الأساس في عملية بناء النظام الخاص ببحثنا بالاعتماد على معلومات الزبون التي تؤخذ منه على شكل جلسات حوارية. تم الاعتماد في هذا البحث على الأداة EA (Enterprise Architect) المصنع من قبل شركة (Sparex Systems) في عمليات التمثيل لمراحل التحليل لأنه الأساس في عمليات التحليل المستخدمة حالياً في العالم وأكثرها انتشاراً وأحدثها. تركز الفكرة الأساسية لهذا العمل على إيجاد النسبة الكلية للخطر الكلي (Rate of aggregative Risk) في المشروع باستخدام النموذج الضبابي الخاص بالتضييب الرقمي (Fuzzy Number) المتبع في خوارزمية لي (Lee Algorithm). تم تطبيق هذا النظام بشكل عملي على بنك الرشيد / الإدارة العامة / المنطقة الشمالية للبيانات الخاصة / تحليل وتقييم مخاطر البنك الائتمانية / قصيرة وطويلة الأجل.

الكلمات المفتاحية: النموذج اللولبي، الأداة EA، التضييب الرقمي، خوارزمية لي.

1. مقدمة

أصبحت صناعة البرمجيات لمجتمعاتنا المعاصرة ترتبط ارتباطاً وثيقاً بمستلزمات حياته ونموه وازدهاره، وهو منهج يهتم بدورة تطوير وإنشاء البرمجيات والتي تتضمن كل من تجميع وتحليل المتطلبات، التصميم والبناء، الاختبار والصيانة، وإدارة اقتصاديات هندسة البرمجيات [1][2]، يطلق على هذه المراحل اسم دورة حياة النظام

البرمجي (Software Life cycle) التي قد يبدو بعضها ليس له علاقة بالبرمجة وهناك الكثير من التصورات والنماذج في هندسة البرمجيات التي تصف عملية إنتاج برنامج والمراحل اللازمة لذلك، كما أن هذه الدورة خاضعة للتطوير دائماً [3].

2 . الأنموذج الحلزوني:

إن الأنموذج المعتمد في بناء النظام هو الأنموذج الحلزوني-ويطلق عليه أيضاً في بعض الأحيان بالأنموذج اللولبي- هذا الأنموذج معقد ومتقدم اقترحه الباحث باري بوهيم 1968م (Barry Boehm)، وهو أنموذج عملي برمجي تطوري يجمع ما بين الطبيعة التكرارية لأسلوب الأنموذج الأولي مع المفاهيم النظامية وسيطرة النموذج الشلال [4]، ويوفر هذا الأنموذج إمكانية التطوير السريع لنسخ أكثر اكتمالا من البرنامج ويتكون من مراحل عديدة:

1. المرحلة الأولى: في هذه المرحلة يجب على فريق العمل أن يضع في حسبانته كل مواطن الأخطار المحدقة بالمشروع ابتداءً من فقدان أو سرقة أو تلف احد الأجزاء المادية الخاصة مروراً بوفاة احد المبرمجين، ويشمل التحليل وضع خطة عند حدوث أي من الأخطار المحدقة بالمشروع، وبعد ذلك يبدأ جمع المتطلبات ووضع خطة ووضع الخطة البديلة. بهذا يكون أنموذج 1 (prototype1) المبدئي للنظام أو المشروع جاهزاً.

2. المرحلة الثانية: يعاد تحليل الأخطار للمرة الثانية بعد استكمال جمع المتطلبات من المستخدم، حيث تؤخذ المعلومات الأدق والتي تهتم بتفصيل أكثر قليلاً وبنفس الوقت التأكد بأنها لا تتعارض مع المتطلبات السابقة التي أرادها الزبون وبذلك نحصل على الأنموذج 2 (prototype2) وهذا الأنموذج يعتمد عليه في إعطاء كافة الأخطار المحدقة بتفاصيل للنظام.

3. المرحلة الثالثة: تحليل الأخطار للمرة الثالثة، وفي هذه المرحلة أيضاً يبدأ عمل النماذج للنظام بأكمله للمقارنة مع ما أراده الزبون وعمل خطة التجميع لكل النماذج.

4. المرحلة الرابعة: في هذه المرحلة يتم ما يلي:

- تحليل الأخطار للمرة الأخيرة.
- إجراء العمليات اللازمة الخاصة بكل نظام.
- عمل التصميم التفصيلي الدقيق.
- كتابة الشفرة.
- التجميع.
- الاختبار الجزئي والكلي والذي يسمى باختبار القبول (Acceptance test).

تسليم الأنموذج العرض الرابع (4 prototype) وهذا الأنموذج يسمى الندية التشغيلية ويجري عليه اختبار الموافقة أو القبول من قبل المستخدم. هذا الأنموذج طويل ومعقد ولكنه يوفر تكاليف باهظة في حالة حصول أخطاء بسبب وجود عملية التقصي عن الأخطار في كل خطوة وبذلك فإن الخطأ لا يتعدى المرحلة اللاحقة [5]. يجب الانتباه إلى المرحلة الأولى بشكل خاص بسبب كونها العمود المهم لمراحل التطوير ويعتمد عليها في بناء التصميم وكلما كانت المعلومات صحيحة ودقيقة (أي قليلة التطرف) كلما وفر الوقت والجهد والكلفة.

الشكل (1) يوضح الأنموذج الحلزوني بكل مراحلها وهذا الشكل هو المخطط الأصلي الذي وضعه Boehm والذي أصبح فيما بعد الأساس للنماذج التي طورت بحسب الشركات المستخدمة للأنموذج وخطة العمل

1.4 المعنى من منظور هندسة البرمجيات:

إن هندسة البرمجيات تعتبر إدارة المخاطر التسلسل الأول في عملية الإدارة بعد مرحلة الجدولة حيث إن عدم التنظيم مع توقع أحداث مستقبلية تؤدي إلى تأثيرات غير ملائمة وقد حددت جمعية إدارة المشاريع (APM Agency of Project Management) بان التعامل مع المخاطر يجب أن يكون باكتشافها و تقديرها إلى الحد الأدنى المقبول، والتأمين ضد حدوثها ونقلها للغير و التعامل وإدارتها بحرص. [7]

2.4 استراتيجيات المخاطر:

إن معهد إدارة المشاريع (Project Management Institute) قام بتصنيف استراتيجيات التدخل لدى حدوث المخاطر وهي كما يلي:

1.2.4 إستراتيجيات المخاطر المنفلة (Reactive Risk Strategies):

تعتمد معظم الفرق البرمجية على الاستراتيجيات المنفلة لإدارة المخاطرة حيث تراقب الإستراتيجية المنفلة وقوع المخاطر المحتملة، وتضع الموارد اللازمة لمعالجتها عندما تصبح مشاكل حقيقية. والأكثر شيوعاً في هذا النمط هو أن الفريق البرمجي لا يفعل شيئاً تجاه المخاطر إلى أن يحدث شيء خاطئ. عندها، "يتحرك الفريق بأقصى سرعة" إلى العمل في محاولة لتصحيح المشكلة بسرعة. ويسمى هذا الأسلوب غالباً "نمط إطفاء الحرق" (Fire Fighting Mode) وعندما يخفق ذلك يجري اعتماد أسلوب "إدارة الأزمات (Crisis Management) ويصبح المشروع في خطر حقيقي [4].

2.2.4 إستراتيجيات المخاطر الفاعلة (Proactive Risk Strategies):

الإستراتيجية الأكثر نكاهاً لإدارة المخاطرة هي الإستراتيجية الفاعلة، والتي تبدأ قبل بدء العمل التقني بكثير. حيث يجري تحديد المخاطر (Risks Identification) المحتملة وتقدير احتمال وقوعها (Occurrence Probability Estimation) وأثرها (Impact) وتصنيفها أيضاً في جدول أولوية حسب أهميتها . بعد ذلك يقوم الفريق البرمجي بوضع خطة لإدارة المخاطرة (Risk Plan Management) وخطة الطوارئ (Contingency Plan) [4].

3.4 صفات المخاطر البرمجية:

- بالرغم من أن هناك العديد من الاقتراحات لتعريف المخاطرة البرمجية (Software Risk) إلا أن هناك اتفاقاً عاماً على أن المخاطرة تتصف دوماً بصفتين:
- عدم اليقين (Uncertainty): قد يحصل الحدث المميز للمخاطرة وقد لا يحصل، أي لا يوجد مخاطر احتمالها 100 %.
- الخسارة (Loss): إذا أصبحت المخاطرة حقيقية فإن التبعات أو الخسائر الناتجة عن ذلك ستحصل.

4.4 أصناف المخاطر البرمجية:

من الضروري عند تحليل المخاطر إعطاء قيمة كمية لمستوى الشك ودرجة الخسارة المتعلقة بكل منها. ولتحقيق ذلك تصنف المخاطرة إلى الأصناف التالية:

المخاطرة التقنية (Technical Risk): تهدد المخاطر التقنية جودة ودقة وتوقيت البرمجية المطلوب إنتاجها. وعند حصول مخاطرة تقنية، يصبح تحقيق البرمجية صعباً أو مستحيلاً. تحدد المخاطر التقنية المشاكل المحتملة في

التصميم، التحقيق، الواجهات، الاختبار، والصيانة. إضافة إلى ذلك هناك عوامل أخرى للمخاطرة في هذا الإطار، كغموض المواصفات (Specification Ambiguity)، الشك التقني (Technical Uncertainty)، التقادم التقني (Technical Forward)، والتقنيات الجديدة. تحصل المخاطرة التقنية في أغلب الأحيان لأن المسألة أصعب حلاً مما تصورنا.

مخاطرة داخلية (Internal Risk): الوقت، الكلفة، النطاق، الجودة، التخطيط، الموارد البشرية، المواد والتجهيزات.

مخاطرة السوق (Market Risk): بناء منتج أو نظام ممتاز لا يرغب فيه أحد وهل سيكون المنتج الجديد مفيداً وقابلاً للتسويق للآخرين.

مخاطرة الجدول الزمني (Schedule Risk): وهي درجة الشك في أن يحافظ على الجدول الزمني للمشروع وأن يسلم المنتج في موعده.

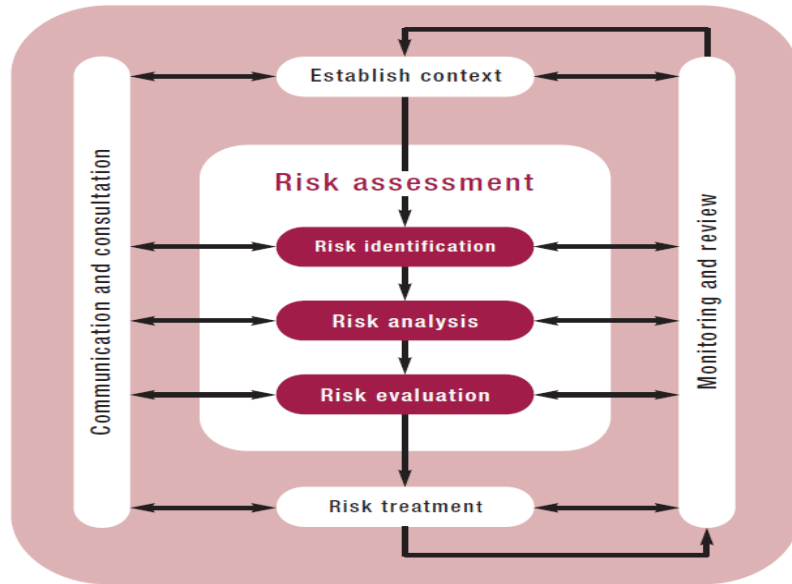
مخاطرة الدعم (support Risk): وهي درجة الشك في أن تكون البرمجيات سهلة التصحيح والتكيف والتحسين.

مخاطرة الأداء (Performance Risk): وهي درجة الشك في أن يتوافق المنتج مع المتطلبات المطلوبة منه، وأن يناسب الاستخدام المخطط له.

من المهم ملاحظة أن هذا التصنيف البسيط لن يعمل دوماً، فبعض المخاطر لا يمكن التنبؤ بها سلفاً. [4][5]

5. تقييم المخاطر:

تعتبر الفكرة الأساسية القائم عليها النظام المصمم هي تقييم المخاطر (Risk Assessment) للمشاريع دون التطرق لطرق المعالجة والسيطرة (Risk Mitigate & Monitor) والمراحل الآتية تعرف بشكل مفصل لكل مرحلة من مراحل عملية التقييم [4][9][10]. الشكل (2) يوضح الخطوات الأساسية للنظام المستخدم في التقييم.



شكل (2). يوضح مراحل عملية التقييم

1.5 تعريف الأخطار:

تعريف المخاطرة أو تحديد هوية المخاطرة (Risk Identification) هو إجراء لتوصيف التهديدات التي تعترض خطة المشروع عندما يقوم مدير المشروع بتعيين هوية المخاطر، فإنه يكون قد خطا الخطوة الأولى باتجاه تجنبها عند الإمكان والتحكم فيها أيضًا عند الضرورة.

هناك نوعان متميزان من المخاطر لجميع أصناف أو فئات المخاطر، مخاطر العامة (Generic Risks) والمخاطر الخاصة (Specific Risks). المخاطر العامة هي تهديد محتمل لكل مشروع برمجي، أما المخاطر الخاصة بالمنتج فلا يستطيع تعيينها إلا أولئك الذين لديهم فهم واضح للقضايا التقنية وللناس وللبيئة الخاصة بالمشروع الجاري تنفيذه. يجري فحص خطة المشروع وبيان نطاق البرمجيات بهدف تحديد المخاطر، ويوضع جواب عن السؤال التالي: " ما هي الصفات الخاصة لهذا المنتج التي قد تهدد خطتنا للمشروع؟ ". يجب تعيين كل من المخاطر العامة والخاصة بالمنتج بشكل نظامي، إحدى طرائق تحديد المخاطر هي أن نقوم بإنشاء قائمة حصر لعناصر المخاطرة (Risk Item Checklist). وهو ما سنتناوله الباحثة في تطبيق النظام. وتعتبر هذه المرحلة من أهم خطوات العمل. [9][10]

2.5 تحليل المخاطر:

كل نوع من أنواع الأخطار يتم أخذه وتجرى له عملية توصيف (description)، هناك عدة طرق لعملية تحليل الأخطار سنذكر منها قائمة حصر عناصر المخاطر .

1.2.5 قائمة حصر عناصر المخاطر:

إحدى طرائق تحليل المخاطر هي أن نقوم بإنشاء قائمة حصر عناصر المخاطرة يمكن استخدام هذه القائمة لتحديد المخاطر وتركيز الاهتمام في مجموعة جزئية من المخاطر المعروفة والقابلة للتنبؤ بها في الفئات الجزئية العمومية والتي تختلف من مشروع لآخر وبذلك تختلف قائمة تفقد العناصر المتعلقة بكل منها. إن التقييم الذاتي يقوم على إعداد قائمة بالعناصر القابلة للتعرض إلى المخاطر (مثلا: القيادة، العمال، الزبائن، الإستراتيجية والعمليات، الموارد الأخرى، نتائج الشركة) وقياس مدى التغيرات الحاملة للخسائر بواسطة مصفوفة محتواة في جدول القيادة، يُمكن من تحويل القياسات الكيفية إلى تقييمات كمية للمخاطرة المترتبة. الجدول (1) التالي يوضح شكل Check list لنظام معين كمثال على المخاطر القياسية التي تتعرض لها أمنية منظمة ما [4][11].

جدول (1). يوضح هيئة قائمة حصر لعناصر الخطر لنظام أمنية منظمة ما.

External parties	To maintain the security of the organization's information and information processing facilities that are accessed processed, communicated to, or managed by external parties.
Identification of risks related to external parties	The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
Addressing security when dealing with customers	All identified security requirements shall be addressed before giving customers access to the organization's information or assets.

Addressing security in third party agreements	Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.
Asset management	
Responsibility for assets	To achieve and maintain appropriate protection of organizational assets.
Inventory of assets	All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.
Ownership of assets	All information and assets associated with information processing facilities shall be owned by a designated part of the organization.
Acceptable use of assets	Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented and implemented.

2.2.5 توقع المخاطر:

تقوم هذه المرحلة بتوقع المخاطرة بمحاولة تقدير المخاطرة بطريقتين:

- **الأرجحية (Likelihood):** هنا يكون احتمال أن تكون المخاطرة حقيقية.
 - **العواقب (Consequence):** النتائج أو التبعات الناتجة عن المشاكل المتعلقة بالمخاطرة عند وقوعها.
- إن لأثر المخاطرة واحتمالها وقعاً متميزاً على اهتمام الإدارة [4][10]. حيث أنه يجب الانتباه إلى المخاطر الشديدة الأثر التي احتمال حدوثها كبيراً كان أو متوسطاً، وكذلك المخاطر التي لها أثر ضئيل واحتمال حدوث كبير، يمكن تحديد احتمال المخاطرة بإجراء تقديرات إفرادية ثم تطوير قيمة واحدة متفق عليها. ومع أن هذه الطريقة قابلة للتطبيق، فقد طورت طرائق أكثر تطوراً لتحديد احتمال المخاطرة. وإذا أخذنا في الحسبان نتائج واحتمالات كل خطر متضمنها مثل الجدول رقم (1)، يصبح من الممكن إعطاء الأولوية للأخطار الرئيسية والتي تحتاج إلى التحليل بطريقة أكثر تفصيلاً. [10] نفحص، خلال تقييم المخاطرة، دقة التقديرات التي أجريت أثناء توقع المخاطرة، ونحاول ترتيب أولويات المخاطر التي كشف عنها والبدء بالتفكير بطرائق لضبط أو تجنب المخاطر التي يحتمل حدوثها يتم قبل البدء بتقييم المخاطرة تحديد واحد من النوعين:

- **المستوى المرجعي للمخاطر (Risk Referent Level):** يجب تعريف المستوى المرجعي للمخاطرة حتى يكون التقييم مفيداً. في حالة معظم المشاريع البرمجية، تمثل أيضاً مكونات المخاطر (الأداء والكلفة والدعم والجدول الزمني) لمستويات مرجعية المخاطرة. أي أن هناك انخفاض حاد في مستوى الأداء، تجاوز الكلفة، صعوبة في توفر الدعم، انزلاق الجدول الزمني، أو مزيج من الأربعة، سوف يؤدي إلى إيقاف المشروع. يتوقف العمل إذا سبب مزيج من المخاطر مشاكل تؤدي إلى تجاوز واحد أو أكثر من المستويات المرجعية [4].
- **النقطة المرجعية (Reference Point):** في سياق تحليل المخاطر البرمجية، يكون لمستوى المخاطرة نقطة مفردة، تسمى النقطة المرجعية أو نقطة الانكسار (Break Point) يكون فيها القرار باستمرار المشروع أو إلغائه (حين تكون المشاكل كبيرة).

يكون لقرارات الاستمرار أو الإنهاء عند النقطة المرجعية الوزن ذاته في بعض الوقت بل يكون في معظم الحالات منطقة فيها مساحات من الشك يتنبأ المختصون بذلك بمجموعة من النقاط المرجعية التي تعرف منطقة الإنهاء، أي غالبا ما تكون محاولة التنبؤ بقرار الإدارة اعتمادًا على مزيج من قيم مرجعية هي محاولة صعبة. [9][4]

3.5 تخمين المخاطر:

إن الطريقة التي سنتبعها في تقدير أو تخمين المخاطر هي طريقة من الطرق الذكائية الخاصة بنظام التضييب الرقمي.

6. الأتمودج الضبابي المستخدم:

إن المجموعة الضبابية هي أصناف من العناصر مع درجة انتماء وان هذه المجموعات ميزت بدالة انتماء والتي خصصت لكل عنصر درجة انتماء ذات مدى ما بين الصفر والواحد [14]. إي عندما يأخذ العنصر درجة انتماء (1) فهذا يعني أن العنصر ينتمي بالتمام إلى المجموعات الضبابية، وعندما تكون درجة الانتماء (صفر) فهذا يعني إن العنصر لا ينتمي إلى المجموعة الضبابية، والدرجات الأخرى تتفاوت ما بين الصفر والواحد، عندما تكون درجة الانتماء العنصر (0.5) فهذا يعني أن العنصر ينتمي بنسبة (0.5) إلى المجموعات الضبابية ولا ينتمي إلى المجموعة بالنسبة نفسها ويدعى هذا العنصر بنقطة التوازن (Equilibrium Point) وقد تكون نقطة واحدة أو عدة نقاط. وعندما تكون درجة الانتماء (0.9) فهذا يعني أن العنصر ينتمي إلى المجموعة الضبابية بنسبة (0.9) ولا ينتمي إليها بنسبة (0.1) وهو أقرب إلى الانتماء من عدم الانتماء. أما المجموعة الاعتيادية "crisp set" فتعرف على أنها مجموعة من العناصر و أي عنصر يمكن أن ينتمي أو لا ينتمي إلى المجموعة، وأن المجموعة قد تكون محددة أو غير محددة وقد قدم باحثون آخرون تعاريف للمجموعات الضبابية [11]. -لا يسعنا ذكرها الآن-. إن اعتماد أتمودج التضييب الذي يحاكي المتغيرات في أتمودجنا المستخدم هو الاعتماد على بيئة القرارات التي تمثل إحدى طرائق المعالجة الحديثة لآليات اتخاذ القرار خلال بيئة المتغيرات، ويعبر عن درجة العضوية بدالة الانتماء $MA(X)$ التي تمثل درجة انتماء العنصر من المتغير X إلى المجموعة الضبابية A وتكتب بالشكل الآتي:

$$\mu_A : X \rightarrow [0,1] \quad \dots(1)$$

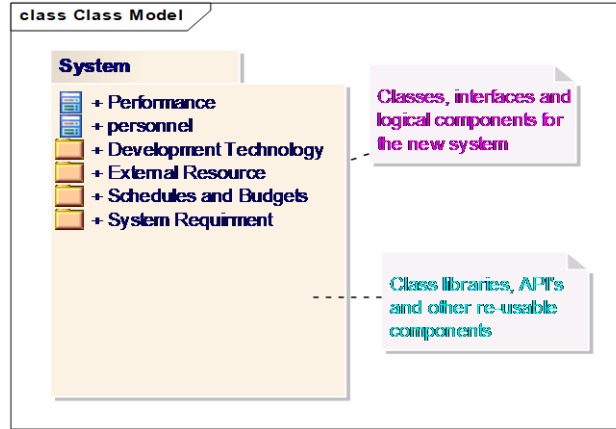
حيث أن:

$$\mu_A(x) = \begin{cases} 0 & \text{if } x \notin A \\ 1 & \text{if } x \in A \end{cases} \quad \dots(2)$$

يتغير الانتماء للعناصر من العضوية التامة إلى عدم العضوية، فهي إما أن تمتلك عضوية تامة، أو عضوية جزئية أو لا تمتلك عضوية، عليه فان عناصر المجموعات الاعتيادية لها انتماء تام أي أن $(MA(x)=1)$ أو أنها تأخذ قيم مختلفة حسب درجة انتماءها. [13]

1.6 العدد المضيب:

عند العمل مع قيم مضيبة وجعل الأداء الحسابي واضح، يجب استخدام مساحة كبيرة من التقييمات والتي تكون من نصيب الخبراء (أصحاب القرار الخاصين بالمشروع)، كما ويتم تنفيذ العمليات الحسابية أيضا، مثل الأرقام التقليدية، ويمكن للأعداد الغامضة أن تكون سلبية أو إيجابية، كما أخذ هذا في الاعتبار أثناء القيام بمرحلة الـ (Code) للنظام الحالي والمعادلة (3) توضح دالة الانتماء للأعداد المضيبة [13]



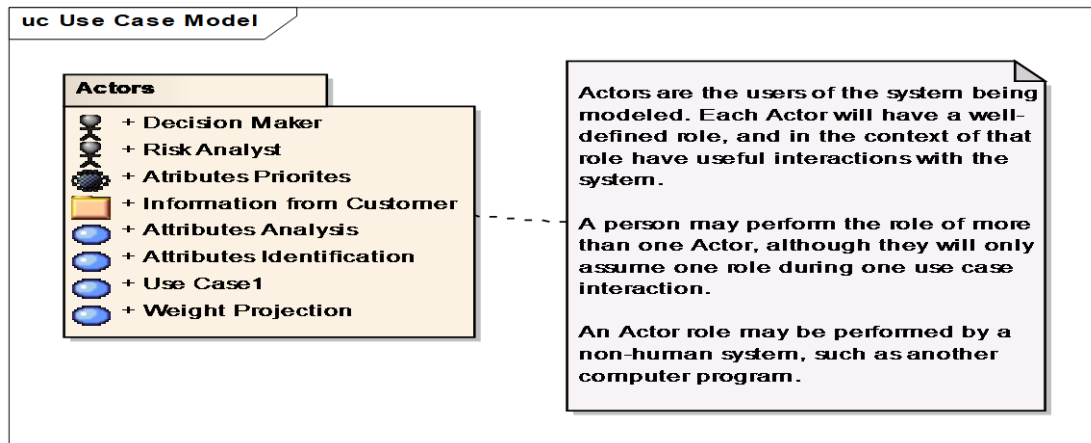
شكل (4). يوضح واجهة مخطط الصنف لأخطار بوهيم

حيث:

- إن كل من (Development Technology, External Recourses, Schedule and Budgets,) (System Requirement) تحوي مجموعة من (Risk) Items وتسمى بالمجموعة (Package).
 - إن كل من (personnel, Performance) تعرف بالصنف (Class).
- بعد ذلك نقوم بتحليل كل (Attribute) على حدة وتحديد نوعها ونوع التصنيف الذي ترجع إليه ويقوم بهذه العملية محلل المخاطر (Risk Analyst).

وبعد عملية تحديد السمات يأتي دور صناع القرار وذلك بتحديد أوزان للسمات (Attributes) بحسب درجة الخطر لها وحسب المتغيرات اللغوية المحددة سابقا حيث يكون أصحاب القرار أصحاب خبرة ومقيمين ماهرين ومتمرنين حيث كل سمة تحدد قيمتها وفق حدود أو فترات مغلقة لكل سمة حيث كل سمة تختلف عن الأخرى من ناحية أقصى حد علوي وأدنى حد سفلي. بعد ذلك يتم تطبيق المعادلة رقم (3) كما في الملحق رقم (3).

فيما يلي الشكل (5) يوضح أنموذج مخطط حالة الاستخدام الكلي، الذي تكون بعد عملية تحليل السمات الخاصة حسب تحليلات Barry Boehm.



شكل (5). أنموذج واجهة مخطط حالة الاستخدام الكلي

فيما يلي توضيح للشكل حيث:

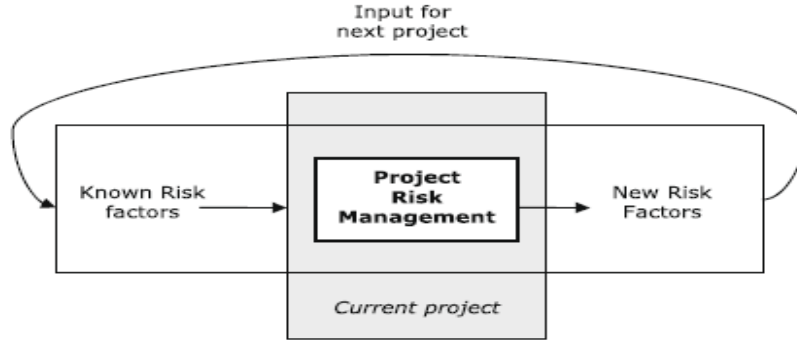
- يعرف (Decision Maker, Risk Analysis) كتمثيل بالمستخدمين (Actors).

- يعرف (Attributes Priorities) بالارتباطات (Collaborations) المتعلقة بالسمات.
- يعرف (Information From Customer) بالمجموعة الخاصة بالسمات (Package).
- يعرف كل من (Attributes identification, Attributes Analysis, Weight Projection) بحالة الاستخدام.

بعد ذلك تتم معالجة الأوزان وذلك بتطبيق الدالة المثلثية للأعداد المضطبة (Triangular Fuzzy Numbers) حيث سينتج لنا لكل قيمة من الأوزان الخاصة بال (Attributes) أعداد مضطبة تساعد في تقييم القيمة الكلية لنسبة المخاطر للمشروع.

2.7 المرحلة الثانية (تحليل عناصر الخطر):

وفقاً لأنموذج (Spiral Model) إن تحليل السمات في المرحلة السابقة تعتبر تحليلاً أولياً، في هذه المرحلة سيتم تحليلها مرة أخرى بشكل أدق وتعتبر الجلسة الثانية مع الزبون تكون أوسع شمولاً من الجلسة الأولى حيث سيظهر لنا ما يسمى بعناصر الخطر (Risk Items). تعرف (Risk Items) بأنها تفصيل لأنواع السمات (Attributes) حيث تكون أكثر تحديداً للنوع. وبالاعتماد على دراسات Boehm كما في ملحق (1) يتم تحليل السمات (Attributes) إلى عناصر الخطر (Risk Items) التي تعتبر التفصيل الدقيق لها. [4]



شكل (6). يوضح عملية التحليل التفصيلي

نلاحظ من الشكل (6) إن في كل جلسة حوارية مع الزبون تنتج لنا معلومات جديدة [4]. بعد ذلك يأتي دور مصنعي القرار في تقييم الوزن الخاص لكل (Risk Item). ومن ثم تطبيق القيم المقيمة على الدالة المثلثية للأعداد المضطبة، سينتج ثلاث أعداد مضطبة خاصة بكل عنصر من عناصر الخطر الخاصة بكل السمات التابعة للمشروع.

3.7 المرحلة الثالثة (تحليل درجة الخطورة):

في هذه المرحلة سيكون الاهتمام فقط على عناصر الخطر دون السمات لتحديد قيمة الخطورة لكل (Risk Item) الخاصة بالسمة الواحدة (Attribute) بالاعتماد على التصنيفات الخاصة للمخاطر ودرجة الأولوية لكل (Risk Items) وحسب أقصى حد علوي وأدنى حد سفلي. تختلف تقييمات الـ (Decision Makers) من شخص إلى آخر كل حسب نظريته في التقييم ويحدث انه يتفقان على قيمة معينة ويحدث أيضاً عدم الاتفاق بل والاختلاف يكون شاسعاً بعض الأحيان. بعد ذلك سنقوم بتطبيق القيم المقيمة بالدالة المثلثية للأعداد المضطبة. [14]

4.7 المرحلة الرابعة (تحليل درجة الأهمية):

نتبع في هذه المرحلة نفس خطوات المرحلة الثالثة بكل التفاصيل، لكن في هذه المرحلة سيتم تحديد درجة الأهمية الخاصة فقط بكل (Risk Item) دون السمات لاعتبار أن المرحلة الأولى فقط خاصة بالتحليل أما المراحل اللاحقة فخاصة بالتصميم والتطبيق والمراحل اللاحقة بحسب الأنموذج المتبع الخاص بنا [14].

8. إجراء العمليات الخاصة بعملية التضييب الرقمي:

بعد مرحلة التحليل التي شملت كل من (Attributes, Risk item, Grad of Risk Grade of Importance) تبدأ العمليات الخاصة بالتضييب الرقمي (Fuzzy Number) والتي تطبق على المعلومات الخاصة التي تم تقييمها من قبل مصنعي القرار حسب نظرية المجموعة المضببة لصناع القرار (Fuzzy group Decision Makers) وبعد تحويلها جميعاً إلى الأعداد المضببة بتطبيق الدالة المثلثية للأعداد المضببة التي تؤخذ بشكل كامل حتى لو حصل تكرار للبيانات بنفس القيم. سنرمز لعملية إيجاد المعدل الخاص بالسمات (Attributes) بالرمز A2 علماً أن عدد السمات ثابت وهو 6. [15]، وكما يلي:

$$A2(h) = \frac{\sum_{i=1}^2 D(\tilde{W}_{2(i,h)})}{2} \quad \dots(4)$$

حيث أن:

D هي الرمز الذي يمثل صناع القرار.

W2 تمثل الوزن المقيم الخاص بالسمات.

i تمثل عدد صناع القرار باعتبار أن لدينا اثنين من صناع القرار.

h تمثل عدد السمات والتي تمثل 6.

وبعد إيجاد المعدل الكلي الخاص بكل سمة لكل مصنعي القرار نقوم بإيجاد المعدل الكلي الخاص بكل عنصر تابع لكل سمة على حدة ونرمز لها بالرمز A1 وكما في المعادلة الآتية:

$$A1(h,k) = \frac{\sum_{i=1}^2 D(\tilde{W}_{1(i,h,k)})}{2} \quad \dots(5)$$

حيث أن:

D هي الرمز الذي يمثل صناع القرار

W1 تمثل الوزن المقيم الخاص بعناصر الخطر

i تمثل عدد صناع القرار باعتبار أن لدينا اثنين من صناع القرار

h تمثل عدد السمات والتي تمثل 6.

k تمثل رقم عنصر الخطر التابع لسمة معينة.

بعد ذلك نقوم بإيجاد معدل درجة الخطر (average of grade of risk) لكل عنصر خطر فقط وليس السمات، نرمز لهذه العملية بالرمز AR [14] وكما يأتي:

$$AR(h,k) = \frac{\sum_{i=1}^2 D(\tilde{F}_{(i,h,k)})}{2} \quad \dots(6)$$

حيث أن:

i تمثل عدد صناع القرار باعتبار أن لدينا اثنين من صناع القرار

h تمثل عدد السمات والتي تمثل 6.
 k تمثل رقم عنصر الخطر التابع لسمة معينة.
 \tilde{r} تمثل الوزن الخاص بدرجة الخطر الخاصة بعنصر الخطر تابع لسمة معينة.
 بعد ذلك نجد معدل درجة الأهمية لكل عنصر خطر من عناصر الخطر التابعة للسمات لكلا المقررين في المجموعة كما في المعادلة:

$$AI(h, k) = \frac{\sum_{i=1}^2 D(\tilde{i}(i, h, k))}{2} \quad \dots(7)$$

حيث أن:

i تمثل عدد صناعات القرار باعتبار أن لدينا اثنين من صناعات القرار
 h تمثل عدد السمات والتي تمثل 6.
 k تمثل رقم عنصر الخطر التابع لسمة معينة.
 i تمثل الوزن الخاص بدرجة الخطر الخاصة بعنصر الخطر التابع لسمة معينة.
 جميع الخطوات السابقة كانت تمهيد للمراحل القادمة ولتهيئة البيانات الخاصة التي قيمت من قبل DM الخاصين بالمشروع، حيث يؤخذ معدل نسبة الخطر الخاص بال Risk Item التابعة لل (Attribute) الواحد لكل وحدة على حدة كما في المعادلة الآتية:

$$G(h, k) = AR(h, k) \times AI(h, k) \quad \dots(8)$$

حيث أن:

G : تمثل معدل نسبة الخطر الخاصة بال (Risk Items) الواحد بشكل منفرد.
 AR : تمثل درجة الخطورة (grad of risk) الخاصة بال (Risk Items) الواحد بشكل منفرد.
 AI : تمثل درجة الأهمية (grad of importance) الخاصة بال (Risk Items) الواحد بشكل منفرد [14].
 بعد هذه المرحلة سنحتاج إلى إيجاد القيمة المطلقة للأوزان الخاصة بالسمات أيضا بشكل منفرد كل سمة على حدة لكل سمة محددة كما في المعادلة رقم (6):

$$W(X_h) = \frac{A2(h)}{\sum_{i=1}^6 A2(i)} \quad \dots(9)$$

حيث أن:

Xh رقم تسلسل الوزن الخاص بالسمة (Attribute).

$A2$ تمثل الوزن الخاص بالسمة الواحدة

h تمثل تسلسل أرقام السمات

وبنفس الوقت نقوم بإيجاد القيمة المطلقة للأوزان الخاصة بكل عنصر خطر بحسب التسلسل الخاص ضمن السمة الواحدة حيث يعد الترتيب بالتسلسل مهم من حيث درجة الخطورة والأهمية. المعادلة التالية توضح هذه العملية:

$$W(X_{hk}) = \frac{A1(h, k)}{\sum_{i=1}^{n(h)} A1(h, i)} \quad \dots(10)$$

أي أن:

W هو المتغير الخاص بالوزن

Xhk : تمثل القيمة المطلقة للأوزان الخاصة بكل عنصر خطر بحسب التسلسل الخاص ضمن السمة الواحدة

$A1$: تمثل الوزن الخاص بكل عنصر خطر

$n(h)$: تمثل التسلسل الخاص بكل عنصر خطر ضمن تسلسل السمة الواحدة

في الخطوات السابقة قمنا بإيجاد مطلق معدل نسبة الخطر لكل (Attribute) وأيضا معدل نسبة الخطورة لكل مطلق معدل نسبة الخطورة لكل (Risk Item)، بعد هذه المرحلة تأتي مرحلة إيجاد نسبة الخطورة الكلي للمشروع (Final Rate Of Aggregative Risk Of the Project) - RARP. بعد ذلك نقوم بعملية ضرب كل من معدل نسبة الخطر الخاص بال Risk Item التابعة لـ (Attribute) الواحد لكل واحدة على حدة في القيمة المطلقة للأوزان الخاصة بكل عنصر خطر بحسب التسلسل الخاص ضمن السمة الواحدة حيث يعد الترتيب بالتسلسل مهم من حيث درجة الخطورة والأهمية، ثم يجمع الناتج الخاص بكل واحدة بشكل كلي وبذلك نحصل على (The rate of aggregative risk for project) - RARP. تتم المقارنة مع المصفوفات الخاصة بالمقاييس والمعايير الدولية مثل مصفوفة 3×3 و 5×5 [16].

9. مرحلة التصميم:

استخدمنا في مرحلة التصميم الأداة EA (Enterprise Architect) حيث تم استخدام ما يسمى بالمخطط التسلسلي للأداة من أجل توضيح التسلسل الذي تقوم به الأداة بتنفيذ العمل بالاعتماد على ذكر مكونات الأداة بشكل أفقي وكل منها يحتوي على خط عمودي يوضح الفترة الزمنية التي يستمر بها في العمل خلال فترة حياة تطوير الأداة في حين يتم تناقل عدد من الرسائل والإيعازات بين هذه المكونات بالاعتماد على الوقت. يتم إرسال الرسائل بين المكونات التي تتعامل مع بعضها بالتسلسل المطلوب. تمثل هذه الرسائل عمليات أو معلومات يتم تنفيذها أو تناقلها لغرض القيام بعمل معين. يوضح الملحق رقم (2) مخطط التسلسل للأداة. أنّ كل عملية إرسال أو استقبال بين أي مكونين في الملحق (2) تحتوي على اسم وتسلسل يوضح هذا الإرسال.

10. مرحلة كتابة البرنامج للنظام (مرحلة الترميز):

تمت كتابة البرنامج باستخدام لغة (Express Edition Visual C# 2010) وهي من لغات شركة (Microsoft Office) التي تزيل العديد من التعقيدات والعقبات الموجودة في اللغات الأخرى مثل (C)، (C++)، و (JAVA) والتي كانت تترك المبرمجين وتسبب مشاكل من ناحية التصميم خاصة. كذلك، فإن (C#2008) تعد سهلة الاستخدام وهي تحتوي على العديد من الخواص الحديثة تمتعها بالقوة والمرونة، حيث إن اللغة لا تضع أي قيود على المبرمجين ومجال عملهم. وتستخدم في العديد من المجالات. كما إنها جهزت بالعديد من المزايا التي تجعل التعامل مع قواعد البيانات حيث يتم بشكل وجيد (مع وجود بعض التعقيدات). وقد تم تصميم النظام بدون استخدام أي مكتبات جاهزة للتعامل مع بيانات صانعي القرار المستدعاة من (Data Base Access) حيث كانت حاجتنا بنقل واجهة البيانات نفسها على واجهة النظام الخاص بنا بنفس شكلها في (Data Base Access) وكذلك تمت برمجة كل عملية من العمليات الرياضية.

11. مرحلة الاختبار:

تم اختبار النظام على نظامين من أنظمة البنوك الموجودة في العراق / الموصل. البنك الأول هو بنك الرشيد/ الإدارة العامة / المنطقة الشمالية، وهو بنك يدير واحداً وعشرين فرعاً تضم المنطقة الشمالية بأكملها، أما البنك الثاني فهو بنك الرافدين/ فرع موصل 3، ويعد أحد فروع بنك الرافدين الموجودة في الموصل. هذا النظام

لبيانات ثلاثة مصنعي قرار بدرجات وظيفية معاون مدير عام مكتب مندوب/ بنك الرشيد / الإدارة العامة / المنطقة الشمالية ومعاون مدير قسم المخاطر الائتمانية / بنك الرافدين / فرع موصل 3 وكانت النتائج جيدة جدا بالمقارنة مع نسب البنوك للمخاطر الائتمانية التي عدت سابقا بمعدل 88% بالأخذ بنظر الاعتبار النسب التي أخذت من صانعي القرار بشكل كلي.

12. النتائج والاستنتاجات:

1. التلازم بين النشاط الاقتصادي والمخاطرة يجعل كشف وتقييم المخاطر بشكل آني أمراً غير ممكن، لكن ذلك لا يعني بالضرورة عدم إمكانية التعامل معها وفق مجموعة من السياسات والاستراتيجيات التي تجعل آثارها ونتائجها متحكم فيها إلى حد بعيد.
 2. إن النموذج اللولبي هو من أيقن النماذج وأكثرها شمولاً في إدارة المخاطر من النماذج الأخرى المتبعة في هندسة البرمجيات، كما تم تنفيذ هذا النظام لبيانات ثلاثة مصنعي قرار بدرجات وظيفية: معاون مدير عام مكتب مندوب/ بنك الرشيد / الإدارة العامة / المنطقة الشمالية ومعاون مدير قسم المخاطر الائتمانية / بنك الرافدين / فرع موصل 3.
 3. يعد النموذج الضبابي للأعداد المضطربة أكثر دقة من العمليات الحسابية المتبعة في البنوك مثل قوانين كفاية رأس المال وغيرها، ويوفر هذا النموذج طريقة بسيطة جداً للحصول على استنتاجات محددة من معلومات غير دقيقة وغامضة ومهمة. وبمعنى آخر، فإن التضييب الرقمي يحاكي حالات اتخاذ القرارات لدى الإنسان مقرونة بالمحاولات لإيجاد حلول دقيقة من بيانات غير دقيقة أو تقريبية.
- حيث وجد أن النموذج الضبابي للأعداد المضطربة مع استخدام برنامج EA بتمثيل مراحل التحليل والتصميم يجعل من النظام الحاسوبي الذي تم إعداده يمكن الاستفادة منه بنسبة كبيرة بسبب الدقة الموجودة فيه لأن هذا الأسلوب مخصص أصلاً لإدارة مخاطر النظم المعقدة. عند المقارنة مع النسب السابقة التي أخذت من البنك لعمليات إيجاد نسبة الخطورة للقروض الائتمانية سابقة وتطبيقها بالنظام الخاص بالبحث نجد أن نسبة النجاح للقيم الناتجة من التطبيق المضطرب تفوق النسب الناتجة من العمليات الخاصة بالبنك التقليدية حيث كانت النسبة 88% من النسب بالأخذ بنظر الاعتبار النسب التي أخذت من صانعي القرار بشكل كلي. الجدول رقم (2) يوضح النسب الناتجة.

جدول (2). يوضح تباين النسب الكلية

النسبة الناتجة للتقييم بالتصنيف الرقمي	النسب الناتجة للتقييم بالطرق التقليدية	الطريقة المتبعة للتقييم
%88-80	%70	تقييم المخاطر الخاصة ببنك الرشيد بوجود 6 Attribute و 2 من صناع القرار
%86-77	%60	تقييم المخاطر ببنك الرافدين 3 بوجود 6 attribute و 1 صانع قرار
%80-70	%63	تقييم المخاطر ببنك الرشيد بوجود 3 attribute و 2 من صناع القرار
%88-80	%60	تقييم المخاطر ببنك الرافدين 3 بوجود 3 attribute و 1 صانع قرار

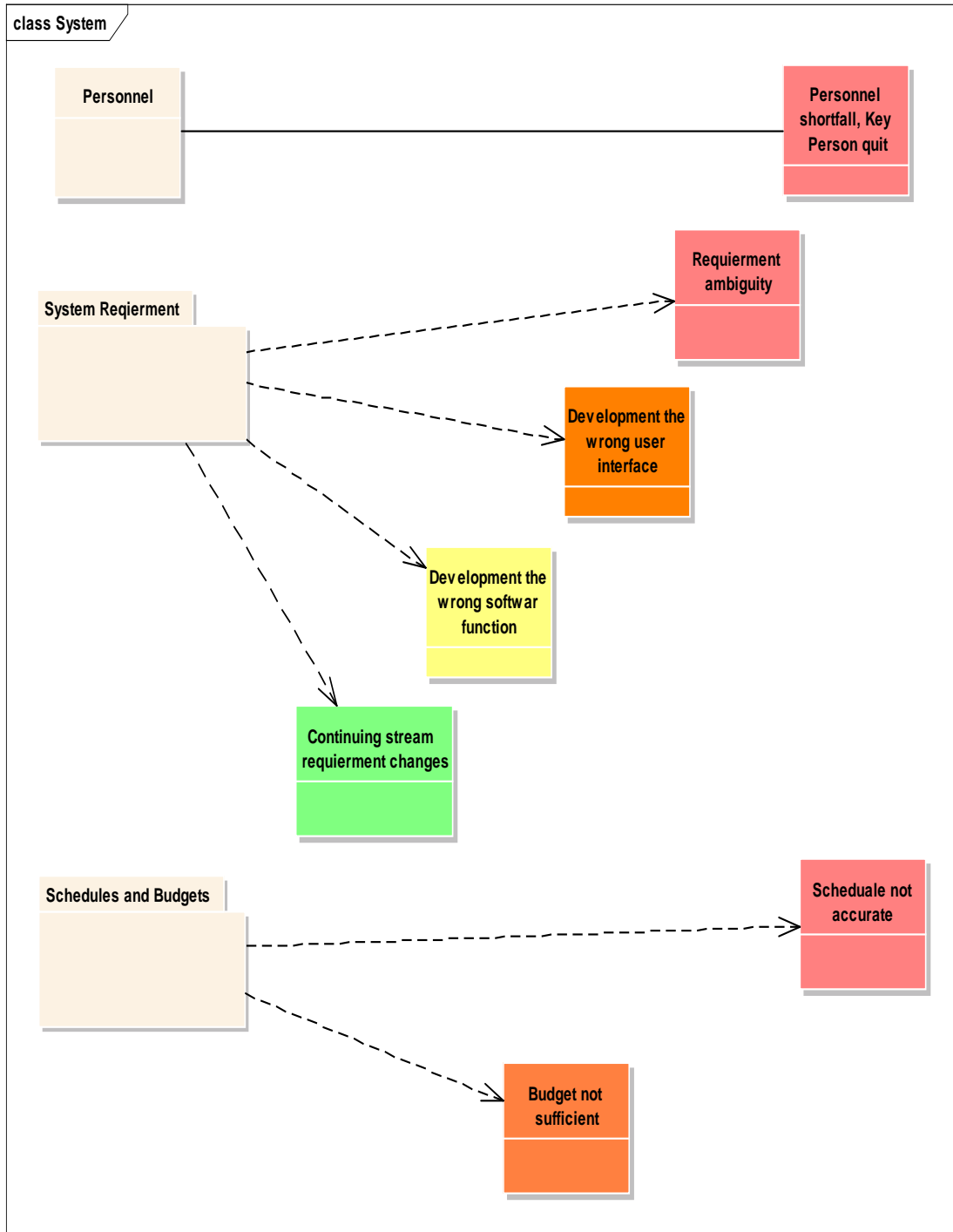
13. التوصيات:

1. يمكن تطوير العمل الحالي باتجاهات مختلف. ولعل من التوصيات الملحة هو تطوير النظام لمعالجة الأخطار بشكل آني ليشمل جميع طرق المعالجة والسيطرة في إدارة مخاطر هندسة البرمجيات وبطبيعة الحال فان مثل هذا المشروع يتطلب معلومات وتفصيل إضافية تحتاج إلى جهود وتخصصات إضافية.
2. ومن التوصيات العامة فإننا نوصي بإنشاء مركز تخصصي لإدارة المخاطر للبنوك العراقية في كلاً من جوانبه (التقييم والمعالجة) وليس للبنوك فقط ولكن المشاريع التجارية كافة وكذلك استخدامات المنطق المضرب في عمليات التحليل والسيطرة لدقته في التقييم.

المصادر

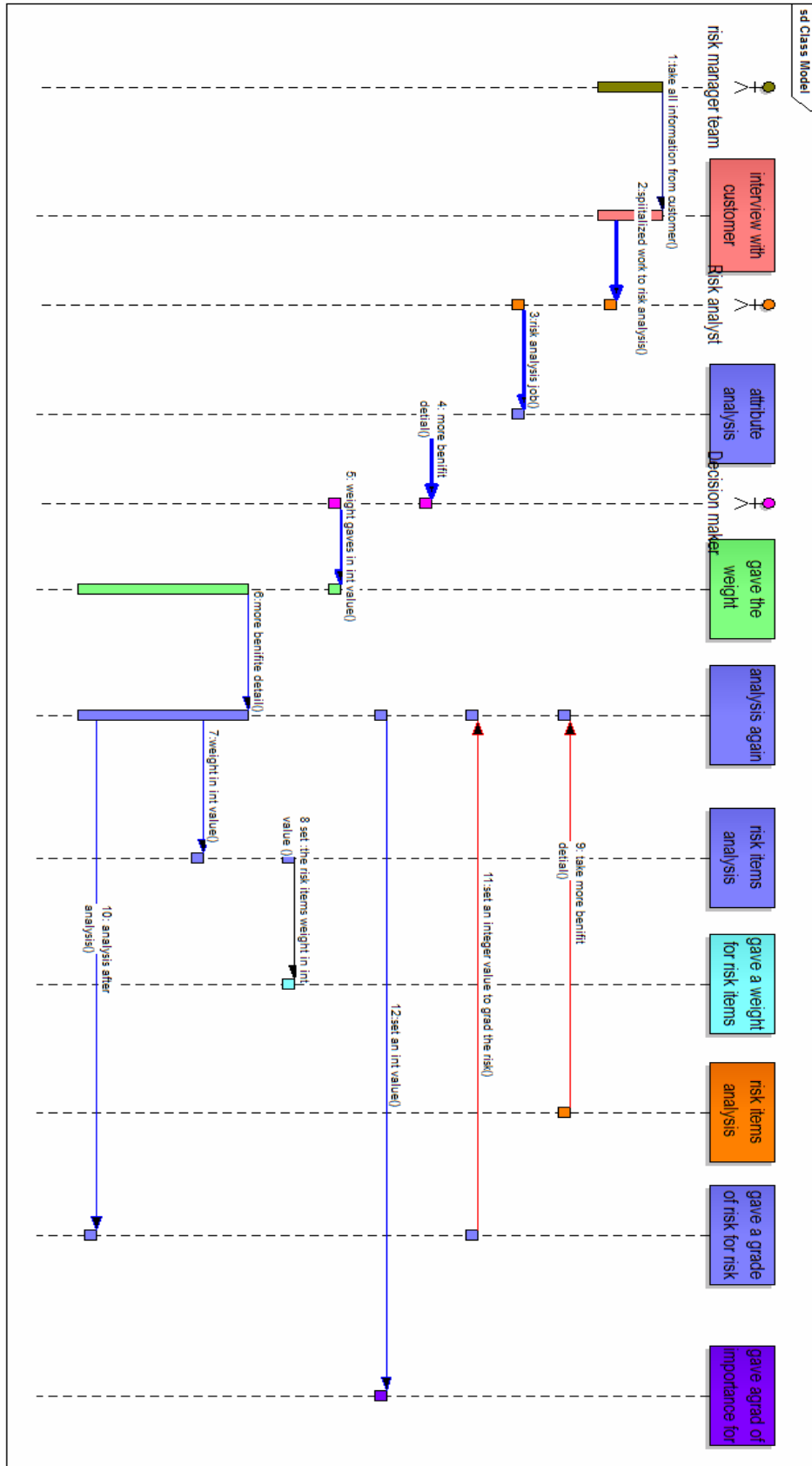
- [1] Mohamad, Jasni Zain Wan Maseri Wan Mohd Eyas El-Qawasmeh (Eds.) "Software Engineering and Computer Systems" Second International Conference, ICSECS 2011, Kuantan, Pahang, Malaysia, June 27-29, 2011 Proceedings, Part III
- [2] Gillian Adens "The Role of Risk in a Modern Software Development" Process First Published: February 2004 ,Last Updated: January 2011 ,Copyright 2004-2010, Tassc Limited. All Rights Reserved.
- [3] Karin van den Berg "Finding Open options An Open Source software evaluation model with a case study on Course Management Systems "Master Thesis Tilburg, August 2005
- [4] Roger S. Pressmqn, Ph.D. "Software Engineering: Practitioner, Sa Pproachs, seven Edition .published by McGraw-Hill, a business unit of The McGraw-Hill Companies, Inc.c opyright @2010 by The McGraw-Hill Companies
- [5] Gillian Adens, Robert Armstrong "Software Project Risks" First published: August 2001 Last Updated: January 2011 Copyright 2001-2009, Tassc Limited. All Rights Reserved.
- [6] Pratap k.j .mohapatra "software Engineering", Copyright © 2010, New Age International (P) Ltd., Publishers Published by New Age International (P) Ltd., Publishers
- [7] Jakub Miler, Janusz Górski, October -2001 "Implementing risk Management in software projects" *Department of Applied Informatics Technical University of Poland*
- [8] Jonsas.Ekeroot, "Audio Software Developmet", 2007, Master Thesis, Lulea University of Technology
- [9] بلعزوز بن علي، جامعة الشلف، "استراتيجيات إدارة المخاطر في المعاملات المالية"، 2009، مجلة الباحث.
- [10] Jim Stevens, Alex Sprague "Risk Assessment in Software Development Projects, Contributors November 20, 2011. "Examining the Value of Risk Assessment and the Models of Risk in Software Development, Version 2.3.
- [11] فاضل عباس، الطائي ونجلاء، سعد أشرابي، "نموذج الانحدار الذاتي المضيب مع التطبيق"، المجلة العراقية للعلوم الإحصائية، 2009.
- [12] Alexia, Pacheco, Oldemar, Rodrguez, "Principal Components Analysis for Trapezoidal Fuzzy Numbers", Costarican Institute of Electricity.
- [13] Lily Lin, and Huey-Ming Lee A Fuzzy Assessment Model, 2007, International Journal Of Computers, Issue 3, Volume, 2007.
- [14] Jared, Bene, "Risk Management for Software Intensive Systems Common Risks" 2003, DOD Acquistion.
- [15] Shyi-Ming Chen, "Fuzzy group decision making", 1997, Department of Electronic Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan, Republic of China.
- [16] Paul Barringer, P.E "Risk Matrix: Know when to accept the risk. Know when to reject the risk. Barringer & Associates, Inc. 2006

ملحق (1):



يوضح مخطط الصنف لتحليل المخاطر، عناصر الخطر، الأولوية

ملحق (2):



شكل (2). يوضح المخطط التسلسلي لتصميم النظام

ملحق (3)

مثال على حساب قيم السمات:

يتم وضع القيمة الخاصة بالسمة من قبل فريق العمل وكمثال على ذلك يهتم المحلل_ الذي يعتبر احد أهم الأشخاص الذين يعملون في فريق هندسة البرمجيات- بالأخطار المتعلقة بدرجة الخطورة الخاصة بالمتطلبات للنظام (والتي بدورها تحوي 4 عناصر خطر بعد تحليلها) وبعد ذلك يأتي دور صانع القرار رقم 1 فيعطيها قيمة مثلا 60% (فقط للسمة دون عناصر الخطر) فتؤخذ هذه القيمة وتتم معالجتها بالدالة المثلثية للأعداد المضطبة التي يجب ذكر أقصى حد علوي وأدنى حد سفلي والمركز مثلا [56-64-68] كقيم p, q, r . نفس العملية تتم بالنسبة لصانع القرار رقم 2 ثم تؤخذ القيم ليتم معالجتها في خوارزمية Lee.