



COURSE OVERVIEW DM0443

API-780: Security Risk Assessment Methodology for the Petroleum & Petrochemical Industries

Course Title

API-780: Security Risk Assessment Methodology for the Petroleum & Petrochemical Industries

Course Date/Venue

October 04-08, 2026/Online Virtual Training

Course Reference

DM0443

Course Duration/Credits

Five days/2.75 CEUs/27.5 PDHs



Course Description



This practical and highly-interactive course includes various practical sessions and exercises. Theory learnt will be applied using our state-of-the-art simulators.



This course is designed to provide participants with a detailed and up-to-date overview of API-780: Security Risk Assessment Methodology for the Petroleum & Petrochemical Industries. It covers the fundamentals of security risk assessment, security risk management principles and security risk assessment concepts; the security threats, security consequences and API's five-step SRA methodology; the security risk assessment planning, building the SRA team and defining scope and objectives; the information collection and sources of information; and the site inspection and previous incident analysis.



During this interactive course, participants will learn the security risk assessment, threat intelligence, layers of security protection and vulnerability ranking; the risk analysis, risk ranking, countermeasure identification and evaluating countermeasures; the documentation and reporting including validation and follow-up; the characterization worksheet, threat assessment worksheet, vulnerability assessment worksheet and recommendation worksheet; the pipeline threats, remote asset protection, critical infrastructure considerations and risk reduction strategies; and the truck transportation, rail transportation, marine transportation and supply chain security.



Course Objectives/Outcomes & Benefits for the Participants

Upon the successful completion of this course, each participant will be able to:-

- Get certified as a “*Certified Security Risk Assessor (SRA)*”
- Discuss the fundamentals of security risk assessment, security risk management principles and security risk assessment concepts
- Identify security threats, security consequences and API's five-step SRA methodology
- Carryout security risk assessment planning, build the SRA team and define scope and objectives
- Review information collection and sources of information and perform site inspection and previous incident analysis
- Perform security risk assessment covering asset characterization, threat assessment and vulnerability assessment
- Recognize threat intelligence, layers of security protection and vulnerability ranking
- Apply risk analysis, risk ranking, countermeasure identification and evaluating countermeasures
- Carryout documentation and reporting including validation and follow-up
- Review characterization worksheet, threat assessment worksheet, vulnerability assessment worksheet and recommendation worksheet
- Assess pipeline threats and apply remote asset protection, critical infrastructure considerations and risk reduction strategies
- Monitor truck transportation, rail transportation, marine transportation and supply chain security

Who Should Attend

This course provides an overview of all significant aspects and considerations of security risk assessment for risk management professionals, corporate security and asset protection professionals, security managers, supervisors and officers, security engineers and security systems specialists, emergency response and crisis management personnel and for those who are involved in physical and cyber security, facility and process design and operations, safety, logistics, emergency response, management and other disciplines as necessary.

Training Methodology

All our Courses are including **Hands-on Practical Sessions** using equipment, State-of-the-Art Simulators, Drawings, Case Studies, Videos and Exercises. The courses include the following training methodologies as a percentage of the total tuition hours:-

30% Lectures

20% Practical Workshops & Work Presentations

30% Hands-on Practical Exercises & Case Studies

20% Simulators (Hardware & Software) & Videos

In an unlikely event, the course instructor may modify the above training methodology before or during the course for technical reasons.

Learning Design & Customization

This course can be customized to the exact requirements of clients. Haward Technology is so proud of our huge capabilities in tailoring our courses to the training needs of our valued clients.





Course Certificate(s)

- (1) Internationally recognized Competency Certificates and Plastic Wallet Cards will be issued to participants who completed a minimum of 80% of the total tuition hours and successfully passed the exam at the end of the course. Successful candidate will be certified as a "Certified Security Risk Assessor (SRA)". Certificates are valid for 5 years.

Sample of Certificates

The following are samples of the certificates that will be awarded to course participants:-





- (2) Official Transcript of Records will be provided to the successful delegates with the equivalent number of ANSI/IACET accredited Continuing Education Units (CEUs) earned during the course.

Haward Technology * CEUs * Haward Technology * CEUs * Haward Technology * CEUs * Haward Technology *

 **Haward Technology Middle East**
Continuing Professional Development (HTME-CPD)

CEUs

CEU Official Transcript of Records

TOR Issuance Date: 14-Nov-25
HTME No. 74851
Participant Name: Waleed Al Habeeb

Program Ref.	Program Title	Program Date	No. of Contact Hours	CEU's
DM0443	API-780: Security Risk Assessment Methodology for the Petroleum & Petrochemical Industries	Nov 10-14, 2025	30	3.0

Total No. of CEU's Earned as of TOR Issuance Date **3.0**

TRUE COPY

Jaryl Castillo
Academic Director

Haward Technology has been approved as an Accredited Provider by the International Association for Continuing Education and Training (IACET), 2201 Cooperative Way, Suite 500, Herndon, VA 20171, USA. In obtaining this approval, Haward Technology has demonstrated that it complies with the ANSI/IACET 1-2018 Standard which is widely recognized as the standard of good practice internationally. As a result of their Authorized Provider membership status, Haward Technology is authorized to offer IACET CEUs for programs that qualify under the ANSI/IACET 1-2018 Standard.

Haward Technology's courses meet the professional certification and continuing education requirements for participants seeking Continuing Education Units (CEUs) in accordance with the rules & regulations of the International Association for Continuing Education & Training (IACET). IACET is an international authority that evaluates programs according to strict, research-based criteria and guidelines. The CEU is an internationally accepted uniform unit of measurement in qualified courses of continuing education.

Haward Technology is accredited by



P.O. Box 26070, Abu Dhabi, United Arab Emirates | Tel.: +971 2 3091 714 | E-mail: info@haward.org | Website: www.haward.org

Haward Technology * CEUs * Haward Technology * CEUs * Haward Technology * CEUs * Haward Technology *



Certificate Accreditations

Haward's certificates are accredited by the following international accreditation organizations: -

-  British Accreditation Council (BAC)

Haward Technology is accredited by the **British Accreditation Council** for **Independent Further and Higher Education** as an **International Centre**. Haward's certificates are internationally recognized and accredited by the British Accreditation Council (BAC). BAC is the British accrediting body responsible for setting standards within independent further and higher education sector in the UK and overseas. As a BAC-accredited international centre, Haward Technology meets all of the international higher education criteria and standards set by BAC.

-  The International Accreditors for Continuing Education and Training (IACET - USA)

Haward Technology is an Authorized Training Provider by the International Accreditors for Continuing Education and Training (IACET), 2201 Cooperative Way, Suite 600, Herndon, VA 20171, USA. In obtaining this authority, Haward Technology has demonstrated that it complies with the **ANSI/IACET 2018-1 Standard** which is widely recognized as the standard of good practice internationally. As a result of our Authorized Provider membership status, Haward Technology is authorized to offer IACET CEUs for its programs that qualify under the **ANSI/IACET 2018-1 Standard**.

Haward Technology's courses meet the professional certification and continuing education requirements for participants seeking **Continuing Education Units** (CEUs) in accordance with the rules & regulations of the International Accreditors for Continuing Education & Training (IACET). IACET is an international authority that evaluates programs according to strict, research-based criteria and guidelines. The CEU is an internationally accepted uniform unit of measurement in qualified courses of continuing education.

Haward Technology Middle East will award **2.75 CEUs** (Continuing Education Units) or **27.5 PDHs** (Professional Development Hours) for participants who completed the total tuition hours of this program. One CEU is equivalent to ten Professional Development Hours (PDHs) or ten contact hours of the participation in and completion of Haward Technology programs. A permanent record of a participant's involvement and awarding of CEU will be maintained by Haward Technology. Haward Technology will provide a copy of the participant's CEU and PDH Transcript of Records upon request.

Course Fee

US\$ 2,750 per Delegate + **VAT**.



Course Instructor(s)

This course will be conducted by the following instructor(s). However, we have the right to change the course instructor(s) prior to the course date and inform participants accordingly:



Mr. Terry Boes, MBA, BSc, NFPA-CFPS, ProBoard, BCSP-CSP, NEBOSH-IOGC, CBRN, CEM, OSHA, is a **Senior Security Consultant** with over **25 years** of extensive practical experience within the **Oil & Gas, Refinery and Petroleum** industries. His expertise widely covers in the areas of **Accident/Incident Investigation & Root Cause Analysis**, Strategic **Security Management**, **Security Risk Management**, **Security Threat Identification**, **Risk Analysis Evaluation & Management**, **Security Systems**, **Security Intelligence**, **Security Operations Management**, **Investigation & Security Surveying**, **Security Crisis Management**, **Security Investigations & Criminal Evidence**, **Incident Investigation Techniques**, **Firefighting Techniques**, **Fire Hazard Identification & Risk Assessment**, **Fire Prevention & Detection**, Automatic **Sprinkler Systems**, **Fire Suppression Systems**, Portable **Fire Extinguishers**, **Smoke Control & Management Systems**, **Emergency Evacuation & Response Plans**, Incident Command System (ICS), **Firefighter Safety & Coordination**, **Fire Risk Management Strategies**, **Explosion Protection & Prevention**, **Fire Investigation**, **Incident Reporting & Documentation**, **Hazmat & Emergency Management**, **Emergency Response**, **Emergency Management Planning**, **Crisis Response & EOC Operation**, **Continuity Planning & Stakeholder Engagement**, Cross-Agency Coordination, Hazardous Materials (**HazMat**), **Hazmat Operating Site Practices**, Oil & **Hazardous Materials Response**, **Hazmat Cad Systems**, **Hazardous Materials Contingency Planning**, Chemistry for **Emergency Response**, **Business Continuity & Crisis Management**, Air Monitoring & Gas Testing, Advanced **Hazard & Risk Assessment Using Air Monitoring Devices**, **Propane Emergencies**, Ludlum Radiological Response Kit, MultiRAE PID Multi-Gas Meter, Draeger Chip Measurement System & Civil Defense System, APD 2000 Chemical Agent Detector, Rail Car Hazmat Emergency Response, **Emergency Response to Terrorism**, Chemical Warfare Response & Assessment, WMD Incident Complexities, Chemical & Biological Counterterrorism, WMD Detection Technologies, **Gas Chromatograph & Mass Spectrometry**, Mass Violence & Domestic Terrorism Preparedness, Terrorism Response Planning, Gas Plant Fire Protection, Gas Leak & Explosion Investigation, Advanced Gas Leak Response Strategies & Tactics and Cold Tapping, Hot Tapping Grounding and Bonding.

During his career life, Mr. Boes has gained his practical and field experience through his various significant positions and dedications as the **Project Manager**, **Deputy Logistics Section Manager**, **Senior Technical Specialist**, **Emergency Management Specialist**, **Senior Technical Advisor**, **Senior Emergency Preparedness Consultant**, **State HazMat Administrator**, **Adult Educator**, **National Field Trainer**, **Senior HSE & Fire Officer**, **Terrorist Incident Safety Officer**, **Senior Security Risk Assessment Consultant**, **CBRN Operations & Technician**, **Radiological Technician** and **Certified Gas Tester** for various companies such as the FEMA & DOJ, Ureco USA, Texas Division of Emergency Management, Abu Dhabi National Oil Company (**ADNOC**), National Fire Academy, Fort Wayne Fire Department, ICF, Hagerty Consulting, Abelard Construction, ASG-Kuwait Fire and Emergency Services and Jamalco.

Mr. Boes has a **Master's degree (MBA)** in **Project Management**, **Bachelor's degree in Education** and **Associate's degree in Emergency Management** from the **Grantham University**, **Eastern Illinois University** and **Frederick College, USA**, respectively. Further, he is a Certified Fire Protection Specialist (**NFPA-CFPS**), an **NFPA Approved Training Instructor**, **NFPA 1041 Instructor I-III**, **NFPA Fire Officer I-III**, **NFPA Fire Inspector I-II**, **NFPA Certified Hazard Recognition Specialist**, **ProBoard Fire Instructor I-III**, **ProBoard Fire Officer I-III**, **ProBoard Incident Commander**, United States Fire Administration (USFA) **National Fire Academy Adjunct Instructor**, Certified Safety Professional (**CSP**) - Board of Certified Safety Professionals (**BCSP**), **Subject Matter Expert Panellist**, Certified Emergency Manager (**CEM**)- International Association of Emergency Managers, Certified International Technical Certificate in Oil and Gas Operational Safety – **NEBOSH**, **FEMA Certified Instructor & Train-the-Trainer** and **OSHA Certified Occupational Health and Safety Professional**. He has further delivered innumerable courses, trainings, workshops and conferences globally.



Virtual Training (If Applicable)

If this course is delivered online as a Virtual Training, the following limitations will be applicable:-

Certificates	Only soft copy certificates will be issued to participants through Haward's Portal. This includes Wallet Card Certificates if applicable
Training Materials	Only soft copy Training Materials (PDF format) will be issued to participant through the Virtual Training Platform
Training Methodology	30% of the program will be theory and 70% will be practical sessions, exercises, case studies, simulators or videos
Training Program	The training will be for 6 hours per day starting at 0800 and ending at 1400
H-STK Smart Training Kit	Not Applicable
Hands-on Practical Workshops	Not Applicable
Site Visit	Not Applicable
Simulators	Only software simulators will be used in the virtual courses. Hardware simulators are not applicable and will not be used in Virtual Training

Course Program

The following program is planned for this course. However, the course instructor(s) may modify this program before or during the course for technical reasons with no prior notice to participants. Nevertheless, the course objectives will always be met:

Day 1: Sunday, 04th of October 2026

0800 – 0830	Registration & Coffee
0830 – 0845	Welcome & Introduction
0845 – 0900	PRE-TEST
0900 – 0930	Introduction to API STD 780 Purpose and Objectives of API STD 780 • Scope of Application across Petroleum and Petrochemical Industries • Relationship with Corporate Security Management • Benefits of a Standardized Security Risk Assessment (SRA)
0930 - 0945	Break
0945 – 1100	Security Risk Management Principles Risk Management Fundamentals • Security versus Safety Risk • Risk Management Lifecycle • Integration with Enterprise Risk Management
1100 – 1145	Security Risk Assessment Concepts Definition of Security Risk • Components of Security Risk • Relationship between Threat, Vulnerability and Consequence • Security Risk Terminology and Definitions
1145 – 1215	Understanding Security Threats Criminal Threats • Insider Threats • Terrorism and Sabotage • Emerging Cyber-Physical Threats
1215 - 1230	Break
1230 – 1300	Security Consequences Human Consequences • Environmental Consequences • Business Interruption • Reputation and Financial Impacts



1300 - 1350	Overview of API's Five-Step SRA Methodology Step 1 – Characterization • Step 2 – Threat Assessment • Step 3 – Vulnerability Assessment • Steps 4 & 5 – Risk Evaluation and Countermeasures
1350 – 1400	Recap Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow
1400	End of Day One

Day 2: Monday, 05th of October 2026

0800 – 0900	Security Risk Assessment Planning Planning Process • Defining Objectives • Establishing Assessment Boundaries • Resource Planning
0900 – 0945	Building the SRA Team Team Composition • Roles and Responsibilities • Required Competencies • Stakeholder Participation
0945 – 1000	Break
1000 – 1130	Defining Scope & Objectives Asset Selection • Facility Boundaries • Operational Assumptions • Risk Acceptance Criteria
1130 – 1200	Information Collection Facility Documentation • Process Information • Security Documentation • Operational Information
1200 – 1215	Break
1215 – 1300	Sources of Information Internal Data Sources • External Intelligence • Regulatory Requirements • Historical Records
1300 – 1350	Site Inspection & Previous Incident Analysis Conducting Site Walkthroughs • Identifying Critical Observations • Incident Investigation Review • Lessons Learned
1350 – 1400	Recap Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow
1400	End of Day Two

Day 3: Tuesday, 06th of October 2026

0800 – 0900	Asset Characterization Identifying Critical Assets • Asset Prioritization • Consequence Identification • Asset Documentation
0900 – 0945	Step 2 – Threat Assessment Threat Identification • Threat Likelihood Evaluation • Threat Ranking • Target Attractiveness
0945 – 1000	Break
1000 – 1130	Threat Intelligence Intelligence Sources • Threat Trends • Adversary Capabilities • Threat Credibility
1130 – 1200	Step 3 – Vulnerability Assessment Physical Vulnerabilities • Procedural Vulnerabilities • Personnel Vulnerabilities • Cyber Vulnerabilities
1200 – 1215	Break



1215 – 1300	Layers of Security Protection <i>Deterrence • Detection • Delay • Response</i>
1300 – 1350	Vulnerability Ranking <i>Ranking Methodology • Existing Safeguards • Residual Vulnerabilities • Documentation</i>
1350 – 1400	Recap <i>Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow</i>
1400	<i>End of Day Three</i>

Day 4: Wednesday, 07th of October 2026

0800 – 0900	Step 4 – Risk Analysis <i>Risk Calculation Methodology • Likelihood Evaluation • Consequence Evaluation • Risk Prioritization</i>
0900 – 0945	Risk Ranking <i>Risk Matrices • Risk Categories • Risk Acceptance Criteria • Decision-Making</i>
0945 – 1000	<i>Break</i>
1000 – 1130	Step 5 – Countermeasure Identification <i>Risk Treatment Options • Security Improvements • Administrative Controls • Engineering Controls</i>
1130 – 1200	Evaluating Countermeasures <i>Effectiveness Evaluation • Cost-Benefit Considerations • Implementation Priorities • Residual Risk</i>
1200 – 1215	<i>Break</i>
1215 – 1300	Documentation & Reporting <i>Recording Assessment Results • Preparing Recommendations • Management Reporting • Action Tracking</i>
1300 – 1350	Validation & Follow-up <i>Review Process • Verification of Recommendations • Continuous Improvement • Reassessment Scheduling</i>
1350 – 1400	Recap <i>Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow</i>
1400	<i>End of Day Four</i>

Day 5: Thursday, 08th of October 2026

0800 – 0900	API Worksheets & Forms <i>Characterization Worksheet • Threat Assessment Worksheet • Vulnerability Assessment Worksheet • Recommendation Worksheet</i>
0900 – 0930	Petroleum Terminal Case Study <i>Asset Identification • Threat Assessment • Vulnerability Evaluation • Risk Prioritization</i>
0930 – 0945	<i>Break</i>
0945 – 1100	Refinery Case Study <i>Process Hazards • Security Scenarios • Countermeasure Selection • Lessons Learned</i>
1100 – 1200	Pipeline Security Assessment <i>Pipeline Threats • Remote Asset Protection • Critical Infrastructure Considerations • Risk Reduction Strategies</i>
1200 – 1215	<i>Break</i>



1215 – 1300	Transportation Security <i>Truck Transportation • Rail Transportation • Marine Transportation • Supply Chain Security</i>
1300 – 1315	Course Conclusion <i>Using this Course Overview, the Instructor(s) will Brief Participants about the Course Topics that were Covered During the Course</i>
1315 – 1415	COMPETENCY EXAM
1415 – 1430	<i>Presentation of Course Certificates</i>
1430	<i>End of Course</i>

Suggested Practical Exercises Throughout the Course

- Facility characterization workshop
- Threat identification exercise
- Security walkthrough simulation
- Vulnerability assessment workshop
- Risk ranking matrix exercise
- Countermeasure selection workshop
- Case study analysis
- Group presentation
- Final Security Risk Assessment project

Learning Outcomes

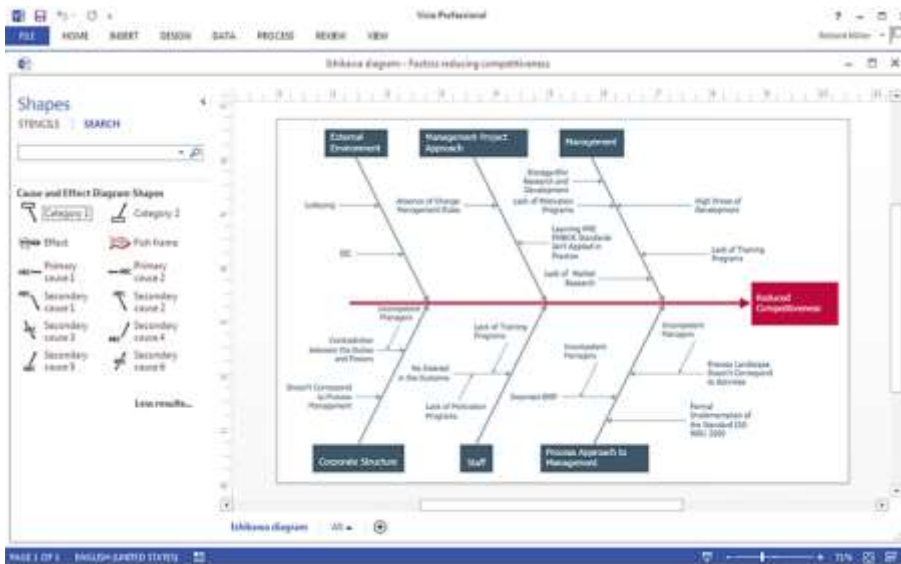
By the end of the course, participants will be able to:

- Explain the principles of API STD 780 Security Risk Assessment
- Plan and organize a structured Security Risk Assessment
- Build and facilitate an effective multidisciplinary SRA team
- Characterize assets and identify security threats
- Evaluate vulnerabilities using a systematic methodology
- Analyze and rank security risks using qualitative risk assessment techniques
- Develop practical and risk-based security countermeasures
- Document findings and prepare professional SRA reports
- Apply the methodology to terminals, refineries, pipelines, and transportation assets
- Support continuous improvement of security risk management programs

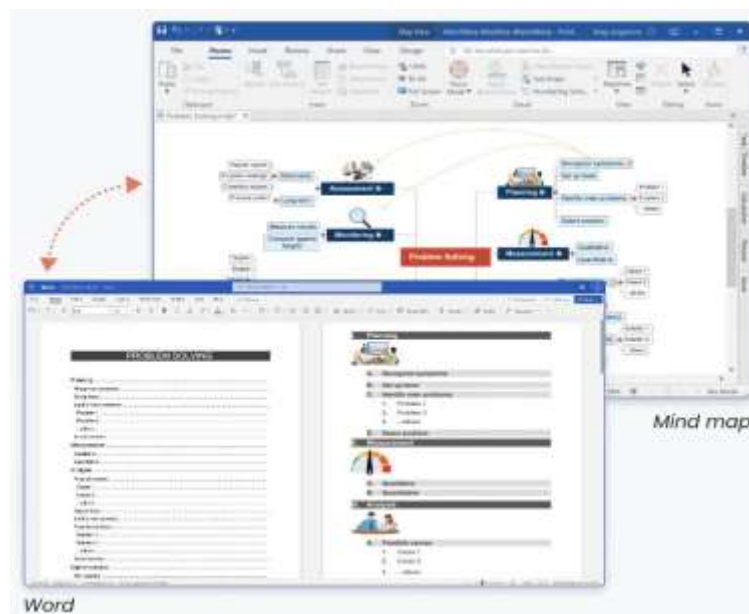


Simulators (Hands-on Practical Sessions)

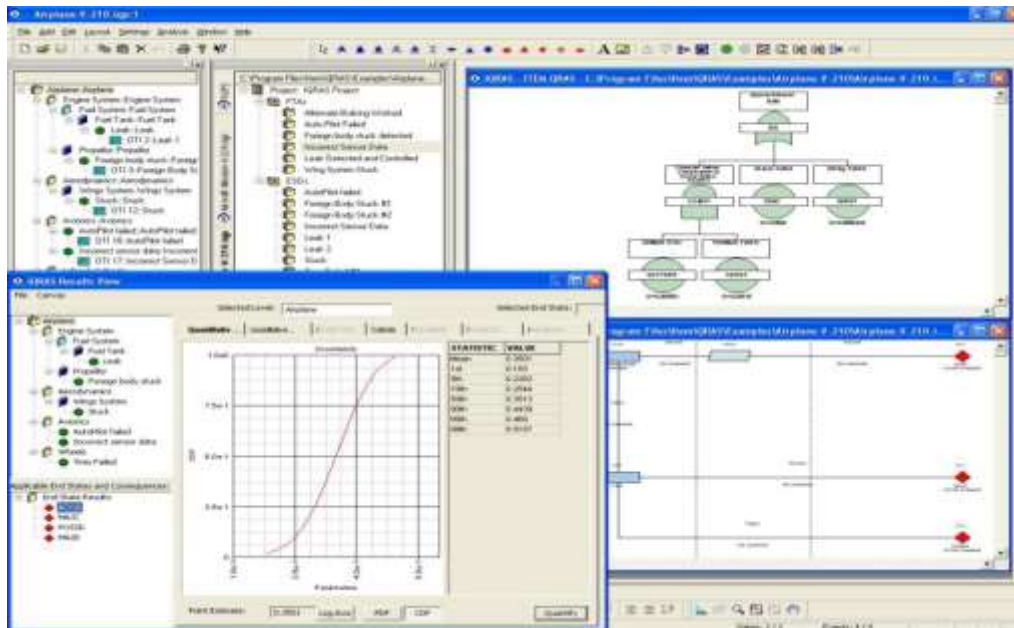
Practical sessions will be organized during the course for delegates to practice the theory learnt. Delegates will be provided with an opportunity to carryout various exercises using our state-of-the-art “Visio”, “Mindview” and “QRA System” simulators.



Visio Software



Mindview Software



QRA System Simulator

Course Coordinator

Mari Nakintu, Tel: +971 2 30 91 714, Email: mari1@haward.org