

OMNEX



DRIVING WORLDWIDE BUSINESS EXCELLENCE

Automotive

Training & Workshop Catalog



AUTOMOTIVE
QMS



CORE
TOOLS



PROBLEM
SOLVING



IMPROVEMENT
METHODOLOGIES



SOFTWARE

USA | CANADA | CHINA | EUROPE | INDIA | MALAYSIA | MEXICO | MIDDLE EAST | UAE | SINGAPORE | THAILAND

www.omnex.com

Overview/Company History

Omnex is an international consulting, training and software development organization specializing in management system solutions that elevate the performance of client organizations. Omnex provides consulting and training services in Quality, Environmental, and Health and Safety standards-based management systems like ISO 9001:2015, ISO 14001:2015, IATF 16949:2016 and QOS. Omnex also leads the way with Lean, Six Sigma and other breakthrough systems and methods of performance enhancement, supported by Omnex Systems, LLC, software solutions for Enterprise Wide Quality Management Systems®.

The Omnex mission is to help clients achieve and sustain customer-focused competitive advantage with significant bottom-line impact. Omnex combines extensive knowledge in business excellence practices with deep industry experience to build and strengthen client capabilities. Omnex reflects this commitment to quality and results by maintaining its own certified ISO 9001 quality management system.

One of the largest quality consulting companies in the world with 35 years of professional service experience & strategic operations consulting

Every hour, somewhere,
someone is getting trained by Omnex



Contents

Courses	4
CTO Message	8
Worldwide Locations	9
Profile	10
Omnex Training Overview	14
Automotive Training & Workshops	15
■ IATF 16949 Series	16
■ ISO 27001/TISAX/CMMC	26
■ Automotive SPICE® Series	37
■ ISO 26262 Functional Safety Series	42
■ Cybersecurity Series	54
■ VDA	62
■ Others	69

IATF 16949 Series

- IATF 16949:2016 Executive Overview
- Understanding the Requirements of IATF 16949:2016 AQMS
- Understanding, Documenting and Implementing IATF 16949:2016
- IATF 16949:2016 Internal Auditor Training for AQMS
- IATF 16949:2016 Lead Auditor Training for AQMS
- IATF 16949:2016 Second Party (Supplier Auditor) Training for AQMS
- IATF 16949:2016 Manufacturing Process Auditor Training for AQMS
- IATF 16949:2016 Product Auditor Training for AQMS
- Transition Training for IATF 16949:2016 and ISO 9001:2015
- Automotive OEM Detailed Customer Specific Requirements Workshop
- IATF 16949:2016 Employee Awareness
- AIAG-VDA DFMEA (SFMEA and DFMEA) for Practitioners and Facilitators
- AIAG-VDA FMEA for Managers and Implementers – Implementation Training
- AIAG-VDA FMEA Understanding, Implications, and Strategy Executive Overview
- AIAG-VDA Process FMEA and Control Plans for Practitioners and Facilitators
- Functional Safety Core Tools: DFMEAs for Monitoring and System Response
- Reverse Failure Mode and Effect Analysis – RFMEA

ISO 27001/TISAX/CMMC

- Understanding the Requirements of ISO/IEC 27001:2013 for Information Security Management Systems
- ISO/IEC 27001:2013 Internal Auditor Training for Information Security Management Systems
- ISO/IEC 27001:2013 Lead Auditor Training for Information Security Management Systems
- ISO/IEC 27001:2013 for Information Security Management Systems Executive Overview
- Information Security Awareness Training
- Understanding the Requirements of ISO/IEC 27001:2013 and VDA ISA TISAX
- ISO/IEC 27001:2013 and VDA ISA TISAX Internal Auditor Training for Information Security Management Systems
- ISO/IEC 27001:2013 and VDA ISA TISAX Lead Auditor Training for Information Security Management Systems
- Understanding the Requirements of Cybersecurity Maturity Model Certification (CMMC) and ISO/IEC 27001:2013
- Cybersecurity Maturity Model Certification (CMMC) and ISO/IEC 27001:2013 Internal Auditor Training for Information Security Management Systems
- Cybersecurity Maturity Model Certification (CMMC) and ISO/IEC 27001:2013 Lead Auditor Training for Information Security Management Systems

Automotive SPICE® Series

- Mechanical Engineering Plug-In for Automotive SPICE®
- Understanding Automotive SPICE® Including Integration with ISO 26262 and IATF 16949
- Internal Quality Assurance Practitioners of Automotive SPICE®
- Creating Test Cases for Automotive Software
- Intacs™ Certified Provisional Assessor
- Conducting Automotive SPICE® Assessments
- Writing Effective Requirements and Test Cases for Automotive Software Performance Improvement and Capability determination (Automotive SPICE®) and HWE PRM/PAM
- Understanding PRM/PAM Hardware Engineering Processes and Integration with Automotive SPICE®

ISO 26262 Functional Safety Series

- ISO 26262:2018 Functional Safety Executive Overview
- ISO 26262:2018 Overview for Functional Safety Engineers
- ISO 26262:2018 Overview for Project Managers
- Automotive Functional Safety ISO 26262:2018 Certification
- ISO 26262:2018 Automotive Functional Safety Certification with Truck & Bus Focus
- ISO 26262:2018 Automotive Functional Safety Certification with Motorcycle Focus
- ISO 26262:2018 Program Manager/Functional Safety Manager Certification Level I
- ISO 26262:2018 Functional Safety Auditing and Assessment
- Preparing a Safety Case for ISO 26262:2018
- Writing Effective Requirements, Test Cases and Hardware/Software Interface (HIS) for Automotive Spice®
- ISO 26262:2018 Automotive Functional Safety Engineer Level II Certification
- ISO 26262:2018 Program Manager / Functional Safety Manager Certification Level II
- ISO 26262:2018 Product Development at the Hardware Level in Semiconductors Certification
- Functional Safety Core Tools: DFMEA and Diagnostic Analysis Overview
- Functional Safety Core Tools: DFMEAs for Monitoring and System Response
- Functional Safety Core Tools: 2-day DFMEAs for Monitoring and System Response
- Functional Safety Core Tools: Fault Tree Analysis
- Functional Safety Core Tools: Hazard Analysis and Risk Assessment
- Assessments, Audits, and Confirmation Measures For ISO 26262:2018 Functional Safety Management Systems Standards
- Assessment of a Safety Case based on SS 7740-2018
- Software DFMEA ISO 26262:2018 Functional Safety Core Tools
- Writing Effective Requirements and Test Cases at System, Software and Hardware levels for Functional Safety (ISO 26262) products
- ISO 26262:2018 Product Development at the Hardware Level Certification

Cybersecurity Series

- SAE J3061, ISO/SAE 21434, and Related Standards: Automotive Cybersecurity Executive Overview
- SAE J3061, ISO/SAE 21434, and Related Standards: Overview for Functional Safety Engineers
- SAE J3061 and ISO/SAE 21434 Cybersecurity Engineering Certification
- SAE J3061 and ISO 21434:2019 Automotive Cybersecurity Auditing and Assessment Certification
- SAE J3061 and ISO/SAE 21434 Cybersecurity Threat Analysis and Risk Assessment (TARA)
- SAE J3061 and ISO/SAE 21434 Conducting a Cybersecurity FMEA and Vulnerability Analysis Testing for Systems, Hardware and Software
- SAE J3061 and ISO/SAE 21434 Cybersecurity Engineering Defense & Protection Against Attacks
- Introduction to Autonomous and Electric Vehicles: A Functional Safety, SOTIF, and Cybersecurity Perspective
- Preparing a Cybersecurity Case
- Writing Effective Requirements, Test Cases, and H/S Interfaces for Cybersecurity
- SAE J3061 and ISO/SAE 21434 Automotive Cybersecurity Certification
- Introduction to Systems Engineering: A Safety and Cybersecurity Perspective
- WP.29, ISO/SAE 21434 and VDA CSMS – Auditing Automotive Cybersecurity Management Systems

VDA

- Production Part Approval Process (PPAP) VDA Volume 2
- System FMEA / DFMEA / DVP&R / Characteristics Linkage
- Process Flow, PFMEA and Control Plans
- Measurement Systems Analysis (VDA 5)
- Contamination Identification and Control Utilizing VDA 19
- Certification for Product Safety and Conformance Process Owners
- Understanding VDA 6.3 Process Audits
- VDA 6.3 Executive Overview
- Conducting Product Audits to VDA 6.5
- Conducting Process Audits to VDA 6.3

Others

- Introduction to Systems Engineering: A Safety and Cybersecurity Perspective
- Introduction to Autonomous and Electric Vehicles: A Functional Safety, SOTIF, and Cybersecurity Perspective
- Information Security Awareness Training
- Writing Effective Requirements and Test Cases
- VDA ISA based TISAX Internal Assessor
- Software/Algorithm Failure Modes and Effect Analysis Onsite Workshop
- ISO 26262:2018 Product Development at the Hardware Level
- Multipoint DFMEA for Mechatronic and Electronic Systems
- Understanding AIAG-VDA DFMEA (SFMEA and DFMEA) for Design and Project Team Members
- Understanding AIAG-VDA Process FMEA and Control Plans for Process and Project Team Members
- Advanced Product Quality Planning (APQP) Overview
- Understanding the Five Phases of APQP
- Role of Top Management in APQP
- Product Development using SFMEA, DFMEA and Associated Tools
- Design Review Based on Failure Modes
- Machine Failure Mode Effect Analysis (MFMEA)
- Measurement Systems Analysis (MSA) including Advanced Analysis (ANOVA)
- Manufacturing Process Development using PFMEA
- APQP Manufacturing Process Development using PFMEA and PPAP
- Production Part Approval Process (PPAP) Overview
- Service Production Part Approval Process (PPAP) Overview
- Reverse Failure Mode and Effect Analysis – RFMEA
- Statistical Process Control (SPC) and Associated Tools - 2 days
- Statistical Process Control (SPC) and Associated Tools - 3 days
- Understanding Core Tools: Advance Product Quality Planning (APQP) and Production Part Approval Process (PPAP)
- Understanding Core Tools (APQP/PPAP, DFMEA, PFMEA, Control Plans, SPC and MSA)
- Understanding Core Tools: Design Failure Modes and Effects Analysis (DFMEA) and Design Validation Plan & Report (DVP&R)
- Understanding Core Tools: PFMEA and Control Plans
- Understanding Core Tools: Statistical Process Control (SPC)
- Understanding Core Tools: Measurement Systems Analysis (MSA)



MESSAGE FROM THE CTO

At Omnex, we have the world's leading quality experts at work. If you have a quality or productivity issue that doesn't seem solvable, contact me directly. I will personally work with you to find a solution.

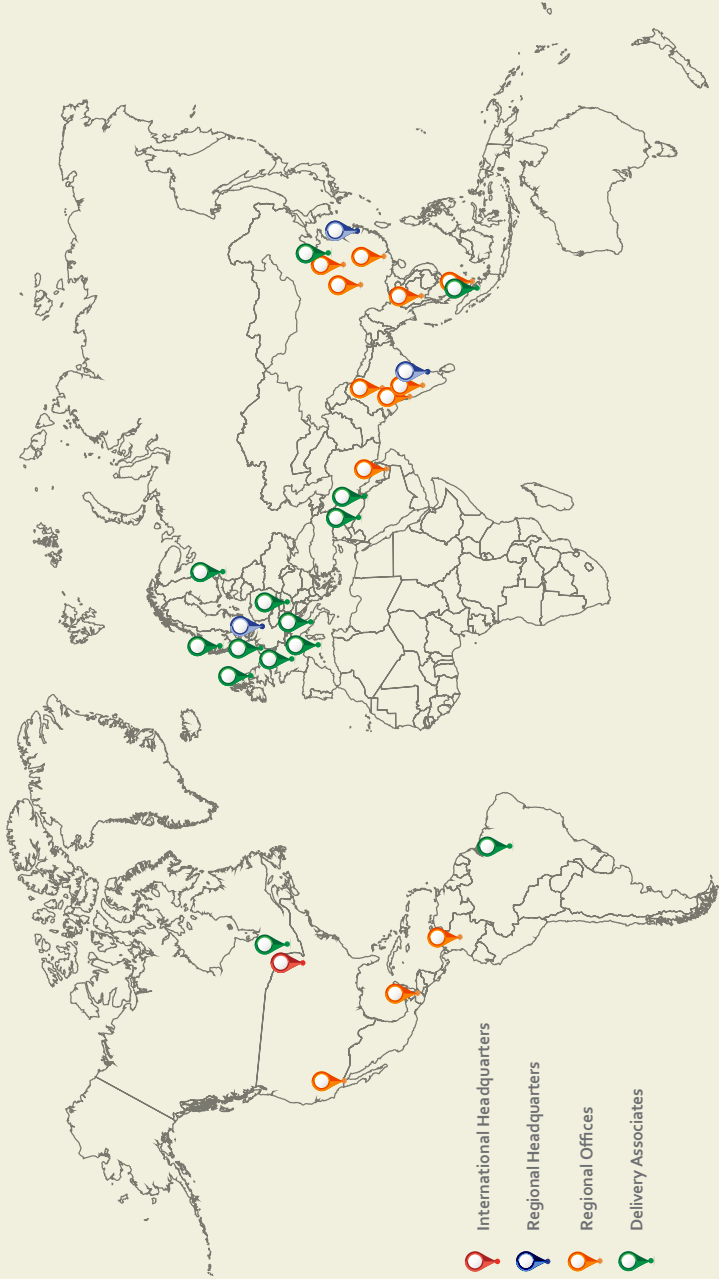
Chad Kymal

cto@omnexus.com

Founded in 1985, Omnex is headquartered in Ann Arbor, Michigan and has branch offices throughout the world. Omnex is strategically placed globally to better serve the expanding international marketplace and has worked in over 51 countries. Omnex is also a global leader in consulting and training that directly impact clients profitability by significantly improving quality and productivity through a unique integrated methodology designed to continuously improve their business management systems.

Omnex is the leading provider of performance-focused training to both the manufacturing and service sectors, regularly conducting public and in-company seminars on many subjects. Omnex has more than 200 workshops that are being conducted worldwide. The training workshops are available in more than a dozen languages and dialects. Every month Omnex trains more than a 1000 people worldwide. Many of our workshop training programs are accredited worldwide by renowned bodies such as Exemplar, RAB QSA, AIAG, IRCA, to name a few.

Worldwide locations



- 📍 International Headquarters
- 📍 Regional Headquarters
- 📍 Regional Offices
- 📍 Delivery Associates

Worldwide Staff

USA, Europe
Consultants 328
Sales/Support 22
SMEs Engaged 40



Africa, Asia Pacific
Consultants 255
Sales/Support 25
SMEs Engaged 3



China, Japan, Far East
Consultants 185
Sales/Support 35



Total 888



USA - Global Headquarters
 315 E. Eisenhower Parkway,
 Suite. 214
 Ann Arbor, MI 48108
 Phone: (734) 761-4940
 Fax: (734) 761-4966
 Email: info@omnexus.com
www.omnexus.com



EUROPE - Headquarters
 Omnexus Europe GmbH,
 Fidicinstrasse 3
 10965 Berlin
 +4930 61285 700
 Email: info@omnexus.eu
www.omnexus.eu



ASIA PACIFIC - Headquarters
 1/807A, Pillayar Koil Street
 Thorapakkam, Chennai
 Tamilnadu, India - 600097
 Phone: +91-44-24960682
 Fax: +91-44-24960655
 Email: info-in@omnexus.com



CHINA / Far East - Headquarters
 Suite 3003-3004, 30th Floor,
 388 Xijiangwan Rd,
 Hongkou Plaza, Hongkou,
 Shanghai, China 200083
 Tel: 021-3360 8488
 Email: info-cn@omnexus.com
www.omnexus.com.cn

Who do we serve? Our global clients will tell you...



Mercedes-Benz



Profile



Omnex is an ISO 9001:2015
QMS Certified Company



Omnex Management and Engineering Consultants, LLC specializes in creating management systems that elevate the performance of client organizations. As a leading international consulting and training organization, Omnex brings together world-class talent with local presence to deliver high impact expertise in today's global business environment.

Founded in 1985, Omnex is headquartered in Ann Arbor, Michigan and has branch offices throughout the world. Omnex is strategically placed globally to better serve the expanding international marketplace and has worked in over 51 countries. Omnex is also a global leader in consulting and training that directly impact clients' profitability by significantly improving quality and productivity through a unique integrated methodology designed to continuously improve their business management systems.

Omnex emphasizes and facilitates cost savings and improvement to business processes while meeting and exceeding customer expectations for product quality. This enables our clients to maintain and expand their existing business in the face of a more competitive world market. Our goal is to transfer our knowledge and industry experience to our clients so that they may fully utilize this competitive advantage.



CONSULTING

Omnex provides Quality, Environmental, Safety and Performance Enhancement consulting/integrated training to an extensive array of service and manufacturing sector companies. Omnex identifies and effectively deploys strategies, goals and methodologies in close participation with its clients to achieve and sustain operational excellence. The consulting services deployed and available worldwide to our client base include the implementation of the following standards: ISO 9001, ISO 14001, AS9100D and a host of other standards including a unique integrated management system of EMS, OH&S and QMS.



TRAINING SERVICES

Omnex is the leading provider of performance-focused training to both the manufacturing and service sectors, regularly conducting public and in-company seminars on many subjects. Omnex has more than 240 workshops that are being conducted worldwide. The training workshops are available in more than a dozen languages and dialects. Every month Omnex trains more than a 1000 people worldwide. Many of our workshop training programs are accredited worldwide by renowned bodies such as Exemplar Global, AIAG, IRCA to name a few.



CONSULTING AND TRAINING INTEGRATED APPROACH

Recognizing the strategic importance of product commercialization, Omnex integrates consulting and training services to support the development and deployment of effective processes for product planning, development (product and process design), verification, launch and continual improvement to help ensure the supplier's ability to meet all of its customers' requirements. We have notable experience in having framed the New Product Development methods and strategies for our OEM clients from Truck, Automotive, Aerospace, Engineering and Railway industries specifically.



SOFTWARE

Omnex's EwQIMS or Enterprise-wide Quality and Integrated Management Systems Suite is a revolutionary software suite of 12 modules that are completely integrated to form Enterprise Quality Planning Suite, QHSE/IMS Solutions, Automotive QMS, Aerospace QMS and Supplier Management. It empowers you to run quality and business processes efficiently.

Omnex has worked with most of the major Automotive and Truck OEMS and tier ones worldwide. In fact, Omnex has been at the forefront of developing and deploying all major Automotive OEM initiatives, starting with QOS for Ford Motor Company in 1990s. When Ford wanted to move QOS from a Cost of Quality-based measurable-driven process to a strategically-driven Customer-Focused process, Omnex assisted them in developing the QOS methodology and the QOS assessment tool which is currently being used by Ford and Ford Suppliers worldwide.

Subsequently, Omnex helped write the Automotive Quality System standard QS-9000 and Omnex principals performed the first QS-9000 witness audit worldwide. Omnex collaborated with the Automotive Electronic Council in rewriting the Semiconductor Supplement to QS-9000 as an ISO/TS 16949-based standard. Omnex developed and provided the Second Party Auditing Course for AIAG to Truck OEMs and Automotive Suppliers.

Omnex principals are members of the AIAG writing committees of the SPC, APQP, EPS, FMEA and MSA Reference Manuals that are being followed by thousands of companies worldwide. Omnex is also an innovator of Lean and Six Sigma integration methodology. Omnex is the provider of Lean and Six Sigma worldwide for the Automotive Industry as the AIAG Provider of Choice. We provide the only AIAG certified Lean Six sigma workshops that are accepted by the Automotive industry worldwide.

It is not hubris that we sometimes call ourselves “Inventors of Automotive Quality.” We have had a long association with many OEMs worldwide; from Hyundai in Chennai to DFM in China to Ford, GM, Mack, and Magna in the USA. From conducting Operational audits with suggested detailed Action Plans to improve poorly performing suppliers to having played an active role in new product launches, Omnex has been right in the thick of action when it comes to Automotive and Truck industry. At the time, this was known as the 3PSD process by DCX. For Ford Motor Company, we have served the role of keeper of the Q1 Knowledge for Service Organizations, conducting training for Quality and Purchasing every few years. We are also proud of the role we have played with their global supply bases starting from Brazil, Venezuela, Argentina, Thailand, China, India, and Vietnam.

Omnex has been hands-on for the development of suppliers for OEMS making Electric vehicles. Our projects have been executed in US, India, China and Thailand to this effect.

Our offices worldwide are working with leading Automotive OEMs and Tier Ones in various projects that ultimately aim for a safer riding and passenger experience for these vehicles.

Omnex has extensive expertise in many industries including:

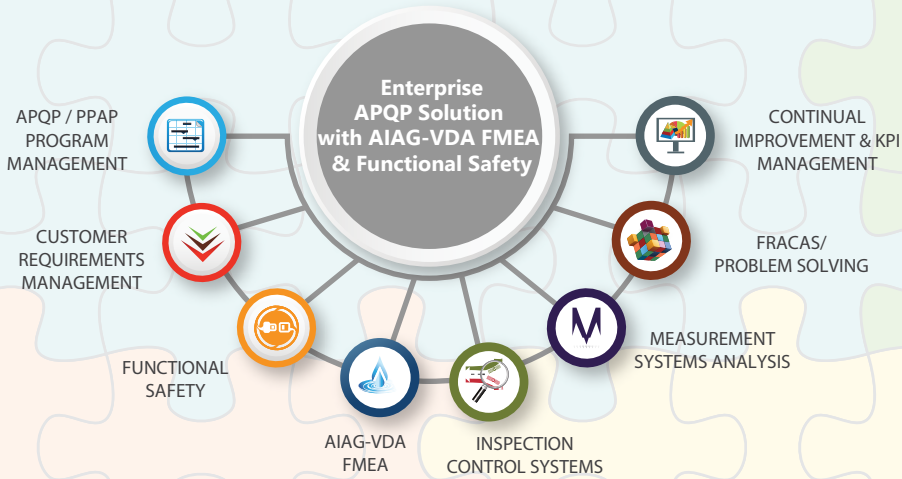
MANUFACTURING

- Automotive
- Semiconductor
- Medical Devices
- Pharmaceutical
- Aerospace

SERVICE

- Transportation
- Health Care
- Construction
- Telecommunication
- Electronics
- Engineering
- Oil/ Natural gas
- Banking
- Hospitality
- Information technology/ BPO

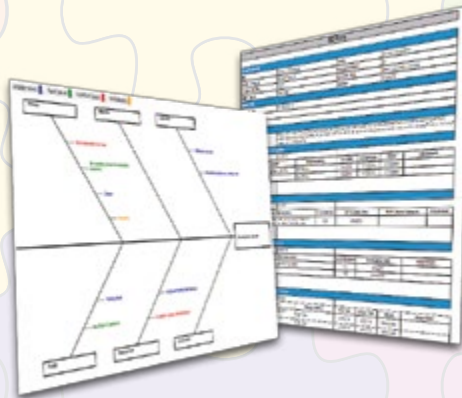
Our capability and global reach provides clients a reliable approach in use of methodologies, training/workshop materials and consistent deployment methods at all their locations even in the local languages used by our clients.



NPD/APQP Program Management

FRACAS / Problem Solving

Functional Safety

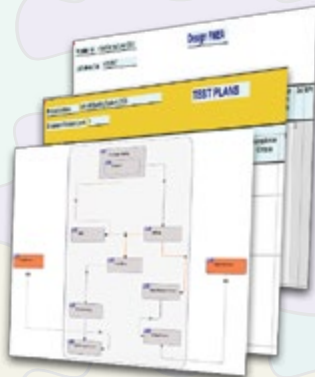


VOC/Requirements

Block Dia, Test Plans

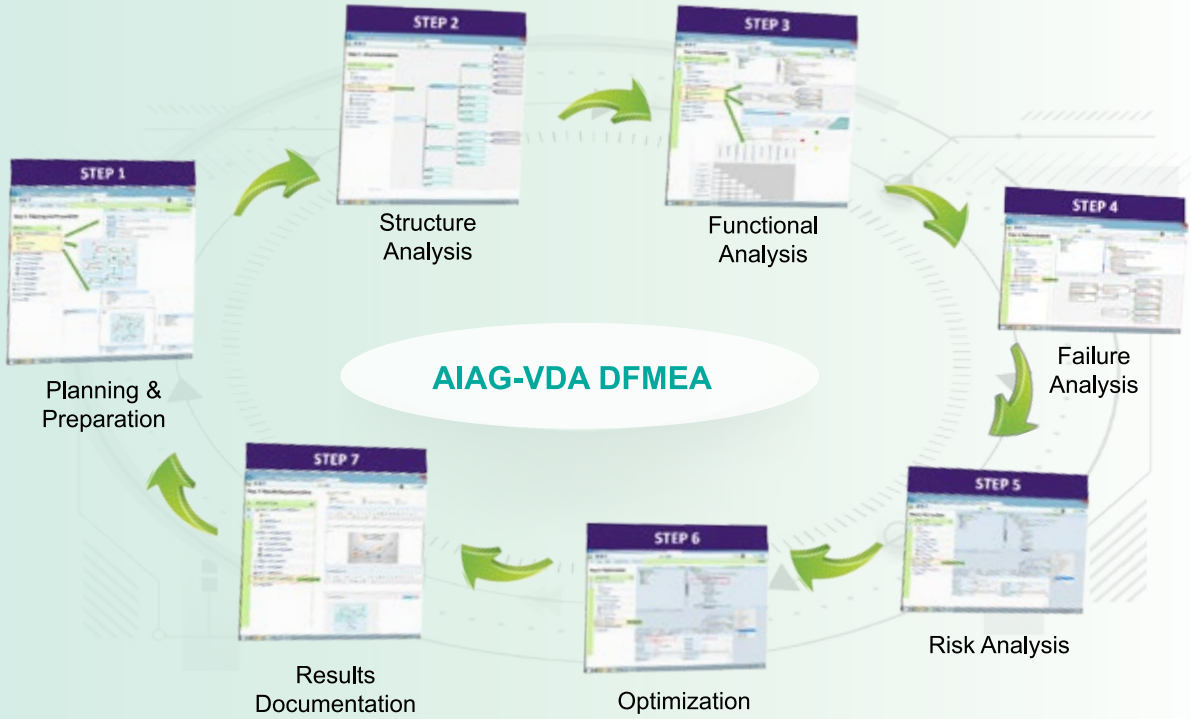
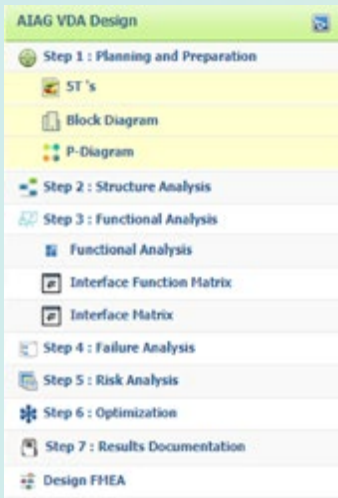
AIAG-VDA FMEA

Inspection, FAI & PPAP

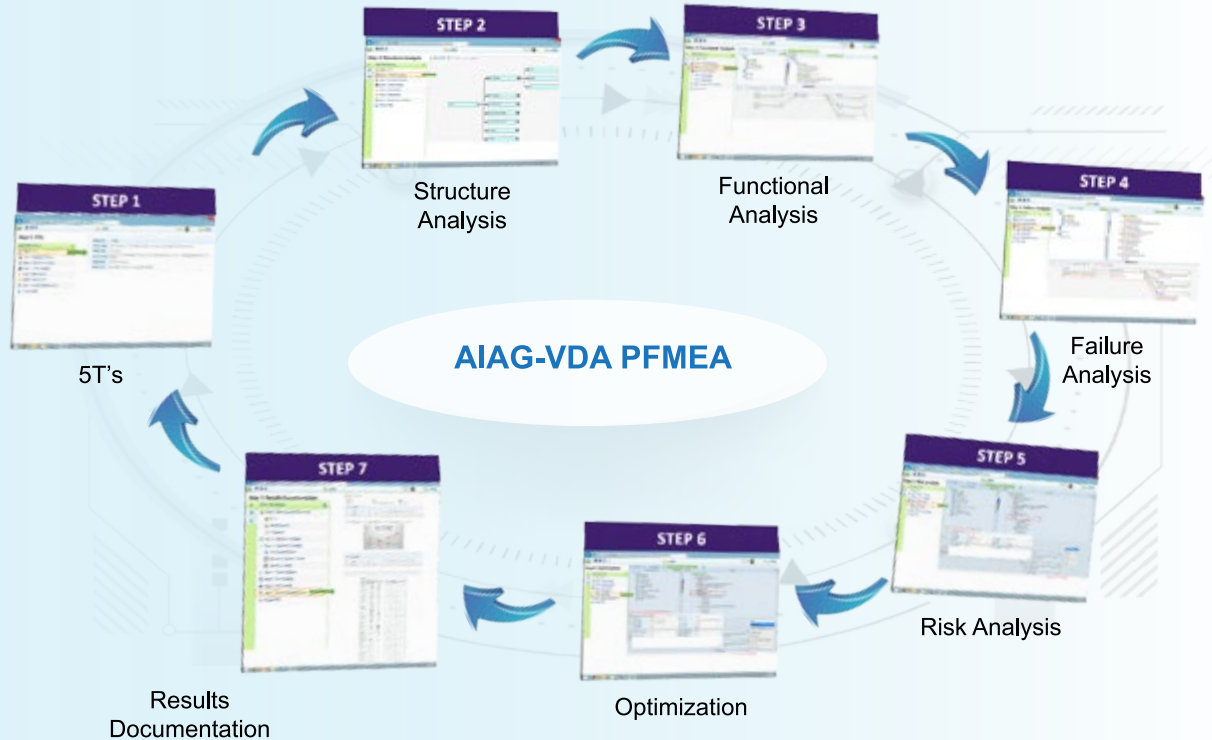
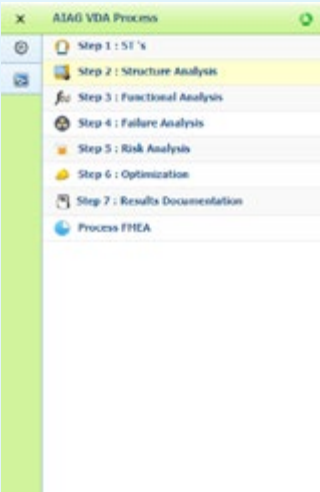


OTHER SOLUTIONS

AIAG-VDA DESIGN FMEA - 7 STEPS



AIAG-VDA PROCESS FMEA - 7 STEPS



Omnex Training Overview

Operational and Business Excellence

Each hour, somewhere in the world, Omnex is educating people on how to achieve their business and operational excellence objectives. Omnex has taught more than 400,000 individuals in over 30 countries. Recognizing that people learn in different ways and that knowledge transfer is critical to learning, Omnex offers a variety of approaches from the traditional classroom approach to hands-on workshops to project-based learning experiences-in over a dozen languages and dialects.

Training at the Cutting Edge

Our business is knowing the management systems, methodologies, technologies and standards that are constantly changing in your business. We stay on top of these changes. By working with Omnex, you know you are getting the most up-to-date information that conforms with the latest requirements for business excellence in your industry.

Omnex Educators: Operational People

With an average of 25 years' experience in their industries of specialty, our trainers teach you the latest innovations, techniques, procedures and systems that they are deploying with our current consulting clients.

Certifying Bodies

Omnex worldwide training is regularly evaluated and certified by the governing bodies like Exemplar Global and IRCA. If you are a Lead or Internal Auditor, you can be confident that you are receiving auditor training that has been certified or approved and that meets customer specific requirements.

On-site Training / Workshop Approach

On-site training courses are delivered to your team, at your location, on your schedule, without sacrificing your organization's project plans. This training method eliminates your travel-related expenses and it offers the convenience of arranging the training to fit your time constraints. If your goal is to train five or more employees in the near term, then on-site training generally is your most cost-effective strategy.

On-site training allows you to focus course content on the issues that are affecting your organization today. This level of personal attention cannot be accomplished through public seminars, videos, or any other training option. The on-site allows you to dive deeper into your most important corporate issues and determine their root causes.

Project-based Workshop Approach

Many companies find that a traditional training-based approach is less-than-effective for participants' ability to learn. The Omnex Project-based Workshop is only taught by educators/trainers who have extensive and in-depth knowledge of product and process engineering. In fact, our educators/instructors have an average of 25 years of industry experience.

This project-based workshop approach has two major advantages:

- ◆ Your investment in training is measurable when the project is completed
- ◆ By the end of the workshop, the participants successfully manage a project of your choosing under the direction of Omnex consultants

This results in substantial business improvements even while people are still in training, and helps your employees develop self-sufficiency. The project-based workshop approach provides the ultimate in value, cost savings and profitability

Automotive Training & Workshops (IATF 16949; Automotive/Production Core Tools)

Omnex has worked with most of the major Automotive and Truck OEMs and Tier Ones worldwide. In fact, Omnex has been at the forefront of developing and deploying all major Automotive OEM initiatives, starting with QOS for the Ford Motor Company in the early 90s. When Ford wanted to move QOS from a Cost of Quality-based measurable-driven process to a strategically driven Customer-Focused process, Omnex assisted them in developing the QOS methodology and the QOS assessment tool for use by Ford and Ford Suppliers.

Subsequently, Omnex helped write QS-9000 and Omnex principals performed the first QS-9000 witness audit worldwide. Omnex collaborated with the Automotive Electronic Council in rewriting the Semiconductor Supplement to QS-9000 as an ISO/TS 16949-based standard. Omnex developed and provided the Second Party Auditing Course for AIAG to Truck OEMs and Automotive Suppliers. Omnex principals are members of the AIAG writing committees of the SPC, FMEA and MSA Reference Manuals. Omnex is also an innovator of Lean and Six Sigma by integrating Lean into the Six Sigma methodology. Omnex is the provider of Lean and Six Sigma worldwide for the Automotive Industry as the AIAG Provider of Choice.



IATF 16949 Series

IATF 16949:2016 Executive Overview

Understanding the Requirements of IATF 16949:2016 AQMS

Understanding, Documenting and Implementing IATF 16949:2016

IATF 16949:2016 Internal Auditor Training for AQMS

IATF 16949:2016 Lead Auditor Training for AQMS

IATF 16949:2016 Second Party (Supplier Auditor) Training for AQMS

IATF 16949:2016 Manufacturing Process Auditor Training for AQMS

IATF 16949:2016 Product Auditor Training for AQMS

Transition Training for IATF 16949:2016 and ISO 9001:2015

Automotive OEM Detailed Customer Specific Requirements Workshop

IATF 16949:2016 Employee Awareness

AIAG-VDA DFMEA (SFMEA and DFMEA) for Practitioners and Facilitators

AIAG-VDA FMEA for Managers and Implementers – Implementation Training

AIAG-VDA FMEA Understanding, Implications, and Strategy Executive Overview

AIAG-VDA Process FMEA and Control Plans for Practitioners and Facilitators

Functional Safety Core Tools: DFMEAs for Monitoring and System Response

Reverse Failure Mode and Effect Analysis – RFMEA

IATF 16949 Executive Overview

Duration: Half-day

Seminar Goals

- ◆ Discuss the differences between the 2009 version of the ISO/TS 16949 standard and the 2016 revision
- ◆ Be aware of the transition timeline and requirements
- ◆ Apply knowledge and understanding of the IATF 16949:2016 standard to begin planning and preparation of an existing Quality Management System to comply with IATF 16949:2016

Seminar Content

- Why was IATF 16949 Revised?
- What are the Key Changes?
- Implications of the Changes to Management Systems
- Responsibilities of Top Management
- Responsibilities of Process Owners
- What are the Revision Timelines?
- Transition Guidance

Understanding, Documenting and Implementing IATF 16949:2016

Duration: 4 Days



Seminar Goals

- ◆ Understand management systems and the process approach
- ◆ Understand linkages between context, interested party expectations, and planning including risk based thinking
- ◆ Risk based thinking approaches for IATF 16949 and ISO 9001:2015
- ◆ Integrating Code of Conduct, Environmental Policy, Protecting the Environment and Social Responsibility
- ◆ Importance of integrated management systems to transition in the Automotive industry with the advent of the High Level Structure (HLS)
- ◆ Organize documentation according to IATF 16949:2016 to demonstrate effective planning, operation, and control of processes
- ◆ Understand the intent and content of the requirement changes from the perspective of the IATF and Writing Committee
- ◆ Develop an implementation plan for transition
- ◆ Understand the IATF requirements for transition
- ◆ Determine key strategies and actions to ensure effective implementation
- ◆ Understand the process approach and its application in managing performance and continual improvement in a sustainable management system
- ◆ Understand organizational context and the importance of interested party and customer expectations in setting objectives and establishing effective monitoring, measurement and data analysis
- ◆ Employ an effective and efficient approach to documentation
- ◆ Provide guidance on how to plan and execute the implementation process

Seminar Content

- Automotive Industry Standard – Background and History
- Key Drivers of change for IATF 16949 and the key changes
- Management systems, process approach and documentation recommendations (clause 4.4 and 7.5)
- Understanding the requirements of IATF 16949 and ISO 9001:2015 (Focus on understanding the intent and content of IATF Writing Committee)
- Transition Planning and Key Strategies
- Review of Gap Analysis Tool and Q and A
- Planning the Management System
- Documenting the Management System
- Implementing the Management System
- Conducting Management Review

IATF 16949:2016 Internal Auditor Training for Automotive Quality Management Systems

Duration: 4 Days



Seminar Goals

- ◆ Understand the application of quality management principles in the context of ISO 9001:2015 and IATF 16949:2016
- ◆ Relate the quality management system to the organizational products, services, activities and operational processes
- ◆ Relate organization's context and interested party needs and expectations to the planning and implementation of an organization's quality management system
- ◆ Understand the application of the principles, procedures and techniques of auditing
- ◆ Understand the conduct of an effective audit in the context of the auditee's organizational situation
- ◆ Understand the application of the regulations, and other considerations that are relevant to the management system, and the conduct of the audit
- ◆ Practice personal attributes necessary for the effective and efficient conduct of a management system audit
- ◆ Understand the purpose and applicable uses of the core tools
- ◆ Link the core tools to IATF 16949:2016 requirements
- ◆ Explain the importance of Customer-Specific Requirements

Seminar Content

- Introduction and Welcome
- The ISO and IATF Standards Explained
- Introduction to ISO 9001 and IATF 16949
- ISO 9001:2015 and IATF 16949:2016 Requirements
 - Group Exercise: Context of the Organization
 - Group Exercise: Interested Parties
 - Group Exercise: Audit Scenarios

DAY 1

- ISO 9001:2015 and IATF 16949:2016 Requirements
 - Group Exercises: Audit Scenarios
 - Independent QMS Written Exercise
- Introduction to Turtle Diagrams and Audit Trails
- Management of Audit Programs
- Audit Planning and Preparation
 - Breakout Exercise 1: Writing an Objective and Scope Statement
 - Breakout Exercise 2: Documentation Review
 - Breakout Exercise 3: Creating an Audit Plan

DAY 2

- Performing the Audit
 - Breakout Exercise 4: Performing an Audit
- Conducting a Process Approach Audit
- Conducting an Audit of Risk Planning (6.1)
- Writing Nonconformity Statements
 - Breakout Exercise 5: Writing Nonconformity Statements
- Closing Meeting
- Completing the Audit Report
- Corrective Action and Closeout

DAY 3

- Linking Automotive Core Tools to IATF 16949
- Customer-Specific Requirements
 - Management Systems Auditing Written Exercise
 - CSR/Core Tools Examination

DAY 4

IATF 16949:2016 Lead Auditor Training for Automotive Quality Management Systems

Duration: 5 Days



Seminar Goals

- ◆ Understand the application of quality management principles in the context of ISO 9001:2015 and IATF 16949:2016
- ◆ Relate the quality management system to the organizational products, services, activities and operational processes
- ◆ Relate organization's context and interested party needs and expectations to the planning and implementation of an organization's quality management system
- ◆ Understand the application of the principles, procedures and techniques of auditing
- ◆ Understand the conduct of an effective audit in the context of the auditee's organizational situation
- ◆ Understand the application of the regulations, and other considerations that are relevant to the management system, and the conduct of the audit
- ◆ Practice personal attributes necessary for the effective and efficient conduct of a management system audit
- ◆ Establish, plan and task the activities of an audit team
- ◆ Communicate effectively with the auditee and audit client
- ◆ Organize and direct audit team members
- ◆ Prevent and resolve conflict with the auditee and/or within the audit team
- ◆ Prepare and complete the audit report
- ◆ Understand the purpose and applicable uses of the core tools
- ◆ Link the core tools to IATF 16949:2016 requirements
- ◆ Explain the importance of Customer-Specific Requirements

Seminar Content

- Introduction and Welcome
- The ISO and IATF Standards Explained
- Introduction to ISO 9001 and IATF 16949
- ISO 9001:2015 and IATF 16949:2016 Requirements

DAY 1

- ISO 9001:2015 and IATF 16949:2016 Requirements
- Introduction to Turtle Diagrams and Audit Trails
- Management of Audit Programs
- Audit Planning and Preparation

DAY 2

- Performing the Audit
- Writing Nonconformity Statements
- Closing Meeting
- Completing the Audit Report
- Corrective Action and Closeout

DAY 3

- Linking Automotive Core Tools to IATF 16949
- Customer-Specific Requirements

DAY 4

- Leading Audit Teams
- Management System Certification Scheme and Auditor Qualifications
- Review of Audit Process and Audit Management Strategies
- Practical Application of Audit Principles and Instructor Interviews

DAY 5

IATF 16949:2016 Second Party (Supplier Auditor) Training for Automotive Quality Management Systems

Duration: 5 Days



Seminar Goals

- ◆ Understand the application of quality management principles in the context of ISO 9001:2015 and IATF 16949:2016
- ◆ Relate the quality management system to the organizational products, services, activities and operational processes
- ◆ Relate organization's context and interested party needs and expectations to the planning and implementation of an organization's quality management system
- ◆ Understand the application of the principles, procedures and techniques of auditing
- ◆ Understand the conduct of an effective audit in the context of the auditee's organizational situation
- ◆ Understand the application of the regulations, and other considerations that are relevant to the management system, and the conduct of the audit
- ◆ Practice personal attributes necessary for the effective and efficient conduct of a management system audit
- ◆ Understand the purpose and applicable uses of the core tools
- ◆ Link the core tools to IATF 16949:2016 requirements
- ◆ Explain the importance of Customer-Specific Requirements
- ◆ Understand how to conduct Process Flow, FMEA, Control Plans and Process Review audits at a supplier site

Seminar Content

- Introduction and Welcome
- The ISO and IATF Standards Explained
- Introduction to ISO 9001 and IATF 16949
- ISO 9001:2015 and IATF 16949:2016 Requirements
 - Group Exercise: Context of the Organization
 - Group Exercise: Interested Parties
 - Group Exercise: Audit Scenarios

DAY 1

- ISO 9001:2015 and IATF 16949:2016 Requirements
 - Group Exercises: Audit Scenarios
 - Independent QMS Written Exercise
- Introduction to Turtle Diagrams and Audit Trails
- Management of Audit Programs
- Audit Planning and Preparation

DAY 2

- Performing the Audit
- Writing Nonconformity Statements
- Closing Meeting
- Completing the Audit Report
- Corrective Action and Closeout

DAY 3

- Linking Automotive Core Tools to IATF 16949
- Customer-Specific Requirements
 - Management Systems Auditing Written Exercise
 - CSR/Core Tools Examination

DAY 4

- Understanding the Manufacturing Process – Drawing, Process Flow, PFMEA, Control Plan, SPC, and MSA
- Walking through a Case Study
- Conducting a Process Review

DAY 5

IATF 16949:2016 Manufacturing Process Auditor Training for Automotive Quality Management Systems

Duration: 5 Days

Seminar Goals

- ◆ Understand the application of quality management principles in the context of ISO 9001:2015 and IATF 16949:2016
- ◆ Relate the quality management system to the organizational products, services, activities and operational processes
- ◆ Relate organization's context and interested party needs and expectations to the planning and implementation of an organization's quality management system
- ◆ Understand the application of the principles, procedures and techniques of auditing
- ◆ Understand the conduct of an effective audit in the context of the auditee's organizational situation
- ◆ Understand the application of the regulations, and other considerations that are relevant to the management system, and the conduct of the audit
- ◆ Practice personal attributes necessary for the effective and efficient conduct of a management system audit
- ◆ Understand the purpose and applicable uses of the core tools
- ◆ Link the core tools to IATF 16949:2016 requirements
- ◆ Explain the importance of Customer-Specific Requirements
- ◆ Understand how to conduct Process Flow, FMEA, Control Plans and Process Review audits at a supplier site

Seminar Content

- Introduction and Welcome
- The ISO and IATF Standards Explained
- Introduction to ISO 9001 and IATF 16949
- ISO 9001:2015 and IATF 16949:2016 Requirements

DAY 1

- ISO 9001:2015 and IATF 16949:2016 Requirements
- Introduction to Turtle Diagrams and Audit Trails
- Management of Audit Programs
- Audit Planning and Preparation

DAY 2

- Performing the Audit
- Writing Nonconformity Statements
- Closing Meeting
- Completing the Audit Report
- Corrective Action and Closeout

DAY 3

- Linking Automotive Core Tools to IATF 16949
- Customer-Specific Requirements

DAY 4

- Understanding the Manufacturing Process – Drawing, Process Flow, PFMEA, Control Plan, SPC, and MSA
- Walking through a Case Study
- Conducting a Process Review

DAY 5

IATF 16949:2016 Product Auditor Training for Automotive Quality Management Systems

Duration: 3 Days

Seminar Goals

- ◆ Understand how Blueprint Reading related to IATF 16949:2016
- ◆ Interpret orthographic projection
- ◆ Recognize first-angle and third-angle projection
- ◆ Know when to use various types of lines
- ◆ Identify auxiliary and section views and place them properly
- ◆ Correctly interpret title and revision blocks
- ◆ Understand and apply dimensioning & tolerancing to a print
- ◆ Recognize GD&T symbols and datums
- ◆ Identify and explain manufacturing callouts such as screw threads and surface finish
- ◆ Understanding Variation and its effects on measurement
- ◆ Conducting MSA Studies and its applications
- ◆ Understand Gages and Gage Equipment
- ◆ To provide participants with an understanding of
- ◆ The importance of basic measuring equipment and its Measurement Systems
- ◆ Measurement systems as a process for decision making
- ◆ The basic definitions used in measurement systems
- ◆ Measurement techniques of common equipment including application, handling, and methods to use
- ◆ Overview of causes of variation and its impact
- ◆ Basic concepts to be adopted during the measurements

Seminar Content

- Blueprint Reading DAY 1
 - Introduction
 - Importance of Engineering Drawings
 - Basic Steps in Reading a Print
 - Line Types: Visible, Hidden, Center, Extension, Dimension, Section, Leader, Phantom
 - The Title Block
 - Orthographic Projection Views
 - Visualizing in 3D
 - First vs. Third Angle Projection
 - Section Views
 - Dimensioning Practices
 - Plus/Minus vs. Limit Dimensions
 - Special Dimensions/Tolerances
- Geometric Dimensioning and Tolerancing DAY 2
- Basic Definitions & Terminology DAY 3
 - Benefits of Correct Measurements
 - Impact of Measurement Variation
 - Causes of Measurement Variation
 - Calibration and MSA – an overview
 - Measuring Equipment & Measurement System

Transition Training for IATF 16949:2016 and ISO 9001:2015

Duration: 2 Days

Seminar Goals

- ◆ Understand management systems and the process approach
- ◆ Understand linkages between context, interested party expectations, and planning including risk based thinking
- ◆ Risk based thinking approaches for IATF 16949 and ISO 9001:2015
- ◆ Integrating Code of Conduct, Environmental Policy, Protecting the Environment and Social Responsibility
- ◆ Importance of integrated management systems to transition in the Automotive industry with the advent of the High Level Structure (HLS)
- ◆ Organize documentation according to IATF 16949:2016 to demonstrate effective planning, operation, and control of processes
- ◆ Understand the intent and content of the requirement changes from the perspective of the IATF and Writing Committee
- ◆ Develop an implementation plan for transition
- ◆ Understand the IATF requirements for transition
- ◆ Determine key strategies and actions to ensure effective implementation

Seminar Content

- Automotive Industry Standard – Background and History
- Key Drivers of change for IATF 16949 and the key changes
- Management systems, process approach and documentation recommendations (clause 4.4 and 7.5)
- Understanding the requirements of IATF 16949 and ISO 9001:2015 (Focus on understanding the intent and content of IATF Writing Committee)
- Transition Planning and Key Strategies
- Review of Gap Analysis Tool and Q and A

Note: This training will provide a gap analysis tool for IATF 16949 including ISO 9001:2015

Automotive OEM Detailed Customer Specific Requirements Workshop

Duration: Half-day



Seminar Goals

- ◆ Understand OEM customer-specific requirements relating to business, product, material, delivery and the Quality Management System per IATF 16949:2016
- ◆ Explain methods for gathering, communicating and applying customer-specific requirements (and customer information) within the organization
- ◆ Let participants share the OEM-specific areas of knowledge and expertise with one another

Seminar Content

- Introductions and Welcome
- Customer-Specific Requirements per IATF 16949
- Overview to OEM-specific Customer-Specific Requirements for IATF 16949:2016
 - Ford Customer-Specific Requirements
 - GM Customer-Specific Requirements
 - FCA Customer-Specific Requirements
 - VW Customer-Specific Requirements (optional)
 - BMW Customer-Specific Requirements (optional)
 - Honda Customer-Specific Requirements (optional)

IATF 16949:2016 Employee Awareness

Duration: Half-day

Seminar Goals

- ◆ Discuss the differences between the 2009 version of the ISO/TS 16949 standard and the 2016 revision
- ◆ Apply knowledge and understanding of the IATF 16949:2016 standard to begin planning and preparation of an existing Quality Management System to comply with IATF 16949:2016

Seminar Content

- Why was IATF 16949 Revised?
- IATF 16949:2016 Requirements Significantly Pertinent to Employees
- Tips for Answering Auditor Questions

AIAG-VDA DFMEA (SFMEA and DFMEA) for Practitioners and Facilitators

Duration: 3 Days

Seminar Goals

- ◆ Provide a hands-on approach to the DFMEA process and its relationship to program deliverables and status reporting to provide the competencies needed to introduce new products and processes smoothly
- ◆ Apply the AIAG-VDA Seven Step Approach to developing SFMEA and DFMEA
- ◆ Apply the major changes, improvements, and benefits of AIAG-VDA DFMEA
- ◆ Study the changes and differences between AIAG VDA FMEA and AIAG FMEA 4th Edition. How to make the results of both approaches the same?
- ◆ Detail best in class methods of AIAG VDA Design FMEA implementations
- ◆ Create a Block Diagram, P Diagram, and Interface Diagram
- ◆ Link DFMEA with DVPR and use Prevention Checklists
- ◆ Link SFMEA, DFMEA, Process Flow, PFMEA, and Control Plans
- ◆ Learn how to link DFMEA to failure and warranty history and Cost of Poor Quality (COPQ)
- ◆ Hands on “use of AIAG-VDA FMEA software” and understand role of software in AIAG-VDA FMEA
- ◆ Implementation of the AIAG-VDA and other Supply Chain Standards
- ◆ Use of AIAG-VDA DFMEA Checklist to evaluate DFMEAs completed and to provide consistency when DFMEA is applied
- ◆ Developing AIAG-VDA DFMEA Transition and Implementation Plan

Seminar Content

- Course Overview and Introductions
- Setting the Stage: APQP Overview
- Chapter 1 – Introduction to Failure Modes and Effects Analysis (FMEA)
- Chapter 2 – Developing an FMEA
- Chapter 3 – Design FMEA Prerequisites
- Chapter 4 – Developing the Design FMEA
- Chapter 5 – Test Planning and Reporting (DVP&R)
- Chapter 6 – Implications of the AIAG-VDA FMEA
- Summary
- Certification Exam for AIAG-VDA DFMEA – Optional

Note 1: Breakouts will be conducted using AIAG-VDA FMEA Software

Note 2: Omnex can offer training in IQFMEA, Plato or AQuA Pro for onsite training

Note 3: You can add two additional days for Facilitator Training (onsite training only)

Note 4: You can add one or two days to develop a DFMEA using your product. It will be best if you have a 4th Edition DFMEA for comparison purposes. This training can include your component suppliers.

AIAG-VDA FMEA for Managers and Implementers – Implementation Training

Duration: 2 Days

Seminar Goals

- ◆ Understand the AIAG-VDA FMEA process and its relationship to program deliverables and status reporting to provide the competencies needed to introduce new products and processes smoothly
- ◆ Understanding the AIAG-VDA Seven Step Approach to developing FMEA and the differences to AIAG-VDA 4th Edition
- ◆ Understand the major changes, improvements, and benefits of AIAG-VDA FMEA
- ◆ Understand the “use of AIAG-VDA FMEA software” and the role of software in AIAG-VDA FMEA
- ◆ Implementation Steps of the AIAG-VDA and other Supply Chain Standards
- ◆ Developing AIAG-VDA DFMEA and also AIAG DFMEA 4th Edition and transitioning approach internally
- ◆ Use of AIAG-VDA FMEA Transition and Implementation Checklist and complete an Action Plan
- ◆ Understand steps needed for developing in house competencies and linkages needed with Design, Customer, and Supply Chain

Seminar Content

- Understand the Seven Step Process for AIAG-VDA DFMEA and AIAG-VDA PFMEA
- Chapter 1: Background to AIAG and VDA
- Chapter 2: Comparing AIAG 4th edition and AIAG-VDA FMEA first edition Steps
- Chapter 3: AIAG-VDA FMEA 7 Steps – DFMEA
- Chapter 4: AIAG-VDA FMEA 7 Steps – PFMEA

DAY 1

Implementing AIAG VDA FMEA in the New Product Development Process with APQP

- Changes to the organization and Supply Chain
- AIAG-VDA DFMEA and PFMEA and Changes and implications to the New Product Development and APQP process
- Design and Process Reuse and the product and process architecture
- Linkages of SFMEA, DFMEA, and PFMEA including PPAP
- Requirements Management for AIAG-VDA FMEA
- Software needs for AIAG-VDA FMEA
- Changes to the Purchasing, Supplier Development and Purchase Order requirements
- How to use the AIAG-VDA FMEA to improve Cost of Quality and including External and Internal PPM
- Change Management and FMEA Updates
- Getting Started Transition Checklist and Action Plan Summary

DAY 2

AIAG-VDA FMEA Understanding, Implications, and Strategy Executive Overview

Duration: 1 Day

Seminar Goals

- ✦ Understanding of the AIAG-VDA FMEA approach and changes to the previous approaches used by the organization. Provide top management and other key management understanding on the strategic implications with the AIAG-VDA FMEA and Supply Chain standards evolving out of the industry shift from Gas and Diesel mechanical vehicles to Electric and Autonomous Vehicles
- ✦ Importance of the Supply Chain and how these standards link the supply chain
- ✦ Requirements flow down the supply chain
- ✦ Software to support a 3 dimensional FMEA structure and requirements flow down
- ✦ Design Reuse and product family/process family orientation.
- ✦ Linkage of failure databases and the AIAG-VDA FMEA and reduction of PPM (Cost of Quality)
- ✦ Linkages between System, Sub System, Components and Assembly and Manufacturing Processes

Seminar Content

- What has changed in the AIAG-VDA FMEA vs the 4th Edition
- The Seven Steps of the AIAG-VDA FMEA DFMEA and PFMEA
- Implications of the change to the organization and Supply Chain
 - o What are Supply Chain Standards and why they are important
- Requirements Management for AIAG-VDA FMEA
- Software needs with AIAG-VDA FMEA
 - o AIAG 4th Edition is 2 dimensional and AIAG-VDA FMEA is 3 Dimensional
 - o Reuse of Information and Products/Process Families and Continual Improvement
- Linkages of SFMEA, DFMEA, and PFMEA including PPAP
- Change Management and FMEA Updates
- PPM Defect history, Cost of Poor Quality and FMEA linkages
- Getting Started Checklist and Action Plan

AIAG-VDA Process FMEA and Control Plans for Practitioners and Facilitators

Duration: 3 Days

Seminar Goals

- ✦ Provide a hands-on approach to the FMEA process and its relationship to program deliverables and status reporting to provide the competencies needed to introduce new processes smoothly.
- ✦ Apply the AIAG-VDA Seven Step Approach to developing Process Flow, PFMEA and Control Plans
- ✦ Apply the major changes, improvements, and benefits of AIAG-VDA PFMEA
- ✦ Study the changes and differences between AIAG VDA FMEA and AIAG FMEA 4th Edition. What are the changes and differences in the two approaches? How to make the results of both approaches the same?
- ✦ Link SFMEA, DFMEA, Process Flow, PFMEA, and Control Plans
- ✦ Hands on “use of AIAG-VDA FMEA software” and understand role of software in AIAG-VDA FMEA
- ✦ Developing AIAG-VDA PFMEA and also AIAG PFMEA 4th Edition and transitioning approach internally
- ✦ Use of AIAG-VDA PFMEA and Control Plan Checklists to evaluate PFMEAs completed and to develop consistency between PFMEAs and Control Plans in the organization
- ✦ Learn how to link PFMEA to failure and warranty history and Cost of Poor Quality (COPQ)
- ✦ Developing AIAG-VDA PFMEA Transition and Implementation Plan
- ✦ After this training, the participants will have a clear understanding of the following
 - Process Flow and AIAG-VDA PFMEA Structure Analysis
 - Links between Process Flow, PFMEA, Control Plan and Work Instructions
 - Process FMEA and Control Plan
 - All aspects of the 1st edition of FMEA handbook (2019) released by AIAG and VDA

Seminar Content

- Chapter 1: Introduction to Failure Mode and Effects Analysis (FMEA)
- Chapter 2: Developing a PFMEA
- Chapter 3: Process FMEA Prerequisites
- Chapter 4 – Process Control Plans
- Chapter 5 – Implications of the AIAG-VDA FMEA
- Summary
- Certification Exam for AIAG-VDA PFMEA – Optional

Note 1: Breakouts will be conducted using AIAG-VDA FMEA Software

Note 2: Omnex can offer training in IQFMEA, Plato or AQUA Pro for onsite training

Note 3: You can add two additional days for Facilitator Training (onsite training only)

Note 4: You can add one or two days to develop a PFMEA using your product. It will be best if you have a 4th Edition PFMEA and Control Plan for comparison purposes.

Functional Safety Core Tools: DFMEAs for Monitoring and System Response

Duration: 2 Days

Seminar Goals

- ◆ Understand the use of the supplemental FMEA for monitoring and response, potential failures which might occur under customer operating conditions are analyzed with respect to their effect on the system or vehicle. How this tool can be used to identify safety risk for ISO 26262
 - ◆ Provide a hands-on approach to the DFMEA with MSR process and their relationship to ISO 26262 deliverables
- Review example applied to ISO 26262

Seminar Content

- Chapter 1: APQP and ISO 26262
 - Chapter 2: MSR FMEA in ISO 26262
 - Chapter 3: Introduction to FMEA for Monitoring and Response (FMEA-MSR)
 - Chapter 4: Review of the AIAG-VDA Handbook
 - Chapter 5: FMEA-MSR Preparation
 - Breakout Exercise 1: Boundary Diagram
 - Breakout Exercise 2: Structure Diagram
-
- Chapter 6: Developing the FMEA-MSR
 - Breakout Exercise 3: Function Analysis
 - Breakout Exercise 4: Failure Analysis
 - Breakout Exercise 5: Risk Analysis
 - Breakout Exercise 6: Optimization
 - Chapter 7: Communicating the Risk
 - Case study review

Reverse Failure Mode and Effect Analysis – RFMEA

Duration: 2 Days

Seminar Goals

- ◆ Explain the difference between DFMEA and RFMEA
 - o Demonstrate an ability to properly construct a RFMEA check-sheet
- ◆ Demonstrate an ability to properly and effectively complete all items in the RFMEA process
 - o Identify high risk areas, evaluate and test control plan gaging and measurement.
- ◆ Demonstrate how to use the output from a RFMEA to identify additional risk and work it back into the PFMEA
- ◆ Identify special characteristics in product design and assure that the control methods are effective.

Seminar Content

- Intro to FMEA
 - APQP and FMEA
 - Development of a good conventional PFMEA
 - VDA PFMEA 7 Step Process
 - Intro to Reverse - FMEA
 - 7 Step Reverse Process
 - Assemble Malfunction team
 - Review of PFMEA, develop plan
-
- Development of Reverse FMEA check-sheet
 - Go and See- Evaluate process using check-sheet
 - Evaluate detection method through testing
 - Re-access risk
 - Develop action plan
 - Reporting Results to Customer
 - Continuous improvement- Updating Baselines and Requirements
-
- Work on in-plant example

Understanding the Requirements of IATF 16949:2016 Automotive Quality Management Systems



Duration: 2 Days

Seminar Goals

- Understand the application of quality management principles in the context of ISO 9001:2015 and IATF 16949:2016
- Relate the quality management system to the organizational products, services, activities and operational processes
- Relate organization's context and interested party needs and expectations to the planning and implementation of an organization's quality management system

Seminar Content

-
- Introduction and Welcome
 - The ISO and IATF Standards Explained
 - Introduction to ISO 9001 and IATF 16949
 - ISO 9001:2015 and IATF 16949:2016 Requirements
 - Group Exercise: Context of the Organization
 - Group Exercise: Interested Parties
 - Group Exercise: Audit Scenarios
-
- ISO 9001:2015 and IATF 16949:2016 Requirements
 - Group Exercises: Audit Scenarios
 - Independent QMS Written Exercise

DAY
1

DAY
2

ISO 27001/TISAX/CMMC

**Understanding the Requirements of
ISO/IEC 27001:2013 for Information Security Management Systems**

**ISO/IEC 27001:2013 Internal Auditor Training for
Information Security Management Systems**

**ISO/IEC 27001:2013 Lead Auditor Training for
Information Security Management Systems**

**ISO/IEC 27001:2013 for Information Security
Management Systems Executive Overview**

Information Security Awareness Training

**Understanding the Requirements of
ISO/IEC 27001:2013 and VDA ISA TISAX**

**ISO/IEC 27001:2013 and VDA ISA TISAX Internal Auditor
Training for Information Security Management Systems**

**ISO/IEC 27001:2013 and VDA ISA TISAX Lead Auditor Training for
Information Security Management Systems**

**Understanding the Requirements of Cybersecurity Maturity Model
Certification (CMMC) and ISO/IEC 27001:2013**

**Cybersecurity Maturity Model Certification (CMMC) and ISO/IEC
27001:2013 Internal Auditor Training for Information Security
Management Systems**

**Cybersecurity Maturity Model Certification (CMMC) and
ISO/IEC 27001:2013 Lead Auditor Training for Information Security
Management Systems**

Understanding the Requirements of ISO/IEC 27001:2013 for Information Security Management Systems

Duration: One day

Seminar Goals

- Understand the application of Information Security Management principles in the context of ISO/IEC 27001:2013.
- Relate the Information Security Management system to the organizational products, services, activities and operational processes.
- Relate organization's context and interested party needs and expectations to the planning and implementation of an organization's Information Security Management system.

Seminar Content

- Fundamentals of Information Security Management Systems (ISMS)
 - Information Security
 - What is an Information Security Management System (ISMS)
 - The ISO/IEC 270000 Fundamentals and Vocabulary
 - The ISO/IEC 270001 ISMS Described
- ISO/IEC 27001:2013 Requirements Descriptions
 - ISO/IEC 27001:2013 Clauses
 - Annex A
 - The Process Approach
- Risk-based Thinking
 - ISMS Risks
 - ISMS Risk Assessment
 - ISMS Risk Treatment
- ISO/IEC 27001 Clause 4 – Context of the Organization
 - Group Exercise 1: Context of the Organization
- ISO/IEC 27001 Clause 5 – Leadership
- ISO/IEC 27001 Clause 6 – Planning
 - Group Exercise 2: Assessing and Evaluating Risk
- ISO/IEC 27001 Clause 7 – Support
- ISO/IEC 27001 Clause 8 – Operation
- ISO/IEC 27001 Clause 9 – Performance Evaluation
- ISO/IEC 27001 Clause 10 – Improvement
- ISO/IEC 27001 Annex A
 - Group Exercise 3: Annex A – Required Elements and Risk Treatments
- Understanding ISMS Final Exam

DAY 1

ISO/IEC 27001:2013 Internal Auditor Training for Information Security Management Systems

Duration: 3 Days



Seminar Goals

- Understand the application of Information Security Management principles in the context of ISO/IEC 27001:2013
- Relate the Information Security Management system to the organizational products, services, activities and operational processes.
- Relate organization's context and interested party needs and expectations to the planning and implementation of an organization's Information Security Management system.
- Understand the application of the principles, procedures and techniques of auditing.
- Understand the conduct of an effective audit in the context of the auditee's organizational situation.
- Understand the application of the regulations, and other considerations that are relevant to the management system, and the conduct of the audit.
- Practice personal attributes necessary for the effective and efficient conduct of a management system audit.

Seminar Content

- Fundamentals of Information Security Management Systems (ISMS)
 - Information Security
 - What is an Information Security Management System (ISMS)
 - The ISO/IEC 270000 Fundamentals and Vocabulary
 - The ISO/IEC 270001 ISMS Described
- ISO/IEC 27001:2013 Requirements Descriptions
 - ISO/IEC 27001:2013 Clauses
 - Annex A
 - The Process Approach
- Risk-based Thinking
 - ISMS Risks
 - ISMS Risk Assessment
 - ISMS Risk Treatment
- ISO/IEC 27001 Clause 4 – Context of the Organization
 - Group Exercise 1: Context of the Organization
- ISO/IEC 27001 Clause 5 – Leadership
- ISO/IEC 27001 Clause 6 – Planning
 - Group Exercise 2: Assessing and Evaluating Risk
- ISO/IEC 27001 Clause 7 – Support
- ISO/IEC 27001 Clause 8 – Operation
- ISO/IEC 27001 Clause 9 – Performance Evaluation
- ISO/IEC 27001 Clause 10 – Improvement
- ISO/IEC 27001 Annex A
 - Group Exercise 3: Annex A – Required Elements and Risk Treatments
- Understanding ISMS Final Exam

DAY 1

ISO/IEC 27001:2013 Internal Auditor Training for Information Security Management Systems

Cont'd



Seminar Content

- Process Approach to Auditing, Turtle Diagrams and Audit Trails
- Audit Guidance, Definitions and Principles
- The Audit Program
- Audit Planning and Preparation including ISO 27007 Guidelines for Information Security Management Systems Auditing
 - Breakout Exercise 1: Writing an Objective and Scope Statement
 - Breakout Exercise 2: Documentation Review
 - Breakout Exercise 3: Creating an Audit Plan

DAY 2

- Performing the Audit
 - Breakout Exercise 4: Performing an Audit
- Writing Nonconformity Statement
 - Breakout Exercise 5: Writing Nonconformity Statements
- Closing Meeting
- Completing the Audit Report
- Corrective Action and Close-Out
- Management Systems Auditing Final Exam

DAY 3

ISO/IEC 27001:2013 Lead Auditor Training for Information Security Management Systems

Duration: Five days



Seminar Goals

- Understand the application of Information Security Management principles in the context of ISO/IEC 27001:2013.
- Relate the Information Security Management system to the organizational products, services, activities and operational processes.
- Relate organization's context and interested party needs and expectations to the planning and implementation of an organization's Information Security Management system.
- Understand the application of the principles, procedures and techniques of auditing.
- Understand the conduct of an effective audit in the context of the auditee's organizational situation.
- Understand the application of the regulations, and other considerations that are relevant to the management system, and the conduct of the audit.
- Practice personal attributes necessary for the effective and efficient conduct of a management system audit.
- Establish, plan and task the activities of an audit team.
- Communicate effectively with the auditee and audit client.
- Organize and direct audit team members.
- Prevent and resolve conflict with the auditee and/or within the audit team.
- Prepare and complete the audit report.

Seminar Content

- Fundamentals of Information Security Management Systems (ISMS)
 - Information Security
 - What is an Information Security Management System (ISMS)
 - The ISO/IEC 270000 Fundamentals and Vocabulary
 - The ISO/IEC 270001 ISMS Described
- ISO/IEC 27001:2013 Requirements Descriptions
 - ISO/IEC 27001:2013 Clauses
 - Annex A
 - The Process Approach
 - Risk-based Thinking
 - ISMS Risks
 - ISMS Risk Assessment
 - ISMS Risk Treatment
 - ISO/IEC 27001 Clause 4 – Context of the Organization
 - Group Exercise 1: Context of the Organization
 - ISO/IEC 27001 Clause 5 – Leadership
 - ISO/IEC 27001 Clause 6 – Planning
 - Group Exercise 2: Assessing and Evaluating Risk
 - ISO/IEC 27001 Clause 7 – Support
 - ISO/IEC 27001 Clause 8 – Operation
 - ISO/IEC 27001 Clause 9 – Performance Evaluation
 - ISO/IEC 27001 Clause 10 – Improvement
 - ISO/IEC 27001 Annex A
 - Group Exercise 3: Annex A – Required Elements and Risk Treatments
- Understanding ISMS Final Exam


DAY 1


ISO/IEC 27001:2013 Lead Auditor Training for Information Security Management Systems


Cont'd


Seminar Content



- Process Approach to Auditing, Turtle Diagrams and Audit Trails 
- Audit Guidance, Definitions and Principles
- The Audit Program
- Audit Planning and Preparation including ISO 27007 Guidelines for Information Security Management Systems Auditing
 - Breakout Exercise 1: Writing an Objective and Scope Statement
 - Breakout Exercise 2: Documentation Review
 - Breakout Exercise 3: Creating an Audit Plan

- Performing the Audit 
 - Breakout Exercise 4: Performing an Audit
- Writing Nonconformity Statement
 - Breakout Exercise 5: Writing Nonconformity Statements
- Closing Meeting
- Completing the Audit Report
- Corrective Action and Close-Out
- Management Systems Auditing Final Exam

- Leading Audit Teams 
- Management System Certification Scheme and Auditor Qualifications
- Leading Management Systems Audit Teams Mock Audit Case Study

- Review of Audit Process and Audit Management Strategies 
- Leading Management Systems Audit Teams Final Exam
- Practical Application of Audit Principles and Instructor Interviews

ISO/IEC 27001:2013 for Information Security Management Systems Executive Overview

Duration: Half-day

Seminar Goals

- Understand the application of Information Security Management principles in the context of ISO/IEC 27001:2013.
- Relate the Information Security Management system to the organizational products, services, activities and operational processes.
- Relate organization's context and interested party needs and expectations to the planning and implementation of an organization's Information Security Management system.

Seminar Content

- The Need for Information Security
- What is Information Security?
- High Level Structure and Integrated Management Structure
- Importance of Context, Interested Parties, Scope, and Process Approach
- Role of Leadership in IT Security
- Risk Treatment and Controls
- Implementation Steps for ISO/IEC 27001:2013
- What are the Revision Timelines?
- Transition Guidance


Information Security Awareness Training

Duration: One Day

Seminar Goals

- Understand the application of Information Security Management principles in the context of ISO/IEC 27001:2013.
- Relate the Information Security Management system to the organizational products, services, activities and operational processes.
- Relate organization's context and interested party needs and expectations to the planning and implementation of an organization's Information Security Management system.

Seminar Content

- Introduction and Welcome 
- Introduction to the course
 - Pre-test
- Typical information policies
- Global incidents on information security breaches
- Common Intrusion Points
- Types of Threats and Attacks
- IT Best Practices – At office environments, mobile environment
- Email practices
- Managing access
- Travel precautions and working remote.
- Breakout scenarios and group discussions will be held after each chapters

Understanding the Requirements of ISO/IEC 27001:2013 and VDA ISA TISAX

Duration: One and Half days

Seminar Goals

- ◆ Understand the application of Information Security Assessment principles, and maturity of controls
- ◆ Relate the Information Security Management system clauses of ISO/IEC 27001:2013 to the organizational information, assets, product designs, services, activities and operational processes
- ◆ Relate organization's context and interested party needs and expectations to security risk assessment, planning and implementation of an organization's Information Security Management system

Seminar Content

- **Fundamentals of Information Security Management Systems (ISMS)**
 - Information Security
 - What is an Information Security Management System (ISMS)
 - The ISO/IEC 270000 Fundamentals and Vocabulary
 - The ISO/IEC 270001 ISMS Described
- ISO/IEC 27001:2013 Requirements Descriptions
 - ISO/IEC 27001:2013 Clauses
 - Annex A
 - The Process Approach
- Risk-based Thinking
 - ISMS Risks
 - ISMS Risk Assessment
 - ISMS Risk Treatment
- ISO/IEC 27001 Clause 4 – Context of the Organization
 - Group Exercise 1: Context of the Organization
- ISO/IEC 27001 Clause 5 – Leadership
- ISO/IEC 27001 Clause 6 – Planning
 - Group Exercise 2: Assessing and Evaluating Risk
- ISO/IEC 27001 Clause 7 – Support
- ISO/IEC 27001 Clause 8 – Operation
- ISO/IEC 27001 Clause 9 – Performance Evaluation
- ISO/IEC 27001 Clause 10 – Improvement
- ISO/IEC 27001 Annex A
 - Group Exercise 3: Annex A – Required Elements and Risk Treatments

DAY 1

- TISAX: Trusted Information Security Assessment Exchange
 - Roles Within TISAX
 - Assessment Model: Simplified Group Assessment
 - Assessment Methodology
 - Maturity Model
- VDA ISA TISAX and ISO/IEC 27001 Compared
 - ISO/IEC 27001:2013 Annex A
 - TISAX Overlap with ISO/IEC 27001:2013
 - TISAX Additional Controls not in ISO/IEC 27001
- TISAX Controls
 - Information Security Controls
 - Prototype Protection Controls
 - Data Protection Controls
- TISAX Measurement and Analysis
 - Group Exercise 4: TISAX Measurement and Analysis
- Understanding ISMS and TISAX Final Exam

DAY 2

ISO/IEC 27001:2013 and VDA ISA TISAX Internal Auditor Training for Information Security Management Systems



Duration: Three days

Seminar Goals

- ◆ Understand the application of Information Security Assessment principles, and maturity of controls
- ◆ Understand the application of Information Security Management principles in the context of ISO/IEC 27001:2013.
- ◆ Relate the Information Security Management system to the organizational products, services, activities and operational processes.
- ◆ Relate organization's context and interested party needs and expectations to the planning and implementation of an organization's Information Security Management system.
- ◆ Understand the application of the principles, procedures and techniques of auditing.
- ◆ Understand the conduct of an effective audit in the context of the auditee's organizational situation.
- ◆ Understand the application of the regulations, and other considerations that are relevant to the management system, and the conduct of the audit.
- ◆ Practice personal attributes necessary for the effective and efficient conduct of a management system audit.

Seminar Content

- **Fundamentals of Information Security Management Systems (ISMS)**
 - Information Security
 - What is an Information Security Management System (ISMS)
 - The ISO/IEC 270000 Fundamentals and Vocabulary
 - The ISO/IEC 270001 ISMS Described
- ISO/IEC 27001:2013 Requirements Descriptions
 - ISO/IEC 27001:2013 Clauses
 - Annex A
 - The Process Approach
- Risk-based Thinking
 - ISMS Risks
 - ISMS Risk Assessment
 - ISMS Risk Treatment
- ISO/IEC 27001 Clause 4 – Context of the Organization
 - Group Exercise 1: Context of the Organization
- ISO/IEC 27001 Clause 5 – Support
- ISO/IEC 27001 Clause 6 – Planning
 - Group Exercise 2: Assessing and Evaluating Risk
- ISO/IEC 27001 Clause 7 – Support
- ISO/IEC 27001 Clause 8 – Operation
- ISO/IEC 27001 Clause 9 – Performance Evaluation
- ISO/IEC 27001 Clause 10 – Improvement
- ISO/IEC 27001 Annex A
 - Group Exercise 3: Annex A – Required Elements and Risk Treatments

DAY 1

ISO/IEC 27001:2013 and VDA ISA TISAX Internal Auditor Training for Information Security Management Systems



Cont'd

Seminar Content

- TISAX: Trusted Information Security Assessment Exchange
 - Roles Within TISAX
 - Assessment Model: Simplified Group Assessment
 - Assessment Methodology
 - Maturity Model
- VDA ISA TISAX and ISO/IEC 27001 Compared
 - ISO/IEC 27001:2013 Annex A
 - TISAX Overlap with ISO/IEC 27001:2013
 - TISAX Additional Controls not in ISO/IEC 27001
- TISAX Controls
 - Information Security Controls
 - Prototype Protection Controls
 - Data Protection Controls
- TISAX Measurement and Analysis
 - Group Exercise 4: TISAX Measurement and Analysis
- Understanding ISMS and TISAX Final Exam
- Process Approach to Auditing, Turtle Diagrams and Audit Trails
- Audit Guidance, Definitions and Principles
- The Audit Program
- Audit Planning and Preparation including ISO 27007 Guidelines for Information Security Management Systems Auditing
 - Breakout Exercise 1: Writing an Objective and Scope Statement
 - Breakout Exercise 2: Documentation Review
 - Breakout Exercise 3: Creating an Audit Plan

DAY
2

- Performing the Audit
 - Breakout Exercise 4: Performing an Audit
- Writing Nonconformity Statements
 - Breakout Exercise 5: Writing Nonconformity Statements
- Closing Meeting
- Completing the Audit Report
- Corrective Action and Close-Out
- Management Systems Auditing Final Exam

DAY
3

ISO/IEC 27001:2013 and VDA ISA TISAX Lead Auditor Training for Information Security Management Systems



Duration: Five Days

Seminar Goals

- Understand the application of Information Security Assessment principles, and maturity of controls
- Understand the application of Information Security Management principles in the context of ISO/IEC 27001:2013.
- Relate the Information Security Management system to the organizational products, services, activities and operational processes.
- Relate organization's context and interested party needs and expectations to the planning and implementation of an organization's Information Security Management system.
- Understand the application of the principles, procedures and techniques of auditing.
- Understand the conduct of an effective audit in the context of the auditee's organizational situation.
- Understand the application of the regulations, and other considerations that are relevant to the management system, and the conduct of the audit.
- Practice personal attributes necessary for the effective and efficient conduct of a management system audit.
- Establish, plan and task the activities of an audit team.
- Communicate effectively with the auditee and audit client.
- Organize and direct audit team members.
- Prevent and resolve conflict with the auditee and/or within the audit team.
- Prepare and complete the audit report.

Seminar Content

- Fundamentals of Information Security Management Systems (ISMS)
 - Information Security
 - What is an Information Security Management System (ISMS)
 - The ISO/IEC 270000 Fundamentals and Vocabulary
 - The ISO/IEC 270001 ISMS Described
- ISO/IEC 27001:2013 Requirements Descriptions
 - ISO/IEC 27001:2013 Clauses
 - Annex A
 - The Process Approach
- Risk-based Thinking
 - ISMS Risks
 - ISMS Risk Assessment
 - ISMS Risk Treatment
- ISO/IEC 27001 Clause 4 – Context of the Organization
 - Group Exercise 1: Context of the Organization
- ISO/IEC 27001 Clause 5 – Leadership
- ISO/IEC 27001 Clause 6 – Planning
 - Group Exercise 1: Context of the Organization

DAY
1

ISO/IEC 27001:2013 and VDA ISA TISAX Lead Auditor Training for Information Security Management Systems



Cont'd

Seminar Content

- ISO/IEC 27001 Clause 7 – Support
- ISO/IEC 27001 Clause 8 – Operation
- ISO/IEC 27001 Clause 9 – Performance Evaluation
- ISO/IEC 27001 Clause 10 – Improvement
- ISO/IEC 27001 Annex A
 - Group Exercise 3: Annex A – Required Elements and Risk Treatments

- TISAX: Trusted Information Security Assessment Exchange
 - Roles Within TISAX
 - Assessment Model: Simplified Group Assessment
 - Assessment Methodology
 - Maturity Model
- VDA ISA TISAX and ISO/IEC 27001 Compared
 - ISO/IEC 27001:2013 Annex A
 - TISAX Overlap with ISO/IEC 27001:2013
 - TISAX Additional Controls not in ISO/IEC 27001
- TISAX Controls
 - Information Security Controls
 - Prototype Protection Controls
 - Data Protection Controls
- TISAX Measurement and Analysis
 - Group Exercise 4: TISAX Measurement and Analysis
- Understanding ISMS and TISAX Final Exam
- Process Approach to Auditing, Turtle Diagrams and Audit Trails
- Audit Guidance, Definitions and Principles
- The Audit Program
- Audit Planning and Preparation including ISO 27007 Guidelines for Information Security Management Systems Auditing
 - Breakout Exercise 1: Writing an Objective and Scope Statement
 - Breakout Exercise 2: Documentation Review
 - Breakout Exercise 3: Creating an Audit Plan

- Performing the Audit
 - Breakout Exercise 4: Performing an Audit
- Writing Nonconformity Statements
 - Breakout Exercise 5: Writing Nonconformity Statements
- Closing Meeting
- Completing the Audit Report
- Corrective Action and Close-Out
- Management Systems Auditing Final Exam

- Leading Audit Teams
- Management System Certification Scheme and Auditor Qualifications
- Leading Management Systems Audit Teams Mock Audit Case Study

- Review of Audit Process and Audit Management Strategies
- Leading Management Systems Audit Teams Final Exam
- Practical Application of Audit Principles and Instructor Interviews

Understanding the Requirements of Cybersecurity Maturity Model Certification (CMMC) and ISO/IEC 27001:2013

Duration: One and Half days

Seminar Goals

- ◆ Understand the application of Information Security Assessment principles, and maturity of controls
- ◆ Relate the Information Security Management system clauses of ISO/IEC 27001:2013 to the organizational information, assets, product designs, services, activities and operational processes
- ◆ Relate organization's context and interested party needs and expectations to security risk assessment, planning and implementation of an organization's Information Security Management system

Seminar Content

- Fundamentals of Information Security Management Systems (ISMS)
 - Information Security
 - What is an Information Security Management System (ISMS)
 - The ISO/IEC 270000 Fundamentals and Vocabulary
 - The ISO/IEC 270001 ISMS Described
- ISO/IEC 27001:2013 Requirements Descriptions
 - ISO/IEC 27001:2013 Clauses
 - Annex A
 - The Process Approach
- Risk-based Thinking
 - ISMS Risks
 - ISMS Risk Assessment
 - ISMS Risk Treatment
- ISO/IEC 27001 Clause 4 – Context of the Organization
 - Group Exercise 1: Context of the Organization
- ISO/IEC 27001 Clause 5 – Leadership
- ISO/IEC 27001 Clause 6 – Planning
 - Group Exercise 2: Assessing and Evaluating Risk
- ISO/IEC 27001 Clause 7 – Support
- ISO/IEC 27001 Clause 8 – Operation
- ISO/IEC 27001 Clause 9 – Performance Evaluation
- ISO/IEC 27001 Clause 10 – Improvement
- ISO/IEC 27001 Annex A
 - Group Exercise 3: Annex A – Required Elements and Risk Treatments

- Cybersecurity Maturity Model Certification (CMMC)
 - Description
 - Assessment Criteria and Methodology
- NIST 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
 - NIST 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
 - NIST 800-171A Assessing Security Requirements for Controlled Unclassified Info
 - NIST Handbook 162 NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements
 - What it Consists of
 - Controls
 - How It Was Supposed to be Applied and How It Was Actually Applied
 - Compliance and How It Was Evaluated

Understanding the Requirements of Cybersecurity Maturity Model Certification (CMMC) and ISO/IEC 27001:2013

Cont'd

Seminar Content

- How CMMC Applies the NIST 800-171 Controls
 - Certification
 - CMMC Level Control Methods (Level 1 – 5)
 - Group Exercise 4: CMMC Measurement and Analysis
- Understanding ISMS and CMMC Final Exam

Cybersecurity Maturity Model Certification (CMMC) and ISO/IEC 27001:2013 Internal Auditor Training for Information Security Management Systems



Duration: Three days

Seminar Goals

- ◆ Understand the application of Information Security Assessment principles, and maturity of controls
- ◆ Understand the application of Information Security Management principles in the context of ISO/IEC 27001:2013.
- ◆ Relate the Information Security Management system to the organizational products, services, activities and operational processes.
- ◆ Relate organization's context and interested party needs and expectations to the planning and implementation of an organization's Information Security Management system.
- ◆ Understand the application of the principles, procedures and techniques of auditing.
- ◆ Understand the conduct of an effective audit in the context of the auditee's organizational situation.
- ◆ Understand the application of the regulations, and other considerations that are relevant to the management system, and the conduct of the audit.
- ◆ Practice personal attributes necessary for the effective and efficient conduct of a management system audit.

Seminar Content

- Fundamentals of Information Security Management Systems (ISMS)
 - Information Security
 - What is an Information Security Management System (ISMS)
 - The ISO/IEC 270000 Fundamentals and Vocabulary
 - The ISO/IEC 270001 ISMS Described
- ISO/IEC 27001:2013 Requirements Descriptions
 - ISO/IEC 27001:2013 Clauses
 - Annex A
 - The Process Approach
- Risk-based Thinking
 - ISMS Risks

Cont'd

- ISMS Risk Assessment
- ISMS Risk Treatment
- ISO/IEC 27001 Clause 4 – Context of the Organization
 - Group Exercise 1: Context of the Organization
- ISO/IEC 27001 Clause 5 – Leadership
- ISO/IEC 27001 Clause 6 – Planning
 - Group Exercise 2: Assessing and Evaluating Risk
- ISO/IEC 27001 Clause 7 – Support
- ISO/IEC 27001 Clause 8 – Operation
- ISO/IEC 27001 Clause 9 – Performance Evaluation
- ISO/IEC 27001 Clause 10 – Improvement
- ISO/IEC 27001 Annex A
 - Group Exercise 3: Annex A – Required Elements and Risk Treatments

- Cybersecurity Maturity Model Certification (CMMC)
 - Description
 - Assessment Criteria and Methodology
- NIST 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
 - NIST 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
 - NIST 800-171A Assessing Security Requirements for Controlled Unclassified Info
 - NIST Handbook 162 NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements
 - What it Consists of
 - Controls
 - How It Was Supposed to be Applied and How It Was Actually Applied
 - Compliance and How It Was Evaluated
- How CMMC Applies the NIST 800-171 Controls
 - Certification
 - CMMC Level Control Methods (Level 1 – 5)
 - Group Exercise 4: CMMC Measurement and Analysis
- Understanding ISMS and CMMC Final Exam
- Process Approach to Auditing, Turtle Diagrams and Audit Trails
- Audit Guidance, Definitions and Principles
- The Audit Program
- Audit Planning and Preparation including ISO 27007 Guidelines for Information Security Management Systems Auditing
 - Breakout Exercise 1: Writing an Objective and Scope Statement
 - Breakout Exercise 2: Documentation Review
 - Breakout Exercise 3: Creating an Audit Plan

- Performing the Audit
 - Breakout Exercise 4: Performing an Audit
- Writing Nonconformity Statements
 - Breakout Exercise 5: Writing Nonconformity Statements
- Closing Meeting
- Completing the Audit Report
- Corrective Action and Close-Out
- Management Systems Auditing Final Exam

Cybersecurity Maturity Model Certification (CMMC) and ISO/IEC 27001:2013 Lead Auditor Training for Information Security Management Systems



Duration: Five days

Seminar Goals

- ◆ Understand the application of Information Security Assessment principles, and maturity of controls
- ◆ Understand the application of Information Security Management principles in the context of ISO/IEC 27001:2013.
- ◆ Relate the Information Security Management system to the organizational products, services, activities and operational processes.
- ◆ Relate organization's context and interested party needs and expectations to the planning and implementation of an organization's Information Security Management system.
- ◆ Understand the application of the principles, procedures and techniques of auditing.
- ◆ Understand the conduct of an effective audit in the context of the auditee's organizational situation.
- ◆ Understand the application of the regulations, and other considerations that are relevant to the management system, and the conduct of the audit.
- ◆ Practice personal attributes necessary for the effective and efficient conduct of a management system audit.
- ◆ Establish, plan and task the activities of an audit team.
- ◆ Communicate effectively with the auditee and audit client.
- ◆ Organize and direct audit team members.
- ◆ Prevent and resolve conflict with the auditee and/or within the audit team.
- ◆ Prepare and complete the audit report.

Seminar Content

- **Fundamentals of Information Security Management Systems (ISMS)**
 - Information Security
 - What is an Information Security Management System (ISMS)
 - The ISO/IEC 270000 Fundamentals and Vocabulary
 - The ISO/IEC 270001 ISMS Described
- **ISO/IEC 27001:2013 Requirements Descriptions**
 - ISO/IEC 27001:2013 Clauses
 - Annex A
 - The Process Approach
- **Risk-based Thinking**
 - ISMS Risks
 - ISMS Risk Assessment
 - ISMS Risk Treatment
- **ISO/IEC 27001 Clause 4 – Context of the Organization**
 - Group Exercise 1: Context of the Organization

Cont'd

Seminar Content

- ISO/IEC 27001 Clause 5 – Leadership
- ISO/IEC 27001 Clause 6 – Planning
- Group Exercise 2: Assessing and Evaluating Risk ISO/IEC 27001 Clause 7 – Support
- ISO/IEC 27001 Clause 8 – Operation
- ISO/IEC 27001 Clause 9 – Performance Evaluation
- ISO/IEC 27001 Clause 10 – Improvement
- ISO/IEC 27001 Annex A
 - Group Exercise 3: Annex A – Required Elements and Risk Treatments

- **Cybersecurity Maturity Model Certification (CMMC)**
 - Description
 - Assessment Criteria and Methodology
- **NIST 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations**
 - NIST 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
 - NIST 800-171A Assessing Security Requirements for Controlled Unclassified Info
 - NIST Handbook 162 NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements
 - What it Consists of
 - Controls
 - How It Was Supposed to be Applied and How It Was Actually Applied
 - Compliance and How It Was Evaluated
- **How CMMC Applies the NIST 800-171 Controls**
 - Certification
 - CMMC Level Control Methods (Level 1 – 5)
 - Group Exercise 4: CMMC Measurement and Analysis
- **Understanding ISMS and CMMC Final Exam**
- **Process Approach to Auditing, Turtle Diagrams and Audit Trails**
- **Audit Guidance, Definitions and Principles**
- **The Audit Program**
- **Audit Planning and Preparation including ISO 27007 Guidelines for Information Security Management Systems Auditing**
 - Breakout Exercise 1: Writing an Objective and Scope Statement
 - Breakout Exercise 2: Documentation Review
 - Breakout Exercise 3: Creating an Audit Plan

- **Performing the Audit**
 - Breakout Exercise 4: Performing an Audit
- **Writing Nonconformity Statements**
 - Breakout Exercise 5: Writing Nonconformity Statements
- **Closing Meeting**
- **Completing the Audit Report**
- **Corrective Action and Close-Out**
- **Management Systems Auditing Final Exam**

Cont'd

Seminar Content

- Leading Audit Teams
- Management System Certification Scheme and Auditor Qualifications
- Leading Management Systems Audit Teams Mock Audit Case Study

DAY
4

-
- Review of Audit Process and Audit Management Strategies
 - Leading Management Systems Audit Teams Final Exam
 - Practical Application of Audit Principles and Instructor Interviews

DAY
5

Functional Safety Core Tools: DFMEAs for Monitoring and System Response

Duration: 2 Days

Seminar Goals

- ◆ Understand the use of the supplemental FMEA for monitoring and response, potential failures which might occur under customer operating conditions are analyzed with respect to their effect on the system or vehicle. How this tool can be used to identify safety risk for ISO 26262
 - ◆ Provide a hands-on approach to the DFMEA with MSR process and their relationship to ISO 26262 deliverables
- Review example applied to ISO 26262

Seminar Content

- Chapter 1: APQP and ISO 26262
 - Chapter 2: MSR FMEA in ISO 26262
 - Chapter 3: Introduction to FMEA for Monitoring and Response (FMEA-MSR)
 - Chapter 4: Review of the AIAG-VDA Handbook
 - Chapter 5: FMEA-MSR Preparation
 - Breakout Exercise 1: Boundary Diagram
 - Breakout Exercise 2: Structure Diagram
-
- Chapter 6: Developing the FMEA-MSR
 - Breakout Exercise 3: Function Analysis
 - Breakout Exercise 4: Failure Analysis
 - Breakout Exercise 5: Risk Analysis
 - Breakout Exercise 6: Optimization
 - Chapter 7: Communicating the Risk
 - Case study review

Reverse Failure Mode and Effect Analysis – RFMEA

Duration: 2 Days

Seminar Goals

- ◆ Explain the difference between DFMEA and RFMEA
 - o Demonstrate an ability to properly construct a RFMEA check-sheet
- ◆ Demonstrate an ability to properly and effectively complete all items in the RFMEA process
 - o Identify high risk areas, evaluate and test control plan gaging and measurement.
- ◆ Demonstrate how to use the output from a RFMEA to identify additional risk and work it back into the PFMEA
- ◆ Identify special characteristics in product design and assure that the control methods are effective.

Seminar Content

- Intro to FMEA
 - APQP and FMEA
 - Development of a good conventional PFMEA
 - VDA PFMEA 7 Step Process
 - Intro to Reverse - FMEA
 - 7 Step Reverse Process
 - Assemble Malfunction team
 - Review of PFMEA, develop plan
-
- Development of Reverse FMEA check-sheet
 - Go and See- Evaluate process using check-sheet
 - Evaluate detection method through testing
 - Re-access risk
 - Develop action plan
 - Reporting Results to Customer
 - Continuous improvement- Updating Baselines and Requirements
-
- Work on in-plant example

Automotive SPICE® Series

Mechanical Engineering Plug-In for Automotive SPICE®

Understanding Automotive SPICE® and Integration with ISO 26262 and IATF 16949

Internal Quality Assurance Practitioners of Automotive SPICE®

Creating Test Cases for Automotive Software

Intacs™ Certified Provisional Assessor

Conducting Automotive SPICE® Assessments

Writing Effective Requirements and Test Cases for Automotive Software Performance Improvement and Capability Determination (Automotive SPICE®) and HWE PRM/PAM

Mechanical Engineering Plug-In for Automotive SPICE®

Duration: 2 Days

Seminar Goals

- ◆ Become aware of the importance of implementing mechanical engineering PAM SPICE
- ◆ Explain the main concepts of Automotive SPICE®
- ◆ Understand the Mechanical Engineering Plug-In Concept in Automotive SPICE®
- ◆ Assess the mechanical engineering processes of a typical automotive project

Seminar Content

- Review of Automotive SPICE® VDA Scope
- System & HW Requirements, PAM Performance Indicators and the SYS.2 Process
- Breakout 1
- Mechanical System Engineering Process Group (MSE)
 - MSE.1 – Mechanical System Engineering Analysis
 - MSE.2 - Mechanical System Architectural Design
 - MSE.3 - Mechanical System Integration and Integration Test
 - MSE.4 - Mechanical System Qualification Test
- Breakout 2

DAY 1

- Mechanical Component Engineering Process Group (MSE)
 - MSE.1 – Mechanical Component Requirement Analysis
 - MSE.2 - Mechanical Component Design
 - MSE.3 - Mechanical Component Sample Production
 - MSE.4 – Test Against Mechanical Component Design
 - MSE.4 - Test Against Mechanical Component Requirements
- Breakout 3
- Generic Practices (GP) and Process Attributes (PAs)
- Breakout 4
- Complementary Supporting Processes (MAN.3)
- Summary

DAY 2

Understanding Automotive SPICE® including Integration with ISO 26262 and IATF 16949

Duration: 3 Days

Seminar Goals

- ◆ Detailed understanding of what Automotive SPICE® is and the motivation behind the model
- ◆ Detailed understanding of process capability level 1 (HIS-Scope)
- ◆ Detailed understanding of traceability requirements
- ◆ Understanding of how to evaluate process risks and drive process improvements
- ◆ Understanding of how Automotive SPICE® integrates with other standards (ISO 26262 and IATF 16949)

Seminar Content

- Introduction and Overview
- What is Automotive SPICE®?
- Process Overview and HIS-Scope
- Process Structure
 - Breakout Exercise – Project Management (MAN 3)
- Capability Dimension and Comparison of Levels 1, 2 and 3
- Understanding Requirements (SYS 2, SW 1)
- Breakout Exercise – Requirements

DAY 1

- Architecture, Design and Implementation (SYS 3, SW 2, SW 3)
 - Breakout Exercise – Testing (SW 4, SW 5, SW 6, SYS 4, SYS 5)
- Automotive SPICE® Traceability Requirements
- Supporting Processes (SUP 8, SUP 9, SUP 10)
 - Breakout Exercise – Quality Assurance (SUP 1)

DAY 2

- Breakout Exercise – Scenario Evaluation
- Integration of Automotive SPICE® with ISO 26262
- Integration of Automotive SPICE® with IATF 16949
 - Breakout Exercise – Scenario Evaluation
- Automotive SPICE® Final Exam

DAY 3

Internal Quality Assurance Practitioners of Automotive SPICE®

Duration: 5 Days

Seminar Goals

- ◆ Detailed understanding of what Automotive SPICE® PAM 3.0 is and the motivation behind the model
- ◆ Detailed understanding of process capability levels 1 (HIS-Scope), 2 and 3
- ◆ Detailed understanding of traceability requirements according to Automotive SPICE®
- ◆ Understanding of how to evaluate process risks and drive process improvements
- ◆ Understanding of how Automotive SPICE® integrates with other standards (ISO 26262 and IATF 16949)
- ◆ Sufficient knowledge and understanding of the assessment process according to Automotive SPICE®
- ◆ Detailed understanding of how to perform internal and/or second party assessments
- ◆ Understanding of how to rate and determine the capability level

Seminar Content

- Introduction to Automotive SPICE®: Definition, History, Structure, Key Concepts DAY 1
 - Breakout Exercise – Project Management (MAN.3)
- Understanding Automotive SPICE® Requirements (SYS.2, SW.1)
 - Breakout Exercise – Requirements (SYS.2, SW.1)
- Understanding Architectural, Design, Implementation, and Testing (SYS.3, SW.2, SW.3) DAY 2
 - Breakout Exercise – Testing (SW.4, SW.5, SW.6, SYS.4, SYS.5)
- Supporting Processes and Supplier Monitoring (SUP.8, SUP.9, SUP.10, ACQ.4)
 - Breakout Exercise – Quality Assurance (SUP.1)
- Understanding Capability Levels 2 and 3 DAY 3
 - Breakout Exercise – Evaluation of PA 2.1 and 2.2
 - Breakout Exercise – Evaluation of PA 3.1 and 3.2
- Integration of Automotive SPICE® with ISO 26262 and IATF 16949
 - Breakout Exercise – Mapping HIS Automotive SPICE® Processes to IATF 16949 Clauses
 - Breakout Exercise – Mapping Automotive SPICE® to ISO 26262
 - Breakout Exercise – Scenario Evaluation (SUP.9)
- Automotive SPICE® Final Exam
- Introduction to Assessment Programs DAY 4
 - Assessment Planning and Preparation
 - Breakout Exercise – Creating Assessment Plan and Schedule
 - Performing the Assessment
 - Audit Findings and Nonconformity Statements
 - Reporting the Assessment Results
- Assessment Follow-up DAY 5
 - Breakout Exercise – Performing Automotive SPICE® Assessment

Creating Test Cases for Automotive Software

Duration: 2 Days

Seminar Goals

- ◆ Detailed understanding of what Automotive SPICE® is and the motivation behind the model
- ◆ Detailed understanding of process capability level 1 (HIS-Scope)
- ◆ Detailed understanding of traceability requirements
- ◆ Understanding of how to evaluate process risks and drive process improvements
- ◆ Understanding of how Automotive SPICE® integrates with other standards (ISO 26262 and IATF 16949)

Seminar Content

- Introduction to Software Testing Models
 - o V Models
 - o Agile
 - o Other
- Failure Mode Effects Analysis (FMEA) and Testing (Preventive and Detective)
 - o Understanding FMEA for Software
 - o Relationship of FMEA to Test Requirements
 - o Breakout Exercise – Developing Test Protocols using DFMEA
 - o Requirements of Automotive SPICE® and ISO 26262 for Testing
 - o Building Good Software Test Cases
 - o Breakout Exercise – Critiquing Good and Bad Test Cases
 - o Documentation of Test Cases and Traceability Requirements
 - o Breakout Exercise – Building Test Cases

Intacs™ Certified Provisional Assessor

Duration: 5 Days

Seminar Goals

- ✦ Provide fundamental understanding of the Automotive SPICE® process improvement and assessment model
- ✦ Be able to conduct process assessments according to Automotive SPICE®
- ✦ Gain initial exposure to the planning, running and documentation of assessments
- ✦ Gain certification as an intacs™-certified Provisional Assessor

Seminar Content

- What is intacs™ - Goals and Objectives
- Overview and Motivation
 - Understanding the Levels of Abstraction of “Process”
 - Understanding the Capability Levels
 - Understanding of a Process Assessment
 - Process Improvement Success Statistics
 - Basic Understanding of ISO/IEC 30xxx and ISO/IEC 15504
- PAM Details – Capability Levels 2 and 3
 - Capability Levels and Process Attributes
 - Generic Practices for Capability Level 2
 - Generic Practices for Capability Level 3
 - Interdependencies Between Pas and Processes at Capability Level 1
- PAM Details – Capability Level 1
 - Engineering Processes: Systems Engineering SYS.1 – SYS.3
- Assessment Skills and Techniques
 - Techniques for Work Product Reviews
 - Interviewing Techniques
 - Listening Techniques
 - Notetaking Techniques
- Rating Guidelines
 - General Guidelines
 - Dependencies Between Process and PAs
- Assessment Process Overview
 - General Information
 - Assessment Process Elements
 - intacs™ Assessment Log Template

DAY 4

- Introduction to Assessment Programs
- Assessment Planning and Preparation
 - Breakout Exercise – Creating Assessment Plan and Schedule
- Performing the Assessment
- Audit Findings and Nonconformity Statements
- Reporting the Assessment Results

DAY 5

- Assessment Follow-up
 - Breakout Exercise – Performing Automotive SPICE® Assessment

Conducting Automotive SPICE® Assessments

Duration: 5 Days

Seminar Goals

- ✦ Detailed understanding of what Automotive SPICE® PAM 3.0 is and the motivation behind the model
- ✦ Detailed understanding of process capability levels 1 (His-Scope), 2 and 3
- ✦ Detailed understanding of traceability requirements according to Automotive SPICE®
- ✦ Understanding of how to evaluate process risks and drive process improvements
- ✦ Understanding of how Automotive SPICE® integrates with other standards (ISO 26262 and IATF 16949)
- ✦ Sufficient knowledge and understanding of the assessment process according to Automotive SPICE®
- ✦ Detailed understanding of how to perform internal and/or second party assessments
- ✦ Understanding of how to rate and determine the capability level

Seminar Content

- Introduction to Automotive SPICE®: Definition, History, Structure, Key Concepts
 - Breakout Exercise – Project Management (MAN.3)
- Understanding Automotive SPICE® Requirements (SYS.2, SW.1)
 - Breakout Exercise – Requirements (SYS.2, SW.1)

DAY 1

- Understanding Architectural, Design, Implementation, and Testing (SYS.3, SW.2, SW.3)
 - Breakout Exercise – Testing (SW.4, SW.5, SW.6, SYS.4, SYS.5)
- Supporting Processes and Supplier Monitoring (SUP.8, SUP.9, SUP.10, ACQ.4)
 - Breakout Exercise – Quality Assurance (SUP.1)

DAY 2

- Understanding Capability Levels 2 and 3
 - Breakout Exercise – Evaluation of PA 2.1 and 2.2
 - Breakout Exercise – Evaluation of PA 3.1 and 3.2
- Integration of Automotive SPICE® with ISO 26262 and IATF 16949
 - Breakout Exercise – Mapping HIS Automotive SPICE® Processes to IATF 16949 Clauses
 - Breakout Exercise – Mapping Automotive SPICE® to ISO 26262
 - Breakout Exercise – Scenario Evaluation (SUP.9)
- Automotive SPICE® Final Exam

DAY 3

- Introduction to Assessment Programs
- Assessment Planning and Preparation
 - Breakout Exercise – Creating Assessment Plan and Schedule
- Performing the Assessment
- Audit Findings and Nonconformity Statements
- Reporting the Assessment Results

DAY 4

- Assessment Follow-up
 - Breakout Exercise – Performing Automotive SPICE® Assessment

DAY 5

Writing Effective Requirements and Test Cases for Automotive Software Performance Improvement and Capability Determination (Automotive SPICE®) and HWE PRM/PAM

Duration: 3 Days

Seminar Goals

- ◆ Detailed understanding of what Automotive SPICE® is and the motivation behind the model
- ◆ Detailed understanding of process capability level 1 (VDA-Scope)
- ◆ Detailed understanding of traceability requirements
- ◆ Detailed understanding of creating requirements for software and its elements at various levels
- ◆ Understanding of how to evaluate process risks and drive process improvements

Seminar Content

- Chapter 1: Introduction and Overview DAY 1
 - Definition
 - History
 - Structure
 - Key Concepts
- Chapter 2: Understanding System/Software Requirements
 - Defining Requirements
 - Types of Requirements
 - Notation for Requirements
 - Requirements Elicitation
 - Breakout Exercise 1: Introduction of Case Study System Requirements (SYS.2)
 - Breakout Exercise 2: SWE Requirements (SWE.1)
- Chapter 3: Architectural Design
 - Notation for System Architecture
 - Notation for Software Architecture
 - Breakout Exercise 3: Develop the Software Architecture using Block Diagram, Timing Chart, and Allocation Matrix for Architectural (SWE.2)Chapter 3: Architectural Design
- Chapter 1: Introduction and Overview
- Chapter 4: Developing Software Detailed Design, Unit Construction, and Software Unit Verification DAY 2
 - Develop Software Detailed Design
 - Coding Style
 - Coding Rules
 - Breakout Exercise 4: Deriving Software Detailed Design and Unit Construction (SWE.3)
 - Breakout Exercise 5: Software Unit Verification (SWE.4)
 - Unit Testing
- Chapter 5: Conducting Software Integration and Integration Testing, and Software Qualification Test
 - Test Case Development
 - Test Methods
 - Breakout Exercise 6: Integration Testing (SWE.5)
 - Breakout Exercise 7: Conducting Software Qualification Testing (SWE.6)
- Chapter 7: Developing Hardware Requirements DAY 3
 - Defining HW Requirements
 - HW Design
 - Breakout Exercise 8 – Hardware Requirements Analysis
 - Test Methods
- Chapter 8: Creating the V-Model using DFMEA and DVP&R

Understanding PRM/PAM Hardware Engineering Processes and Integration with Automotive SPICE®

Duration: 2 Days

Seminar Goals

- ◆ Detailed understanding of what PRM/PAM Hardware Engineering Processes are and the motivation behind the model
- ◆ Detailed understanding of traceability requirements
- ◆ Understanding of how to evaluate process risks and drive process improvements
- ◆ Understanding of how to integrate with Automotive SPICE®

Seminar Content

Introduction and Overview DAY 1

- What is PRM/PAM Hardware Engineering Processes
- Process Overview, Automotive SPICE® and VDA-Scope
- Process Structure, plug-in and other key concepts
- System Requirements and Architecture
 - Breakout Exercise
- Hardware requirements and design
 - Breakout Exercise

- Verification against Hardware Design DAY 2
- Verification against Hardware Requirements
 - Breakout Exercise
- System integration and qualification testing
 - Breakout Exercise
- Supporting Processes (From Automotive SPICE® VDA scope)
 - MAN.3 (Project Management)
 - SUP 8, (Configuration management)
 - SUP 9, (Problem resolution management)
 - SUP 10, (Change management)
 - SUP.1 (Quality Assurance)
 - Breakout Exercise
- PRM/PAM Hardware Engineering Processes Final Exam

ISO 26262 v Series

ISO 26262:2018 Functional Safety Executive Overview

ISO 26262:2018 Overview for Functional Safety Engineers

ISO 26262:2018 Overview for Project Managers

ISO 26262:2018 Automotive Functional Safety Certification

ISO 26262:2018 Functional Safety Certification for Trucks and Buses

ISO 26262:2018 Functional Safety Certification for Motorcycles

ISO 26262:2018 Program Manager/Functional Safety Manager
Certification Level I

ISO 26262:2018 Functional Safety Auditing and Assessment

Preparing a Safety Case for ISO 26262:2018

Writing Effective Requirements, Test Cases and Hardware/Software
Interface (HIS) for Automotive SPICE®

Functional Safety Level 2 Certification (Engineers)

ISO 26262:2018 Program Manager/Functional Safety Manager
Certification Level II

ISO 26262:2018 Product Development at the Hardware Level in
Semiconductors Certification

Functional Safety Core Tools: DFMEA and Diagnostic Analysis Overview

Functional Safety Core Tools: DFMEAs for Monitoring and System Response

Functional Safety Core Tools: Fault Tree Analysis

Functional Safety Core Tools: Hazard Analysis and Risk Assessment

Software DFMEA ISO 26262:2018 Functional Safety Core Tools

Assessments, Audits, and Confirmation Measures For
ISO 26262:2018 Functional Safety Management Systems Standards

ISO 26262:2018 Functional Safety Executive Overview

Duration: 1 Day

Seminar Goals

- Identify the purpose and scope of ISO 26262
- Describe the framework of the ISO 26262 standard
 - Enumerate the 12 parts of the standard
 - Identify the influences and drivers of the standard
- Be able to interpret ISO 26262 ASIL tables
- Understand key aspects of functional safety management
- Identify the requirements for the organization after the release of the design to serial production
- Describe the impact of ISO 26262 on production and operational activities
- Enumerate the requirements of ISO 26262 which support the design and development activities for functional safety
- Describe the requirements for distributed development
- Organize the development of a SEooC consistent with ISO 26262
- Describe the item definition and initiate the safety lifecycle
- Understand the development of the hazard analysis and risk assessment and the related safety goals and functional safety concept

Seminar Outline

- Introduction and Overview to ISO 26262
 - Purpose and Scope
 - ASIL Driven Activities
- Management of Functional Safety (Part 2)
 - Overall Safety Management
 - Project Dependent Safety Management
 - Safety Case
 - Confirmation Measures
 - Safety Management regarding Production, Operation, Service and Decommissioning
- ISO 26262 Part 7 – Production and Operation
 - Overview of Production and Operation Phase
- Safety Element out of Context (Part 10 – Informative)
- ISO 26262 Part 3 – Concept Phase
 - Item Definition
 - Hazard Analysis and Assessment
 - Functional Safety Concept
- System Level Development (Part 4)
 - Technical Safety Concept
- The Need for Functional Safety and Getting Started

ISO 26262:2018 Overview for Functional Safety Engineers

Duration: 2 Days

Seminar Goals

- Tailor the necessary activities to support automotive safety lifecycle management, development, production, operation, service and decommissioning
- Understand the integration of ISO 26262 with APQP and IATF 16949
- Understand functional safety aspects of the entire development process (requirements specification, design, implementation, integration, verification, validation and configuration)
- Understand the automotive-specific risk-based approach for determining risk classes Automotive Safety Integrity Levels (ASILs)
- Use ASILs for specifying the necessary safety requirements for achieving an acceptable residual risk
- Provide requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety is being achieved

Seminar Outline

- Chapter 1: Introduction and Overview to ISO 26262
- ISO 26262 Purpose, Scope and Framework
- Chapter 2: Management of Functional Safety (Part 2)
- Safety Culture • Project Dependent Safety Management
- Safety Case • Breakout Exercise 1: Safety Case Outline
- Confirmation Measures
- Chapter 3: Production and Operation (Part 7)
- Chapter 4: Safety Element out of Context (Part 10)
- Chapter 5: Concept Phase (Part 3)
- Item Definition
- Breakout Exercise 2: Item Definition

DAY 1

- Chapter 5: Concept Phase (Part 3) (cont'd)
- Hazard Analysis and Risk Assessment (HARA)
- Severity, Exposure and Controllability
- Safety Goals
- Breakout Exercise 3: HARA
- Functional Safety Requirements
- Breakout Exercise 4: Functional Safety Requirements
- Chapter 6: ASIL-Oriented and Safety-Oriented Analyses (Part 9)
- Example Scenario
- Safety Analyses in ISO 26262
- Chapter 7: System Level Development I (Part 4)
- Technical Safety Concept
- Hardware-Software Interface (HSI)

DAY 2

ISO 26262:2018 Overview for Project Managers

Duration: 2 Days

Seminar Goals

- ✦ Tailor the necessary activities to support automotive safety lifecycle management, development, production, operation, service and decommissioning
- ✦ Understand the integration of ISO 26262 with APQP and IATF 16949
- ✦ Understand functional safety aspects of the entire development process (requirements specification, design, implementation, integration, verification, validation and configuration)
- ✦ Understand the automotive-specific risk-based approach for determining risk classes Automotive Safety Integrity Levels (ASILs)
- ✦ Use ASILs for specifying the necessary safety requirements for achieving an acceptable residual risk
- ✦ Provide requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety is being achieved

Seminar Content

- DAY 1**
- Chapter 1: Introduction and Overview to ISO 26262
 - ISO 26262 Purpose, Scope and Framework
 - Chapter 2: Management of Functional Safety (Part 2)
 - Safety Culture
 - Project Dependent Safety Management
 - Safety Plan
 - Safety Case
 - Breakout Exercise 1: Safety Case Outline
 - Confirmation Measures
 - Chapter 3: Production and Operation (Part 7)
 - Chapter 4: Safety Element out of Context (Part 10)
 - Chapter 5: Concept Phase (Part 3)
 - Item Definition
 - Breakout Exercise 2: Item Definition

- DAY 2**
- Chapter 5: Concept Phase (Part 3)
 - Hazard Analysis and Risk Assessment (HARA)
 - Severity, Exposure and Controllability
 - Safety Goals
 - Breakout Exercise 3: HARA
 - Functional Safety Requirements
 - Breakout Exercise 4: Functional Safety Requirements
 - Chapter 6: ASIL-Oriented and Safety-Oriented Analyses (Part 9)
 - Example Scenario
 - Safety Analyses in ISO 26262
 - Chapter 7: System Level Development I (Part 4)
 - Technical Safety Concept
 - Hardware-Software Interface (HSI)

Automotive Functional Safety ISO 26262:2018 Certification

Duration: 5 Days

Seminar Goals

- ✦ Tailor the necessary activities to support automotive safety lifecycle management, development, production, operation, service, and decommissioning
- ✦ Information provided in the class can be used for ISO 26262 implementation
- ✦ Understand functional safety aspects of the entire development process including requirements specification, design, implementation, integration, verification, validation, and configuration.
- ✦ Understand the risk-based approach for determining risk classes Automotive Safety Integrity Levels (ASILs)
- ✦ Use ASILs for achieving an acceptable residual risk
- ✦ Provide requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety is being achieved

Seminar Content

- DAY 1**
- Chapter 1: Introduction and Overview to ISO 26262
 - Chapter 2: Management of Functional Safety (Part 2)
 - Chapter 3: Production and Operation (Part 7)
 - Chapter 4: Safety Element out of Context (Part 10)
 - Chapter 5: Concept Phase (Part 3)

- DAY 2**
- Chapter 5: Concept Phase (Part 3)
 - Chapter 6: ASIL-Oriented and Safety-Oriented Analyses (Part 9)
 - Chapter 7: System Level Development I (Part 4)

- DAY 3**
- Chapter 8: Hardware Level Development I (Part 5)
 - Chapter 9: Evaluation of Hardware Elements (Part 8)
 - Chapter 10: Hardware Level Development II (Part 5 revisited)
 - Chapter 11: Software Level Development (Part 6)

- DAY 4**
- Chapter 11: Software Level Development (Part 6) (*continued*)
 - Chapter 12: System Level Development II (Part 4 revisited)
 - Chapter 13: Supporting Processes (Part 8)

- DAY 5**
- Chapter 13: Supporting Processes (Part 8)
 - Chapter 14: Guideline on Application of ISO 26262 to Semiconductors (Part 11)
 - Chapter 15: Adaption of ISO 26262 to Motorcycles (Part 12)
 - Chapter 16: ISO 26262 Implementation Strategy

Optional ISO 26262 Certification Exam – Final 3 hours of Day

ISO 26262:2018 Automotive Functional Safety Certification with Truck & Bus Focus

Duration: 5 Days

Seminar Goals

- ◆ Tailor the necessary activities to support vehicle safety lifecycle management, development, production, operation, service, and decommissioning
- ◆ Information provided in the class can be used for ISO 26262 implementation
- ◆ Understand functional safety aspects of the entire development process including requirements specification, design, implementation, integration, verification, validation, and configuration.
- ◆ Understand the risk-based approach for determining risk classes Automotive Safety Integrity Levels (ASILs)
- ◆ Use ASILs for achieving an acceptable residual risk
- ◆ Provide requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety is being achieved

Seminar Content

- Chapter 1: Introduction and Overview to ISO 26262
- Chapter 2: Management of Functional Safety (Part 2)
- Chapter 3: Production and Operation (Part 7)
- Chapter 4: Safety Element out of Context (Part 10)
- Chapter 5: Concept Phase (Part 3)

DAY 1

- Chapter 5: Concept Phase (Part 3)
- Chapter 6: ASIL-Oriented and Safety-Oriented Analyses (Part 9)

DAY 2

- Chapter 7: System Level Development I (Part 4)
- Chapter 8: Hardware Level Development I (Part 5)
- Chapter 9: Evaluation of Hardware Elements (Part 8)
- Chapter 10: Hardware Level Development II (Part 5 revisited)

DAY 3

- Chapter 11: Software Level Development (Part 6)
- Chapter 12: System Level Development II (Part 4 revisited)

DAY 4

- Chapter 13: Supporting Processes (Part 8)
- Chapter 14: Guideline on Application of ISO 26262 to Semiconductors (Part 11)
- Chapter 15: Adaption of ISO 26262 to Motorcycles (Part 12)
- Chapter 16: ISO 26262 Implementation Strategy

DAY 5

Optional ISO 26262 Certification Exam – Final 3 hours of Day

ISO 26262:2018 Automotive Functional Safety Certification with Motorcycle Focus

Duration: 5 Days

Seminar Goals

- ◆ Tailor the necessary activities to support automotive safety lifecycle management, development, production, operation, service, and decommissioning
- ◆ Information provided in the class can be used for ISO 26262 implementation
- ◆ Understand functional safety aspects of the entire development process including requirements specification, design, implementation, integration, verification, validation, and configuration.
- ◆ Understand the risk-based approach for determining risk classes Automotive and Motorcycle Safety Integrity Levels (ASILs and MSILs)
- ◆ Use ASILs for achieving an acceptable residual risk
- ◆ Provide requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety is being achieved

Seminar Content

- Chapter 1: Introduction and Overview to ISO 26262
- Chapter 2: Management of Functional Safety (Part 2)
- Chapter 3: Production and Operation (Part 7)
- Chapter 4: Safety Element out of Context (Part 10)

DAY 1

- Chapter 5: Concept Phase (Part 3)

DAY 2

- Chapter 6: ASIL-Oriented and Safety-Oriented Analyses (Part 9)
- Chapter 7: System Level Development I (Part 4)
- Chapter 8: Hardware Level Development I (Part 5)
- Chapter 9: Evaluation of Hardware Elements (Part 8)
- Chapter 10: Hardware Level Development II (Part 5 revisited)

DAY 3

- Chapter 11: Software Level Development (Part 6)
- Chapter 12: System Level Development II (Part 4 revisited)

DAY 4

- Chapter 13: Supporting Processes (Part 8)
- Chapter 14: Guideline on Application of ISO 26262 to Semiconductors (Part 11)
- Chapter 15: Adaption of ISO 26262 to Motorcycles (Part 12)
- Chapter 16: ISO 26262 Implementation Strategy

DAY 5

Optional ISO 26262 Certification Exam – Final 3 hours of Day

ISO 26262:2018 Program Manager / Functional Safety Manager Certification Level I

Duration: 5 Days

Seminar Goals

- ◆ Tailor the necessary activities to support automotive safety lifecycle management, development, production, operation, service, and decommissioning
- ◆ Information provided in the class can be used for ISO 26262 implementation
- ◆ Understand functional safety aspects of the entire development process including requirements specification, design, implementation, integration, verification, validation, and configuration.
- ◆ Understand the risk-based approach for determining risk classes Automotive Safety Integrity Levels (ASILs)
- ◆ Use ASILs for achieving an acceptable residual risk
- ◆ Provide requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety is being achieved

Seminar Content

- Chapter 1: Introduction and Overview to ISO 26262
- Chapter 2: Management of Functional Safety (Part 2)
- Chapter 3: Production and Operation (Part 7)
- Chapter 4: Safety Element out of Context (Part 10)
- Chapter 5: Concept Phase (Part 3)

DAY 1

- Chapter 5: Concept Phase (Part 3)
- Chapter 6: ASIL-Oriented and Safety-Oriented Analyses (Part 9)
- Chapter 7: System Level Development I (Part 4)

DAY 2

- Chapter 8: Hardware Level Development I (Part 5)
- Chapter 9: Evaluation of Hardware Elements (Part 8)
- Chapter 10: Hardware Level Development II (Part 5 revisited)
- Chapter 11: Software Level Development (Part 6)

DAY 3

- Chapter 11: Software Level Development (Part 6)
- Chapter 12: System Level Development II (Part 4 revisited)
- Chapter 13: Supporting Processes (Part 8)

DAY 4

- Chapter 13: Supporting Processes (Part 8)
- Chapter 14: Guideline on Application of ISO 26262 to Semiconductors (Part 11)
- Chapter 15: Adaption of ISO 26262 to Motorcycles (Part 12)
- Chapter 16: ISO 26262 Implementation Strategy

DAY 5

Optional ISO 26262 Certification Exam – Final 3 hours of Day

ISO 26262:2018 Functional Safety Auditing and Assessment

Duration: 5 Days

Seminar Goals

- ◆ Identify key definitions, ideas and principles of ISO 26262
- ◆ Assess HARA, ASIL, Safety Goals, Safety Plan and Safety Requirements
- ◆ Evaluate a Safety Plan and Safety Case
- ◆ Evaluate a confirmation measures program
- ◆ Evaluate Functional Safety Concept (FSC) and a related Technical Safety Concept (TSC)
- ◆ Evaluate associated test plans against ASIL using the correct tables
- ◆ Evaluate Control Measures in manufacturing
- ◆ Evaluate a Distributed Interface Agreement (DIA)
- ◆ Evaluate a Software and Hardware product qualification
- ◆ Evaluate a Decomposition and Independence
- ◆ Evaluate Safety Evaluations – DFMEA and Fault Tree Analysis (FTA)
- ◆ Evaluate Safety Metrics in Hardware and Software

Seminar Content

- Chapter 1: Introduction and Overview to ISO 26262
- Explaining the V Cycle
- Interdependency Between System, Hardware and Software
- Chapter 2: Setting up the Project and Associated Safety Plan
- Impact at the Item and Element Levels
- Safety Element out of Context (SEoC)
- Breakout Exercise 1: Evaluate a Safety Plan
- Chapter 3: What are Safety Goals, FSR, FSC, TSR, TSC, HW and SW SRs?
- Relationship With and Among Safety Architecture
- Breakout Exercise 2: Evaluate Flow Down of Requirements
- Chapter 4: Achieving Safety Goals, FSR, FSC, TSR, TSC, HW and SW SRs
- Safety Strategies, Measures and Mechanisms (Diagnostics)
- Breakout Exercise 3: Evaluate Functional Safety Implementation
- Chapter 5: Decomposition and Dependent Failure Analysis
- Breakout Exercise 4: Evaluate Validity of a Decomposition
- Chapter 6: Verifying FSR, FSC, TSR, TSC, HW and SW SRs to Specifications (Test Plans)
- Breakout Exercise 5: Evaluate Test Plan for HW Part, Unit SW, Item Integration
- Chapter 7: Safety Analysis including Safety Evaluations and Metrics
- Breakout Exercise 6: Evaluate HW DFMEA, SW DFMEA, FMEDA and HW Metrics, SW Metrics, FTA
- Chapter 8: Safety Case and Release to Serial Production
- Breakout Exercise 7: Evaluate Safety Case
- Chapter 9: Control Measures in Manufacturing and in the Field
- Breakout Exercise 8: Evaluate Process Flow and Control Plan Link to ASILs
- Chapter 10: Distributed Interface Agreement
- Chapter 11: Management of Safety Reviews, Audits and Assessments

Preparing a Safety Case for ISO 26262:2018

Duration: 2 Days

Seminar Goals

- ✦ Explain the importance of the safety argumentation
- ✦ Understanding and developing each building block of a Safety Case
- ✦ Product and process argumentation
- ✦ Nominal performance of functionality safety (SOTIF)
- ✦ Implementation safety
- ✦ Development effort safety
- ✦ Supporting argumentation safety
- ✦ Supplier Safety Case

Seminar Content

- Requirements of a Safety Case
- Breakout Exercise 1: Reviewing a Safety Case and Identify potential Improvements
- Safety Case Argumentation
- Planning for the Development of the Safety Case and Documentation – Documentation Plan
- Confirmation Reviews and Safety Case Development
- Overview of the GSN Approach
- Introduction of a running case study for an Air Bag Safety Case – Walkthrough of Air Bag Safety Goal development through Functional Safety Concept
- Breakout Exercise 2: Develop a Table of Contents for Each Safety Case – Product and Process Argument

DAY 1

- Overview of Argument Structures to Develop Safety Arguments
- Use of Argument Structures for Specific Items
- Evaluating a Safety Case
- Evaluating Supplier Product Safety including Distributed Interface Agreement (DIA)
- Breakout Exercise 3: Develop a Safety Case Argumentation for Product Argument
- Breakout Exercise 4: Develop a Safety Case Argumentation for Process Argument
- Summary

DAY 2

Writing Effective Requirements, Test Cases and Hardware/Software Interface (HIS) for Automotive SPICE®

Duration: 2 Days

Seminar Goals

- ✦ Detailed understanding of what Automotive SPICE® is and the motivation behind the model
- ✦ Detailed understanding of process capability level 1 (VDA-Scope)
- ✦ Detailed understanding of traceability requirements
- ✦ Understanding of how to evaluate process risks and drive process improvements
- ✦ Understanding of how Automotive SPICE® integrates with other standards (ISO 26262 and IATF 16949)

Seminar Content

- Introduction and Overview
- What is Automotive SPICE®?
- Process Overview and VDA-Scope
- Introduction to Software Testing Models
 - o V Models
 - o Agile
 - o Other
- Understanding Requirements (SYS 2, SW 1)
 - o Breakout Exercise – Requirements
- Breakout Exercise – Testing (SW 4, SW 5, SW 6, SYS 4, SYS 5)
- Failure Mode Effects Analysis (FMEA) and Testing (Preventive and Detective)
 - o Understanding FMEA for Software
 - o Relationship of FMEA to Test Requirements
 - o Breakout Exercise – Developing Test Protocols using DFMEA
 - o Requirements of Automotive SPICE® and ISO 26262 for Testing
 - o Building Good Software Test Cases
 - o Breakout Exercise – Critiquing Good and Bad Test Cases
 - o Documentation of Test Cases and Traceability Requirements
 - o Breakout Exercise – Building Test Cases

ISO 26262:2018 Automotive Functional Safety Engineer Level II Certification

Duration: 5 Days

Seminar Goals

- ◆ Gain a complete understanding of a Safety Case
- ◆ Review of Tailoring – practice deciding on the necessary activities to support vehicle safety lifecycle management, development, production, operation, service and decommissioning
- ◆ Use the information gained and the workshop work products developed in class for ISO 26262 implementation
- ◆ Review functional safety aspects of the entire development process
- ◆ Understand the risk-based approach for determining risk classes ASILs and MSILs

Seminar Outline

- Intro and Review of ISO 26262
 - Safety Case Fundamentals
 - Safety Case Outline/Table of Contents
 - Part 2 Work Products/ASIL Tables
 - Safety Case Index
- DAY 1
-
- Requirements Sources and Organization
 - Parts 3 and 4 Work Products/ASIL Tables
 - FMEA, Fault Tree and Test Plans
- DAY 2
-
- Parts 5 and 6 Work Products/ASIL Tables
 - Hardware Metrics
 - Software Metrics
 - Selected Work Products Sent for Independent Review
- DAY 3
-
- Parts 7 and 8 Work Products/ASIL Tables
 - PFMEA, Control Plans and Capability Studies
 - Selected Work Products Review Results Discussed
- DAY 4
-
- Part 9 through 12
 - MSILs and Conversion to ASILs
 - Safety Argumentation and Design
 - Review of Safety Case and Index
- DAY 5

ISO 26262:2018 Program Manager / Functional Safety Manager Certification Level II

Duration: 5 Days

Seminar Goals

- ◆ Gain a complete understanding of a Safety Case
- ◆ Generating and maintaining Safety Plan
- ◆ Review of Tailoring – practice deciding on the necessary activities to support vehicle safety lifecycle management, development, production, operation, service and decommissioning
- ◆ Use the information gained and the workshop work products developed in class for ISO 26262 implementation
- ◆ Review functional safety aspects of the entire development process
- ◆ Understand the risk-based approach for determining risk classes ASILs and MSILs

Seminar Content

- Intro and Review of ISO 26262
 - Safety Case Fundamentals
 - Safety Case Outline/Table of Contents
 - Part 2 Work Products/ASIL Tables
 - Safety Case Index
- DAY 1
-
- Requirements Sources and Organization
 - Parts 3 and 4 Work Products/ASIL Tables
 - FMEA, Fault Tree and Test Plans
- DAY 2
-
- Parts 5 and 6 Work Products/ASIL Tables
 - Hardware Metrics
 - Software Metrics
 - Selected Work Products Sent for Independent Review
- DAY 3
-
- Parts 7 and 8 Work Products/ASIL Tables
 - PFMEA, Control Plans and Capability Studies
 - Selected Work Products Review Results Discussed
- DAY 4
-
- Part 9 through 12
 - MSILs and Conversion to ASILs
 - Safety Argumentation and Design
 - Review of Safety Case and Index
- DAY 5

ISO 26262:2018 Product Development at the Hardware Level in Semiconductors Certification

Duration: 2 Days

Seminar Goals

- ◆ Understand the Requirements of ISO 26262 Parts 4 and 6 and how they affect Hardware development
- ◆ Describe Hardware Evaluation requirements and Requirements Verification
- ◆ Describe the impact on Semiconductor development
- ◆ Describe the different types of Hardware Metrics
 - Implement the development of Structural Metrics
 - Describe the development of Safety Reliability Metrics
- ◆ Understand the impact of ISO 26262 Parts 4 and 6 on hardware development

Seminar Content

- Introduction and Overview to ISO 26262
- Management of Functional Safety (Part 2)
 - o Three clauses
 - Overall management
 - Project management
 - After Release management
 - o Impact Analysis
 - o Confirmation measures
 - o Breakout: – Safety Case
- Safety Element Out of Context
- Concept Phase (Part 3)
 - o Breakout: – Item Definition
 - o Breakout: – HARA and Safety Goals
- Safety Requirements
 - o Breakout: – Functional Safety Requirements / Concept

DAY 1

- System Level Development I (Part 4) - overview
 - o ASIL and Safety Oriented Analysis
 - o ASIL Decomposition Case Study
 - o Safety Analyses in ISO 26262
 - o HSI development
 - o The V model; Planning for V&V testing
- Hardware Level Development (Part 5)
- Hardware Safety Requirements
 - o How to consider semiconductor components
 - Semiconductor component development
 - o Case Study

DAY 2

Functional Safety Core Tools: DFMEA and Diagnostic Analysis Overview

Duration: 1 Day

Seminar Goals

- ◆ Understand how to develop and use FMEDA to identify and address design malfunctions during the product development of hardware to achieve safety goals

Seminar Content

- Chapter 1: APQP and ISO 26262
- Chapter 2: Introduction to Failure Mode, Effect and Diagnostic Analysis (FMEDA)
- Chapter 3: FMEDA Preparation
- Breakout Exercise 1: Boundary (Schematic) Diagram/Part Identification
- Breakout Exercise 2: Using FIT Tables
- Chapter 4: Developing the FMEDA
- Breakout Exercise 3: Starting the FMEDA
- Breakout Exercise 4: Transfer Information from Part Identification
- Breakout Exercise 5: Component FIT/Design Failure Modes and FM Distribution
- Breakout Exercise 6: SPFM and LFM
- Chapter 5: Results of FMEDA and the Safety Plan

Functional Safety Core Tools: DFMEAs for Monitoring and System Response

Duration: 1 Day

Seminar Goals

- ◆ Understand the use of the supplemental FMEA for monitoring and response, potential failures which might occur under customer operating conditions are analyzed with respect to their effect on the system or vehicle. How this tool can be used to identify safety risk for ISO 26262
- ◆ Provide a hands-on approach to the DFMEA with MSR process and their relationship to ISO 26262 deliverables

Seminar Content

- Chapter 1: APQP and ISO 26262
- Chapter 2: Introduction to FMEA for Monitoring and Response (FMEA-MSR)
- Chapter 3: FMEA-MSR Preparation
- Breakout Exercise 1: Boundary Diagram
- Breakout Exercise 2: Structure Diagram
- Chapter 4: Developing the FMEA-MSR
- Breakout Exercise 3: Function Analysis
- Breakout Exercise 4: Failure Analysis
- Breakout Exercise 5: Risk Analysis
- Breakout Exercise 6: Optimization
- Chapter 5: Communicating the Risk

Functional Safety Core Tools: 2-day DFMEAs for Monitoring and System Response

Duration: 2 Days

Seminar Goals

- ◆ Understand the use of the supplemental FMEA for monitoring and response, potential failures which might occur under customer operating conditions are analyzed with respect to their effect on the system or vehicle. How this tool can be used to identify safety risk for ISO 26262
- ◆ Provide a hands-on approach to the DFMEA with MSR process and their relationship to ISO 26262 deliverables
- ◆ Review example applied to ISO 26262

Seminar Content

- Chapter 1: APQP and ISO 26262
- Chapter 2: MSR FMEA in ISO 26262
- Chapter 3: Introduction to FMEA for Monitoring and Response (FMEA-MSR)
- Chapter 4: Review of the AIAG-VDA Handbook
- Chapter 5: FMEA-MSR Preparation
- Breakout Exercise 1: Boundary Diagram
- Breakout Exercise 2: Structure Diagram

DAY
1

- Chapter 6: Developing the FMEA-MSR
- Breakout Exercise 3: Function Analysis
- Breakout Exercise 4: Failure Analysis
- Breakout Exercise 5: Risk Analysis
- Breakout Exercise 6: Optimization
- Chapter 7: Communicating the Risk
- Case study review

DAY
2

Functional Safety Core Tools: Fault Tree Analysis

Duration: 1 Day

Seminar Goals

- ◆ Be able to perform a fault tree analysis during any phase of the development process
- ◆ Be proficient in fault tree analysis immediately after completing this workshop
- ◆ Study examples of actual fault trees from real-world systems

Seminar Content

- Chapter 1: Introduction to Fault Tree Analysis
- Chapter 2: Pre-work for FTA
- Breakout Exercise 1: Design Scope and Item Diagram
- Breakout Exercise 2: Evaluate Design Based on Quality Goal
- Chapter 3: Developing the Fault Tree Analysis
- Breakout Exercise 3: Constructing FTA Structure
- Breakout Exercise 4: Cut Set of FTA Structure
- Chapter 4: Analyzing FTA Results
- Breakout Exercise 5: Analyzing FTA Results

Functional Safety Core Tools: Hazard Analysis and Risk Assessment

Duration: 1 Day

Seminar Goals

- ◆ Be able to perform a hazard analysis during any phase of the development process
- ◆ Be proficient in hazard analysis immediately after completing this workshop
- ◆ Study examples of real hazard analysis from real systems

Seminar Content

- Chapter 1: Introduction to Hazard Analysis
- Chapter 2: Pre-work for Hazard Analysis
- Breakout Exercise 1: Design Scope and Item Diagram
- Breakout Exercise 2: Assumptions About Vehicle, rider, Passenger, Environmental
- Breakout Exercise 3: Hazard Checklist
- Breakout Exercise 4: Operational Scenarios and Exposure
- Chapter 3: Developing the Hazard Analysis
- Breakout Exercise 5: Hazard Analysis Matrix
- Breakout Exercise 6: Hazard Analysis and Risk Assessment (Severity, Exposure, Controllability and ASIL)
- Chapter 4: Quality Goals
- Breakout Exercise 7: Quality Goals

Assessments, Audits, and Confirmation Measures For ISO 26262:2018 Functional Safety Management Systems Standards

Duration: 5 Days

Seminar Goals

- ◆ Identify key definitions, ideas and principles of ISO 26262
- ◆ Assess HARA, ASIL, Safety Goals, Safety Plan and Safety Requirements
- ◆ Evaluate a Safety Plan and Safety Case
- ◆ Evaluate a confirmation measures program
- ◆ Evaluate Functional Safety Concept (FSC) and a related Technical Safety Concept (TSC)
- ◆ Evaluate associated test plans against ASIL using the correct tables
- ◆ Evaluate Control Measures in manufacturing
- ◆ Evaluate a Distributed Interface Agreement (DIA)
- ◆ Evaluate a Software and Hardware product qualification
- ◆ Evaluate a Decomposition and Independence
- ◆ Evaluate Safety Evaluations – DFMEA and Fault Tree Analysis (FTA)
- ◆ Evaluate Safety Metrics in Hardware and Software

Seminar Content

- Chapter 1: Introduction and Overview to ISO 26262
- Chapter 2: Setting up the Project and Associated Safety Plan
- Chapter 3: What are Safety Goals, FSR, FSC, TSR, TSC, HW and SW SRs?
- Chapter 4: Achieving Safety Goals, FSR, FSC, TSR, TSC, HW and SW SRs
- Chapter 5: Decomposition and Dependent Failure Analysis
- Chapter 6: Safety Analysis including Safety Evaluations and Metrics
- Chapter 7: Verifying FSR, FSC, TSR, TSC, HW and SW SRs to Specifications (Test Plans)
- Chapter 8: Safety Case and Release to Serial Production
- Chapter 9: Control Measures in Manufacturing and in the Field
- Chapter 10: Distributed Interface Agreement
- Chapter 11: Management of Safety Reviews, Audits and Assessments
- Chapter 12: ISO 26262 Confirmation Measures and Supplier Audits/Assessments
- Chapter 13: Audit Guidance, Definitions and Principles
- Chapter 14: The Audit Program
- Chapter 15: Audit Planning and Preparation
- Chapter 16: Performing the Audit
- Chapter 17: Writing Nonconformity Statements
- Chapter 18: Closing Meeting
- Chapter 19: Completing the Audit Report
- Chapter 20: Corrective Action and Close-Out

Assessment of a Safety Case based on SS 7740-2018

Duration: 3 Days

Seminar Goals

- ◆ Detailed understanding of what SS 7740 Functional Safety Process assessment is and the motivation behind the model
- ◆ Applicable information from ISO 26262 and Automotive SPICE®
- ◆ Detailed understanding of traceability requirements
- ◆ Detailed understanding of creating requirements for software and its elements at various levels
- ◆ Understanding of how to evaluate process risks and drive process improvements

Seminar Content

- Chapter 1: Introduction and Overview DAY 1
- Chapter 2: Management Process Group
- Chapter 3: Understanding System/Software Requirements
- Chapter 4: Creating System Architecture
- Chapter 5: Developing Software Detailed Design, Unit Construction, and Software Unit Verification DAY 2
- Chapter 6: Conducting Software Integration and Integration
- Chapter 7: Understanding Acquisition Processes DAY 3
- Chapter 8: Understanding Support Processes
- Chapter 9: SE.MAN.3 Confirmation measures

Software DFMEA ISO 26262:2018 Functional Safety Core Tools

Duration: 1 Day

Seminar Goals

- ◆ Be able to perform a Software FMEA analysis during any phase of the development process
- ◆ Be proficient in Software FMEA immediately after completing this workshop
- ◆ Study examples of Software FMEA from real-world systems

Seminar Content

- Chapter 1: Software Risk Analysis introduction
- Chapter 2: Design Failure Mode and Effects Analysis (DFMEA) Introduction
- Chapter 3: DFMEA Preparation
- Breakout Exercise 1: Boundary (Block) Diagram
- Chapter 4: Developing the DFMEA
- Breakout Exercise 2: Starting the DFMEA
- Breakout Exercise 3: Design Failure Modes
- Breakout Exercise 4: Potential Design Causes
- Breakout Exercise 5: Design Controls
- Breakout Exercise 6: Design Effects & Classification
- Breakout Exercise 7: RPNs and Improvements
- Chapter 5 – Design Verification Plan and Report (DVP&R)
- Chapter 6 – Algorithm FMEAs

Writing Effective Requirements and Test Cases at System, Software and Hardware levels for Functional Safety (ISO 26262) products

Duration: 3 Days

Seminar Goals

- Detailed understanding of what Automotive SPICE® is and the motivation behind the model
- Detailed understanding of process capability level 1 (VDA-Scope)
- Detailed understanding of traceability requirements
- Detailed understanding of creating requirements for software and its elements at various levels
- Understanding of how to evaluate process risks and drive process improvements

Seminar Content

-
- Chapter 1: Introduction and Overview
 - Chapter 2: Understanding System/Software Requirements
 - Chapter 3: Architectural Design

DAY 1

-
- Chapter 4: Developing Software Detailed Design, Unit Construction, and Software Unit Verification
 - Chapter 5: Conducting Software Integration and Integration Testing, and Software Qualification Test

DAY 2

-
- Chapter 7: Developing Hardware Requirements
 - Chapter 8: Creating the V-Model using DFMEA and DVP&R

DAY 3

ISO 26262:2018 Product Development at the Hardware Level Certification

Duration: 5 Days

Seminar Goals

- Tailor the necessary activities to support automotive safety lifecycle management, development, production, operation, service and decommissioning with a focus on hardware development including semiconductors
- Understand the integration of ISO 26262 with APQP and IATF 16949
- Understand functional safety aspects of the entire development process (requirements specification, design, implementation, integration, verification, validation and configuration)
- Understand the automotive-specific risk-based approach for determining risk classes Automotive Safety Integrity Levels (ASILs)
- Use ASILs for specifying the necessary safety requirements for achieving an acceptable residual risk
- Provide requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety is being achieved

Seminar Content

-
- Chapter 1: Introduction and Overview to ISO 26262
 - Chapter 2: Management of Functional Safety (Part 2)
 - Chapter 3: Production and Operation (Part 7)
 - Chapter 4: Safety Element out of Context (Part 10)
 - Chapter 5: Concept Phase (Part 3)

DAY 1

-
- Chapter 6: ASIL-Oriented and Safety-Oriented Analysis
 - Chapter 7: System Level Development (Part 4)
 - Chapter 8: Hardware Level Development (Part 5)

DAY 2

-
- Chapter 9: Evaluation of Hardware Elements (Part 8)
 - Chapter 10: Hardware Level Development (Part 5 continued)
 - Chapter 11: Guidelines on Application of ISO 26262 to Semiconductors (Part 11)

DAY 3

-
- Chapter 12: Software Level Development (Part 6)
 - Chapter 13: System Level Development (Part 4 continued)

DAY 4

-
- Chapter 14: Supporting Processes (Part 8)
 - Chapter 15: ISO 26262 Implementation Strategy

DAY 5

Optional ISO 26262 Certification Exam – Final 3 hours of Day Five

Cybersecurity Series

SAE J3061, ISO/SAE 21434, and Related Standards:
Automotive Cybersecurity Executive Overview

SAE J3061, ISO/SAE 21434, and Related Standards:
Overview for Functional Safety Engineers

SAE J3061 and ISO/SAE 21434 Cybersecurity Engineering Certification

SAE J3061 and ISO/SAE 21434 Automotive Cybersecurity
Auditing and Assessment Certification

SAE J3061 and ISO/SAE 21434 Cybersecurity Threat Analysis and
Risk Assessment (TARA)

SAE J3061 and ISO/SAE 21434 Conducting a Cybersecurity FMEA and
Vulnerability Analysis Testing for Systems, Hardware and Software

ISO 21434:2019 Cybersecurity Engineering Defense & Protection
Against Attacks

Introduction to Autonomous and Electric Vehicles: A Functional Safety,
SOTIF, and Cybersecurity Perspective

Preparing a Cybersecurity Case

Writing Effective Requirements, Test Cases, and H/S Interfaces
for Cybersecurity

SAE J3061 and ISO/SAE 21434 Automotive Cybersecurity Certification

Introduction to Systems Engineering: A Safety and
Cybersecurity Perspective

SAE J3061, ISO/SAE 21434, and Related Standards: Automotive Cybersecurity Executive Overview

Duration: 1 Day

Seminar Goals

- ◆ Identify the purpose and scope of ISO/SAE 21434, ISO/IEC 27001, WP.29, and VDA ACMS
- ◆ Describe the framework of the ISO 21434 standard
 - o Enumerate the 14 parts of the standard
 - o Identify the influences and drivers of the standard
- ◆ Be able to interpret ISO/SAE 21434 CAL tables
- ◆ Understand key aspects of cybersecurity management
- ◆ Identify the requirements for the organization after the release of the design to serial production
- ◆ Describe the impact of ISO/SAE 21434 on production and operational activities
- ◆ Enumerate the requirements of ISO 26262 which support the design and development activities for automotive cybersecurity
- ◆ Describe the requirements for distributed development
- ◆ Organize the development of a CSooC consistent with ISO/SAE 21434
- ◆ Describe the item definition and initiate the safety lifecycle
- ◆ Understand the development of the Threat Analysis and Risk Assessment (TARA) and the related cybersecurity goals including the cybersecurity concept and the refined cybersecurity design

Seminar Content

- Introduction and Overview to SAE J3061, ISO/SAE 21434, ISO/IEC 27001, WP.29, and VDA ACMS
- ISO/SAE 21434 Purpose, Scope and Framework
- Overall Cybersecurity Management (Clause 5)
- Cybersecurity Governance
- Cybersecurity Culture
- Cybersecurity Risk Management
- Cybersecurity Audit
- Information Sharing
- Confirmation Measures
- Project Dependent Cybersecurity Management (Clause 6)
- Tailoring of Cybersecurity Activities
- System or Component out of Context
- Cybersecurity Planning
- Cybersecurity Case
- Post-Development Phases (Clauses 10-13)
- Production, Operation, Maintenance, and Decommissioning
- Concept Phase (Clause 8)
- Cybersecurity Relevance
- Item Definition
- Threat Analysis and Risk Assessment (TARA)
- Cybersecurity Concept
- Product Development (Clause 9.1)
- Introduction to Design & Verification
- Refined Cybersecurity Design
- The Need for Cybersecurity and Getting Started

SAE J3061, ISO/SAE 21434, and Related Standards: Overview for Functional Safety Engineers

Duration: 2 Days

Seminar Goals

- ◆ Tailor the necessary activities to support automotive cybersecurity lifecycle management, development, production, operation, maintenance and decommissioning
- ◆ Understand the integration of ISO/SAE 21434 with ISO 26262, APQP, IATF 16949 and other related standards
- ◆ Understand cybersecurity aspects of the entire development process (requirements specification, design, implementation, integration, verification, validation and validation)
- ◆ Understand the automotive-specific risk-based approach for determining Cybersecurity Assurance Levels (CALs)
- ◆ Use CALs for specifying the necessary cybersecurity requirements for achieving an acceptable residual risk
- ◆ Provide requirements for validation and confirmation measures to ensure a sufficient and acceptable level of cybersecurity is being achieved

Seminar Content

- Introduction and Overview to SAE J3061, ISO/SAE 21434, ISO/IEC 27001, WP.29, and VDA ACMS
- ISO/SAE 21434 Purpose, Scope and Framework
- Overall Cybersecurity Management (Clause 5)
- Cybersecurity Governance
- Cybersecurity Culture
- Cybersecurity Risk Management
- Cybersecurity Audit
- Information Sharing
- Confirmation Measures
- Project Dependent Cybersecurity Management (Clause 6)
- Tailoring of Cybersecurity Activities
- System or Component out of Context
- Cybersecurity Planning
- Cybersecurity Case
- Breakout Exercise 1: Safety Case Outline
- Post-Development Phases (Clauses 10-13)
- Production, Operation, Maintenance, and Decommissioning
- Concept Phase (Clause 8)
- Cybersecurity Relevance
- Item Definition
- Breakout Exercise 2: Item Definition

DAY 1

- Concept Phase (Clause 8)
- Threat Analysis and Risk Assessment (TARA)
- Breakout Exercise 3: Threat and Risk Analysis
- Cybersecurity Goals
- Cybersecurity Concept
- Breakout Exercise 4: Cybersecurity Requirements
- CAL-Oriented and Cybersecurity-Oriented Analyses (Annex F)
- Cybersecurity Assurance Levels (CAL)
- Usage of CALs
- Risk Assessment Methods (Clause 7)
- Asset Identification
- Vulnerability Analysis
- Breakout Exercise 5: Vulnerability Analysis
- Attack Feasibility Analysis
- Risk Determination
- Risk Treatment

DAY 2

SAE J3061 and ISO/SAE 21434 Cybersecurity Engineering Certification

Duration: 5 Days

Seminar Goals

- ✦ Tailor the necessary activities to support vehicle cybersecurity lifecycle management, development, production, operation, service, and decommissioning
- ✦ Information provided in the class can be used for ISO 21434 implementation
- ✦ Understand cybersecurity aspects of the entire development process including requirements specification, design, implementation, integration, verification, validation, and configuration
- ✦ Understand the risk-based approach for determining risk classes cybersecurity assurance levels (CALs)
- ✦ Use CALs for achieving an acceptable residual risk
- ✦ Provide requirements for validation and confirmation measures to ensure a sufficient and acceptable level of cybersecurity is being achieved

Seminar Content

- Chapter 1: Introduction and Overview to ISO 21434
- Chapter 2: Overall Cybersecurity Management (Clause 5)
- Chapter 3: Project Dependent Cybersecurity Management (Clause 6)
- Chapter 4: Post-Development Phases (Clauses 10-13)
- Chapter 5: Concept Phase (Clause 8)

- Chapter 5: Concept Phase (Clause 8) (cont'd)
- Chapter 6: CAL-Oriented and Cybersecurity - Oriented Analyses (Annex F)
- Chapter 7: Risk Assessment Methods (Clause 7)

- Chapter 8: Product Development I (Clause 9.1)
- Chapter 9: Product Development II (Clause 9.1)
- Chapter 10: Product Development III (Clause 9.1)

- Chapter 11: Product Development IV (Clause 9.1)
- Chapter 12: Validation at Vehicle Level & Release for Post-Development (Clauses 9.2 & 9.3)

- Chapter 13: Supporting Processes (Clause 14)
- Chapter 14: ISO 21434 Implementation Strategy

Optional ISO 21434 Certification Exam – Final 3 hours of Day Five

SAE J3061 and ISO/SAE 21434 Automotive Cybersecurity Auditing and Assessment Certification

Duration: 5 Days

Seminar Goals

- ✦ List and apply the main processes at the organizational and product levels that impact audits and assessments
- ✦ Review and understand a product's CS requirements, goals, and prepare a cybersecurity Plan
- ✦ Develop the Cybersecurity Concept & Refined Cybersecurity Design
- ✦ List appropriate evidence for supporting audits and assessments
- ✦ Use risk levels and CALs for achieving an acceptable residual risk
- ✦ List the main elements and develop the structure of Audit and Assessment reports

Seminar Content

- Chapter 1: Introduction and Overview to ISO/SAE 21434, ISO/IEC 27001, WP.29, and VDA ACMS
- Chapter 2: Organizational Level Processes for Audit
- Chapter 3: Cybersecurity Goals & Requirements
- Chapter 4: Preparing the Cybersecurity Plan
- Chapter 5: Risk Assessment Methods (Clause 7)

- Chapter 5: Risk Assessment Methods (Clause 7)
- Chapter 6: Cybersecurity Architecture
- Chapter 7: Cybersecurity Concept & Refined Cybersecurity Design

- Chapter 8: Supporting Processes
- Chapter 9: Gathering Evidence for Achieving CS Goals
- Chapter 10: Producing Arguments for Achieving CS Goals

- Chapter 11: Preparing Work Products
- Chapter 12: Preparing the Cybersecurity Case

- Chapter 13: Preparing the Audit Report
- Chapter 14: Preparing the Assessment Report

SAE J3061 and ISO/SAE 21434 Cybersecurity Threat Analysis and Risk Assessment (TARA)

Duration: 3 Days

Seminar Goals

- ◆ Determine the relationship between SAE J3016/ ISO/SAE 21434 and TARA
- ◆ Plan and perform activities of cybersecurity risk management
- ◆ Determine the applicability of risk assessment methods of ISO/SAE 21434 and SAE J3016
- ◆ Determine the impact rating of a damage scenario
- ◆ Determine the attack feasibility rating for an attack path
- ◆ Evaluate the risk associated with a damage scenario and attack path
- ◆ Select the risk treatment commensurate to the risk.
- ◆ Determine the applicability of other risk assessment methods
- ◆ Plan of TARA activities

Seminar Content

- Overview of ISO/SAE 21434 and SAE J3061 DAY 1
 - o Overview of TARA
 - o Relationship between ISO 21434 and TARA
- Overview of ISO 31000 DAY 1
 - o Cybersecurity Activities of ISO 31000
 - o Risk Assessment Methods in ISO/SAE 21434 and SAE J3061
 - o Threat Analysis and Damage Scenarios
 - o Impact Rating
- Attack Surfaces DAY 2
 - o Attack Paths
 - o Attack Feasibility Rating
 - o Risk Assessment Methods: Attack Potential
 - o Risk Value Evaluation
 - o CAL Evaluation
- Risk Mitigation & Treatment DAY 3
 - o Management Cybersecurity Controls
 - o Technical Cybersecurity Controls
 - o Other Risk Assessment Methods
 - o Plan to Implement TARA

SAE J3061 and ISO/SAE 21434 Conducting a Cybersecurity FMEA and Vulnerability Analysis Testing for Systems, Hardware and Software

Duration: 3 Days

Seminar Goals

- ◆ Learning a general methodology for conducting vulnerability analysis and assessments
- ◆ Understand Scanning and mapping network topology
- ◆ Be able to Identify listening ports/services on hosts
- ◆ Learn to Fingerprinting operating systems remotely
- ◆ Conducting vulnerability scans
- ◆ Audit gateway, switch, and firewall security
- ◆ Performing MCU, hardware, and software vulnerability

Seminar Content

- Chapter 1: Introduction and Overview to ISO 21434 DAY 1
- Chapter 2: Pre-requisites for Vulnerability Analysis
- Chapter 3: Scanning and Exploits
- Chapter 4: Uncovering infrastructure Vulnerabilities
- Chapter 5: Exposing and Revealing MCU Vulnerabilities DAY 2
- Chapter 6: Threat Analysis FMVEA: Failure Modes, Vulnerabilities and Effects Analysis
- Chapter 7: Implementing Scanner Operations and Configuration
- Chapter 8: Creating and Interpreting Reports
- Chapter 9: Researching Alert Information DAY 3
- Chapter 10: Identifying Factors That Affect risk
- Chapter 11: The vulnerability management cycle
- Chapter 12: Vulnerability Assessment Report

SAE J3061 and ISO/SAE 21434 Cybersecurity Engineering Defense & Protection Against Attacks

Duration: 5 Days

Seminar Goals

- ◆ Critically analyze and apply information from vehicular threat and vulnerability reports on a regular basis.
- ◆ Identify vehicle assets and their network topologies and how to monitor the vehicle environment for abnormalities and threats.
- ◆ Apply methodologies such as in-vehicle network security monitoring and approaches to reducing the control system threat landscape will be introduced and reinforced.
- ◆ Determine cybersecurity impact ratings and describe strategies for minimizing exposure
- ◆ Identify vehicular assets and describe strategies for lowering their impact rating
- ◆ Outline effective implementations of cybersecurity controls

Seminar Content

- Chapter 1: Introduction to Course
- Chapter 2: Threat Analysis

DAY 1

- Chapter 3: Attack Analysis
- Chapter 4: Asset Identification and Network Security Monitoring

DAY 2

- Chapter 5: Access Control and Monitoring
- Chapter 6: Cybersecurity Protection

DAY 3

- Chapter 7: System Management
- Chapter 8: Threat and Environment Manipulation

DAY 4

- Chapter 9: Asset Protection and Response
- Chapter 10: Active Defense and Incident Response

DAY 5

Introduction to Autonomous and Electric Vehicles: A Functional Safety, SOTIF, and Cybersecurity Perspective

Duration: 2 Days

Seminar Goals

Participants successfully completing this course will be able to:

- ◆ List and explain the basic components, functionality, and architectures of EVs and AVs
- ◆ Explain the nature of the Functional Safety and Cybersecurity requirements in the development of EVs and AVs
- ◆ Analyze the SOTIF objectives for safety in the design of AVs
- ◆ Analyze the perspectives of SOTIF, Functional Safety, and Cybersecurity in the design of EVs and AV.
- ◆ List and explain the commonalities and design issues of safety and cybersecurity involving EVs and AVs

Seminar Content

- Overview of Electric Vehicles
 - o Vehicle Architectures
 - o Brushless DC Motor
 - o Induction Motor
 - o Power Converters
 - o Batteries and battery management systems
 - o Powertrain controllers
- Overview of Automated Vehicles
 - o Perception system and sensors
 - o Localization and mapping
 - o Path planning and decision making
 - o Motion control
- Overview of Functional Safety (ISO 26262)
- Overview of Automotive Cybersecurity (ISO/SAE 21434), ISO/IEC 27001, WP.29, and VDA ACMS
- Nature of Functional Safety Requirements in the Development of EVs and AVs.
- Nature of Cybersecurity Requirements in the Development of EVs and AVs

DAY 1

- Overview of SOTIF Principles
 - o SOTIF Process Flow
 - o SOTIF Activities and Supporting Processes
 - o Analysis of the SOTIF Objectives for Safety in the Design of AVs
- Chapter 5: SOTIF Perspective
- Functional Safety Perspective
- Cybersecurity Perspective
- Commonalities and Design Issues of Safety and Cybersecurity Involving EVs and AVs

DAY 2


Preparing a Cybersecurity Case


Duration: 2 Days

Seminar Goals

- ◆ Determine the relevance of the Cybersecurity Goals, Arguments, and evidence in the Cybersecurity Case
- ◆ Analyze a layered model for structuring Cybersecurity Arguments
- ◆ Apply the layered model to ISO/SAE 21434 and SAE J3061
- ◆ Apply the generic argument structure to Cybersecurity Goals

Seminar Content

- Building Blocks of a Cybersecurity Case 
- Cybersecurity Goals
- Cybersecurity Case Arguments
- Cybersecurity Case Evidence
- Layered Model for Structuring Cybersecurity Arguments
- Rationale
- Satisfaction
- Means
- Organizational Environment
- Methods, Processes and Tools for Preparing a Cybersecurity Case: Goal Structuring Notation (GSN)

- Applying the Layered Model to ISO/SAE 21434 and SAE J3061 
- The ISO/SAE 21434 Implicit Argument
- The MISRA Argument Structure
- Applying the Generic Argument Structure to Cybersecurity Goals Argument Structure
- Example for Cybersecurity Goals


Writing Effective Requirements, Test Cases, and H/S Interfaces for Cybersecurity


Duration: 2 Days

Seminar Goals

- ◆ Determine the role and importance of Cybersecurity requirements
- ◆ Determine the role and importance of the Cybersecurity test cases
- ◆ Determine the role and importance of the Cybersecurity HSI
- ◆ Write effective requirements, test cases, and HIS based on HARA building blocks

Seminar Content

- Building Blocks of TARA per ISO 21434 
- Breakout Exercise 1: Reviewing a TARA
- Threat Identification
- Introduction to the Running Case Study for an Air Bag Cybersecurity Case – Walkthrough of Air Bag Cybersecurity Goal Development Through Functional Cybersecurity Concept
- Breakout Exercise 2: High Level Architecture of an Air Bag System
- Breakout Exercise 3: Identifying Threats for the Air Bag Case Study
- Attack Tree Generation
- Breakout Exercise 4: Develop an Attack Tree for the Air Bag Case Study
- Writing Effective Requirements

- Test Case Derivation 
- Breakout 5: Specify Cybersecurity Requirements and Test Cases for the Air Bag Case Study
- Threat Modeling
- Breakout 6: Determining Threats for the Air Bag Case Study
- Risk Countermeasures
- Breakout 7: Listing Countermeasures for the Air Bag Case Study
- Specification of Hardware/Software Interfaces
- Summary

SAE J3061 and ISO/SAE 21434 Automotive Cybersecurity Certification

Duration: 5 Days

Seminar Goals

- ✦ Tailor the necessary activities to support vehicle cybersecurity lifecycle management, development, production, operation, service, and decommissioning
- ✦ Information provided in the class can be used for ISO 21434 implementation
- ✦ Understand cybersecurity aspects of the entire development process including requirements specification, design, implementation, integration, verification, validation, and configuration
- ✦ Understand the risk-based approach for determining risk classes cybersecurity assurance levels (CALs)
- ✦ Use CALs for achieving an acceptable residual risk
- ✦ Provide requirements for validation and confirmation measures to ensure a sufficient and acceptable level of cybersecurity is being achieved

Seminar Content

- Chapter 1: Introduction and Overview to ISO/SAE 21434, ISO/IEC 27001, WP.29, and VDA ACMS
- Chapter 2: Overall Cybersecurity Management (Clause 5)
- Chapter 3: Project Dependent Cybersecurity Management (Clause 6)
- Chapter 4: Post-Development Phases (Clauses 10-13)
- Chapter 5: Concept Phase (Clause 8)

DAY 1

- Chapter 5: Concept Phase (Clause 8)
- Chapter 6: CAL-Oriented and Cybersecurity - Oriented Analyses (Annex F)
- Chapter 7: Risk Assessment Methods (Clause 7)

DAY 2

- Chapter 8: Product Development I (Clause 9.1)
- Chapter 9: Product Development II (Clause 9.1)
- Chapter 10: Product Development III (Clause 9.1)

DAY 3

- Chapter 11: Product Development IV (Clause 9.1)
- Chapter 12: Validation at Vehicle Level & Release for Post-Development (Clauses 9.2 & 9.3)

DAY 4

- Chapter 13: Supporting Processes (Clause 14)
- Chapter 14: ISO 21434 Implementation Strategy

DAY 5

Optional ISO 21434 Certification Exam – Final 3 hours of Day Five

Introduction to Systems Engineering: A Safety and Cybersecurity Perspective

Duration: 5 Days

Seminar Goals

- ✦ Articulate the concepts of system life cycle, requirements, and the various design activities
- ✦ Describe importance of verification and validation (V&V) activities
- ✦ Define and illustrate what is meant by model based system engineering (MBSE)
- ✦ Explain the main features of SysML as a SE language
- ✦ Specify the structure, behavior, and requirements of a specific sub-system using SysML
- ✦ Articulate the use of systems engineering in the Safety and Cybersecurity standards ISO 26262, ISO/SAE 21434, and ISO/PAS 21448.

Seminar Content

- Systems Life Cycle
- Introduction to Systems Engineering
- The V-Model of Systems Engineering
- Major Phases: Requirements, Conceptual Design, Preliminary and Detailed Design, Construction, Production, and Utilization Phases
- Breakout Exercise 1: List the Functionalities of an Anti-Lock Braking System (ABS)
- The Four Pillars of SysML: Structure, Behavior, Requirements, and Parameters
- Demo of SysML: Structure, Behavior, Requirements, and Parametrics for an Anti-Lock Braking System (ABS) Model Using Modelio
- Breakout Exercise 2: List a Set of Requirements and Specify the Structure and Behavior of an ABS in a Manual Fashion (i.e. not using specialized tools)
- Defining Systems Thinking
- Breakout Exercise 3: Analysis and Modification of the Structure, Behavior, and Requirements for an Anti-Lock Braking System (ABS) Model using SysML. (The open source Modelio tool will be used as the SysML)

DAY 1

- Architecture of Complex Systems
- The V-Model and AIAG-VDA FMEA/DVPR
- Model-Based Systems Engineering (MBSE)
- Breakout Exercise 4: List and Summarize the Functionalities of the AV Perception System of a Well-known Commercial Vehicle (Audi A8) Featuring ADAS & Autonomous Driving Technologies
- SysML as an Example Language for MBSE
- Developing SysML Models: Structure, Behavior, Requirements, and Parameters.
- SE Management
- Breakout Exercise 5: List a Set of Requirements and Specify the Structure, Behavior, and Parametrics of the Radar Sub-System Component of the AV Perception System of the Previous Exercise in a Manual Fashion (i.e., not using a specialized tool).
- Roles of System Architect, Safety Manager
- Using SysML: Developing Models for an Obstacle Detection and Avoidance Mechanism
- Breakout Exercise 6: Develop SysML Models for the Structure, Behavior, Requirements, and Parametrics for the Radar Sub-System Component of the Previous Exercise using Modelio.
- Course Summary, Wrap-up, and Takeaways

DAY 2

WP.29, ISO/SAE 21434 and VDA CSMS – Auditing Automotive Cybersecurity Management Systems

Duration: 2 Days

Seminar Goals

- Become aware of the importance of implementing cybersecurity
- List the features and clauses of ISO/SAE 21434
- Understand the WP.29 requirements for a CSMS
- Understand the VDA guidelines for a CSMS audit

Seminar Content

-
- Overview of ISO/SAE 21434, ISO/IEC 27001, WP.29, and VDA ACMS
 - Breakout Exercise 1
 - Management Aspects of ISO/SAE 21434
 - Overall Cybersecurity Management
 - Project-dependent Cybersecurity Management
 - Other Clauses of ISO 21434:
 - Concept Phase
 - Product Development
 - Post Development Phases
 - Continuous Cybersecurity Activities
 - Breakout Exercise 2
 - Introduction to WP.29
 - WP.29 Requirements

DAY
1

-
- WP.29 CSMS Requirements
 - VDA Guidelines for CSMS audit
 - Breakout Exercise 3
 - Auditing Process and Auditor Qualification
 - Rating of the Automotive CSMS Audit
 - Audit Questionnaire
 - Breakout Exercise 4
 - Guidelines for Auditors
 - Summary

DAY
2

VDA

Production Part Approval Process (PPAP) VDA Volume 2
System FMEA / DFMEA / DVP&R / Characteristics Linkage
Process Flow, PFMEA and Control Plans
Measurement Systems Analysis (VDA 5)
Contamination Identification and Control Utilizing VDA 19
Certification for Product Safety and Conformance Process Owners
Understanding VDA 6.3 Process Audits
VDA 6.3 Executive Overview
Conducting Product Audits to VDA 6.5
Conducting Process Audits to VDA 6.3

Production Part Approval Process (PPAP) VDA Volume 2

Duration: 1 Day

Seminar Goals

- ◆ Explain all items listed as PPAP requirements
- ◆ Explain the purpose of PPAP levels
- ◆ Explain when the customer should be notified of changes
- ◆ Identify all aspects of an initial production run

Seminar Content

- Course Overview and Introductions
- Introduction to a PPAP
- PPAP in a QMS
- Managing Changes and Submissions, VDA PPA
- Submission Levels, VDA PPA
- Record Retention
- Significant Production Run
- PPAP Submission Elements
- Requirements and Deliverables
- Product Design Elements
- General Elements
- Part Submission Warrant and Status
- VDA PPA Specific Elements
- Assessing a PPAP Package

System FMEA / DFMEA / DVP&R / Characteristics Linkage

Duration: 3 Days

Seminar Goals

- ◆ Understand the differences between DFMEA and SFMEA and the use of Boundary Diagrams
- ◆ Explain the use of an interrelationship matrices to identify relationships between components and higher level systems
- ◆ Understand the differences between the VDA and the AIAG approach for DFMEA development
- ◆ Know the importance of product-design to ensure quality products
- ◆ Demonstrate an ability to properly and effectively complete all items in the DFMEA development process
- ◆ Identify functions, requirements, failure modes, causes and controls, and properly enter the information in a DFMEA template
- ◆ Demonstrate how to use the output from a DFMEA to develop a test plan (DVP&R)
- ◆ Explain how a DFMEA can help identify effects and severity for a failure mode
- ◆ Identify special characteristics in process design
- ◆ Establish a priority system for design improvements, development and validation testing and risk-analysis

Seminar Content

- Course Overview and Introductions
- Introduction to Failure Modes and Effects Analysis (FMEA)
- Developing an FMEA
- Realizing a DFMEA according to VDA
- Structure Analysis
- Function Analysis
- Failure Analysis
- Action Analysis
- Optimization
- Difference between DFMEA and SFMEA and definition of scope using Block (Boundary) and Parameter (P) Diagrams
- Differences between the AIAG FMEA and the VDA Approach to FMEA
- Identification Special Characteristics

Process Flow, PFMEA and Control Plans

Duration: 2 Days

Seminar Goals

- ◆ Demonstrate an ability to properly and effectively complete all items in the PFMEA process
 - o Demonstrate an ability to properly construct a Process Flow Diagram
 - o Identify steps, requirements, failure modes, causes and controls, and properly enter the information in a PFMEA
- ◆ Explain the relationships among a Process Flow Diagram, PFMEA and Control Plan
- ◆ Identify special characteristics in manufacturing process design
- ◆ Explain how to prioritize continual improvements with a focus on the use of Sev, Sev x Occ, and Sev x Occ x Det ratings

Seminar Content

- Course Overview and Introductions
- Introduction to Failure Modes and Effects Analysis (FMEA)
- Developing an FMEA
- Process FMEA Prerequisites
- Process Flow Diagram Breakout Exercise
- Developing the Process FMEA according to VDA
- VDA Five-Step FMEA Approach
- QM-Tools
- Potential Causes
- Process Controls
- Risk Analysis (RPN)
- PFMEA: conducting and evaluating
- Control Plan
- Work Instructions

Measurement Systems Analysis (VDA 5)

Duration: 2 Days

Seminar Goals

- ◆ What is a Measurement System Analysis?
- ◆ What is the purpose of the analysis, how does it work?
- ◆ MSA procedure.
- ◆ Meaning of the individual elements such as resolution, linearity and measurement stability.
- ◆ The methods for determining the capability of measurement processes.
- ◆ Statistical evaluation of the processes with the Solara software.
- ◆ Evaluation of the results.
- ◆ Dealing with incapable measuring systems.
- ◆ Assessment of attributive measuring systems.
- ◆ How does VDA approach relate to the measurement system analysis according to MSA 4?

Seminar Content

- Introduction
- The Effects of Capability Studies
- The Measurement Process
- Measurement Errors
- Capability of Measurement Processes
- Resolution
- Measurement Standards
- Linearity
- Stability
- Type 1 Study: Systematic Measurement Error, Repeatability, Cg and Cgk
- Type 2 Study: %GRR with Appraiser Variation
- Type 3 Study: Measurement Systems without Appraiser Influence
- Non-capable Measurement Systems
- Conditional Release
- Attribute Measurement Processes
- MSA 4 and VDA 5

Contamination Identification and Control Utilizing VDA 19

Duration: 2 Days

Seminar Goals

- ◆ Understand the Contamination Philosophy
- ◆ Communication of Contamination Control Requirements to the Tiered Supply Base
- ◆ Identify Detrimental Contaminants
- ◆ Define the Six major types of Contamination
- ◆ Develop Procedures and Work Instructions for the Six Types of Contamination

Seminar Content

- Understand the Contamination Philosophy
- Identify Detrimental Contaminants
- Identify Equipment and Methods used in Contamination Control
- Define the Six Major Types of Contamination
- Have procedures and Work Instructions for the Six Types of Contamination
- Best Practices / Lessons Learned

Certification for Product Safety and Conformance Process Owners

Duration: 2 Days

Seminar Goals

- ◆ Enable the prospective or existing Product Safety Representative to handle their everyday work more professionally
- ◆ Define the responsibilities for managing product safety and conformity throughout the entire supply chain; from development through manufacture and delivery, and up to the end of the period of intended use
- ◆ Discuss product integrity in the product life cycle and give direction for dealing with issues of product non-conformance

Seminar Content

- Module 1
- Intro to Product Safety and Legal Compliance
- Recalls and Safety Concerns
- Product Liability and Compliance Obligations
- IATF 16949 on Product Safety
- Module 2
- Intro – Product Integrity in the Organization
- VDA Volume on Product Integrity
- Functional Responsibilities
- Delegation of Responsibilities
- Module 3
- Product Specific Qualification
- Process Specific Qualification
- Awareness and Product Safety Requirements Flowdown
- Capturing Lessons Learned (FMEA) and Prevention
- Module 4
- Product Integrity Over the Product Lifecycle
- Product Development Phase
- Production Phase and Line Walk Reporting
- Usage Phase
- Product Monitoring
- Module 5
- Conformity of Production (CoP)
- Response to Deviations
- Corrective Action

Understanding VDA 6.3 Process Audits

Duration: 2 Days

Seminar Goals

- ◆ Understand the requirements of VDA 6.3
- ◆ Complete a preliminary document review (for on-site classes)
- ◆ Prepare an implementation or “next steps” plan (for on-site classes)

Seminar Content

- VDA Overview
- Chapter 1: Understanding Process Audits
- Chapter 2: Using the Questionnaire
- P2: Project Management
- Breakout Exercise 1: Open Questions
- Breakout Exercise 2: Auditing Project Management
- P3: Planning the Product and Process Development
- Breakout Exercise 3: Planning the Product and Process Development
- P4: Implementation of the Product and Process Development
- Breakout Exercise 4: Implementation of the Product and Process Development

DAY
1

- Review of Day One
- Chapter 2: Using the Questionnaire (cont'd)
- P5: Supplier Management
- Breakout Exercise 5: Supplier Management
- P6: Process Analysis Production
- P7: Customer Care, Customer Satisfaction, Service
- Breakout Exercise 6: Assessing the Requirements
- Chapter 3: Potential Analysis (PI)
- Assessing the Potential Analysis
- Breakout Exercise 7: Potential Supplier Audit
- Chapter 4: Assessing a Process Audit for Material Products
- VDA Evaluation Matrix
- Breakout Exercise 8: Evaluation Matrix

DAY
2

VDA 6.3 Executive Overview

Duration: 2-4 hours

Seminar Goals

- ◆ Understand the process audit approach
- ◆ Understand the requirements of VDA 6.3

Seminar Content

- Introduction to Omnex
- VDA Organization Overview (including Process Approach)
- Understanding VDA 6.3 Process Audits
- Using the Questionnaire
- The VDA 6.3 Audit Process
- Assessing a Process Audit for Material Products
- Potential Analysis (PI) – optional
- Assessing the Potential Analysis – optional
- Auditor Qualifications – optional
- Questions and Answers

Conducting Product Audits to VDA 6.5

Duration: 1 Day

Seminar Goals

- ◆ Understand the product audit
- ◆ Understand the requirements of VDA 6.5
- ◆ Prepare, perform and complete an audit to VDA 6.5

Seminar Content

- Understanding the Product Audit and its Uses
- The Audit Process
- Audit Program
- Audit Contract
- Preparation
- Execution
- Assessment
- Planning an Audit of New Suppliers, Locations or Technologies using VDA 6.5
- Conducting the VDA 6.5 Assessment
- Best Practices / Lessons Learned

Conducting Process Audits to VDA 6.3

Duration: 3 Days

Seminar Goals

- ◆ Understand the process audit approach
- ◆ Understand the requirements of VDA 6.3
- ◆ Prepare, perform and complete an audit to VDA 6.3

Seminar Content

- VDA Overview
- Chapter 1: Understanding Process Audits
- Chapter 2: Using the Questionnaire
- P2: Project Management
- Breakout Exercise 1: Open Questions
- Breakout Exercise 2: Auditing Project Management
- P3: Planning the Product and Process Development
- Breakout Exercise 3: Planning the Product and Process Development
- P4: Implementation of the Product and Process Development
- Breakout Exercise 4: Implementation of the Product and Process Development

DAY 1

- Review of Day One
- Chapter 2: Using the Questionnaire (cont'd)
- P5: Supplier Management
- Breakout Exercise 5: Supplier Management
- P6: Process Analysis Production
- P7: Customer Care, Customer Satisfaction, Service
- Breakout Exercise 6: Assessing the Requirements
- Chapter 3: Potential Analysis (PI)
- Assessing the Potential Analysis
- Breakout Exercise 7: Potential Supplier Audit
- Chapter 4: Assessing a Process Audit for Material Products
- VDA Evaluation Matrix
- Breakout Exercise 8: Evaluation Matrix

DAY 2

- Review of Days One and Two
- Chapter 4: The VDA 6.3 Audit Process
- Audit Program
- Audit Request
- Breakout Exercise 9: Draw Up an Audit Request
- Preparation
- Breakout Exercise 10: Audit Plan
- Conducting the Audit
- Evaluation
- Presentation of Results
- Follow Up and Closure
- Course Review and Final Exam

DAY 3

Introduction to Systems Engineering: A Safety and Cybersecurity Perspective

Introduction to Autonomous and Electric Vehicles: A Functional Safety, SOTIF, and Cybersecurity Perspective

Information Security Awareness Training

Introduction to Systems Engineering: A Safety and Cybersecurity Perspective

Duration: 2 Days

Seminar Goals

Participants successfully completing this course will be able to:

- Identify key definitions, ideas and principles of ISO 26262
- Articulate the concepts of system life cycle, requirements, and the various design activities
- Describe importance of verification and validation (V&V) of requirements
- Define and illustrate what is meant by model based system engineering (MBSE)
- Explain the main features of SysML as a SE language
- Specify the structure, behavior, and requirements of a specific sub-system using SysML
- Articulate the use of systems engineering in the Safety and Cybersecurity standards ISO 26262, ISO/SAE 21434, and ISO/PAS 21448

Seminar Content

- Introduction to course
- Systems life cycle
- Introduction to Systems Engineering
- The V model of Systems Engineering
- Major Phases: Requirements, Conceptual Design, Preliminary & Detailed Design, Construction, Production, and Utilization phases
- Breakout Exercise 1: List the functionalities of an Anti-Lock Braking System (ABS)
- The four pillars of SysML: Structure, Behavior, Requirements & Parameters
- Demo of SysML: Structure, behavior, requirements & parametrics for an Anti-Lock Braking System (ABS) model using Modelio
- Breakout Exercise 2: List a set of requirements and specify the structure and behavior of an ABS in a manual fashion (i.e., not using specialized tools)
- Defining systems thinking
- Breakout Exercise 3: Analysis and modification of the structure, behavior, and requirements for an Anti-Lock Braking System (ABS) model using SysML. The open source Modelio tool will be used as the SysML

DAY 1

- Architecture of complex systems
- The V model and AIAG-VDA FMEA/DVPR
- Model based systems engineering (MBSE)
- Breakout Exercise 4: List and summarize the functionalities of the AV perception system of a well-known commercial vehicle (Audi A8) featuring ADAS & Autonomous Driving technologies.
- SysML as an example language for MBSE
- Developing SysML models: Structure, Behavior, Requirements & Parameters.
- SE Management
- Breakout Exercise 5: List a set of requirements and specify the structure, behavior, and parametrics of the Radar Sub-system component of the AV perception system of the previous exercise in a manual fashion (i.e., not using a specialized tool).
- Roles of system architect, safety manager
- Using SysML: Developing models for an obstacle detection and avoidance mechanism.
- Breakout Exercise 6: Develop SysML models for the structure, behavior, requirements, and parametrics for the Radar Sub-system component of the previous exercise using Modelio.
- Course Summary and Wrap-up
- Course Takeaways

DAY 2

Introduction to Autonomous and Electric Vehicles: A Functional Safety, SOTIF, and Cybersecurity Perspective

Duration: 2 Days

Seminar Goals

Participants successfully completing this course will be able to:

- List and explain the basic components, workings, and architectures of EVs and AVs
- List and explain the safety and cybersecurity requirements for the development of EVs and AVs
- Understand the application of systems engineering in the design of EVs and AVs
- Understand the perspectives of safety and cybersecurity in the design of EVs and AVs
- List and explain the commonalities and design issues of safety and cybersecurity involving EVs and AVs

Seminar Content

- Chapter 1: Introduction and Overview of the course
 - o Main issues in the design of AV and EVs
- Chapter 2: Introduction to Electric Vehicles
 - o Vehicle Architectures
 - o Brushless DC Motor
 - o Induction Motor
 - o Power Converters
 - o Batteries
 - o Powertrain controllers
- Chapter 3: Introduction to Automated Vehicles
 - o Perception system and sensors
 - o Localization and mapping
 - o Path planning and decision making
 - o Motion control
 - o Breakout Exercise 1: Components of EVs and AVs
- Chapter 4: Introduction to Systems Engineering
 - o Modular and hierarchical architecture
 - o System life cycle
 - o The V-model
 - o Role of requirements, design, testing, verification, and validation
 - o Management and planning considerations

DAY 1

- Chapter 5: Safety Perspective
 - o Functional Safety Perspective
 - o Role of ISO 26262
 - o SOTIF perspective
 - o Role of ISO/PAS 21448
- Chapter 6: Cybersecurity Perspective
 - o OT/ICS & Vehicular Perspectives
 - o Role of SAE 3061
 - o Role of ISO/SAE 21434
- Chapter 7: Safety and Cybersecurity Commonalities and Design Issues
 - o Commonalities
 - o Design Issues
 - o Course summary and main take away

DAY 2

Information Security Awareness Training

Duration: 1 Day

Seminar Goals

- Understand the application of Information Security Management principles in the context of ISO/IEC 27001:2013
- Relate the Information Security Management system to the organizational products, services, activities and operational processes
- Relate organization's context and interested party needs and expectations to the planning and implementation of an organization's Information Security Management system

Seminar Content

- Introduction and Welcome
- Introduction to the course
 - o Pre-test
- Typical information policies
- Global incidents on information security breaches
- Common Intrusion Points
- Types of Threats and Attacks
- IT Best Practices – At office environments, mobile environment
- Email practices
- Managing access
- Travel precautions and working remote.
 - o Post-test

Breakout scenarios and group discussions will be held after each chapters



www.omnexsystems.com

(734) 761-4940

info@omnexsystems.com

ENTERPRISE-WIDE QUALITY & INTEGRATED MANAGEMENT SYSTEM SOFTWARE SOLUTIONS



ENTERPRISE APQP SOLUTION



ENTERPRISE SUPPLIER QUALITY



ENTERPRISE MANAGEMENT SYSTEMS



- APQP / PPAP PROGRAM MANAGEMENT
- REQUIREMENTS MANAGEMENT
- APQP PPAP DOCUMENTATION
- DOCUMENT CONTROL & MANAGEMENT
- INSPECTION CONTROL SYSTEMS
- MEASUREMENT SYSTEMS ANALYSIS
- FRACAS/PROBLEM SOLVING
- CONTINUAL IMPROVEMENT & KPI MANAGEMENT
- TOTAL PRODUCTIVE MAINTENANCE
- COMPETENCY & TRAINING MANAGEMENT
- FUNCTIONAL SAFETY

Writing Effective Requirements and Test Cases

Duration: 3 Days

Seminar Goals

- Detailed understanding of what Automotive SPICE® is and the motivation behind the model
- Detailed understanding of process capability level 1 (VDA-Scope)
- Detailed understanding of traceability requirements
- Detailed understanding of creating requirements for software and its elements at various levels
- Understanding of how to evaluate process risks and drive process improvements

Seminar Content

-
- Chapter 1: Introduction and Overview
 - Chapter 2: Understanding System/Software Requirements
 - Chapter 3: Architectural Design

-
- Chapter 4: Developing Software Detailed Design, Unit Construction, and Software Unit Verification
 - Chapter 5: Conducting Software Integration and Integration Testing, and Software Qualification Test

-
- Chapter 7: Developing Hardware Requirements
 - Chapter 8: Creating the V-Model using DFMEA and DVP&R

VDA ISA based TISAX Internal Assessor

Duration: 4 Days

Seminar Goals

- Detailed understanding of VDA ISA based TISAX model
- Understanding of relevant requirements of ISO 27001 and 27002 as it applies to VDA ISA based TISAX
- Sufficient knowledge and understanding of the assessment process according to ISO 33002 and auditing best practices from ISO 19011
- Detailed understanding of how to perform internal assessments
- Understanding of how to rate and determine the capability level

Seminar Content

-
- Introduction
 - VDA TISAX model Explained
 - Introduction to ISO/IEC 27001:2013, 27002:2013 and Key Terms from the ISO 27000:2014 – Overview and Vocabulary
 - Information Security General - TISAX
 - Group Exercise: Context of the Organization
 - Group Exercise: Interested Parties
 - Group Exercise : IT Security Controls
 - Connection to 3rd parties
 - Data protection

-
- ENX structure, participants of the assessment
 - Scoping and planning of the assessment
 - Capability levels of TISAX
 - Integration of TISAX requirements to your business management system
 - TISAX understanding final exam

-
- Introduction to Assessment Programs
 - Assessment Planning and Preparation
 - Breakout Exercise – Creating Assessment Plan and Schedule
 - Performing the Assessment
 - Assessment Findings and Nonconformity Statements
 - Reporting the Assessment Results

-
- Assessment Follow-up
 - Breakout Exercise – Performing Assessment

Software/Algorithm Failure Modes and Effect Analysis Onsite Workshop

Duration: 2 Days

Seminar Goals

- ◆ Be able to perform a Software FMEA analysis during any phase of the development process
- ◆ Be proficient in Software FMEA immediately after completing this workshop
- ◆ Study examples of Software FMEA from real-world systems
- ◆ Complete a Software FMEA for use within your own company

Seminar Content

-
- Chapter 1: Software Risk Analysis introduction
 - Chapter 2: Design Failure Mode and Effects Analysis (DFMEA) Introduction
 - Chapter 3: DFMEA Preparation
 - Breakout Exercise 1: Boundary (Block) Diagram
 - Chapter 4: Developing the DFMEA
 - Breakout Exercise 2: Starting the DFMEA
 - Breakout Exercise 3: Design Failure Modes
 - Breakout Exercise 4: Potential Design Causes
 - Breakout Exercise 5: Design Controls
 - Breakout Exercise 6: Design Effects & Classification
 - Breakout Exercise 7: RPNs and Improvements
 - Chapter 5 – Design Verification Plan and Report (DVP&R)
 - Chapter 6 – Algorithm FMEAs

DAY 1

-
- Review of Course Material
 - Begin Work on Customer-supplied Software FMEA

DAY 2

ISO 26262:2018 Product Development at the Hardware Level

Duration: 5 Days

Seminar Goals

- ◆ Understand the requirements of ISO 26262 Parts 4 and 6 and how they affect Hardware Development
- ◆ Describe Hardware Evaluation requirements and Requirements Verification
- ◆ Describe the impact on Semiconductor development
- ◆ Describe the different types of Hardware Metrics
 - Implement the development of Structural Metrics
 - Describe the development of Safety Reliability Metrics

Seminar Content

-
- Chapter 1: Introduction and Overview to ISO 26262
 - Chapter 2: Management of Functional Safety (Part 2)
 - Chapter 3: Safety Element out of Context (Part 10)
 - Chapter 4: Concept Phase (Part 3)
 - Chapter 5: Safety Requirements

DAY 1

-
- Chapter 6: System Level Development (Part 4)
 - Chapter 7: Hardware Level Development (Part 5)
 - Chapter 8: Hardware Safety Requirements

DAY 2

-
- Chapter 9: Hardware Design
 - Chapter 10: Overview of Hardware Metrics

DAY 3

-
- Chapter 11: SPF and LF Metrics
 - Chapter 12: Support Activities (Part 8)

DAY 4

-
- Chapter 13: Software Level Development (Part 6)
 - Chapter 14: Production and Operation (Part 7)
 - Chapter 15: Qualification of Software Tools
 - Chapter 16: Summary

DAY 5

Optional ISO 26262 Certification Exam – Final 3 hours of Day Five


Multipoint DFMEA for Mechatronic and Electronic Systems

Duration: 2 Days

Seminar Goals

- ◆ Explain the difference between DFMEA and SFMEA
 - Demonstrate an ability to properly construct a Boundary (Block) Diagram
- ◆ Explain how to incorporate single and multipoint FMEAs into the same FMEA (Omnex method)
- ◆ How to build a FMEA that links with FTA and FMEDA (Omnex method)
- ◆ Explain the use of an inter-relationship matrix to identify relationships between components and higher level systems
- ◆ Demonstrate an ability to properly and effectively complete all items in the DFMEA process
 - Identify Functions, Requirements, Failure Modes, Causes and Controls and properly enter the information in a DFMEA
- ◆ Demonstrate how to use the output from a DFMEA to develop a test plan (DVP&R)
- ◆ Explain how a DFMEA can help identify effects and severity for a process failure mode
- ◆ Identify special characteristics in product design
- ◆ Continual improvements with a focus on the use of Sev, Sev x Occ, and Sev x Occ x Det ratings

Seminar Content

- 
- Setting the Stage: APQP Overview
 - Introduction to Failure Mode and Effects Analysis (FMEA)
 - Developing an FMEA
 - Design FMEA Prerequisites
 - Breakout Exercise: Function Worksheet
 - Breakout Exercise: Boundary Diagram
 - Developing the Design FMEA
 - Breakout Exercise: Item / Function and Requirements
 - Breakout Exercise: Potential Design Failure Modes
 - Breakout Exercise: Potential Causes
 - Breakout Exercise: Design Controls
 - Breakout Exercise: Effects and Severity
 - Breakout Exercise: Review Identified Special Characteristics
 - Breakout Exercise: Risk Analysis and Mitigation
 - Breakout Exercise: Implementation
 - Breakout Exercise: Thinking Ahead to FTA and FMEDA (instructor-led)
 - Test Planning and Reporting
 - Breakout Exercise: DVBP&R
 - Summary

Understanding AIAG-VDA DFMEA (SFMEA and DFMEA) for Design and Project Team Members

Duration: 1 Day

Seminar Goals

- ◆ Apply the AIAG-VDA Seven Step Approach to developing SFMEA and DFMEA
- ◆ Study the changes and differences between AIAG VDA FMEA and AIAG FMEA 4th Edition. How to make the results of both approaches the same?
- ◆ Detail best in class methods of AIAG VDA Design FMEA implementations.
- ◆ Understand a Block Diagram, P Diagram, and Interface Diagram
- ◆ Link DFMEA with DVPR and use Prevention Checklists
- ◆ Link SFMEA, DFMEA, Process Flow, PFMEA, and Control Plans
- ◆ Learn how to link DFMEA to failure and warranty history and Cost of Poor Quality (COPQ)
- ◆ Discuss AIAG-VDA DFMEA Transition and Implementation Plan.

Seminar Content

- Course Overview and Introductions
- Setting the Stage: APQP Overview
- Chapter 1 – Introduction to Failure Modes and Effects Analysis (FMEA)
- Chapter 2 – Developing an FMEA
- Chapter 3 – Design FMEA Prerequisites
- Chapter 4 – Developing the Design FMEA
- Chapter 5 – Test Planning and Reporting (DVP&R)
- Chapter 7 – Implications of the AIAG-VDA FMEA

Understanding AIAG-VDA Process FMEA and Control Plans for Process and Project Team Members

Duration: 1 Day

Seminar Goals

- ◆ Apply the AIAG-VDA Seven Step Approach to developing Process Flow, PFMEA and Control Plans
- ◆ Apply the major changes, improvements, and benefits of AIAG-VDA PFMEA
- ◆ Study the changes and differences between AIAG VDA FMEA and AIAG FMEA 4th Edition. What are the changes and differences in the two approaches? How to make the results of both approaches the same?
- ◆ Link SFMEA, DFMEA, Process Flow, PFMEA, and Control Plans
- ◆ Learn how to link PFMEA to failure and warranty history and Cost of Poor Quality (COPQ)
- ◆ Discuss AIAG-VDA PFMEA Transition and Implementation Plan
- ◆ After this training, the participants will have an understanding of
 - Process Flow and AIAG-VDA PFMEA Structure Analysis
 - Links between Process Flow, PFMEA, Control Plan and Work Instructions
 - Process FMEA and Control Plan
 - All aspects of the 1st edition of FMEA handbook (2019) released by AIAG and VDA

Seminar Content

- Chapter 1: Software Risk Analysis introduction
- Chapter 1: Introduction to Failure Mode and Effects Analysis (FMEA)
- Chapter 2: Developing a PFMEA
- Chapter 3: Process FMEA Prerequisites
- Chapter 5 – Process Control Plans
- Chapter 6 – Implications of the AIAG-VDA FMEA

Advanced Product Quality Planning (APQP) Overview

Duration: 1 Day

Seminar Goals

- ◆ Understand the five phases of APQP and the benefits of the APQP strategy
- ◆ Identify the inputs and outputs for the five phases.
- ◆ Match the deliverables with the phases of APQP.
- ◆ Understand Phase V and the purpose of feedback, assessment and corrective action.
- ◆ Understand the latest APQP ideas for improving quality and reducing costs

Seminar Content

- APQP Overview
- Breakout Exercise: Inputs and Outputs of APQP
- Phase I – Plan and Define Program
- Breakout Exercise: Planning and Development Inputs
- Breakout Exercise: Risk Categories and Impacts
- Breakout Exercise: The Value of Key Phase I Deliverables
- Phase II – Product Design and Development
- Breakout Exercise: The Value of Key Phase II Deliverables
- Phase III – Process Design and Development
- Breakout Exercise: The Value of Key Phase III Deliverables
- Phase IV – Product and Process Validation
- Phase V – Feedback, Assessment and Continual Improvement

Understanding the Five Phases of APQP

Duration: 2 Days

Seminar Goals

- Understand the five phases of APQP and the benefits of the APQP strategy.
- Identify the inputs and outputs for the five phases.
- Understand Phase V and the purpose of feedback, assessment and corrective action.
- Match the elements of VDA 6.3 with the elements of APQP.
- Understand the latest APQP ideas for improving quality and reducing costs.

Seminar Content

- APQP Overview
- APQP and VDA 6.3 Linkages (optional)
- Phase I – Plan and Define Program
- Breakout Exercise: Planning and Development Inputs
- Breakout Exercise: Risk Categories and Impacts
- Breakout Exercise: The Value of Key Phase I Deliverables
- Phase II – Product Design and Development
- Breakout Exercise: The Value of Key Phase II Deliverables
- Phase III – Process Design and Development
- Breakout Exercise: The Value of Key Phase III Deliverables
- Phase IV – Product and Process Validation
- Breakout Exercise: The Value of Key Phase IV Deliverables
- Phase V – Feedback, Assessment and Continual Improvement

Role of Top Management in APQP

Duration: Half Day

Seminar Goals

- Understand how to plan for and manage the Realization Process using the APQP model
- Understand the linkages and interactions of the five phases of APQP as an integrated process
- Understand the role and responsibilities of program management
- Understand the “symphonic orchestra” concept

Seminar Content

- Overview
- Program Management
- The Five Phases of APQP
- Deliverables
- Program Management Responsibilities
- Strategic Management Issues

Product Development using SFMEA, DFMEA and Associated Tools

Duration: 2 Days

Seminar Goals

- Explain the difference between DFMEA and SFMEA
Demonstrate an ability to properly construct a Boundary (Block) Diagram
- Explain the use of an inter-relationship matrix to identify relationships between components and higher level systems
- Demonstrate an ability to properly and effectively complete all items in the DFMEA process

Identify Functions, Requirements, Failure Modes, Causes and Controls and properly enter the information in a DFMEA

Demonstrate how to use the output from a DFMEA to develop a test plan (DVP&R)

Explain how a DFMEA can help identify effects and severity for a process failure mode

Identify special characteristics in product design

Continual improvements with a focus on the use of Sev, Sev x Occ, and Sev x Occ x Det ratings

Seminar Content

- Setting the Stage: APQP Overview
- Introduction to Failure Mode and Effects Analysis (FMEA)
- Developing an FMEA
- Design FMEA Prerequisites
- Breakout Exercise: Customers and Functional Requirements
- Breakout Exercise: Boundary Diagram
- Developing the Design FMEA
- Breakout Exercise Starting the DFMEA Form
- Breakout Exercise: Failure Modes
- Breakout Exercise: Design Causes
- Breakout Exercise: Design Controls
- Breakout Exercise: Effects, Severity and Action Plans
- Characteristics Flowdown
- Test Planning and Reporting

Design Review Based on Failure Modes

Duration: 4 Days

Seminar Goals

- ◆ Explain the difference between DFMEA and SFMEA
- ◆ Demonstrate an ability to properly construct a Boundary (Block) Diagram
- ◆ Explain the use of an inter-relationship matrix to identify relationships between components and higher level systems
- ◆ Demonstrate an ability to properly and effectively complete all items in the DFMEA process
- ◆ Identify Functions, Requirements, Failure Modes, Causes and Controls and properly enter the information in a DFMEA
- ◆ Demonstrate how to use the output from a DFMEA to develop a test plan (DVP&R)
- ◆ Explain how a DFMEA can help identify effects and severity for a process failure mode
- ◆ Identify special characteristics in product design
- ◆ Continual improvements with a focus on the use of Sev, Sev x Occ, and Sev x Occ x Det ratings

Seminar Content

- Introductions
- DFMEA - Purpose / Benefits / Roadblocks
- Item Functions / Performance Requirements
- Team Exercise - Item Functions / Performance Requirements
- First third of DFMEA Form - Through the Severity Column
- Team Exercise
- Second third of DFMEA Form - Through the RPN Column
- Final third of DFMEA Form - Through the Recalculated RPN
- DFMEA Case Studies
- Discussion – DFMEA Common Mistakes
- Individual Exercise – DFMEA With Errors
- Q & A and Post Test

DAY 1

- DRBFM Training
- DRBFM team activity
- Identify the change to review
- Identify the change points
- Complete the Business Case Analysis
- Complete the Change Point Matrix
- Prepare the DFMEA (Left Side) with product engineer only

DAY 2

- Prepare the DFMEA (Left Side) with product engineer only
- Prepare the DRBFM (Right Side) with entire team including Recommended Actions

DAY 3

- Prepare the DRBFM (Right Side) with entire team including Recommended Actions

DAY 4

Machine Failure Mode Effect Analysis (MFMEA)

Duration: 1 Day

Seminar Goals

- ◆ Understand process review concepts
- ◆ Understand feasibility and contract review
- ◆ Understand the benefits of Process Flow
- ◆ Identify the links between Process Flow, MFMEA, Control Plan and Work Instructions
- ◆ Understand MFMEA and Control Plans

Seminar Content

- Introduction to MFMEA
- What is Machinery FMEA?
- Benefits of MFMEA
- Barriers to MFMEA
- Customers of MFMEA
- Two Approaches to MFMEA
- Functional Approach
- Hardware Approach
- Item / Function / Performance Requirements
- Completing the FMEA Form

Measurement Systems Analysis (MSA) including Advanced Analysis (ANOVA)

Duration: 2 Days

Seminar Goals

- ◆ Explain bias, linearity, stability, repeatability and reproducibility
- ◆ Identify the type of MSA study that is appropriate for the situations
- ◆ Explain discrimination and number of distinct categories
- ◆ Identify all important aspects of setting up a study
- ◆ Explain the acceptance criteria for gage R&R studies
- ◆ Explain ANOVA and apply it to GRR Analysis
- ◆ Analyze automated and non-replicable measurement systems
- ◆ Analyze attribute measurement systems
- ◆ Develop an approach to measurement systems planning

Seminar Content

- What is a Measurement System?
- Statistical Properties of Measurement Systems
- Discrimination & Uncertainty
- Bias, Linearity and Stability
- Breakout Exercise: Bias
- Breakout Exercise: Bias & Linearity
- Breakout Exercise: Stability
- GRR Studies
- Breakout Exercise: Graphing GR&R
- Breakout Exercise: Calculating GR&R
- Advanced Analysis – Analysis of Variance (ANOVA)
- Automated and Non-Replicable Systems
- Non-Replicable Case Study
- Attribute MSA
- Breakout Exercise: Attribute Analysis
- Breakout Exercise: Calculating Attribute Analysis
- Measurement Planning

Manufacturing Process Development using PFMEA

Duration: 2 Days

Seminar Goals

- ◆ Demonstrate an ability to properly and effectively complete all items in the PFMEA process.
- ◆ Demonstrate an ability to properly construct a Process Flow Diagram.
- ◆ Identify steps, requirements, failure modes, causes and controls and properly enter the information in a PFMEA.
- ◆ Explain the relationship among a Process Flow Diagram, PFMEA and Control Plan.
- ◆ Identify special characteristics in manufacturing process design.
- ◆ Explain how to prioritize continual improvements with a focus on the use of Sev, Sev x Occ, and Sev x Occ x Det ratings.

Seminar Content

- Setting the Stage: APQP Overview
- Introduction to Failure Modes and Effects Analysis (FMEA)
- Developing an FMEA
- Process FMEA Prerequisites
- Breakout Exercise: Process Flow Diagram
- Developing the Process FMEA
- Breakout Exercise: Starting the PFMEA Form
- Breakout Exercise: Potential Causes
- Breakout Exercise: Process Controls
- Breakout Exercise: Effects, Severity and Action Plans
- Control Plan
- Breakout Exercise: Creating a Control Plan
- Work Instruction Development

APQP Manufacturing Process Development using PFMEA and PPAP

Duration: 3 Days

Seminar Goals

- ◆ Demonstrate an ability to properly and effectively complete all items in the PFMEA process.
- ◆ Demonstrate an ability to properly construct a Process Flow Diagram.
- ◆ Identify steps, requirements, failure modes, causes and controls and properly enter the information in a PFMEA.
- ◆ Explain the relationship among a Process Flow Diagram, PFMEA and Control Plan.
- ◆ Identify special characteristics in manufacturing process design.
- ◆ Explain how to prioritize continual improvements with a focus on the use of Sev, Sev x Occ, and Sev x Occ x Det ratings.
- ◆ Explain the purpose of PPAP.
- ◆ Describe the PPAP submission process.
- ◆ List the PPAP submission levels and requirements.

Seminar Content

- Advanced Product Quality Planning (APQP) Overview
- The Five APQP Phases
- Program Management for APQP
- Introduction to Failure Modes and Effects Analysis (FMEA)
- Developing an FMEA
- Process FMEA Prerequisites
- Breakout Exercise: Process Flow Diagram
- Developing the Process FMEA
- Breakout Exercise: Starting the PFMEA Form
- Breakout Exercise: Potential Causes
- Breakout Exercise: Process Controls
- Breakout Exercise: Effects, Severity and Action Plans
- Control Plan
- Breakout Exercise: Creating a Control Plan
- Work Instruction Development
- Production Part Approval Process (PPAP)

Production Part Approval Process (PPAP) Overview

Duration: 1 Day

Seminar Goals

- ◆ Participants will understand and be able to list PPAP requirements.
- ◆ Participants will be able to explain the purpose of PPAP levels and the relationship between APQP and PPAP.
- ◆ Participants will be able to assess a PPAP package for conformance to PPAP requirements using a checklist.
- ◆ Participants will be able to explain when the customer should notified of changes.
- ◆ Participants will be able to identify all aspects of an initial production run.

Seminar Content

- Introduction to PPAP
- PPAP in a QMS
- Managing Changes and Submissions
- Submission Levels
- Record Retention
- Significant Production Run
- PPAP Submission Elements
- Requirements and Deliverables
- Product Design Elements
- Manufacturing Process Elements
- General Elements
- Part Submission Warrant and Status
- Assessing a PPAP Package

Service Production Part Approval Process (PPAP) Overview

Duration: 2 Days

Seminar Goals

- ◆ Participants will understand and be able to list PPAP requirements.
- ◆ Participants will understand the supplemental requirements that serve as clarifications to the PPAP process for service parts.
- ◆ Participants will be able to explain the purpose of PPAP levels and the relationship between APQP and PPAP.
- ◆ Participants will be able to assess a PPAP package for conformance to PPAP requirements using a checklist.
- ◆ Participants will be able to explain when the customer should be notified of changes.
- ◆ Participants will be able to identify all aspects of an initial production run.

Seminar Content

- Introduction to PPAP
- PPAP in a QMS
- Managing Changes and Submissions
- Submission Levels
- Record Retention
- Significant Production Run
- PPAP Submission Elements
- Requirements and Deliverables
- Product Design Elements
- Manufacturing Process Elements
- General Elements
- Part Submission Warrant and Status
- Assessing a PPAP Package

Reverse Failure Mode and Effect Analysis – RFMEA

Duration: 2 Days

Seminar Goals

- ◆ Explain the difference between DFMEA and RFMEA
- ◆ Demonstrate an ability to properly construct a RFMEA check-sheet
- ◆ Demonstrate an ability to properly and effectively complete all items in the RFMEA process
- ◆ Identify high risk areas, evaluate and test control plan gaging and measurement.
- ◆ Demonstrate how to use the output from a RFMEA to identify additional risk and work it back into the PFMEA
- ◆ Identify special characteristics in product design and assure that the control methods are effective.

Seminar Content

- Intro to FMEA
- APQP and FMEA
- Development of a good conventional PFMEA
- VDA PFMEA 7 Step Process
- Intro to Reverse - FMEA
- 7 Step Reverse Process
- Assemble Malfunction team
- Review of PFMEA, develop plan

DAY 1

- Development of Reverse FMEA check-sheet
- Go and See- Evaluate process using check-sheet
- Evaluate detection method through testing
- Re-access risk
- Develop action plan
- Reporting Results to Customer
- Continuous improvement- Updating Baselines and Requirements

DAY 2

- Work on in-plant example

DAY 3

Statistical Process Control (SPC) and Associated Tools

Duration: 2 Days

Seminar Goals

- ◆ Identify the different uses of basic variables control charts
- ◆ Explain common and special causes
- ◆ Relate within and between variation to common and special causes
- ◆ Explain the relationship between C and P indices, and the different methods of estimating standard deviations
- ◆ Identify appropriate uses for Cp, Cpk and Pp, Ppk
- ◆ Explain the relationship between the capability indices to determine process improvement actions
- ◆ Explain the relationship between process control and process capability

Seminar Content

- SPC Background
- Breakout Exercise 1: Analyzing Data
- Introduction to Control Charts
- Basic Variable Control Charts
- Breakout Exercise 2: Plotting Data
- Breakout Exercise 3: Control Charts
- Breakout Exercise 4: X & MR Charts
- Basic Attribute Control Charts
- Analyzing Control Charts
- Breakout Exercise 5: Interpreting Control Charts
- Capability Analysis
- Breakout Exercise 6: Calculating Indices

Statistical Process Control (SPC) and Associated Tools

Duration: 3 Days

Seminar Goals

- ◆ Identify the different uses of control charts
- ◆ Explain common and special causes
- ◆ Relate within and between variation to common and special causes
- ◆ Explain the relationship between C and P indices, and the different methods of estimating standard deviations
- ◆ Identify appropriate uses for Cp, Cpk and Pp, Ppk
- ◆ Explain the relationship between the capability indices to determine process improvement actions
- ◆ Explain the relationship between process control and process capability

Seminar Content

- SPC Background
- Normal Theory and Central Limit Theorem
- Introduction to Control Charts
- Breakout Exercise: Sampling Plan
- Variable Control Charts
- Breakout Exercise: X & S Charts
- Breakout Exercise: X & MR Charts
- Attribute Control Charts
- Analyzing Control Charts
- Breakout Exercise: Interpreting Control Charts
- Capability Analysis
- Breakout Exercise: Calculating Indices
- Process Improvement Cycle and Process Control
- Breakout Exercise: Control Chart Concepts

Understanding Core Tools: Advance Product Quality Planning (APQP) and Production Part Approval Process (PPAP)

Duration: 1 Day

Seminar Goals

- ◆ Understand the five phases of APQP for New Product Development and its relationship to program management and the knowledge and skills needed to participate in an APQP team
- ◆ Understand the PPAP protocol, elements, deliverables and submission/approval process

Seminar Content

- APQP Overview
- The Five APQP Phases
- Concurrent Engineering
- APQP and IATF 16949
- The Five APQP Phases
- Phase I – Planning
- Phase II – Product Design & Development
- Phase III – Process Design & Development
- Phase IV – Product & Process Validation
- Phase V – Feedback Assessment & Corrective Action
- PPAP
- PPAP Elements
- PPAP Submission Levels
- Part Submission Warrant (PSW)
- Assessing Process Readiness and PPAP

Understanding Core Tools (APQP/PPAP, DFMEA, PFMEA, Control Plans, SPC and MSA)

Duration: 5 Days

Seminar Goals

- ◆ Understand the five phases of APQP for New Product Development and its relationship to program management and the knowledge and skills needed to participate in an APQP team
- ◆ Understand the PPAP protocol, elements, deliverables and submission/approval process
- ◆ Understand how to develop and use DFMEA and DVP&R to identify and address design risk during the product development process and in support of the manufacturing process development process
- ◆ Understand how to achieve robust and comprehensive process control, process standardization and process improvement using Process Flow Diagrams, PFMEA and Process Control Plans
- ◆ Understand the use of SPC to monitor and measure variation in manufacturing processes and to identify and correct problem where they arise
- ◆ Understand MSA and the statistical tests employed to determine measurement variation and measurement uncertainty for the effective management of measurement systems

Seminar Content

- APQP
- Production Part Approval Process (PPAP)
- DFMEA/DVP&R
- Process Flow
- Process FMEA
- Control Plans
- Work Instructions
- SPC
- MSA

Understanding Core Tools: Design Failure Modes and Effects Analysis (DFMEA) and Design Validation Plan & Report (DVP&R)

Duration: 2 Days

Seminar Goals

- ◆ Understand how to develop and use DFMEA and DVP&R to identify and address design risk during the product development process and in support of the manufacturing process development process

Seminar Content

- APQP Phases: Key Phase Deliverables (Outputs)
- DFMEA Introduction
- DFMEA Purpose
- DFMEA Objectives
- New Products
- Linkages
- DFMEA Preparation
- Define the Customer
- Identify Specific Functions and Requirements
- Robust Designs
- Breakout Exercise 1: Boundary (Block) Diagram
- Breakout Exercise 2: Parameter (P) Diagram
- Other Inputs to DFMEA
- Developing the DFMEA
- Starting the DFMEA Form
- Design Failure Modes
- Potential Design Causes
- Potential Controls & Prevention
- Potential Effect & Severity
- Action Planning
- Evaluating and Maintaining DFMEAs
- Breakout Exercises 3-8: Developing the DFMEA
- Design Verification Plan & Report (DVP&R)
- Objectives of DVP&R
- DVP Format & Flow
- Management Responsibility for DVP
- Challenges to Development

Understanding Core Tools: PFMEA and Control Plans

Duration: 1 Day

Seminar Goals

After this training, the participants will have knowledge and understanding of

- ◆ Process Flow
- ◆ Links between Process Flow, PFMEA, Control Plan and Work Instructions
- ◆ The FMEA as analytical process
- ◆ Process FMEA and Control Plan

Seminar Content

- APQP and PFMEA Introduction
- APQP Phases
- PFMEA Defined
- PFMEA as a Living Document
- APQP Inputs to PFMEA and Process Flow Diagram
- Phase II Inputs/Deliverables
- Phase III Deliverables
- Process Flow Diagram
- Breakout Exercise 1: Developing a Process Flow Diagram
- Print Preparation
- Special Characteristics
- Phase III Inputs/Deliverables
- PFMEA Analytical Sequence
- Developing a Process FMEA
- Preparing the PFMEA
- Failure Mode and Effects
- Controls Prevent / Detect
- Risk Priority Number
- Classification Column
- Breakout Exercises 3-5: Developing a PFMEA
- Developing a Control Plan
- What is a Control Plan?
- Control Plan Header Information
- Control Plan Fields
- Breakout Exercise 6: Creating a Control Plan

Understanding Core Tools: Statistical Process Control (SPC)

Duration: 1 Day

Seminar Goals

- Identify the different uses of basic variables control charts
- Explain common and special causes
- Relate within and between variation to common and special causes
- Explain the relationship between C and P indices, and the different methods of estimating standard deviations
- Identify appropriate uses for Cp, Cpk and Pp, Ppk
- Explain the relationship between the capability indices to determine process improvement actions
- Explain the relationship between process control and process capability

Seminar Content

- SPC Background
- Process Fundamentals
- Prevention vs. Detection
- Process Variation
- Control vs. Capability
- Basic Statistics
- Breakout Exercise 1: Analyzing Data
- Normal Distribution
- Central Limit Theorem
- Introduction to Control Charts
- Statistical Control
- Types of Control Charts
- Basic Control Chart Elements
- Basic Control Charts
- X & R Chart
- Breakout Exercise 2: Plotting Data
- Breakout Exercise 3: Control Limits for X & R Control Charts
- Basic Attribute Control Charts
- Characteristics of Attribute Charts
- Types of Attribute Charts
- Analyzing Control Charts
- Common Out-of-Detection Rules
- Patterns that Signal Out-of-Control
- Breakout Exercise 4: Interpreting Control Charts
- Capability Analysis
- Capability Basics
- Bilateral Tolerances and Capability
- Unilateral Tolerances and Capability
- Breakout Exercise 5: Calculating Indices

Understanding Core Tools: Measurement Systems Analysis (MSA)

Duration: 1 Day

Seminar Goals

- Explain bias, linearity, stability, repeatability and reproducibility
- Identify the type of MSA study that is appropriate for the situations
- Explain discrimination and number of distinct categories
- Identify all important aspects of setting up a study
- Explain the acceptance criteria for gage R&R studies

Seminar Content

- What is a Measurement System?
- Foundations of Measurement Systems Analysis
- Effects of Variation on Process Decisions
- Statistical Properties of Measurement Systems
- The Statistical Properties of Measurement Systems
- Sources of Variability
- Effects of Variation on Capability Indices
- Discrimination & Uncertainty
- Understanding Discrimination and its Effects
- Understanding Uncertainty
- Bias, Linearity and Stability
- Define Reference Value
- Describe and Analyze Bias
- Breakout Exercise 1: Calculating Bias
- Describe and Analyze Uncertainty
- Breakout Exercise 2: Bias & Linearity
- Describe and Analyze Stability
- Breakout Exercise 3: Stability
- GRR Studies
- Define GRR
- Describe and Analyze GRR (Repeatability and Reproducibility)
- Breakout Exercise 4: Graphing GR&R
- Breakout Exercise 5: Calculating GR&R
- Describe Acceptance Guidelines for GRR and ndc

Contact

Global Headquarters

Omnex Inc.,
315 E. Eisenhower Parkway,
Suite 214,
Ann Arbor, MI 48108.
Phone: (734) 761-494
Fax: (734) 761-4966
Email: info@omnexus.com
www.omnexus.com

Omnex Canada

 info-ca@omnexus.com

Omnex China

 info-cn@omnexus.com

Omnex Europe

 info-eu@omnexus.com

Omnex India

 info-in@omnexus.com

Omnex Malaysia

 info-my@omnexus.com

Omnex Mexico

 info-mx@omnexus.com

Omnex Middle East

 info-me@omnexus.com

Omnex Saudi Arabia

 info-sa@omnexus.com

Omnex Singapore

 info-sg@omnexus.com

Omnex Thailand

 info-th@omnexus.com