Automotive Cybersecurity Training (ACT) Program
Continuing Professional Education (CPE) Procedure

Table of Contents

1.0   Automotive Cybersecurity Training (ACT) Program

Automobile manufacturing is a vital element of U.S. critical infrastructure. Accordingly, its operation and technologies must be protected. At the same time, the industry's distinctive ecosystem imposes unique and specialized demands on the cybersecurity process. So, automobile manufacturers must implement and utilize specially tailored cybersecurity best practices. New international regulations further reinforce the fundamental importance of compliance with training and education requirements. The Automotive Cybersecurity Training (ACT) Program satisfies all these conditions. The ACT Program centers on a well-defined and commonly accepted set of practices to conceptualize, design, implement, and sustain practical automotive cybersecurity solutions. The Auto-ISAC and the National Highway Traffic Safety Administration (NHTSA) have supported the development of that content. Thus, it is the most authoritative view of industry practice. In addition, ACT program education satisfies the UNECE R155 requirement for formal cybersecurity training, which allows automotive organizations to comply with ISO/SAE 21434, Clause Five stipulations.

2.0   Intended Audience for the ACT Program

The ACT Program has two levels of instruction: 1) the Fundamental level provides a baseline of automotive cybersecurity knowledge and 2) the Advanced level is geared towards advanced hands-on training on components, software, hardware, and communications unique to the automotive industry.

3.0   Course Prerequisites

No experience. An individual must take six (6) courses. Must take Fundamentals – Basic Cybersecurity Module plus Fundamentals – Secure Engineering or Fundamentals – Secure Operations/Management, then complete all four (4) Advanced Courses. Courses must be taken in the order presented. No extra cost associated to sit for Capability Exercise/Exam (CAPEX).

Intermediate experience. Must take an Advanced Course Module to supplement existing knowledge before taking the CAPEX. No extra fees to sit for CAPEX.

Experienced Automotive and/or Cybersecurity Engineers, Managers, or Professionals. May take an Advanced Course Module to supplement existing knowledge. Eligible to sit for the CAPEX by paying $1,000.

4.0   ACT Program Fundamental Course Module

The audience for the fundamental group of the ACT Program comprises new hires, interns or co-op students, and employees transferring into an area where cybersecurity knowledge is necessary. ACT also helps increase the speed at which the industry can onboard new employees. These courses are all online and on demand. In that respect, anyone interested in building their knowledge of essential cybersecurity for the automobile industry can take them at their own pace and time and from anywhere globally.

The Basic Cybersecurity course is the first course required for the Certified Automotive Cybersecurity Engineer (CASE) pathway. Then the trainee may elect one of two pathways: Secure Engineering or Secure Operations/Management. The fundamental course module can be completed anywhere in the world at your own pace, and it meets the UNECE R155 regulation requirements. When completed, the trainee will receive a Certificate of Completion demonstrating proof of R155 compliance.

5.0   ACT Program Advanced Course Module

These one-week courses were developed working with the top experts from each area. Each class within the module is taught by an expert instructor in that subject matter. All trainers have done extensive work in

their teaching area. Because the ACT program will teach currently relevant topics, students will be asked to fill out surveys asking about potential relevant new topics and the ISAC will poll industry and form an annual advisory committee to review curricula to determine what changes should be made in courses for the following year. ACT courses follow explicit and commonly understood pathways that will fill in the gaps in their knowledge base and allow students to put into practice the lessons that they have learned in their training.

The advanced training courses are hands-on and in-person. The trainee will receive a Certificate of Completion after each course.

6.0   Certificate of Completion

Earning a certificate is a way for you to earn credits in a structured, discipline-specific way. A certificate can prepare you to advance in your career or gain the extra knowledge needed to stay competitive and up to date. Completing the certificate demonstrates evidence of specialized education achievement, as is the case with our ACT Program. Many professional certifications (traditional cybersecurity, project management, accounting) may be recommended or required. The courses you take in a certificate program help you prepare to earn a professional field-specific certification, but earning a certificate is not the same as becoming certified. A Certification of Completion is a result of training or education, while a Certification is the result of an assessment process that indicates mastery/competency measured against a standard which is normally an exam. Typically, when you receive a Certification, it results in a designation to use after one's name (CISSP, PMP, and our new CASE).

7.0   Capability Exercise/Exam (CAPEX)

The Capability Exercise/Exam is a scenario-based online exercise developed to test the knowledge, skills, and abilities of the trainees of the ACT Program. Passing this CAPEX allows the trainee to use the CASE designation. After completing the training, you can schedule your CAPEX, allowing 8 hours to complete the exercise.

8.0   Certified Automotive Cybersecurity Engineer (CASE)

The CASE designation attests to the holder's professional mastery of the field of automotive cybersecurity. The CASE certifies the holder's ability to develop and implement a comprehensive and practical response to cybersecurity threats and risks. The Automotive Information Sharing and Analysis Center (Auto-ISAC), in cooperation with the National Highway Transportation Safety Administration (NHTSA), underwrites this capability. In addition, the CASE endorses the holder's ability to adapt and sustain a coherent set of systematic best practices acquired through the applied training sequences of the ACT Program and completing the CAPEX. These practices ensure vehicular system development, operation, and maintenance integrity and security. This applies to every phase in the vehicle lifecycle. The ACT Program will serve as an officially sanctioned certification authority for the CASE. It will maintain a certification database of all individual certificate activity held current and up to date.

9.0   Continuing Professional Education (CPE) Requirements

Professionals must email / attest to the type of CPE activity they engaged in and the number of hours in email to ACT@automotiveisac.com. ACT Program Manager will update the CASE database upon receipt of CASE Holder's CPE activity and CASE Holders should verify their information is up to date at least annually.

Individuals holding this certification must keep their knowledge. This knowledge currency is represented by Continuing Professional Education (CPE) credits which are a rough gage of how closely a CASE holder

is continuing to be engaged with industry advances. The CPE currency requirements begin three (3) years after first achieving CASE Certification. Starting at the three (3) year mark, the CASE holder shall have 48 CPE credits accumulated over the past three (3) years. Each year on **June 15**, the ISAC's ACT Program will review the CPEs by CASE Holder and send an email to their last email address on file showing the number of CPEs on file. If a CASE holder has insufficient CPEs, the ACT Program will place a one (1) year probation period on that CASE Holder to allow time to return to compliance (i.e., 48 or more hours in the previous three (3) year period)). CPE values are assigned as follows:

1.) Attend a cybersecurity conference (e.g., BlackHat) = 0.5 CPE per hour spent in lectures

2.) Attend an automotive conference (e.g., ESCAR, or the Car Hacking Village from DEFCON) or attend an automotive cybersecurity lecture in a general conference = 1 CPE per hour spent in lecture or training

3.) Read a technical paper on automotive cybersecurity in a peer reviewed journal = 2 CPE

4.) Author an accepted technical paper for a peer reviewed journal = 10 CPE

5.) Give a presentation at an automotive cybersecurity event = 4 CPE per hour of lecture/presentation

6.) Develop corporate cybersecurity training = 2 CPE per target hour for the training

7.) Present at corporate brown bag or "lunch and learn" style training = 1 CPE per delivered talk

8.) Take a cybersecurity college course = 5 CPE per credit hour of course

9.) Attend automotive cybersecurity webinar training = 0.5 CPE per hour of webinar training

10.) Act as a mentor or trainer for STEM outreach or for junior engineers (e.g., volunteering at STEM events or running an after-hours mentoring session at work) = 0.5 CPE per two hours of outreach

10.0   ACT Program Certification Database

The ACT Program will serve as an officially sanctioned certification authority for the CASE. It will maintain a certification database of all individual certificate activity held current and up to date.

11.0   Failure to Meet Requirements

Failure to meet the CPE requirements will result in loss of CASE certification. The ACT Program Manager will notify the certification holder by email that his/her certification has been suspended.

ACT Program | Continuing Professional Education (CPE)

12.0   Revision History

Revision	Date	Description	Author	Approved
0	2023-09-14	Initial Issue	T. Bal	F. Francy