



З моменту створення перших автомобілів їх виробникам доводилося оперативно усувати найрізноманітніші проблеми для забезпечення безпеки і надійності своєї продукції. На початку двадцятого століття в США налічувалося вже кілька десятків автомобільних виробників. У зв'язку з цим, багато інженерів автомобільної індустрії висловили бажання мати «вільний обмін ідеями» з метою збільшення індивідуальної технічної бази. Так, в 1905 році, Ендрю Рікер очолив **Спільноту автомобільних інженерів (SAE)**, зі штатом всього в 30 працівників, і став її президентом.

Протягом перших 10 років членство спільноти неухильно росло, в штаті з'являлися молоді, талановиті інженери, які видавали технічні журнали і повну добірку технічної документації - SAE Транзакції, яка існує і сьогодні, але змінила свою назву на журнали SAE International.

В наші дні співтовариство налічує понад 121000 осіб - інженерів, керівників, викладачів і студентів більш ніж з 97 країн світу. Спільна дослідницька програма сприяє просуванню проектів, які приносять вигоду автомобільної індустрії в цілому. Численні зустрічі та виставки надають світові можливості для мережі SAE і інформацію. SAE також пропонує повний комплект заходів з професійного розвитку, таких як семінари, технічні симпозиуми і навчання в електронній формі.

Сьогодні SAE – це джерело технічної інформації і досвіду, використовуваного в розробці, виробництві, обслуговуванні і управлінні транспортних засобів для використання на землі або море, в повітрі або космосі.

Зараз, у зв'язку зі збільшенням кількості всередині машини електронних приладів, датчиків, а також підключених до інтернету систем автоматизованого управління все більш гостро постає питання з приводу забезпечення кібербезпеки автомобілів.

Тому нещодавно організацією був виданий новий стандарт **SAE J 3061-2016 (SAE J3061-2016) "Керівництво з кібербезпеки для кіберфізических систем транспортних засобів"**, адже експерти відзначають, що проблема кібербезпеки повинна залишатися в центрі уваги на всіх етапах життєвого циклу авто, перелік яких охоплює виробництво машин, їх експлуатацію, обслуговування і виведення з експлуатації.

Документ дозволить інженерам визначати і оцінювати потенційні кіберризики систем транспортних засобів з метою мінімізації ймовірності нанесення шкоди життю, майну або навколишньому середовищу. Якщо точніше, документ дозволяє виявляти потенційні загрози, пов'язані з експлуатацією, конфіденційністю, фінансами і репутацією.