

آینده خودروهای هوشمند و مستقل



صنعت خودروسازی یکی از معدود صنایعی است که فناوری دیجیتال هنوز نفوذ چندانی در آن نداشته است.

صنعت خودروسازی، یک، از معدود صنایع، است که فناور، دیجیتال، هنوز نفوذ چندانی در آن، نداشته است. درواقع اگر به مقایسه بسیاری از مدل های خودروهای فعلی با خودروهای 30 یا 40 سال قبل بپردازیم، می بینیم تنها برخی ویژگی های مکانیکی یا الکتریکی آنها بهبود یافته است و خبر چندانی از به کارگیری فناوری دیجیتال، بهره گیری از بانک های داده یا اتصال به شبکه های اطلاعاتی نیست.

با این حال به نظر می رسد این روند در حال تغییر است. اقبال غول های صنعت خودروسازی به فناوری دیجیتال از یک سو و نیز توجه برخی بزرگان دنیای دیجیتال نظیر گوگل به خودروسازی سبب شده شتاب اولیه ای برای ساخت خودروهای هوشمند ایجاد شود و حتی امیدهایی جدی برای ساخت خودروهای بدون نیاز به راننده شکل بگیرد. شاید تاکنون چیزهای مختلفی درباره کارکردهای خودروهای هوشمند خوانده باشید. برای نمونه توانایی تشخیص موانع یا عابر پیاده، امکان حرکت بین خطوط و شناسایی موانع در هوای مه آلود با استفاده از رادار های ویژه برخی توانمندی های خودروهای هوشمند است، اما این همه ماجرا نیست و مدیریت درون خودرو نیز از مهم ترین توانایی های خودروهای هوشمند البته در آینده ای نزدیک خواهد بود.

کنترل داخلی خودروها

مدتی است توجه بسیاری از کارشناسان خودروسازی به وجه دیگری از خودروهای هوشمند منعطف شده و آن هم تصویربرداری از وضعیت داخلی خودروست. در واقع شناسایی سرنشینان و تعریف مواردی خاص برای هر یک از آنها نه تنها می تواند ایمنی خودرو را افزایش دهد، بلکه جلوی بسیاری از مشکلاتی را که در خودروهای عادی رایج است، می گیرد.

به عنوان مثال می توان برای یک خودروی هوشمند، سامانه ای برای تشخیص چهره تعریف کرد تا تک تک اعضای خانواده را تشخیص دهد و گزینه های مشخصی را برای هر یک از آنها اجرا کند. می توان این سامانه را طوری برنامه ریزی کرد که اگر دختر نوجوان خانواده پشت فرمان بنشیند، در نهایت با حداکثر مشخصی از سرعت خودرو را براند و سیستم صوتی خودرو نیز دارای حداکثر مشخصی از صدا خواهد بود. همچنین می توان حداکثر سرعت برای پسر نوجوان خانواده را به مراتب کمتر انتخاب کرد. یکی دیگر از کاربردهای سامانه تشخیص چهره، امکان تعریف حرکاتی خاص برای توانمندی های مختلف خودروست.

برای نمونه با حرکت دادن دست به سمت راست، سیستم صوتی خودرو، فایل موسیقی بعدی را پخش کند یا با حرکتی دیگر، صدا را پایین آورد یا آن را خاموش کند. همچنین با تعریف ارتباط بین دوربین درون خودرو و نیز ابزارک ویژه تلفن همراه می توان از هر جایی، داخل خودرو را مشاهده کرد و اطلاعاتی درباره سرعت یا موقعیت آن یافت. بی تردید افزودن این توانمندی ها در خودروهای هوشمند موجب شکل گیری و رشد حوزه ای جدید در فناوری دیجیتال می شود که شاید نتایج مثبتی برای مجموعه فناوری های دیجیتال داشته باشد.

رونق کسب و کار سازندگان سخت افزار دیجیتال

بسیاری از کارشناسان بر این باورند که تا حدود 15 سال دیگر، شاهد خودروهای کاملاً مستقل از راننده نخواهیم بود. با این که طراحی نرم افزاری سامانه های مختلف این خودروها کاری بسیار پیچیده و زمانبر است، اما نباید از جنبه سخت افزاری این مساله غافل شد.

گزارشی جدید نشان می دهد تا حدود پنج سال دیگر، بازار میکروکنترلرها و پردازنده ها از 69 میلیون دلار در سال جاری با رشدی 635 درصدی به بیش از نیم میلیارد دلار خواهد رسید.

گوگل و برخی دیگر از سازندگان خودروهای رباتیک قرار است تا حدود سال 1398 خورشیدی نمونه هایی از خودروهای بدون راننده بسازند، اما این خودروها محدودیت هایی دارند. برای نمونه همه آنها با سرعتی پایین و در مناطقی که نقشه دقیق آنها تهیه شده است و مقامات دولتی نیز با حضور آنها در این مناطق موافقت کرده اند در خیابان ها و جاده ها به صورت خودکار رانده می شوند.

فعالان خودروسازی معتقدند برای ساخت خودروهای مستقل و بدون راننده، به پردازنده هایی با سرعت و تعداد هسته های بیشتر نیازمندیم. در واقع پردازش حجم زیادی از داده ها به توان پردازشی بالایی نیاز دارد که باید پاسخی مناسب برای آن یافت.

نیازهای سخت افزاری خودروهای هوشمند تنها به پردازنده های قوی تر خلاصه نمی شود. ذخیره اطلاعات انبوهی که خودرو دریافت می کند داستان دیگری است که باید به طور جدی مورد توجه قرار گیرد. در خودروهای هوشمند آینده، هر لحظه حجم زیادی از داده ها نظیر علائم رانندگی و نیز نقشه و شرایط جاده ها وارد سامانه خودرو می شود. تامین حجم مناسب برای ذخیره

این حجم بالا از اطلاعات، نیازمند سخت افزارهای مناسب است که باید فکری به حال آن شود. همه این نیازمندی های سخت افزاری نشان می دهد در آینده شاهد حضور پررنگ تر صنایع ساخت تراشه و سخت افزارهای مختلف در حوزه خودروسازی باشیم و صدا البته، شاید سودآوری این بخش موجب رونق گرفتن سرمایه گذاری و نوآوری برای بهبود کارکرد سخت افزارهای موجود شود. با این که خودروهای هوشمند مزایای زیادی برای ما به همراه خواهد داشت، اما همانند هر فناوری دیگری، خطراتی نیز در برابرمان ایجاد می کند. در واقع این حوزه از فناوری نیز از گزند خرابکاران و افراد سوءاستفاده گر محفوظ نمی ماند.

خودروهای هوشمند و نگرانی های آن

در چند سال اخیر مدل های مختلف خودروهای مجهز به فناوری های مختلف تشخیصی و ارتباطی طراحی و به بازار عرضه شده اند، اما یکی از نگرانی هایی که همیشه با تجهیزات دیجیتال همراه است، ترس از هک شدن آنهاست.

هک شدن یک خودرو، تفاوتی اساسی با هک شدن رایانه شخصی دارد. برای نمونه، در صورت آسیب پذیر بودن مرورگر اینترنت یا دیگر برنامه های تحت وب، ممکن است هکری به اطلاعات ذخیره شده روی سیستم یا اطلاعاتی نظیر شماره کارت اعتباری که هنگام خرید از یک فروشگاه اینترنتی وارد می کنید، دست یابد؛ اما ورود هکرها به سیستم داخلی خودرو می تواند پیامدهای وخیم تری همراه داشته باشد. برای نمونه هکرها می توانند موقعیت شما را به صورت آنی پایش کرده و حتی کنترل برخی کارکردهای خودرو نظیر شتاب یا ترمز را در دست گیرند. همین تفاوت در تبعات هک شدن خودروست که بسیاری از صاحبان یا متقاضیان این خودروها را نگران می کند. به همین منظور، خودروسازان و بویژه سازندگان خودروهای لوکس، توجه ویژه ای به مساله امنیت سامانه های دیجیتال خود دارند، اما چه خودروهایی در برابر هک شدن آسیب پذیرترند؟

برای پاسخ به این پرسش، تیمی از پژوهشگران به بررسی 21 مدل از خودروهای هوشمند ساخته شده در سال های اخیر پرداختند. به این منظور، سه جزء اصلی حمله به این سامانه ها یعنی شیوه ورود، تجهیزاتی که می تواند هک شود و نیز نتیجه هک مورد بررسی قرار گرفت. در این بررسی، اطلاعات خودرو که از سوی سازندگان اعلام شده بود مورد آزمون قرار گرفت و هیچ گونه اقدام عملی برای هک کردن سیستم های این خودروها انجام نشد.

نتیجه این بررسی نشان داد سه خودروی جیب چروکی 2014، کادیلاک اسکلید 2015 و اینفینیتی کیو 50، بیشترین آسیب پذیری را در برابر هک احتمالی داشتند.

اصلی ترین دلیل هک شدن خودروهای هوشمند را باید در ارتباطات مختلفی که بین خودرو و بخش های مختلف درونی و نیز دیگر تجهیزات بیرونی آن وجود دارد، دانست. در بسیاری از این خودروهای هوشمند، ارتباط از طریق خطوط تلفن همراه، ارتباطات بلوتوثی و نیز ارتباطات رادیویی وجود دارد. همچنین برنامه های مختلفی برای تلفن همراه و نیز خودرو نوشته شده است. همه اینها زمینه ای برای هک شدن بخش های مختلف خودرو را فراهم می کند. در میان این 21 خودروی مورد بررسی قرار گرفته، سه خودروی داج وایپر 2014، آئودی 8 ای و هوندا آکورد 2014، از بیشترین امنیت در برابر احتمال هک برخوردار بودند. برای نمونه خودروی آئودی 8 ای نه تنها راه های ارتباطی (بلوتوث و ارتباطات رادیویی) از بخش های حساس و مهم (نظیر هدایت خودرو، ترمز و شتاب) توسط خودروساز مجزا شده است، بلکه هر یک از آنها روی شبکه ای متفاوت کار می کنند و به این ترتیب در صورت نفوذ از طریق راه های ارتباطی، امکان در دست گرفتن بخش های مهم و حساس خودرو به شکل همزمان وجود ندارد. به هر حال به نظر می رسد با طراحی دقیق سیستم های مختلف داخلی و خارجی خودرو و پیش بینی رفتار نفوذگران می توان تا حد زیادی امنیت این خودروها را تامین کرد.

صالح سپهری فر / منبع: MSN