FREE Download www.aiworld.be

aiworld

Artificial Intelligence UPDATE

Machine Learning - Deep Learning - Software Research
Products - Technology - Applications - Industry News

AI World is a Global Publication of e2mos

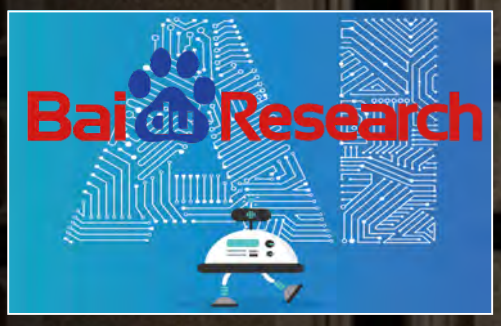
Q2-2017

■ Cybersecurity's Next Frontier: 80+ Companies Using AI To Secure The Future

■ NVIDIA Tesla P100 15.3 billion Transistor GPU

Most Advanced Datacenter Accelerator Ever Built
Featuring Pascal GP100, the World's Fastest GPU

■ ABB and IBM Partner in Industrial AI Solutions



■ AI Agent with Human-like Language Acquisition in a Virtual Environment

■ Security Issues Could Still Crimp the Self-Driving Car

■ Levels of Driving Automation in New SAE Standard J3016

In this Edition

Daniel Dierickx
CEO & co-Founder
at e2mos
Acting Chief Editor

Dear Reader,

Here is your free copy of **AI World**, one of our five e-magazines published by e2mos.

Our aim is to provide you with relevant information directly in relation with your activity.

Those magazines are part of the e2mos « Go-to-Market Platform »

This GLOBAL Platform is a UNIQUE Set of Services for Telecom ICT, Video Broadcast, Embedded Computing, IoT and AI Vendors from Multicore Chips to Application-ready Systems & Rack Space Servers.

Our WORLDWIDE Services include:
• Business Discovery
• Customer Meeting Setup
• Telemarketing
• Call Campaigns
• e-mailings Worldwide
• and our 5 e-magazines, each magazines has its own Website (see below).

It is all based on:
• 30+ Years Customer Relationship and Market & Technology Expertise
• our PREMIER Database started in 1980 and maintained EVERY DAY using many sources and research.

Thank you, Daniel Dierickx

Editor/Publisher:
e2mos www.e2mos.com
Contact mgt@e2mos.com

FREE just Click on the LOGO

aiworld
IoT World
Telecom COTS World
Broadband Broadcast IoT Convergence
Embedded Systems World
ATCA World

NVIDIA Tesla P100

The Most Advanced Datacenter Accelerator Ever Built Featuring Pascal GP100, the World's Fastest GPU

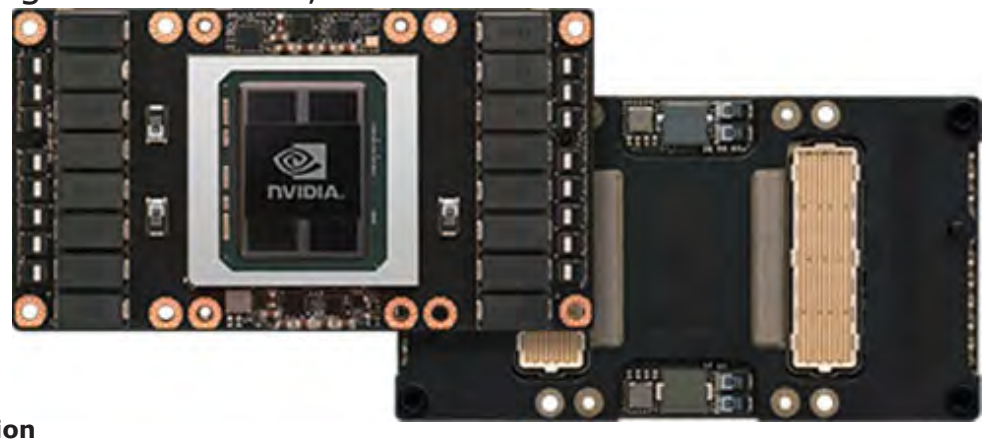


Figure 1.
NVIDIA Tesla P100
with Pascal GP100 GPU

Introduction

Nearly a decade ago, NVIDIA® pioneered the use of GPUs to accelerate computationally-intensive workloads with the introduction of the G80 GPU and the NVIDIA® CUDA® parallel computing platform. Today, NVIDIA® Tesla® GPUs accelerate thousands of High Performance Computing (HPC) applications across many areas including computational fluid dynamics, medical research, machine vision, financial modeling, quantum chemistry, energy discovery, and several others.

NVIDIA Tesla GPUs are installed in many of the world's top supercomputers, accelerating discovery and enabling increasingly complex simulations across multiple domains. Datacenters are using NVIDIA Tesla GPUs to speed up numerous HPC and Big Data applications, while also enabling leading-edge Artificial Intelligence (AI) and Deep Learning systems.

NVIDIA's new **NVIDIA Tesla P100** accelerator (see Figure 1) using the groundbreaking new **NVIDIA® Pascal™ GP100 GPU** takes GPU computing to the next level. This paper details both the Tesla P100 accelerator and the Pascal GP100 GPU architectures.

Also discussed is NVIDIA's powerful new DGX-1 server that utilizes eight Tesla P100 accelerators, effectively an AI supercomputer in a box. The DGX-1 is purpose-built to assist researchers advancing AI, and data scientists requiring an integrated system for Deep Learning.

Tesla P100: Revolutionary Performance and Features for GPU Computing

With a **15.3 billion transistor GPU**, a new high performance interconnect that greatly accelerates GPU peer-to-peer and GPU-to-CPU communications, new technologies to simplify GPU programming, and exceptional power efficiency, Tesla P100 is not only the most powerful, but also the most architecturally complex GPU accelerator architecture ever built.

Key features of Tesla P100 include:

DOWNLOAD THE WHITE PAPER

- **Extreme performance** Powering HPC, Deep Learning, and many more GPU Computing areas
- **NVLink™** NVIDIA's new high speed, high bandwidth interconnect for maximum application scalability
- **HBM2** Fast, high capacity, extremely efficient CoWoS (Chip-on-Wafer-on-Substrate) stacked memory architecture
- **Unified Memory, Compute Preemption, and New AI Algorithms** Significantly improved programming model and advanced AI software optimized for the Pascal architecture;
- **16nm FinFET** Enables more features, higher performance, and improved power efficiency

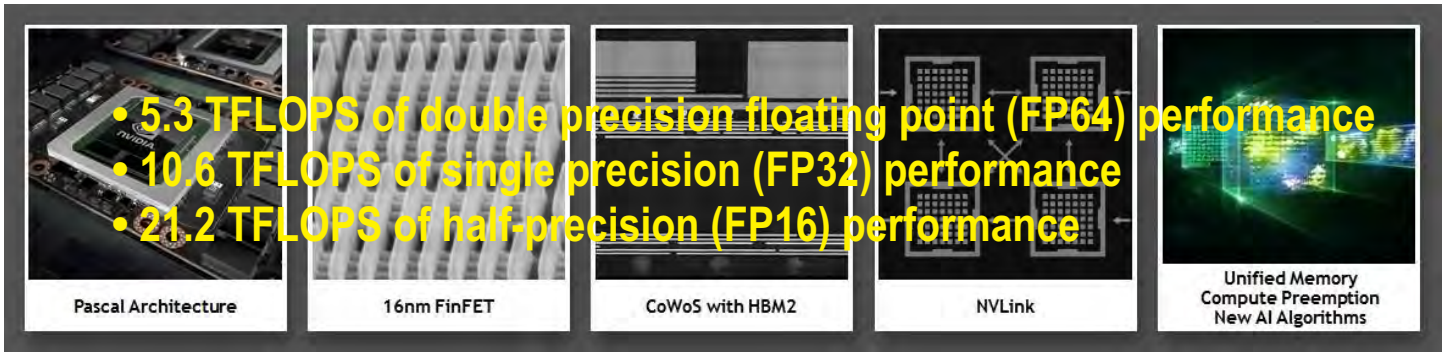


Figure 2. New Technologies in Tesla P100

An AI agent with human-like language acquisition in a virtual environment

March 29th, 2017 -- Despite tremendous progress, artificial intelligence is still limited in many ways. For example, in computer games, if an AI agent is not pre-programmed with game rules, it must try millions of times before figuring out the right moves to win. Humans can accomplish the same feat in a much shorter time, because we are good at transferring past knowledge to new tasks by using language.

In a game in which you must kill a dragon to win, an AI agent would need to try many other actions (firing at wall, a patch of flowers, etc) before understanding that it must kill the dragon. However, if the AI agent understood language, a human could simply use language to instruct it to: "kill the dragon to win the game."

Language, grounded in visuals, plays an important role in how we generalize skills and applying them to new tasks, an ability that remains a major challenge for machines. Developing a sophisticated language system is crucial for machines to become truly intelligent and gain the ability to learn like humans.

As the first step towards this goal, using a combination of supervised learning and reinforcement learning, we developed a system that allowed a virtual teacher to teach language to a virtual AI agent from scratch by connecting the language with perceptions and actions, just like a parent would teach their baby.

After the training, our results show the AI agent is able to correctly interpret the teacher's commands in natural language and take action accordingly. More importantly, the agent developed what we call a "zero-shot learning ability," meaning the agent is able to understand unseen sentences. The research, we believe, brings us one step closer to teaching machines to learn like humans do.

Study Overview

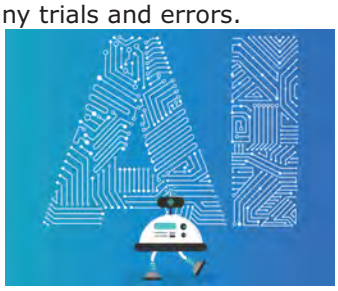
The study takes place in an 2D maze-like environment called XWORLD, where our virtual baby agent needs to navigate under the natural language command issued by a virtual teacher. In the beginning, the agent knows nothing about the language: every word is equally meaningless. However, as it explores the environment, the teacher gives positive (or negative) rewards if it succeeds (or fails) in executing a command. To help it learn faster, the teacher also asks some simple questions about the environment surroundings while the agent is navigating. The agent needs to correctly answer the questions. By encouraging correct actions/answers and penalizing incorrect ones for navigation/QA, the teacher trains the agent to understand natural language after many trials and errors.

Some example commands include:

- Please navigate to the apple.
- Can you move to the grid between the apple and the banana?
- Could you please go to the red apple?

Some example Q&A pairs are:

- Q:What is the object in the north? A:Banana.
- Q:Where is the banana? A:North.
- Q:What is the color of the object in the west of the apple? A:Yellow.

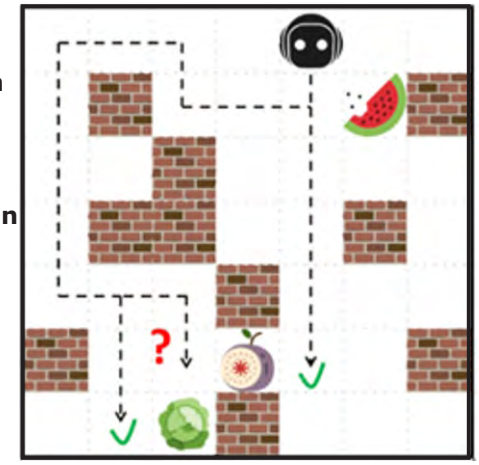


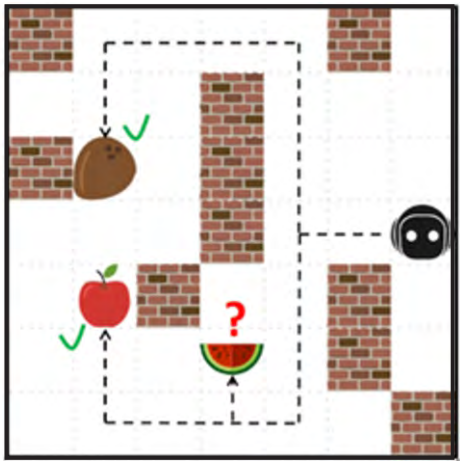
Results

In the end, the agent is able to correctly interpret the teacher's commands and navigate to the right places. More importantly, the agent develops what we call a "zero-shot learning ability." This means that even for a completely new command that was not previously seen, it is still able to correctly execute the task if enough sentences of a similar form were seen before. In other words, the agent is able to understand a new sentence assembled with known words in a known way (grammar).

For example, a human who has learned how to cut an apple with a knife will likely then know how to cut a dragon fruit with a knife. Applying past knowledge to a new task is very easy for humans but still difficult for current end-to-end learning machines. Although machines may know what a "dragon fruit" looks like, they can't perform the task "cut the dragon fruit with a knife" unless they have been explicitly trained with the dataset containing this command. By contrast, our agent demonstrated the ability to transfer what they knew about the visual appearance of a dragon fruit as well as the task of "cut X with a knife" successfully, without explicitly being trained to perform "cut the dragon fruit with a knife." **In the figures below, our agent successfully executed the commands in the navigation tests.**

Navigation Train
Please move to the west of cablage.
Please move to the east of fig.
Recognition Train
Q: What is in the southeast?
A: watermelon
Navigation Test
Please move to the west of fig.





Navigation Train
Could you please go to the coconut?
Could you please go to the apple?
Navigation Test
Could you please go to the watermelon?

Our next steps are two-fold: one is to teach the agent more abilities with natural language commands in the current 2D environment, and the other is to migrate it to a virtual 3D environment. A virtual 3D environment poses more challenges, and it is more like the realistic environment we live in. Our ultimate goal is to train a physical robot in a realistic environment by a human teacher with natural language.

To learn more, please read our paper CLICK HERE

ABB and IBM Partner in Industrial Artificial Intelligence Solutions

Combining ABB Ability and IBM Watson for Superior Customer Value

Hannover, Germany, - 25 Apr 2017: ABB and IBM (NYSE: IBM) today announced a strategic collaboration that brings together ABB's industry leading digital offering, ABB Ability TM, with IBM Watson Internet of Things cognitive capabilities to unlock new value for customers in utilities, industry, transport and infrastructure.

Customers will benefit from ABB's deep domain knowledge and extensive portfolio of digital solutions combined with IBM's expertise in artificial intelligence and machine learning as well as different industry verticals. The first two joint industry solutions powered by ABB Ability and Watson will bring real-time cognitive insights to the factory floor and smart grids.

At Hannover Messe, IBM and ABB announced a new partnership in industrial artificial intelligence that will combine the power of IBM Watson with ABB Ability, the comprehensive digital offering of ABB, to unlock new value for clients in utilities, industry, transport and infrastructure.

Pictured, Harriet Green, General Manager Watson IoT, Customer Engagement and Education, IBM; and Guido Jouret, Chief Digital Officer, ABB, discuss the future of cognitive and industrial machines.

"This powerful combination marks truly the next level of industrial technology, moving beyond current connected systems that simply gather data, to industrial operations and machines that use data to sense, analyze, optimize and take actions that drive greater uptime, speed and yield for industrial customers," said ABB CEO Ulrich Spiesshofer. "With an installed base of 70 million connected devices, 70,000 digital control systems and 6,000 enterprise software solutions, ABB is a trusted leader in the industrial space, and has a four decade long history of creating digital solutions for customers. IBM is a leader in artificial intelligence and cognitive computing. Together, IBM and ABB will create powerful solutions for customers to benefit from the Fourth Industrial Revolution."

New suite of breakthrough solutions

The new suite of breakthrough solutions developed by ABB and IBM will help companies address in a completely new way some of their biggest industrial challenges, such as improving quality control, reducing downtime and increasing speed and yield of industrial processes. These solutions will move beyond current connected systems that simply gather data, to cognitive industrial machines that use data to understand, sense, reason and take actions supporting industrial workers to help eliminate inefficient processes and redundant tasks.

... to next page

ABB and IBM Partner in Industrial Artificial Intelligence Solutions ... from previous page

"This important collaboration with ABB will take Watson even deeper into industrial applications -- from manufacturing, to utilities, to transportation and more," said Ginni Rometty, IBM Chairman, president and CEO. "The data generated from industrial companies' products, facilities and systems holds the promise of exponential advances in innovation, efficiency and safety. Only with Watson's broad cognitive capabilities and our platform's unique support for industries can this vast new resource be turned into value, with trust. We are eager to work in partnership with ABB on this new industrial era."

Bringing real-time cognitive insights to the factory floor

For example, ABB and IBM will leverage Watson's artificial intelligence to help find defects via real-time production images that are captured through an ABB system, and then analyzed using IBM Watson IoT for Manufacturing. Previously these inspections were done manually, which was often a slow and error-prone process. By bringing the power of Watson's real time cognitive insights directly to the shop floor in combination with ABB's industrial automation technology, companies will be better equipped to increase the volume flowing through their production lines while improving accuracy and consistency. As parts flow through the manufacturing process, the solution will alert the manufacturer to critical faults - not visible to the human eye - in the quality of assembly. This enables fast intervention from quality control experts. Easier identification of defects impacts all goods on the production line, and helps improve a company's competitiveness while helping avoid costly recalls and reputational damage.

Bringing real-time cognitive insights to smart grids

In another example. ABB and IBM will apply Watson's capabilities to predict supply patterns in electricity generation and demand from historical and weather data, to help utilities optimize the operation and maintenance of today's smart grids, which are facing the increased complexity created by the new balance of conventional as well as renewable power sources. Forecasts of temperature, sunshine and wind speed will be used to predict consumption demand, which will help utilities determine optimal load management as well as real-time pricing.

About ABB

ABB (ABBN: SIX Swiss Ex) is a pioneering technology leader in electrification products, robotics and motion, industrial automation and power grids, serving customers in utilities, industry and transport & infrastructure globally. Continuing more than a 125-year history of innovation, ABB today is writing the future of industrial digitalization and driving the Energy and Fourth Industrial Revolutions.
ABB operates in more than 100 countries with about 132,000 employees. www.abb.com

About IBM

For more information, please visit www.ibm.com/iot.

AMD Launches the World's Fastest Graphics Card for Machine Learning Development and Advanced Visualization Workloads, Radeon Vega Frontier Edition, Available Now

Cybersecurity's Next Frontier: 80+ Companies Using Artificial Intelligence To Secure The Future In One Infographic

Cybersecurity Market KEY REPORT from: CBINSIGHTS

CB Insights to identifies over 80 private cybersecurity AI companies and categorized them into 9 areas of operation.

Cybersecurity companies saw a record number of funding deals last year and on a quarterly basis Q1'17 was the most active quarter for deals to private cybersecurity companies over the last five years. Alongside overall rising investment activity, a number of cybersecurity companies are emerging to offer up novel solutions to cyber threats by leveraging the advantages of artificial intelligence (AI).

According to CB Insights' AI Deals Tracker, cybersecurity is the fourth most active industry for deals to companies applying AI.

We used CB Insights data to identify over 80 private companies in cybersecurity that are using AI and categorized them into the nine main areas in which they operate. Two unicorn companies valued at over $1B are included in the map: the automated endpoint protection company Tanium and the predictive intelligence company Cylance.

Category Breakdown

Anti Fraud & Identity Management: This is the most populated category within the cybersecurity AI market. Startups in this category mainly help secure online transactions by identifying fraudsters. For example, the company FeedZai utilizes machine learning algorithms to proactively detect fraud in financial transactions. Similarly, companies like Socure can detect fraudulent users on websites and in mobile applications also using machine-learning algorithms.

Mobile Security: Included in this category are startups such as Appthority, which provides a cloud-based platform that automatically identifies and grades risky behavior in mobile apps including known and unknown malware, new malware used in targeted attacks, corporate data ex-filtration, and intellectual property exposure. Similarly, Skycure's predictive technology leverages massive crowd knowledge to proactively identify threats to secure mobile devices.

Predictive Intelligence: Companies such as the unicorn company Cylance aim to couple sophisticated math and machine learning with a unique understanding of a hacker's mentality, and by doing so offer technology and services that are predictive and preventive against advanced cyber threats. Likewise, the company SentinelOne uses predictive execution modeling to detect and protect network devices against targeted, previously unknown threats in real time.

Behavioral Analytics / Anomaly Detection: Startups in this category include Darktrace which uses advanced mathematics and machine learning to detect anomalous behavior in organizations' systems and networks in order detect cyber-attacks. Unlike software that puts locks on doors, Darktrace's approach allows enterprises to protect their information and intellectual property from state sponsored, criminal groups or malicious employees who are already inside the network as well as from external attacks. Companies such as BehavioSec offer a behavioral biometric systems that creates digital fingerprints from an end-user's behavior through monitored keystrokes, mouse behavior, and anomaly detection to ensure security of IT organizations, e-commerce, and more.

Automated Security: Startups in this category include unicorn company Tanium, which couples an application of AI known as natural language processing with endpoint protection on a massive scale. Tanium empowers security and IT operations teams to ask questions about the state of every endpoint across the enterprise in plain English, automatically retrieve data on their current and historical state, and execute change as necessary within seconds. Other companies include Demisto which offers systems that are designed to automate security tasks across 100+ security products and weave human analyst activities and workflows together.

Cyber-Risk Management: Companies in this category range from cyber-insurance oriented companies to those that are security policy and compliance focused. For example, Cyence empowers the insurance industry to understand the impact of cyber risk in the context of dollars and probabilities. Other companies include Cybersaint, which offers solutions for streamlining the cyber-risk compliance process. Slightly different, but still within the business of managing cyber risk is the company Wiretap, which helps secure enterprise social networks, as well as collaboration tools, by securing against intellectual property and confidential data leaks, insider threats, HR policy violations, compliance issues, and external sharing risks.

... to next page

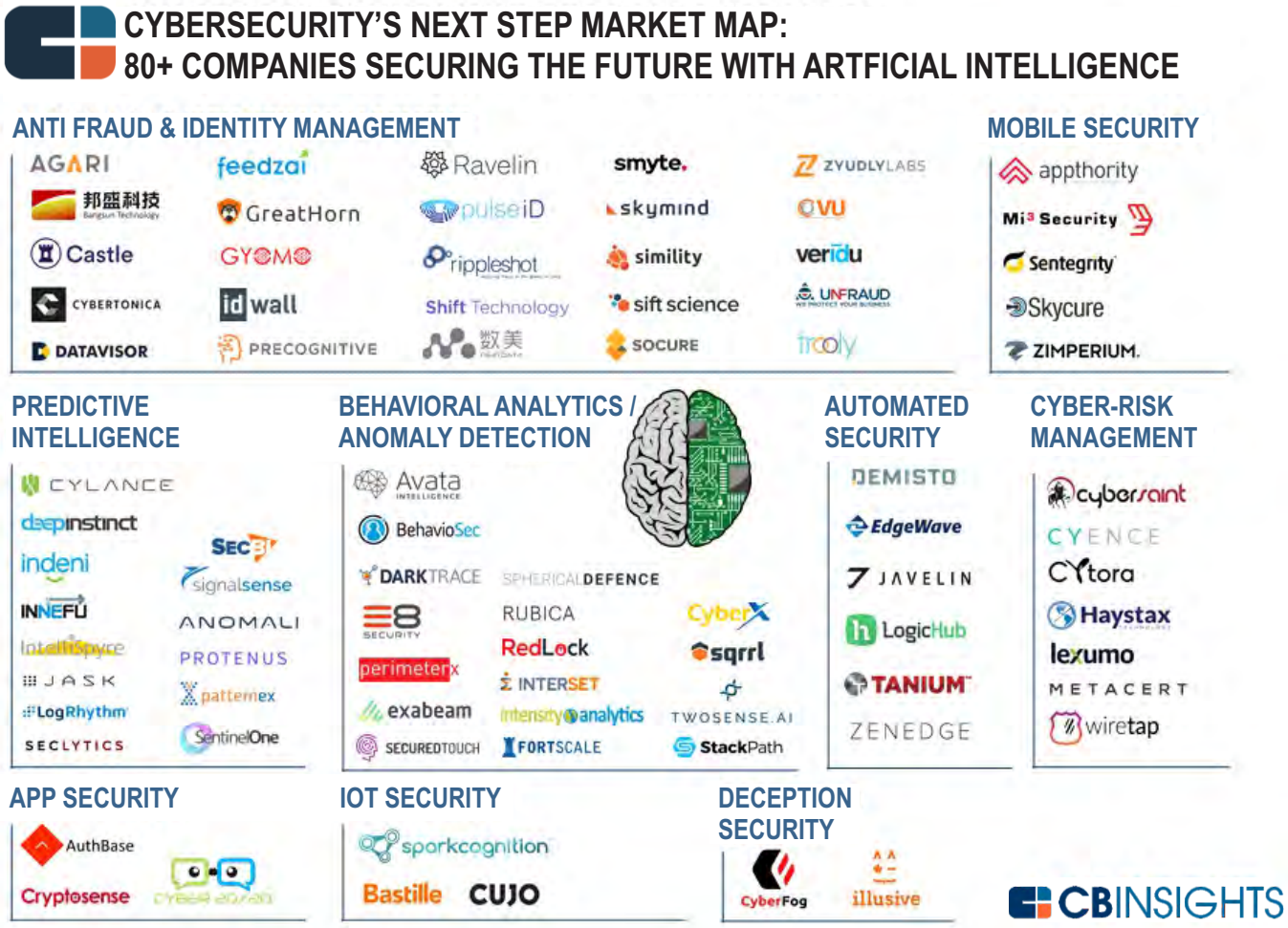
Cybersecurity's Next Frontier: 80+ Companies Using Artificial Intelligence To Secure The Future In One Infographic

... from previous page

App Security: Companies in this category are focused on securing specific enterprise applications rather than entire networks. This includes both web-based and dev-ops oriented applications, and more. This category includes companies such as Authbase, which provides frameworks to help developers secure applications by finding, fixing, and monitoring web, mobile, and networks against current and future vulnerabilities; the company Cryptosense, whose software employs a unique mix of formal analysis and machine learning to find security flaws in cryptographic systems; and Cyber 20/20, which monitors network traffic for suspicious activity within applications and automatically submits them to a machine learning platform, where they are analyzed and shown to be malicious or not.

IoT Security: These startups include SparkCognition, which develops AI-powered asset-protection software for the safety, security, and reliability of the IoT. Bastille Networks utilizes machine learning algorithms to secure the IoT on corporate campuses by identifying airborne threats such as hidden recording devices or transmitters in a conference room, and allow for a preemptive response to data theft. CUJO is a smart firewall that protects a user's connected home from criminal hackers by using a combination of cloud services, machine learning, and mobile apps to manage the network.
Deception Security: illusive networks provides solutions that combat Advanced Persistent Threats by proactively deceiving and disrupting in progress attacks. CyberFog (dba CyberSwarm) offers a deception tool that detects and fights cyber attacks by creating a neural network of thousands of fake computers, devices, and services that act like a fog and work under the supervision of machine learning algorithms.

MARKET MAP



80+ Companies List:
including Web Link, Phone, Country (Headquarters), ... sent request to mgt@e2mos.com

Security Issues Could Still Crimp the Self-Driving Car

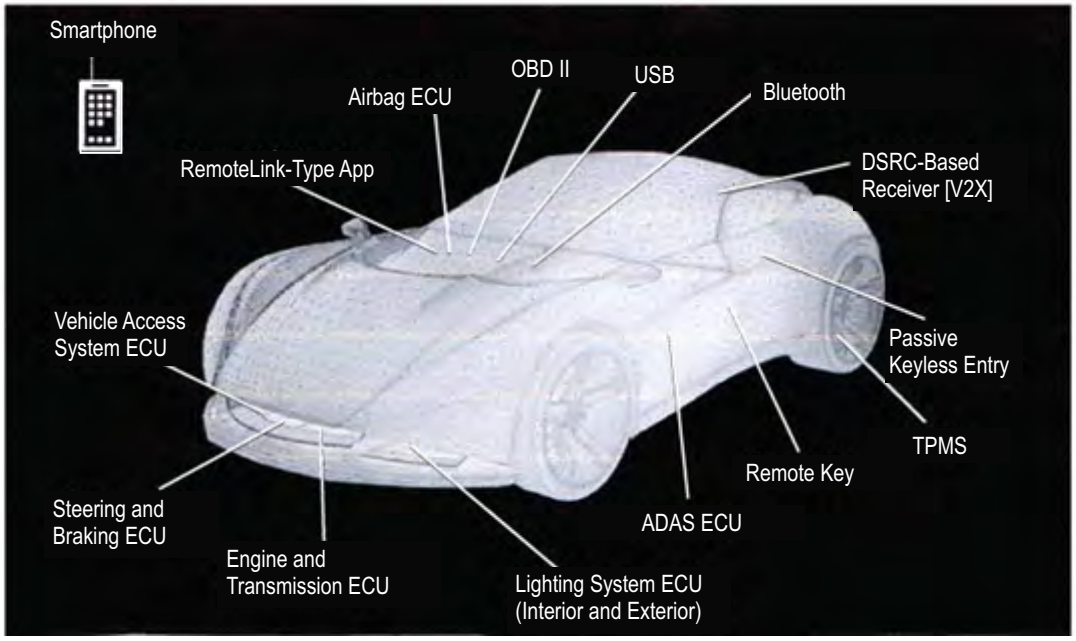
For automakers, addressing cybersecurity vulnerabilities in autonomous cars is Job 1.

Murray Slovick | Jun 28, 2017

Major auto manufacturers, high-tech companies, and startups whose names we're not familiar with all are putting in overtime trying to solve an unprecedented problem accompanying development of the self-driving car: cybersecurity holes that could lead to potentially fatal safety issues.

To borrow a slogan used in1982 by the Ford Motor Company, at the time discussing build quality: For the self-driving car, maintaining the security and integrity of on-board systems is "Job 1."
The potential danger was demonstrated in 2015 when, as part of a research initiative, two hackers remotely took control of a Jeep Cherokee. Afterward Chrysler issued a formal recall of 1.4 million vehicles that may have been affected by the hackable software vulnerability.

One of the central challenges in vehicle cybersecurity is that the various electronic control units (ECUs—cars today have dozens of them) are connected by means of an internal network. So if hackers manage to gain access to a vulnerable ECU (say, the infotainment system), there is concern they may be able to take control of ECUs managing the engine or brakes.



There are 15 main hackable points in the next-generation car.

Earlier this week, the French company Vedecom Tech—a commercial subsidiary of Vedecom Public Foundation, whose members include Renault, Peugeot, and Valeo—said the completely autonomous, self-driving vehicles (SAE Level 5) it plans to launch for commercial use in 2017 and 2018 in municipalities in France, Germany, Italy, Portugal and the Netherlands would represent the first cyberattack-secured, commercially-available automobiles.

Vedecom will be using Israeli startup Karamba Security's Carwall software to protect the cars' ECUs against hacking. Karamba said its security tool is OS- and hardware-agnostic and can run on every ECU, without requiring any changes or upgrades to the ECU's software or hardware. The company further noted that it operates reliably on the ECU without interfering with any of its other functions.

Software from Karamba Security hardens the ECUs of this autonomous car.
Carwall's patent-pending software is embedded during the ECU's software build process. It automatically learns the factory settings, which are the legitimate programs, scripts, and function-calling sequences car manufacturers and tier-one system providers intend to run in the car.

Carwall then creates a control flow graph of all acceptable function call paths showing the calling relationship within a computer program. It then forms a security policy that detects and prevents any deviation from those settings. All detection and prevention decisions are made locally.

When a function call is made, Carwall checks it, in runtime, against the function call map it created during the build process. If the function call hasn't followed a legitimate path, Carwall will not let it execute, since a hacker may have infiltrated a process in the ECU's memory.

... to next page

Security Issues Could Still Crimp the Self-Driving Car

... from previous page

Because Carwall seals the ECU's software, security bugs contained in that code are also hardened, so they can't be exploited to infiltrate the car's safety systems. No malware updates are required, and the ECU is said to be fully capable of protecting itself against potential hacks at all times without any required external connectivity. Karamba Security further claimed there should be no false positives that mistakenly block legitimate vehicle commands.

In the background of cybersecurity issues is the question of what role (if any) government should play in regulating self-driving cars. Most companies, like people, don't like it when government decides to micromanage things. Nevertheless, the regulations game appears to be heating up.

Last week the U.S. Senate Commerce, Science, and Transportation Committee released bipartisan principals for self-driving vehicle legislation. Authored by U.S. Senators John Thune (R-S.D.), Gary Peters (D-Mich.), and Bill Nelson (D-Fla) these principles state that any proposed legislation must:

• Consider both the near-term and long-term regulatory oversight of these vehicles, recognizing that new safety standards governing self-driving vehicles should eventually be set.

• Allow the life-saving safety benefits of self-driving vehicle technology to move forward as new standards development is underway.

• Find ways to preserve and improve safety while addressing incompatibility with old rules that were not written with self-driving vehicles in mind.

• Be technology neutral and avoid favoring the business models of some developers of self-driving vehicles over others.

• Clarify the responsibilities of federal and state regulators to protect the public and prevent conflicting laws and rules from stifling this new technology.

• Address the connectivity of self-driving vehicles and potential cybersecurity vulnerabilities before they compromise safety.

• Review consumer education models for self-driving vehicles and address how companies can inform the public on what self-driving vehicles can and cannot do based on their level of automation and their individual capabilities.

Eighteen states and Washington D.C. have passed legislation related to autonomous vehicles. The legislation ranges from creating a committee to study self-driving cars (Alabama) to letting fully autonomous vehicles on the road without a driver (Florida).

Given that self-driving cars collect large amounts of data, there's also government anxiety about privacy and how the data will be stored and used. But the main point of concern remains: Unless self-driving vehicles are proven to be highly secure against cyberattacks, many other states will attempt to regulate their development.

Uncle Sam will, too.

A.I. World Editor Note

This article « Security Issues Could Still Crimp the Self-Driving Car » was first published by Electronic Design (Penton) on Jun 28, 2017 and written by Murray Slovick, Principal at IntelligentContent Services.

We received this article with an invitation to e-mail it to friends and colleagues, here on page 8 and 9.

This article is quite interesting for the « Autonomous Vehicles Market Opportunities »

The question is: who will buy a Self-Driving Car, why and how much are potential customers prepared to pay.

May be not very much in our time!

Daniel Dierickx, e2mos

PS: see also AUTOMATED DRIVING by SAE International page 11 and 12

AUTOMATED DRIVING

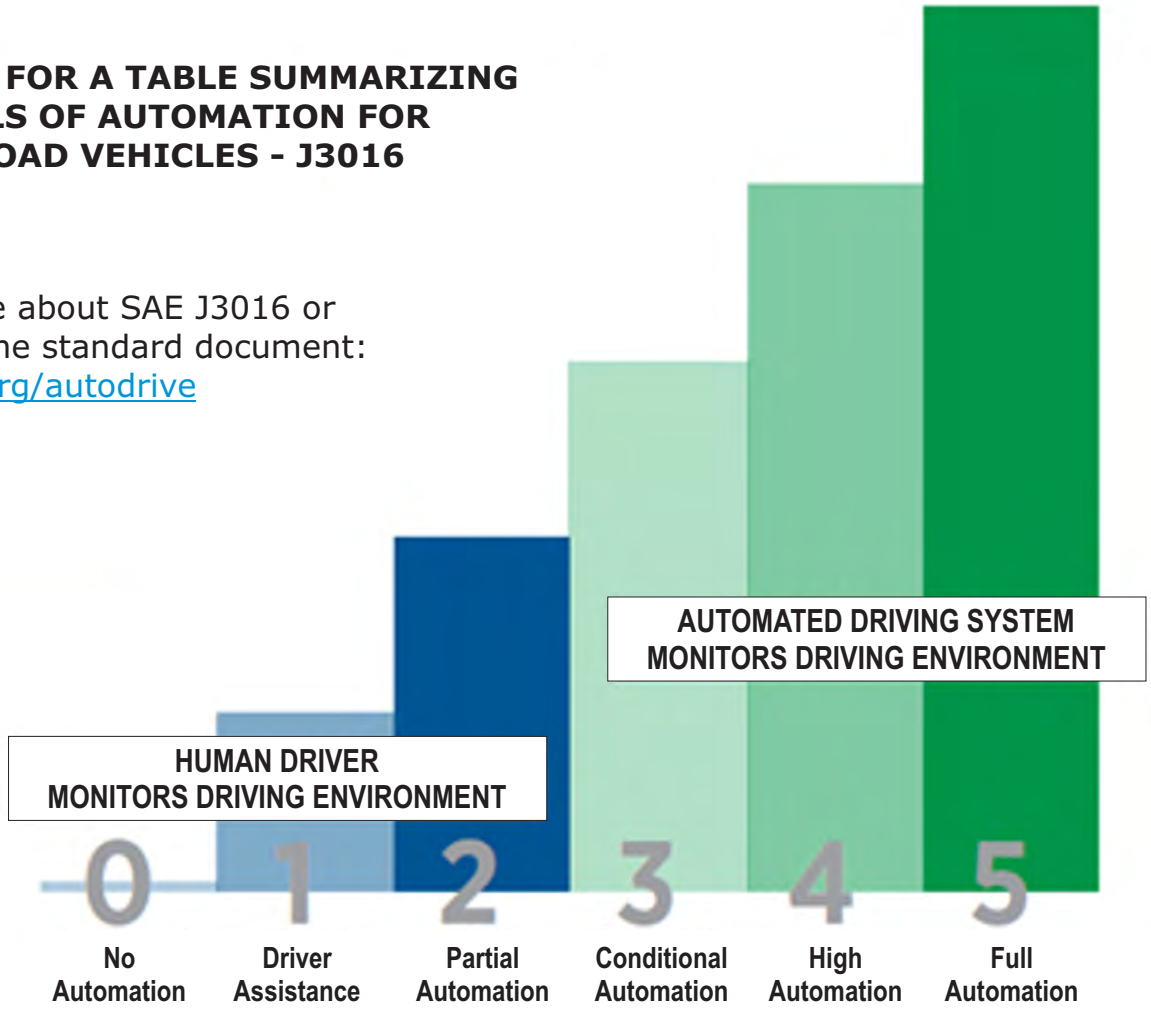
LEVELS OF DRIVING AUTOMATION ARE DEFINED IN NEW SAE INTERNATIONAL STANDARD J3016

With the goal of providing common terminology for automated driving, SAE International's new standard J3016:
Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, delivers a harmonized classification system and supporting definitions that:

- Identify six levels of driving automation from "no automation" to "full automation".
- Base definitions and levels on functional aspects of technology.
- Describe categorical distinctions for a step-wise progression through the levels.
- Are consistent with current industry practice.
- Eliminate confusion and are useful across numerous disciplines (engineering, legal, media, and public discourse).
- Educate a wider community by clarifying for each level what role (if any) drivers have in performing the dynamic driving task while a driving automation system is engaged.

OVER FOR A TABLE SUMMARIZING LEVELS OF AUTOMATION FOR ON-ROAD VEHICLES - J3016

Learn more about SAE J3016 or purchase the standard document:
www.sae.org/autodrive



... to next page

Summary of SAE Internatio nal's Levels of Driving Automation for On-Road Vehicles

... from previous page

Issued January 2014, **SAE international's J3016** provides a common taxonomy and definitions for automated driving in order to simplify communication and facilitate collaboration within technical and policy domains. It defines more than a **dozen key terms**, including those italicized below, and provides **full descriptions and examples** for each level.

The report's **six levels of driving automation** span from no automation to full automation. A n**key distinction** is between level 2, where the *human driver performs part of the dynamic driving task, and level 3, where the automated driving system performs the entire dynamic driving task.*

These levels are **descriptive** rather than normative and **technical** rather than legal. They imply **no particular order** of market introduction. Elements indicate **minimum** rather than maximum system capabilities for each level. A particular vehicle may have multiple driving automation features such that it could operate at **different levels** depending upon the feature(s) that are engaged.

System refers to the driver assistance system, combination of driver assistance systems, or *automated driving system*. **Excluded** are **warning and momentary intervention systems**, which do not automate any part of the dynamic driving task on a sustained basis and therefore do not change *the human driver's role in performing the dynamic driving task.*

SAE level	Name	Narrative Definition	Execution of Steering and Acceleration/ Deceleration	*Monitoring* of Driving Environment	Fallback Performance of *Dynamic Driving Task*	System Capability *(Driving Modes)*
***Human driver* monitors the driving environment**						
0	**No Automation**	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	**Driver Assistance**	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes
2	**Partial Automation**	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/ deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	**System**	Human driver	Human driver	Some driving modes
***Automated driving system* ("system") monitors the driving environment**						
3	**Conditional Automation**	the *driving mode*-specific performance by an *automated driving system* of all aspects of the dynamic driving task with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	**System**	Human driver	Some driving modes
4	**High Automation**	the *driving mode*-specific performance by an automated driving system of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	**System**	Some driving modes
5	**Full Automation**	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	**All driving modes**

Key definitions in J3016 include (among others):

Dynamic driving task includes the operational (steering, braking, accelerating, monitoring the vehicle and roadway) and tactical (responding to events, determining when to change lanes, turn, use signals, etc.) aspects of the driving task, but not the strategic (determining destinations and waypoints) aspect of the driving task.

Driving mode is a type of driving scenario with characteristic dynamic driving task requirements (e.g., expressway merging, high speed cruising, low speed traffic jam, closed-campus operations, etc.).

Request to intervene is notification by the automated driving system to a human driver that s/he should promptly begin or resume performance of the dynamic driving task.

Contact: SAE INTERNATIONAL +1.724.776.4841 • Global Ground Vehicle Standards +1.248.273.2455 • Asia+86.21.61577368