ITS セキュリティ

Mon, 09/23 11:15AM · 76mins

AI Notes

Transcript

Mr. Sikora 00:00
And our vehicle at the moment is following a track, and if needed, and the track is consistently working, the vehicle does not need to communicate with somebody else. Just get the information where it is and where it has to go.
そして、現在、私たちの車両は線路をたどっており、必要に応じて、線路が一貫して機能しているため、車両は他の誰かと通信する必要はありません。情報がどこにあり、どこに行かなければならないかという情報を入手してください。

Mr. Sikora 00:22
So I was wondering, this would be the ideal one, but then coming on to what's nevertheless possible to attack it. And I tried to do a clustering, starting with what's possible, it's a physical attack.
だから、これが理想的なものだろうと思っていましたが、それでもそれを攻撃する可能性のあるものについて考えました。そして、クラスタリングを試みましたが、まず可能なのは物理的な攻撃です。

Mr. Sikora 00:43
We often forget that it's possible to just enter a vehicle, then open the vehicle's command center and do changes. So this is what I mean, unauthorized physical access to temper with hardware components.
私たちはしばしば、車両に乗り込み、車両のコマンドセンターを開いて変更を行うことが可能であることを忘れています。つまり、ハードウェアコンポーネントでテンパリングするための不正な物理的アクセスです。

Mr. Sikora 01:03
That's one way. And the best way to avoid this is to secure the physical interfaces. Maybe you can rely on a private interface that is not available elsewhere, generate an interface, a physical interface that needs additional information to get inside.
それも一つの方法です。そして、これを回避する最善の方法は、物理インターフェイスを保護することです。たぶん、他の場所では利用できないプライベートインターフェイスに依存して、インターフェイス、つまり内部に入るために追加情報が必要な物理インターフェイスを生成できます。

Mr. Sikora 01:31
Then temper -proof hardware design, make sure that the doors are always locked and cannot be easily opened. Things like that, that's it. That's about physical attacks. Then sensor manipulation, it's a physical thing, a physical attack, as well as possible with autonomous shuttles.
次に、テンパープルーフハードウェア設計で、ドアが常にロックされ、簡単に開けられないことを確認します。そんな感じ、それだけです。それは物理的な攻撃についてです。次に、センサーの操作は、物理的なもの、物理的な攻撃であり、自律型シャトルで可能なことです。

Mr. Sikora 01:51
We have, at the moment, six sliders and some cameras to look at the environment. And we have additional. systems for localization and all these sensors can be tempered and what we experienced right now in the project in Finland, which is close to Russia, that's the GPS signal is no longer accurate enough.
現在、6つのスライダーといくつかのカメラで環境を観察することができます。そして、私たちは追加しています。ローカリゼーションのためのシステムやこれらすべてのセンサーはテンパリングすることができますが、ロシアに近いフィンランドでのプロジェクトで今経験したことは、GPS信号がもはや十分に正確でないということです。

Mr. Sikora 02:18
So we need to find a way to overcome this situation. There's augmentation systems to do that and there's other way. I don't want to go into detail but this is a real threat. And then what we might forget sometimes, it's supply chain tech.
ですから、この状況を克服する方法を見つける必要があります。そのための増強システムもあれば、他の方法もあります。詳しくは触れた

くありませんが、これは本当の脅威です。そして、私たちが時々忘れてしまうかもしれないのは、サプライチェーン技術です。

Mr. Sikora 02:40
We are not doing everything alone, we are just putting things together where we need to rely on our supply chain that the equipment that we buy in is tech -approved. It's cyber security -proof and we need to ask our certificates to get that.
私たちはすべてを一人で行っているわけではなく、購入する機器が技術承認されているというサプライチェーンに頼る必要があるところをまとめているだけです。これはサイバーセキュリティに優れているため、証明書を取得する必要があります。

Mr. Sikora 03:03
Yeah, let me go to wireless attacks. And I wanted to cluster it into two different classes as well. The wireless attacks can be unidirectional, so just somebody wants to enter the vehicle or bidirectional where somebody wants to enter the vehicle and get something in return.
はい、無線攻撃に行かせてください。そして、それを2つの異なるクラスにクラスター化したかったのです。無線攻撃は一方向の場合があるため、誰かが車両に侵入したい場合もあれば、誰かが車両に侵入して見返りを得たい双方向の場合もあります。

Mr. Sikora 03:30
So the first one is the very common attack, denial of service attack, or distributed denial of service attack where a lot of different messages come together and try to make the system, try to avoid to make the system work anymore.
ですから、最初の攻撃は、非常に一般的な攻撃、サービス拒否攻撃、または分散型サービス拒否攻撃で、多くの異なるメッセージが集まってシステムを作ろうとし、システムが機能しないようにしようとします。

Mr. Sikora 03:54
So this is one thing, and there's one thing what we are looking at. For example, there's one message on V2X communication, which is a broadcast message. It can come as a bulk of messages and we need to work on that.
ですから、これは一つのことであり、私たちが見ているものが一つあります。たとえば、V2X 通信にはブロードキャスト メッセージというメッセージが 1 つあります。それは大量のメッセージとして来る可能性があり、私たちはそれに取り組む必要があります。

Mr. Sikora 04:16
So this is one threat, and the other one is autonomous decision manipulation, where attackers manipulate inputs or environmental factors to influence the vehicle's decision-making algorithm. So this is unidirectional.
これが1つの脅威であり、もう1つは自律的な意思決定操作であり、攻撃者は入力や環境要因を操作して車両の意思決定アルゴリズムに影響を与えます。したがって、これは一方向です。

Mr. Sikora 04:35
The bidirectional attacks are starting with remote access attacks, where somebody wants to hack the interface of our V code and to get the Wi-Fi Bluetooth or cellular access to get unauthorized control.
双方向攻撃は、誰かがVコードのインターフェースをハッキングし、Wi-Fi Bluetoothまたはセルラーアクセスを取得して不正な制御を取得しようとするリモートアクセス攻撃から始まります。

Mr. Sikora 04:59
over the weekend. To do anything, it could be just to change things, to double things, or whatever. The second is the week to everything communication attacks. It's intercepting or manipulating V2X communication, sending false information or intercepting data.
週末に。何かをするには、物事を変えること、物事を倍にすること、その他何でもかまいません。2つ目は、すべての通信攻撃への週です。V2X通信を傍受または操作したり、虚偽の情報を送信したり、データを傍受したりしています。

Mr. Sikora 05:20
In the meantime, there's a lot of experience there, and there are standards also in place which can be installed and makes it happen that this type of communication is secured. For example, the B -directional standard for secure communication between trusted vehicles, ISO 21177, just an example.
その間、そこには多くの経験があり、設置可能な標準も存在し、この種の通信が保護されることを可能にしています。たとえば、信頼できる車両間の安全な通信のためのB指向性規格であるISO 21177などは、まさに一例です。

Mr. Sikora 05:54
And then somewhere. Malware encrypted vehicle systems or data demanding payment for somebody to just make the vehicle run again. So they just shut it down and ask you for payment to make it running again.
そして、どこかで。マルウェアは、車両システムを暗号化したデータまたはデータを暗号化し、誰かが車両を再び走らせるために支払いを

要求します。それで、彼らはそれをシャットダウンし、それを再び実行するための支払いを要求します。

Mr. Sikora 06:17
Then software and firmware vulnerabilities exploiting unpacked software or firmware vulnerabilities to get unauthorized access and control which is also one thing because we heard that before. One thing to make cyber security to a high topic is to regularly care about the status.
次に、ソフトウェアとファームウェアの脆弱性 開梱されたソフトウェアまたはファームウェアの脆弱性を悪用して、不正アクセスと制御を行いますが、これも以前に聞いたことがあるので1つのことです。サイバーセキュリティを高いトピックにするための1つのことは、定期的にステータスを気にすることです。

Mr. Sikora 06:44
So you need to look at the vehicle, you need to monitor the behavior, you need to monitor software status to constantly deliver patches to it. And if these patches are hacked, then you have these software and firmware vulnerabilities.
ですから、車両を見る必要があり、動作を監視する必要があり、ソフトウェアのステータスを監視して、常にパッチを配信する必要があります。そして、これらのパッチがハッキングされた場合、これらのソフトウェアとファームウェアの脆弱性が発生します。

Mr. Sikora 07:03
Command and control hijacking is also an issue. Firmware tampering and data breaches and privacy violations. I just wanted to get a short overview of what is part of the potential attacks. And for every of these attacks, each and every of these attacks, there is a potential solution as well.
コマンド&コントロールのハイジャックも問題です。ファームウェアの改ざん、データ侵害、プライバシー侵害。私はただ、潜在的な攻撃の一部について簡単に概要を知りたいと思いました。そして、これらの攻撃のすべて、これらの攻撃のすべてに対して、潜在的な解決策もあります。

Mr. Sikora 07:32
But you know as technology is getting better, the threats or the hackers are getting better as well. So it's a constant involvement and a constant thinking about how to make these systems cyber secure.
しかし、テクノロジーが向上するにつれて、脅威やハッカーも良くなっています。ですから、これらのシステムをサイバーセキュアにする方法について、常に関与し、常に考え続ける必要があります。

Mr. Sikora 07:51
Just to end, the autonomous vehicles are constructed in a way that... And if they are constantly monitoring their behavior as well, and if something is not as it should be, for example the GPS reception is from one point to another, suddenly 10 meters away from the further reception, or we experience unexpected behavior or things like that, the vehicle is constantly monitored, and if this is the case then the vehicle would slow down and stop working.
最後に、自律走行車は次のように構築されています...そして、彼らが常に彼らの行動を監視していて、何かが本来あるべき姿でない場合、たとえば、GPSの受信がある地点から別の地点にあったり、突然、さらに受信から10メートル離れていたり、予期しない行動などが発生した場合、車両は常に監視されており、これが事実である場合、車両は減速して動作を停止します。

Mr. Sikora 08:34
And therefore, at the moment, legislation in Europe at least, is asking for an attendant, so -called safety operator, who is constantly in the vehicle, and in the near future this person will be replaced by a tailor operation, so anyway, somebody has to.
したがって、現時点では、少なくともヨーロッパの法律では、常に車両に常駐する、いわゆる安全オペレーターを求めており、近い将来、この人物はテーラーオペレーターに置き換えられます。

Mr. Sikora 08:59
tell the vehicle that it's safe to operate further. Safety always comes first. And safety is based on security. Thank you very much.
さらに安全に運転できることを車両に伝えます。常に安全が最優先されます。そして、安全性はセキュリティに基づいています。ありがとうございました。

host 09:16
Dr. Mansour.
マンスール博士。

Professor R Mansour. 09:23

Good afternoon. My name is Professor R Mansour. I am the dean of College of Engineering and I .T.
こんにちは。私の名前はR・マンスール教授です。私は工学部の学部長であり、私はT.T.です。

Professor R Mansour. 09:31
My specialization is in artificial intelligence. We have at the University of Dubai very strong teams working on the application of artificial intelligence in various applications. And one of them, which is very important and which is the topic of today, is the cybersecurity.
私の専門は人工知能です。ドバイ大学には、さまざまなアプリケーションでの人工知能の応用に取り組む非常に強力なチームがあります。そして、その一つは、非常に重要で、今日のトピックであるサイバーセキュリティです。

Professor R Mansour. 09:58
Also at the University of Dubai we have programs in cybersecurity of the undergraduate and the postgraduate levels. We also have very strong collaboration with the industry here in Dubai and definitely international collaborations.
また、ドバイ大学には、学部および大学院レベルのサイバーセキュリティのプログラムがあります。また、ここドバイの業界とも非常に強力な協力関係を築いており、間違いなく国際的な協力関係を築いています。

Professor R Mansour. 10:23
One of them is the collaboration with DESC. DESC is Dubai Electronic Security. It's a government entity. We have actually a cybersecurity lab at the University of Dubai, fully funded by DESC. And that lab we have done a lot of research of buying AI and cybersecurity.
その一つがDESCとのコラボレーションです。DESC は Dubai Electronic Security です。政府機関です。実は、ドバイ大学にはサイバーセキュリティ研究所があり、DESCが全額出資しています。そして、その研究所では、AIの購入とサイバーセキュリティについて多くの研究を行ってきました。

Professor R Mansour. 10:49
So one of the very important projects is... trying to find out the sources of attacks. So by using honeypots and then gathering the information, the data, and what is important, we have developed many AI models that not just analyze the data or the current attacks, but also could make some predictions for the sources of the cyber security, cyber attack.
ですから、非常に重要なプロジェクトの1つは...攻撃の原因を見つけようとしています。そこで、ハニーポットを使用し、情報、データ、そして重要なことを収集することで、データや現在の攻撃を分析するだけでなく、サイバーセキュリティ、サイバー攻撃の原因を予測できる多くのAIモデルを開発しました。

Professor R Mansour. 11:38
So these kind of things I think is very important with regard to the autonomous vehicle. Autonomous vehicle actually bring in new challenges to all of us in the academia. in the industry, because there would be various levels of attacks on the autonomous vehicle.
ですから、このようなことは、自動運転車に関して非常に重要だと思います。自動運転車は、実は私たちアカデミアに新たな課題をもたらしています。業界では、自動運転車に対するさまざまなレベルの攻撃が存在するためです。

Professor R Mansour. 12:11
So what I mean by various levels, you know, the software levels and the physical levels of attacks. And definitely we are capable of, you know, developing many algorithms to address these attacks, resolve them, okay, and discover them, and that's also important.
ですから、私が言うところの「さまざまなレベル」とは、ソフトウェアレベルと攻撃の物理レベルです。そして、私たちは間違いなく、これらの攻撃に対処し、解決し、発見するための多くのアルゴリズムを開発する能力があり、それも重要です。

Professor R Mansour. 12:40
So discovery of the attacks is the most important thing, that's one aspect. The other aspect is prevention of these kind of attacks. There are many techniques in this regard, like, you know, in the state of you, depending on one source of data to the autonomous vehicle, or autonomous flight taxi, or autonomous drones, we need to work on, work on redundancy.
ですから、攻撃の発見が最も重要なことであり、それが1つの側面です。もう1つの側面は、この種の攻撃の防止です。この点に関しては、あなたの状態では、自律走行車、自律飛行タクシー、自律型ドローンの1つのデータソースに依存して、冗長性に取り組む必要があります。

Professor R Mansour. 13:14
Retentancy, I mean, by providing several sources of data, so that when one source of data is attacked, the others are still there. And then, with the AI, we can monitor this information from various sources and then decide that this kind of data is

not, it's kind of attacked, so in this case it will be ignored.
リテンシーとは、複数のデータソースを提供することで、1つのデータソースが攻撃されても、他のデータソースがまだそこにいるようにすることです。そして、AIを使えば、さまざまなソースからのこの情報を監視し、この種のデータは攻撃されていないと判断し、この場合は無視されることになります。

Professor R Mansour. 13:46
So that's why what I am saying here, that AI is actually critical to resolve a lot of challenges, regarding cyber security in general, but specifically for the autonomous car. The danger of the security, I mean the cyber attacks on autonomous vehicle, is critical because you know for a system it might like, you know, jam the system or something like that.
だからこそ、ここで私が言っているのは、AIは、サイバーセキュリティ全般、特に自動運転車に関する多くの課題を解決するために実際に重要であるということです。セキュリティの危険性、つまり自律走行車に対するサイバー攻撃は、システムがジャミングするなど、システムが好む可能性があるため、非常に重要です。

Professor R Mansour. 14:25
But for the autonomous vehicle it will be very dangerous and might affect loss of several lines, which is very important. So that's why I think as a research community and academia and the expertise and the industry we need to work together to develop an effective system that address these challenges.
しかし、自動運転車にとっては非常に危険であり、非常に重要な複数のラインの損失に影響を与える可能性があります。だからこそ、研究コミュニティとして、学界として、そして専門家として、産業界として、これらの課題に対処する効果的なシステムを開発するために協力する必要があると考えています。

Professor R Mansour. 14:55
I mentioned also that we need to address these challenges as the physical layer as well. So physical layer actually at University of Dubai, we did a very effective and developed a new actually algorithms to address this attack.
また、これらの課題には物理層としても取り組む必要があると述べました。そこで、ドバイ大学では、物理層を非常に効果的に行い、この攻撃に対処するための新しいアルゴリズムを開発しました。

Professor R Mansour. 15:21
And this one will resolve or minimize the severity of the attacks from vehicle to vehicle or from vehicle to infrastructure. And this one we have actually developed a multi -channel ORDM cyber security system algorithm and we got a U .S .A.
そして、これは、車両から車両へ、または車両からインフラストラクチャへの攻撃の重大度を解決または最小限に抑えます。そして、これは実際にマルチチャネルORDMサイバーセキュリティシステムアルゴリズムを開発し、U.S.A.さん

Professor R Mansour. 15:43
patent for it so that when we send the signal, we don't send it in one channel, we send it in multi -channel, we distribute the information through these channels so that if there is a attack on one or two channels, still the attack will not only achieve its objectives.
それに対する特許を取得して、信号を送信するときに1つのチャネルで送信するのではなく、マルチチャネルで送信し、これらのチャネルを通じて情報を配布することで、1つまたは2つのチャネルに攻撃が発生した場合でも、攻撃はその目的を達成するだけではありません。

Professor R Mansour. 16:06
So this is again an as I mentioned that for autonomous cars, because we need 100% efficiency. The cyber security system that we need to develop for autonomous car, it doesn't give room for errors because errors means very dangerous to the lives of the people who are using this autonomous car or autonomous vehicles.
ですから、これもまた、自動運転車の場合、100%の効率が必要なためです。自動運転車のために開発する必要があるサイバーセキュリティシステムは、エラーはこの自動運転車または自律走行車を使用している人々の生活にとって非常に危険を意味するため、エラーの余地はありません。

Professor R Mansour. 16:36
So I think what I'm saying, I just want to conclude my brief introduction about this topic is that we need to work and we need to put a lot of efforts jointly by the government, the academia, and the industry to fund many projects in AI for cybersecurity.
私が言いたいのは、このトピックについての私の簡単な紹介を締めくくりたいのは、政府、学界、産業界が協力して多くの努力をして、サイバーセキュリティのためのAIの多くのプロジェクトに資金を提供する必要があるということです。

host 17:01

Thank you very much. So as you can see our panelists come with significant expertise from the authority, from OEM manufacturers, and from academia. Lots of good things to talk about. We're now going to enter into a short guided discussion where you all can listen and then we'll follow it up with a Q &A where you'll have the opportunity to ask some of our panelists questions and then and then we'll close it out with some closing remarks.
ありがとうございました。ご覧のとおり、パネリストは、当局、OEMメーカー、および学界からの重要な専門知識を持っています。話すべき良いことがたくさんあります。これからは、皆さんがお聞きいただける短いガイド付きディスカッションを行い、その後、パネリストの皆さんに質問する機会を提供するQ&Aを行い、その後、閉会の挨拶で締めくくります。

host 17:44
So we'll go ahead and get started with the guided discussion now. So, that was, again, very thought -provoking, and I'd like to go ahead and start it with Mr. Avodarev with some questions. How can we ensure the safety of passengers and the wider public in the connected and autonomous vehicle space, considering the potential of cyberattacks?
それでは、先に進んで、ガイド付きディスカッションを始めましょう。ですから、これもまた、非常に考えさせられるものでしたので、アボダレフ氏からいくつかの質問を始めたいと思います。サイバー攻撃の可能性を考慮しながら、コネクテッドカーや自動運転車の分野で、乗客や一般の人々の安全をどのように確保できるのでしょうか?

Mr. Avodarev 18:31
Thank you for the question, Rick. I would start because we do have quite an experience in designing or implementing those type of systems. I would start with designing the system from ground up, having security in mind.
リックさん、ご質問ありがとうございます。まず、私たちはこの種のシステムの設計や実装にかなりの経験を持っているからです。まず、セキュリティを念頭に置いて、システムをゼロから設計することから始めます。

Mr. Avodarev 18:49
When it comes to security, I mean security of the public, security of the system itself because they go hand in hand. The other thing is to consider, as part of your security design, a very strong authentication and a secure communication as well.
セキュリティに関して言えば、公共のセキュリティ、システム自体のセキュリティ、それらは密接に関連していることを意味します。もう一つは、セキュリティ設計の一部として、非常に強力な認証と安全な通信も考慮することです。

Mr. Avodarev 19:06
This is never necessary to say that you need to guard those systems with a robust infrastructure. An example is intrusion detection systems and so on. I have seen some implementations, especially when it comes to trials related to autonomous vehicles, that the transmission of data happens over the open network, and this is one of the most interesting things anyone would ever do for a connected or an autonomous vehicle.
これは、堅牢なインフラストラクチャでこれらのシステムを保護する必要があると言う必要はありません。例としては、侵入検知システムなどがあります。特に自動運転車に関連する試験では、データの伝送がオープンネットワークを介して行われる実装をいくつか見てきましたが、これはコネクテッドカーや自動運転車に対して誰もが行う最も興味深いことの1つです。

Mr. Avodarev 19:38
Because as you know, those vehicles have the ability to remotely control certain elements of the vehicle that can lead to a catastrophic accident. So having all of these in mind is very important and crucial.
ご存知のように、これらの車両には、壊滅的な事故につながる可能性のある車両の特定の要素をリモートで制御する能力があるためです。ですから、これらすべてを念頭に置くことは非常に重要で、極めて重要なことです。

Mr. Avodarev 19:52
Why do you design your system? In addition to designing your system, I would like to ask you to consider designing your that, and this is something very important that we should not ignore, is having a proper legislation that covers the security of the assistance, adopting certain standards.
なぜシステムを設計するのですか?あなたのシステムの設計に加えて、私はあなたにあなたの設計を検討していただきたいと思います、そしてこれは私たちが無視すべきではない非常に重要なことですが、特定の基準を採用し、支援のセキュリティをカバーする適切な法律を持つことです。

Mr. Avodarev 20:10
We know that the entire market or the entire world is new to this type of regulation and standards, but we have seen some efforts being done in the European Union, which was published, I believe, mid of last year.
市場全体、あるいは全世界がこの種の規制や基準に慣れていないことは承知していますが、昨年半ばに発表されたと思いますが、欧州連合ではいくつかの取り組みが行われています。

Mr. Avodarev 20:28
This is a very good starting point, and it could be a very good guideline for people who are designing those type of systems. Absolutely, and thank you for those comments. Would any of our other panelists like to expand upon the question?
これは非常に良い出発点であり、この種のシステムを設計している人々にとって非常に良いガイドラインになる可能性があります。もちろんです、そしてそれらのコメントに感謝します。他のパネリストの中に、この質問を詳しく説明したい人はいますか?

Mr. Avodarev 20:48
Thank you.
ありがとうございます。

Mr. Sikora 20:50
Well, I fully agree with you, and I'm I'm proud, to be honest, to be a European where we get some legislation already. We saw this upcoming regulation for type approval for autonomous vehicles.
そうですね、私も全く同感ですし、正直なところ、すでに何らかの法律が制定されているヨーロッパ人であることを誇りに思っています。私たちは、自動運転車の型式認証に関する今後の規制を見てきました。

Mr. Sikora 21:11
We have, as a standardization guide, we developed some standards that need to be implemented. And what I see as an autonomous shuttle provider, more and more customers like RTA are referring to these standards to be fulfilled, which is being able to make a secure application.
標準化のガイドとして、実装が必要ないくつかの標準を開発しました。そして、自律型シャトルのプロバイダーとして、RTAのようなますます多くの顧客が、これらの基準を満たすために言及しており、それは安全なアプリケーションを作成できるということです。

host 21:42
Thank you very much.
ありがとうございました。

Mr. Sikora 21:44
I just re -emphasize the importance of AI energy regarding this aspect. So I think it's the best way of addressing these challenges and reduce the severity of it, just to develop new AI models that could discover, end discovery of the attacks.
私はただ、この側面に関してAIエネルギーの重要性を再度強調します。ですから、これらの課題に対処し、その深刻度を軽減するには、攻撃を発見し、発見を終わらせることができる新しいAIモデルを開発することが最善の方法だと思います。

Mr. Sikora 22:08
In addition to that, by looking at the history of the data in the system, and trying to predict the attacks, and not just predict the attacks, even the source of the attacks. So this one, I think this is the most important aspect regarding this direction.
それに加えて、システム内のデータの履歴を見て、攻撃を予測するだけでなく、攻撃の発生源までも予測しようとします。ですから、これは、この方向性に関して最も重要な側面だと思います。

host 22:34
Dr. Mutsor, thank you for that question. Answer. I'd like to address this to Mr. Sikora. How can we secure a vehicle to everything, communication, to prevent cyberattacks, that could compromise the safety and operation of the autonomous vehicle overall? And you could expand upon that a little bit with the, in regard to autonomous shuttles.
ムトソー博士、その質問をありがとうございます。答える。シコラさんにお話ししたいと思います。自動運転車全体の安全性と運用を損なう可能性のあるサイバー攻撃を防ぐために、通信など、あらゆるものに対して車両をどのように保護できるでしょうか? そして、自律型シャトルに関して、それを少し拡張することができます。

Mr. Sikora 22:59
that you know so well. Thank you very much. Autonomous vehicles, autonomous shuttles, are becoming a reality. And as well, the vehicle to excommunication has become a reality.
あなたがとてもよく知っていること。ありがとうございました。自律走行車、自律走行シャトルが現実のものになりつつあります。そしてまた、破門への手段が現実のものとなりました。

Mr. Sikora 23:13
So, what was necessary to enable this is to define more and more what's about vehicle to excommunication. The messages that come as a broadcast from a vehicle to the environment. And as well, to define the bidirectional communication.

したがって、これを可能にするために必要だったのは、破門への車両について何であるかをますます定義することです。車両から環境へのブロードキャストとして来るメッセージ。また、双方向通信を定義するためにも。

Mr. Sikora 23:35
For example, a rumor fleet say hello here, and the traffic light accepts it and lets it go through. So, it must be an acceptance at home. And therefore, there are some standards in this. can be used and for cyber security I mentioned already there is a standard for broadcast encryption and there is a standard for safe communication between trusted vehicles for a customer asked for a quotation otherwise there is a lot of reasons why these types shouldn't be used.
たとえば、噂の艦隊がここでこんにちはと言うと、信号機はそれを受け入れて通過させます。ですから、それは自宅で受け入れられなければなりません。したがって、これにはいくつかの基準があります。また、サイバーセキュリティについては、すでに述べたように、放送暗号化の規格や、見積もりを求められた顧客のための信頼できる車両間の安全な通信の規格があります。そうでなければ、これらのタイプを使用すべきではない理由はたくさんあります。

Mr. Sikora 24:38
Another thing is always if a communication is over an unsecured network the only thing you can do is to allow for strong encryption and this is the only thing that is possible if you go over an unsecured network.
もう一つは、通信がセキュリティで保護されていないネットワーク上で行われる場合、できることは強力な暗号化を許可することだけであり、これがセキュリティで保護されていないネットワークを経由する場合に可能な唯一のことです。

Mr. Sikora 25:00
Then the authentication mechanism is one way that you can use public key infrastructure or other authentication methods and as mentioned before it is always needed to have in vehicle a so called intrusion detection and prevention system that monitors everything that is going on over the end and what I mentioned as well and it is valid for deep text communication you need to update the system so you need to check it you need to update your standard patches that is what we are used to with our cell phones that is the outcome for the autonomous vehicles as well.
次に、認証メカニズムは、公開鍵インフラストラクチャまたは他の認証方法を使用できる1つの方法であり、前述のように、車両には常に、最終的に起こっていることすべてを監視する侵入検出および防止システムが必要であり、ディープテキスト通信にも有効であるため、システムを更新する必要がありますので、確認する必要があります私たちが携帯電話で慣れ親しんでいることである標準パッチを更新する必要がありますが、これは自動運転車の結果でもあります。

Mr. Sikora 25:56
And last but not least, for these type of things, you need to make regular audits and testings with them. So that's what, it's a bunch of work and a lot of work, but otherwise I think we might have really big problems if we don't have that.
そして最後になりましたが、この種のことについては、定期的な監査とテストを行う必要があります。ですから、それはたくさんの仕事であり、多くの仕事ですが、そうでなければ、それがないと本当に大きな問題になるかもしれないと思います。

host 26:22
Absolutely. Thank you for those comments, Mr. Sikora. Dr. Mansour, I'd like you to comment on the next question. What are the most significant cybersecurity threats to AI systems, which you're very familiar with, obviously, in autonomous and connected vehicles, and how can they effectively be mitigated?
そうですよ。シコラさん、コメントありがとうございます。マンスール博士、次の質問についてコメントをお願いします。自動運転車やコネクテッドカーでは、AIシステムに対する最も重要なサイバーセキュリティの脅威は何であり、それらを効果的に軽減するにはどうすればよいでしょうか?

Professor R Mansour. 26:42
Well, the main challenge is the data, and for AI model, The main objective of the AI model is looking at the current data and the history of the data and then make decisions. So with this, I think we can actually develop a very sophisticated AI model, but that will not be enough.
さて、主な課題はデータであり、AIモデルの場合、AIモデルの主な目的は、現在のデータとデータの履歴を見て、決定を下すことです。ですから、これでは、非常に高度なAIモデルを実際に開発できると思いますが、それだけでは不十分です。

Professor R Mansour. 27:11
We need actually to go as mission by robots and Mr. Muhammad. We need to look at the communication. So the communication as well is very, very important. Like you know, you mentioned the communication between vehicle to vehicle and also from vehicle to infrastructure.
実際にロボットとムハンマドさんにミッションとして行く必要があります。私たちはコミュニケーションに目を向ける必要があります。で

すから、コミュニケーションも非常に重要です。ご存知のように、車両間、および車両からインフラストラクチャへの通信について言及しました。

Professor R Mansour. 27:31
One of the what I think will be more effective so that the AI model can be working in effective way is to reduce the malicious data. And the reducing the research is definitely the tax data. We need to reduce the amount of data to be communicated.
AIモデルが効果的に機能するために、より効果的だと思うことの1つは、悪意のあるデータを減らすことです。そして、研究を減らすことは間違いなく税金データです。通信するデータの量を減らす必要があります。

Professor R Mansour. 27:56
So, for example, for us, that's not to be because we need to choose this flow of data. This data, the right, they always send the enough data for the autonomous vehicle because, you know, autonomous means it works by itself.
ですから、例えば、私たちにとっては、このデータの流れを選択する必要があるからではありません。このデータは、自動運転車には常に十分なデータを送信します。なぜなら、自動運転車とは、自動運転車が単独で機能することを意味するからです。

Professor R Mansour. 28:14
So that's why, because the attacker will see us as a weakness, the communication channel between vehicle to vehicle or vehicle to infrastructure, and then attack that and try to change this data. So I think the less data to be communicated between the vehicle to vehicle or from vehicle to infrastructure, we can really address a lot of challenges.
そのため、攻撃者は私たちを弱点、つまり車両間または車両とインフラストラクチャ間の通信チャネルと見なし、それを攻撃してこのデータを変更しようとします。ですから、車両間、または車両からインフラストラクチャ間で通信されるデータが少なくなればなるほど、多くの課題に対処できると思います。

Professor R Mansour. 28:44
Technically, the corruptions, as I mentioned earlier, on the multi -level algorithms with the right to assist. conventional algorithms or AI models, this definitely will reduce the risks. Thank you.
技術的には、先に述べたように、支援する権利を持つマルチレベルアルゴリズムの破損です。従来のアルゴリズムやAIモデル、これによりリスクは確実に軽減されます。ありがとうございます。

host 29:03
Absolutely. Absolutely. And thank you. Thank you, Dr. Mansour. Go back to Mr. Ahmad Arab. I'd like to ask some more international collaborations. So how can international collaboration, standards, information sharing, how can this contribute to mitigating cyber threats within the mobility sector?
そうですよ。そうですよ。そして、ありがとうございました。マンスール博士、ありがとうございました。アフマド・アラブ氏の話に戻りましょう。もう少し国際的な協力をお願いしたいと思います。では、国際的な協力、標準、情報共有、これらはモビリティセクター内のサイバー脅威の軽減にどのように貢献できるのでしょうか。

Mr. Avodarev 29:31
Well, Eric, international collaboration will help you gain knowledge on what's happening around the world. Whether it's with the OEM suppliers like Robert we have him here, or also with Dr. Wathrop from the academia.
エリック、国際的な協力関係は、世界中で何が起こっているかについての知識を得るのに役立ちます。ロバートのようなOEMサプライヤーであろうと、アカデミアのワスロップ博士であろうと、彼もここにいます。

Mr. Avodarev 29:49
not even on the local level but also regional and global level, it will enrich the knowledge of whoever would like to introduce those type of modes of transportation. It will help also develop any those standards, yes we can adopt certain standards from different regions around the world but you cannot just copy and paste everything and implement it locally because you have different laws, different regulations,
地域レベルだけでなく、地域レベルや世界レベルでも、そのような交通手段を導入したい人の知識を豊かにするでしょう。それはまた、それらの基準を開発するのに役立ちます、はい、私たちは世界中のさまざまな地域から特定の基準を採用することができますが、あなたは単にすべてをコピーして貼り付け、それをローカルに実装することはできません、あなたは異なる法律、異なる規制を持っているからです。

Mr. Avodarev 30:19
you have different stakeholders to satisfy and so on. So gaining this knowledge from the international, let's say partnership that you can have will aid to develop your own standards which will be not far off the international standard and satisfies all the authorities, so this is on one side.

さまざまな利害関係者を満足させる必要があります。ですから、この知識を国際的に得ることは、例えば、パートナーシップを持つことで、国際基準からそれほど離れず、すべての当局を満足させる独自の基準を開発するのに役立ちます。

Mr. Avodarev 30:42
The other side you have spoken about data as we rely on technology a lot of course we will be gathering a lot of data and the question remains is what do we do with this data. Of course we would like to use it to enhance our services, we would like to use it even to take the services to the next level to enrich the experience of our customers and passengers but we need to pick what are those data attributes that we will be looking at.
一方、データについては、テクノロジーに大きく依存しているため、もちろん多くのデータを収集することになりますが、問題はこのデータをどうするかということです。もちろん、私たちはそれを使用してサービスを強化し、サービスをさらにレベルに引き上げてお客様や乗客のエクスペリエンスを豊かにしたいと考えていますが、私たちが見ているデータ属性が何であるかを選択する必要があります。

Mr. Avodarev 31:10
We need to protect the people privacy as well we have to keep it in mind. The way how we store those data, the way how we use them, which type of analytics tool that we use for what purpose especially when it comes to AI because we have seen a lot of AI models that abuses the information that you currently have and without proper let's say recreational governments when it comes to those deep analytics tools that uses AI I think a bigger problem might happen so being aware about what type of data you are you are using.
私たちは人々のプライバシーも保護する必要があります、私たちはそれを心に留めておく必要があります。これらのデータをどのように保存するか、どのように使用するか、どのような目的で分析ツールを使用するか、特にAIに関しては、現在持っている情報を悪用するAIモデルをたくさん見てきましたし、AIを使用する深い分析ツールに関しては、例えばレクリエーション政府といっても過言ではありません使用しているデータの種類について。

Mr. Sikora 31:49
using what type of data you are collecting will help a lot in serving the purpose.
収集しているデータの種類を使用すると、目的を果たすのに大いに役立ちます。

host 32:00
Thank you for those comments as well. Thank you so much. Mr. Socora, what are the primary software and firmware vulnerabilities in autonomous shuttles? How can these be mitigated to prevent unauthorized access and ultimately control?
ご意見もよろしくお願いいたします。どうもありがとうございます。ソコラさん、自律型シャトルの主なソフトウェアとファームウェアの脆弱性は何ですか?不正アクセスを防ぎ、最終的には制御するために、これらをどのように軽減できるでしょうか?

Mr. Sikora 32:18
Yeah, it was stated many times. Thank you. But anyway for this, I think at first these are unpatched systems. You need to care about that the system is always on the present state taking into account unprotected entry points and everything like that.
はい、何度も述べられていました。ありがとうございます。しかし、とにかく、これについては、最初はこれらはパッチが適用されていないシステムだと思います。システムは、保護されていないエントリポイントなどすべてを考慮に入れて、常に現在の状態にあることに注意する必要があります。

Mr. Sikora 32:44
So then insecure protocols. which are still existing, even the Ethernet protocols, to some extent is not secure enough, then weak authentication. If you're using the same password always, it's very easy to intuit a system.
そのため、安全でないプロトコルです。イーサネットプロトコルでさえ、ある程度十分に安全ではなく、認証が弱い場合に、まだ存在しています。常に同じパスワードを使用している場合、システムを直感的に理解するのは非常に簡単です。

Mr. Sikora 33:11
If you buy something and you are using parts from other vendors, it's also very, very important to check whether these parts are secure. Otherwise, you buy something where hackers can intuit a system.
何かを購入し、他のベンダーの部品を使用している場合、これらの部品が安全であるかどうかを確認することも非常に重要です。そうでなければ、ハッカーがシステムを直感できるようなものを買うことになります。

Mr. Sikora 33:38
So these are, according to my perspective, the main threats for this. software and firmware. Absolutely.
ですから、私の見解によれば、これらがこれに対する主な脅威です。ソフトウェアとファームウェア。そうですよ。

host 33:50
Thank you, Mr. Sikora. Dr. Mansoor, let's maybe turn it more towards regulations now. So, what are the key regulatory challenges in ensuring the security of future mobility, and how are these being addressed currently in the global marketplace?
シコラさん、ありがとうございました。マンスール博士、これからはもっと規制に向けましょう。では、将来のモビリティのセキュリティを確保するための主要な規制上の課題は何であり、現在、グローバル市場ではどのように対処されているのでしょうか。

Professor R Mansour. 34:10
Thank you very much. I could tell you about our experience with this. Actually, this is actually a government of the way entities are responsible for issuing regulations and policies, and help various government entities, and even the industry, to help them, support them, to enhance their cyber security system.
ありがとうございました。これに関する私たちの経験についてお話しすることができます。実際には、これは実際には、企業が規制や政策を発行する責任があり、さまざまな政府機関、さらには業界が彼らを支援し、支援し、サイバーセキュリティシステムを強化するのを支援する方法の政府です。

Professor R Mansour. 34:49
So from this regard, I think the bi -government is doing an excellent work as usual. And there are a lot of diplomats being issued by the bi -government in that regard. So definitely regulations policy is very important.
ですから、この点から、バイ政府はいつものように素晴らしい仕事をしていると思います。そして、その点に関して、バイ政府によって多くの外交官が発行されています。ですから、間違いなく規制政策は非常に重要です。

Professor R Mansour. 35:14
And also, as mentioned by Robert, the standards, international standards, frameworks of security systems. So these all together, I think, need to be taken into consideration. Not at the national level, but also at the international level.
また、ロバートが言及したように、セキュリティシステムの標準、国際標準、フレームワーク。ですから、これら全てを総合して考慮に入れる必要があると思います。国内レベルだけでなく、国際レベルでも。

Professor R Mansour. 35:39
Because always, regulation is the main challenge. And we cannot work in silos anymore. We are one entity, a global entity in the world. We need to work together. And there are a lot of international standardization, ISO, IEEE, a lot of international standardization organizations that regulate these kind of things.
なぜなら、常に規制が主な課題だからです。そして、私たちはもはやサイロで作業することはできません。私たちは一つのエンティティであり、世界のグローバルなエンティティです。私たちは一緒に働く必要があります。そして、ISO、IEEE、この種のものを規制する多くの国際標準化組織など、多くの国際標準化があります。

Professor R Mansour. 36:09
But I think this is very important as well, not just for the security, but also for the, like you know, I'm just telling you one interesting project that we are working at the University of Dubai is, for example, some autonomous vehicle, handsome, did some accidents.
しかし、これはセキュリティだけでなく、ドバイ大学で取り組んでいる興味深いプロジェクトの一つとして、例えば、自動運転車がハンサムに事故を起こしたというのも、非常に重要なことだと思います。

Professor R Mansour. 36:35
Who is responsible? So again, this is very important question. And that's why the regulation in this direction will be important so that we could know who is responsible for this fault. I also can take you to the end of the direction, the AI, which is my specialization.
責任者は誰ですか?ですから、繰り返しになりますが、これは非常に重要な質問です。だからこそ、この方向の規制は、この障害の責任者を知るために重要になります。また、私の専門であるAIという方向性の終点にあなたを連れて行くこともできます。

Professor R Mansour. 37:00
And AI is a direction called the explainable AI, responsible AI. And I am, you know, in addition to my role as the dean of engineering at University of Dubai, I am helping opposition as honorary professor at Macquarie University.
そして、AIは説明可能なAI、責任あるAIと呼ばれる方向性です。そして、私は、ご存知のように、ドバイ大学の工学部長としての役割に加えて、マッコーリー大学の名誉教授として反対派を支援しています。

Professor R Mansour. 37:19

And I have many PhD students. So now some of my PhD students in Macquarie University, they are working on explainable AI. Explainable AI means that when you develop AI system, this AI system should be investigated, easy to be investigated.
そして、私には多くの博士課程の学生がいます。ですから、現在、マッコーリー大学の博士課程の学生の中には、説明可能なAIに取り組んでいる人もいます。説明可能なAIとは、AIシステムを開発するときに、このAIシステムを調査しやすく、調査しやすいようにする必要があることを意味します。

Professor R Mansour. 37:42
So there is something wrong. have been the investigator can look at this system and say okay there is a bug or fault in this AI system. The current AI models now they are not explainable all of them is like block box a black box story so this is again one of the important aspect about the importance of the regulation for cyber security and also the use of AI in cyber security.
だから何かが間違っている。調査員がこのシステムを見て、このAIシステムにバグや障害があると言うことができます。現在のAIモデルは、現在、それらは説明可能ではなく、すべてがブロックボックス、ブラックボックスの話のようなものであるため、これもまた、サイバーセキュリティの規制の重要性と、サイバーセキュリティにおけるAIの使用に関する重要な側面の1つです。

Mr. Sikora 38:23
Absolutely, thank you Dr. Mansour. I'd like to expand that same question to Mr. Al -Munarev being with the authority. Key regulatory challenges ensuring the security of the future of ability. How do we address it globally?
マンスール博士、本当にありがとうございました。私は、その同じ質問を、当局と一緒にいるアル・ムナレフ氏にまで広げたいと思います。能力の未来のセキュリティを確保するための主要な規制上の課題。グローバルでどのように対処しますか?

Mr. Avodarev 38:40
I know you had talked a little bit about the international marketplace previously. First of all, it's very hard to come up with a regulation of something new and still evolving. Because you don't work with a regulation that handles the development of those tools.
以前、国際市場について少しお話しされていたと思います。まず第一に、新しくてまだ進化しているものの規制を考え出すのは非常に難しいです。なぜなら、これらのツールの開発を扱う規制に取り組んでいないからです。

Mr. Avodarev 38:57
So you have to design your legal system very carefully. Maybe one of the inhibitors that we have seen in Dubai. Dubai, we have a very agile legal system. The turnaround time for you to change a legislation or even to come up with a new one is fairly fast.
ですから、法制度を非常に慎重に設計する必要があります。たぶん、ドバイで見た阻害剤の1つです。ドバイには、非常に機敏な法制度があります。法律を変更したり、新しい法律を考え出したりするための所要時間はかなり速いです。

Mr. Avodarev 39:16
Because the leadership understands that it's a very evolving market. It's a very evolving technology. Every day there is something new about it. And the main aim is to secure those type of modes as well as protect the people who are going to use it.
なぜなら、リーダーシップは、この市場が非常に進化していることを理解しているからです。これは非常に進化しているテクノロジーです。毎日何か新しいことがあります。そして、主な目的は、これらのタイプのモードを保護するだけでなく、それを使用する人々を保護することです。

Mr. Avodarev 39:37
I'll give an example. Maybe somehow it is related to it as well. Because we are focusing on the community education to ensure that they understand how safe are those modes of transportation. Because they are the modes of transportation for the future.
例を挙げましょう。もしかしたら、それも何かしら関係しているのかもしれません。なぜなら、私たちはコミュニティ教育に焦点を当てており、これらの交通手段がどれほど安全であるかを彼らが理解できるようにしているからです。なぜなら、それらは未来の交通手段だからです。

Mr. Avodarev 39:54
When we have started with the operations of Dubai Metro, and as everyone knows, Dubai Metro is a driverless system. So when we started the operations, although it is a driverless system, we have put a train attendant in every single train opening the driving console.
ドバイメトロの運用を開始したとき、そして誰もが知っているように、ドバイメトロは無人システムです。ですから、運用を開始したと

き、ドライバーレスシステムですが、運転コンソールを開くすべての列車に乗務員を配置しました。

Mr. Avodarev 40:13
Just for people to be comfortable at the beginning. So they are not, let's say, afraid to use this new system. A train by itself in Dubai was something new. So it's a driverless as well. So it was somehow something big for people to digest at the beginning.
ただ、最初は人々が快適に過ごせるように。ですから、彼らは、例えば、この新しいシステムを使用することを恐れていません。ドバイでの列車自体は何か新しいものでした。つまり、ドライバーレスでもあるのです。だから、最初は人々が消化すべき大きなものだったのです。

Mr. Avodarev 40:36
So the way how we approach people, even. talent, we design it very carefully. Another example for us where we have done tons of customer engagement and education as well, when we have introduced the tram.
だから、私たちが人々にアプローチする方法もそうです。才能、私たちはそれを非常に慎重に設計します。また、トラムを導入した際には、顧客エンゲージメントや教育も数多く行いました。

Mr. Avodarev 40:51
Now the tram is not a driver's bus but it is a new mode of transport and a part of Dubai that is full of tourists. So it was a challenge for us and as you know Dubai has over 200 nationalities. When I say 200 nationalities you have 200 different driving behaviour.
現在、路面電車は運転手用バスではありませんが、新しい交通手段であり、観光客でいっぱいのドバイの一部です。ですから、それは私たちにとって挑戦であり、ご存知のように、ドバイには200以上の国籍があります。私が200の国籍と言うとき、あなたは200の異なる運転行動を持っています。

Mr. Avodarev 41:13
So we have redesigned the signage system to introduce the tram. We have even went to the driving schools and we have updated the entire curriculum to introduce those new signage and to educate people that there is a new mode of transport that is available on the road.
そこで、路面電車を紹介するためにサイネージシステムを再設計しました。私たちは自動車教習所にも行き、カリキュラム全体を更新して、新しい標識を導入し、道路上に新しい交通手段があることを人々に教育しました。

Mr. Avodarev 41:34
Now there are a lot of things that you need to do on that. on that regard. You need the public to identify that the car is moving in the road as an autonomous vehicle and you need to know as a driver how to deal with the situation whenever an autonomous vehicle is moving beside you or in front of you or even behind you.
今、あなたがそれについてやるべきことはたくさんあります。その点では。車が自動運転車として道路を動いていることを一般の人々が認識する必要があり、自動運転車があなたの横や前、さらには後ろに移動しているときはいつでも、ドライバーとして状況に対処する方法を知る必要があります。

Mr. Avodarev 41:59
It's very important, it's a big change, we know it's coming, it makes it even more complex when you are in a mixed environment, it is a lot easier if it is a full autonomy. It's way a lot easier when it is a full autonomy but when it's a hybrid model it adds a lot of risks, it needs its time, it has to take its curve and it requires a lot of effort by everyone including the society etc.
これは非常に重要で、大きな変化であり、私たちはそれが来ることを知っていますが、混合環境にいるとさらに複雑になりますが、完全な自律性であれば、はるかに簡単になります。完全な自律性であれば、はるかに簡単ですが、ハイブリッドモデルの場合、多くのリスクが加わり、時間が必要で、カーブを取らなければならず、社会などを含む全員の多大な努力が必要です。

host 42:29
Absolutely, thank you for that as well. I'd like to keep the conversation going with you Mr. Al Mutterib. Enhancing infrastructure, how do we do that to help ensure we don't have vulnerability in our networks for cyber security attacks?
もちろん、それについても感謝しています。アル・ムテリブさんとの会話を続けたいと思います。インフラストラクチャの強化、つまりサイバーセキュリティ攻撃に対するネットワークの脆弱性を防ぐためには、どうすればよいのでしょうか。

Professor R Mansour. 42:46
Well I'll go back maybe to my initial feedback, it's the way how you design your infrastructure. It's very important to have

security in mind, the reliance on technology is increasing. A couple of decades ago we saw engineers only designing vehicles, designing roads and those type of systems but nowadays I think they either need to be as cyber security educated or we involve the cyber security team with them because they need to work hand in hand and designing those systems.
さて、最初のフィードバックに戻るかもしれませんが、それはインフラストラクチャの設計方法です。セキュリティを念頭に置くことは非常に重要であり、テクノロジーへの依存度は高まっています。数十年前までは、エンジニアは車両の設計や道路の設計などのシステムを設計するだけでしたが、今日では、彼らはサイバーセキュリティの教育を受ける必要があるか、サイバーセキュリティチームが協力してシステムを設計する必要があるため、彼らを巻き込む必要があると思います。

Mr. Avodarev 43:25
Another element is to have a robust secured infrastructure, state -of -the -art encryption because you cannot really afford for intrusions to take control of a fuel infrastructure or your autonomous vehicles.
もう一つの要素は、燃料インフラや自律走行車を制御するための侵入を実際に許すことができないため、堅牢で安全なインフラストラクチャ、最先端の暗号化を持つことです。

Mr. Avodarev 43:45
The scenarios are endless, and a disaster could happen. Another thing is to identify those elements as risks within the organization and put the proper mitigation plan and even the emergency response plan, whenever an incident happened, for you to have an easy recovery, to capture the lesson learned, and for you to do the required adjustment and to resume the services even better than the way it used.
シナリオは無限であり、災害が発生する可能性があります。もう一つは、これらの要素を組織内のリスクとして特定し、インシデントが発生するたびに適切な緩和計画や緊急対応計画を立てることで、簡単に回復し、学んだ教訓を捉え、必要な調整を行い、使用方法よりもさらに優れたサービスを再開できるようにすることです。

host 44:18
Thank you so much for that. Mr. Scora, in cadence with infrastructure, and I guess hardware more specifically, for the naive, like myself, where would we see the cyber attacks potentially would it be on the vehicle, on the onboard units, would it be at the airport? Intersection within the traffic control cabinet. Is there is there any area that we should be more focused on rather than the other?
本当にありがとうございました。スコラさん、インフラ、より具体的にはハードウェアと歩調を合わせると、私のようなナイーブな人々にとって、サイバー攻撃はどこで、車両、車載ユニット、空港などで発生する可能性がありますか?交通管制キャビネット内の交差点。他の分野よりも重点を置くべき分野はありますか?

Mr. Sikora 44:49
To be honest the weakest point is always the one which will be attacked first and At the moment, I would not be able to tell which one is the weakest point but The infrastructure could be attacked Because for example at an intersection If you attack the controller for the intersection,
正直なところ、最も弱いポイントは常に最初に攻撃されるポイントであり、現時点では、どちらが最も弱いポイントであるかを判断することはできませんが、インフラストラクチャが攻撃される可能性があります。たとえば、交差点で交差点のコントローラーを攻撃すると、

Mr. Sikora 45:15
it has a big effect It doesn't only affect the autonomous vehicle it affects every part of the of the traffic On the other hand, I think it's also very available to think about following this idea What happens when somebody hacked in the vehicle or hacked in the infrastructure and the disaster is coming so you need to be prepared to solve this problem as soon as possible so from our vehicle perspective we need to be prepared if the vehicle is stopping by a reason of a cyber attack to make it movable again and not to to be an obstacle to other traffic Partners,
それは大きな影響を及ぼします それは自動運転車に影響を与えるだけでなく、交通のあらゆる部分に影響を与えます 一方、誰かが車両にハッキングされたり、インフラストラクチャにハッキングされたりして災害が来るとどうなるかを考えることも非常に可能だと思います したがって、この問題をできるだけ早く解決する準備をする必要があります。車両がサイバー攻撃の理由で停止している場合は、車両を再び移動可能にし、他の交通パートナーの障害にならないように準備する必要があります。

Mr. Sikora 46:15
so these kind of things are as well very important. So not only prevention but also thinking about resilience What happens if something has ended up in the disaster already and this defines more or less the view on the weakest points, so I think it's the whole environment, and we need to have a look at the whole environment.
ですから、このようなことも非常に重要です。ですから、予防だけでなく、レジリエンスについても考える もし何かがすでに災害に終わってしまったらどうなるか、これが多かれ少なかれ最も弱い点についての見方を定義するので、それは環境全体であり、環境全体を見る必要

があると思います。

host 46:53
Absolutely. So I believe I heard mitigation plans at one point during the conversation as well, and I hear that a lot, working with authorities around the world, what's your mitigation plan, generally when you're running pilot.
そうですよ。ですから、会話の中で一度は緩和計画を聞いたこともあると思いますが、世界中の当局と協力して、パイロットを実行しているときには、一般的に緩和計画はどうなっているのか、よく耳にします。

host 47:07
Pilot projects and proof of concepts and things like that, specific to autonomous shuttles, what are mitigation plans that you would use to give yourself a backup in case something happens, something like that. Is there anything that you would do for that, Mr. Sikora?
パイロットプロジェクトや概念実証など、自律型シャトルに特有のもので、何かが起こった場合に自分自身をバックアップするために使用する緩和計画は何ですか?そのために何かすることはありますか、シコラさん?

Mr. Sikora 47:29
Yeah, I think for the shuttles it's kind of easy because there's not so many out there. But if something is happening, then you need to be sure that it cannot be an obstacle.
ええ、シャトルバスはそれほど多くないので、ちょっと簡単だと思います。しかし、何かが起こっている場合は、それが障害にならないことを確認する必要があります。

Mr. Sikora 47:45
So you need to have either a person inside the vehicle who can start it over again or being able to transmit the commands to the vehicle over the air in teleoperation. These things are very important.
したがって、車両内には、最初からやり直すことができる人がいるか、遠隔操作で無線で車両にコマンドを送信できる必要があります。これらのことは非常に重要です。

Mr. Sikora 48:04
And because in the most cases that we had already in our deployments in Europe, in the US, and in Korea, in Australia, and New Zealand, the most cases end up in the vehicle stopping. We did not have accidents on that because the vehicle is always looking for obstacles.
また、ヨーロッパ、米国、韓国、オーストラリア、ニュージーランドでは、ほとんどの場合、車両が停止するケースがほとんどです。車両は常に障害物を探しているため、事故はありませんでした。

Mr. Sikora 48:34
And if there is an obstacle, it will stop. And the stopping is, at the moment, the biggest threat because if there is somebody behind the vehicle, then they cannot move anymore. And therefore, I think it's very important to set up the vehicle to a new state, to be operable again, to start it again. And this could be done on site or on the team.
そして、障害物があれば止まります。そして、停車は、現時点では最大の脅威であり、車両の後ろに誰かがいる場合、彼らはもはや動くことができないからです。ですから、車両を新しい状態にセットアップし、再び操作可能にし、再び始動させることが非常に重要だと思います。そして、これは現場でもチームでも行うことができます。

host 49:01
Absolutely. Thank you, Mr. Sakora. Dr. Mansoor, obviously, strong focus on AI, data privacy. What can we do to ensure data privacy?
そうですよ。サコラさん、ありがとうございました。マンスール博士は、明らかに、AIとデータプライバシーに重点を置いています。データのプライバシーを確保するために何ができますか?

Professor R Mansour. 49:17
Well, actually, I just want to comment more about the place. In autonomous vehicles, I think most importantly, we need to rely on many source of data. So, for example, in the state of using one's sense of... To a certain to collect certain information about the environment.
ええと、実は、私はその場所についてもっとコメントしたいだけです。自動運転車では、最も重要なことは、多くのデータソースに頼る必要があると思います。ですから、例えば、自分の感覚を使って...環境に関する特定の情報を収集するために、特定のこと。

Professor R Mansour. 49:42

We need to put multi -sensor system So I think with this and this guy I'm with this even one sensor Got attacked. So at least we have other sensor and that's why the importance of Because with AI The Scapable the system will be capable to analyze like, you know, big data and the bigger time is many information For certain target of information and that scan cannot be done with the traditional system So we need to develop AI model to analyze various data Instantly and then could discover that's what I'm saying could discover any attacks easily Because if we get no information,
マルチセンサーシステムを配置する必要があるので、これとこの男で私はこれと一緒にいると思いますが、センサーが1つでも攻撃されました。だから、少なくとも私たちは他のセンサーを持っているので、それが重要な理由です AI The Scapable を使用すると、システムは、ビッグデータのように分析することができ、より大きな時間は多くの情報です 情報の特定のターゲットとそのスキャンは、従来のシステムでは行うことができません したがって、さまざまなデータを即座に分析するAIモデルを開発する必要があります 即座に、そして発見することができました それは私が言っていることです簡単に攻撃してしまうので、情報が得られないと、

Professor R Mansour. 50:39
there's no obstacles, for example. Well, there is no obstacles. But if we have many sensors, then that could be only one or two sensors. And that's, I think, the importance, actually, for AI to address this kind of game.
例えば、障害物はありません。まあ、障害はありません。しかし、センサーが多数ある場合、それは1つまたは2つのセンサーだけになる可能性があります。そして、それが、実は、AIがこの種のゲームに取り組むことの重要性だと思います。

Professor R Mansour. 51:00
What I say, I think it's better to build the autonomous vehicle. Also, yeah, it will increase the cost of manufacturing this autonomous vehicle. But for the safety, we need to put some redundancies in the autonomous vehicle components.
私が言うのは、自動運転車を作る方が良いと思います。また、はい、この自律走行車の製造コストが増加します。しかし、安全性のためには、自動運転車のコンポーネントにいくつかの冗長性を持たせる必要があります。

Professor R Mansour. 51:20
With the redundancy, we can easily include the AI model. We can easily address any challenge or any cyber attack on the autonomous vehicle. Absolutely. That's one thing. There is... I'm sorry. Please.
冗長性により、AIモデルを簡単に含めることができます。自動運転車に対するあらゆる課題やサイバー攻撃に容易に対処できます。そうですよ。それが一つのことです。あるんだ。。。ごめんなさい。お願いします。

Professor R Mansour. 51:38
I always say, in my keynote speeches and conferences, always I get some information that might be new to some of the audience, because as a professor, I think there is one aspect of source of danger to the, especially the autonomous vehicle.
私はいつも、基調講演や会議では、聴衆の一部にとっては新しい情報を得ると常に言っていますが、それは教授として、特に自動運転車には危険の源の一つの側面があると考えているからです。

Professor R Mansour. 52:05
Because autonomous vehicle means electric car. That's the future. And as you know, that half of the car is a battery. So from my perspective, I think this is a very vulnerable point in any autonomous vehicle.
なぜなら、自動運転車は電気自動車を意味するからです。それが未来です。そして、ご存知のように、車の半分はバッテリーです。ですから、私の考えでは、これはどの自動運転車でも非常に脆弱な点だと思います。

Professor R Mansour. 52:26
It's the battery. Why I'm saying that? Because if the attacker can overcharge this battery, it might be... exploded, exploded. So this is, I think, this direction need to be addressed very well by the industry, by us as academia, and because we worked actually on wireless power transmission.
それはバッテリーです。なぜ私がそう言っているのですか?なぜなら、攻撃者がこのバッテリーを過充電できるとしたら、それは...爆発、爆発。ですから、この方向性は、産業界、私たち学界、そして私たちが実際にワイヤレス電力伝送に取り組んだことで、非常にうまく対処する必要があると思います。

Professor R Mansour. 52:52
And I am aware of some use of that company that sent through wirelessly high -power signals. So again, I think with the autonomous vehicle, we need to be careful about the charging system of the, not just the autonomous vehicle, but even the electric car.
そして、私は、無線で高出力の信号を送信したその会社のいくつかの使用を知っています。ですから、繰り返しになりますが、自動運転車については、自動運転車だけでなく、電気自動車の充電システムにも注意する必要があると思います。

Professor R Mansour. 53:13
Because this is a very weak point, and the entire car could use this point and get our chance to this battery, which is a huge battery, actually. We are not talking about small battery, we're talking even if the shuttle, half of it will be battery, if it is a truck, it will be.
なぜなら、これは非常に弱い点であり、車全体がこのポイントを使用して、実際には巨大なバッテリーであるこのバッテリーにチャンスを与えることができるからです。小さなバッテリーの話ではなく、シャトルであっても、その半分がバッテリーになり、トラックであればバッテリーになるという話です。

Professor R Mansour. 53:35
So I think this is something that needs to be addressed by the industry and I think it's very critical. And it could be addressed easy, like, you know, if we could protect the over the charging system of autonomous vehicle of the electric system, electric cars, I mean, we can address this and reduce the vulnerability of this point. Thank you.
ですから、これは業界が取り組むべきことであり、非常に重要なことだと思います。そして、電気自動車の自動運転車の過充電システムを保護できれば、この点に対処し、脆弱性を減らすことができるのです。ありがとうございます。

host 54:01
Absolutely. Thank you. Thank you for that Dr. Mansour. Mr. Allmotorib, sticking with data, how can we manage a balance for the need of data in analysis? I know that's critical for the topic we're talking about here, but how do we maybe manage not needing quite so much?
そうですよ。ありがとうございます。マンスール博士、ありがとうございました。Allmotorib氏は、データにこだわって、分析におけるデータの必要性に対してどのようにバランスを管理できるのでしょうか?ここで話しているトピックにとってそれが重要であることはわかっていますが、あまり必要としないためにはどうすればよいでしょうか?

Mr. Avodarev 54:22
Now, what we have done in Dubai, the Dubai government has published the Dubai data law. Within that law, it identified the rights of the data owner, which is the public entity or even the private sector, and also identified the rights and the obligation of the individuals as well.
さて、ドバイで行ったことは、ドバイ政府がドバイデータ法を公表したことです。その法律の中で、公的機関または民間部門であるデータ所有者の権利を特定し、個人の権利と義務も特定しました。

Mr. Avodarev 54:47
So this is very important because it sets the foundation on how to manage the data across all the systems, different platforms, different providers and so on. Other than that, it's very important and I have highlighted this in one of the answers also.
これは、すべてのシステム、さまざまなプラットフォーム、さまざまなプロバイダーなどでデータを管理する方法の基盤を築くため、非常に重要です。それ以外では、それは非常に重要であり、私は答えの1つでもこれを強調しました。

Mr. Avodarev 55:03
What information do we keep? And we use it for what? How do we store it? How do we classify it? Data classification is very important. We have seen a lot of people or the entities that do not, let's say, store critical information in the right way and we have seen it leaked out on the public, or even on that purpose, but it can be sold for quite amount of money.
どのような情報が保持されていますか?そして、私たちはそれを何に使うのでしょうか?どのように保管しますか?どのように分類しますか?データの分類は非常に重要です。私たちは、重要な情報を正しい方法で保存しない多くの人々や団体を見てきました。そして、それが公に漏れたり、その目的で漏洩したりするのを見てきましたが、それはかなりの金額で売ることができます。

Mr. Avodarev 55:35
So having those protections, realizing the amount of data and the type of data that you have is very important for every single entity. Now how do you analyze those data? This is a different subject also that needs to be highlighted.
したがって、これらの保護を持ち、データの量とデータの種類を認識することは、すべてのエンティティにとって非常に重要です。では、これらのデータをどのように分析しますか?これもまた、強調する必要がある別のテーマです。

Mr. Avodarev 55:53
Which tool are you using? Is it a reputable tool or just any tool from the open market? Does it protect your data when it analyzes the data? You know a lot of those tools now available in a cloud based form.
どのツールを使用していますか?それは評判の良いツールですか、それとも公開市場からの任意のツールですか?データの分析時にデータを保護しますか?これらのツールの多くが、クラウドベースの形で利用できるようになりました。

Mr. Avodarev 56:09
So a lot of these data are crossing your borders and you need to check back with the regulator. Are you allowed to share those type of data with an entity outside your country? There is a lot of things that needs to happen within this subject.
そのため、これらのデータの多くは国境を越えており、規制当局に再度確認する必要があります。これらの種類のデータをあなたの国以外のエンティティと共有することは許可されていますか?このテーマでは、多くのことが起こらなければなりません。

Mr. Avodarev 56:24
But the most important thing is for people who are dealing with data. They need to understand what they are dealing with and how to protect it. the data that they have, and how to collect the right data that they need for their own analysis or for the purpose of an assay research and so on.
しかし、最も重要なことは、データを扱っている人々にとってです。彼らは、自分たちが何を扱っているのか、そしてそれをどのように保護するのかを理解する必要があります。彼らが持っているデータ、そして彼ら自身の分析やアッセイ研究の目的で必要な適切なデータをどのように収集するかなど。

host 56:46
Thank you so much. I'd like to turn the topic slightly. I know we're focusing primarily on cybersecurity, but in theme with Vision Zero and theme of ITS World Congress, we hear a lot about safety. Obviously, as a consumer and as many consumers, I think that's one of the biggest concerns when it comes to autonomous vehicles and connected vehicles.
どうもありがとうございます。少し話を転じたいと思います。私たちは主にサイバーセキュリティに焦点を当てていますが、Vision Zeroのテーマ やITS世界会議のテーマでは、安全性についてよく耳にします。明らかに、消費者として、そして多くの消費者として、自動運転車やコネクテッドカーに関しては、それが最大の懸念事項の1つだと思います。

host 57:11
I live in Houston, Texas. We have very few autonomous vehicles. We don't even have really much of a public transportation system either, but there's this common term used called utility, kind of changing the mindset of people to accept maybe a different mode of travel. Not too far from us is Austin, Texas, where you have autonomous taxis driving around the city streets. Nobody's in them, nobody's in them. They're following each other in cadence. Nobody's really riding these vehicles.
私はテキサス州ヒューストンに住んでいます。自動運転車はほとんどありません。公共交通機関もあまりありませんが、ユーティリティと呼ばれる一般的な用語があり、人々の考え方を変えて、おそらく異なる移動手段を受け入れるようにしています。 私たちからそれほど遠くないところにテキサス州オースティンがあり、市内の通りを自動運転タクシーが走っています。誰もいない、誰もいない。彼らはリズムでお互いを追いかけています。誰も本当にこれらの乗り物に乗っていません。

host 57:43
On occasion, they do, and you'll see somebody post a video that they took a ride in an autonomous vehicle. Not really sure they're that excited about taking it onto the highway, but the city street seems a little bit safer, maybe a little bit better place to start.
たまに、自動運転車に乗った動画を投稿する人もいるでしょう。彼らが高速道路に乗ろうとそれほど興奮しているかどうかはわかりませんが、街の通りは少し安全で、おそらく始めるのに少し良い場所のように思えます。

host 57:59
How can we change that mindset and get people to start taking advantage of this mode of travel?
どうすればその考え方を変え、人々がこの移動手段を利用し始めることができるでしょうか?

Mr. Avodarev 58:06
This question is best to me. Joe, I'll keep it with you, please. All right. Now, Eric, I gave you an example on what we have done for the metro.
この質問は私にとって最善です。ジョー、君と一緒に保管しておいてね。大丈夫です。さて、エリックさん、私たちが地下鉄のために行ったことの例を挙げました。

Mr. Avodarev 58:16
So I don't advise that you go a big bang from the beginning. Okay, you need to go easy with people. Different people, they have different mindsets. They have different level of absorbing those type of things.
ですから、最初から大胆にやることはお勧めしません。さて、あなたは人々と気楽に過ごす必要があります。人によって、考え方も異なります。彼らは、この種のものを吸収するレベルが異なります。

Mr. Avodarev 58:30

And I'll be honest with you, I have tried two months ago. I was in San Francisco. and I have tried the way most air service. It is available for the public to be used in certain areas and you have ever experienced a drive in San Francisco, we have a very complicated road network.
そして、正直に言うと、私は2ヶ月前に試しました。私はサンフランシスコにいました。そして、私はほとんどの航空サービスを試しました。それは特定の地域で使用するために一般の人々が利用可能であり、あなたはこれまでにサンフランシスコでドライブを経験したことがあります、私たちは非常に複雑な道路網を持っています。

Mr. Avodarev 58:47
So I have decided to try one and believe it or not, I do have an experience jumping into different autonomous vehicles because we are testing them here in Dubai. But in San Francisco when I tried it, trust me, it was not a pleasant journey for the first couple of minutes.
だから、私は1つ試してみることに決めました、そして信じられないかもしれませんが、私たちはここドバイでそれらをテストしているので、私はさまざまな自律走行車に飛び込んだ経験があります。しかし、サンフランシスコで試してみたとき、信じてください、最初の数分間は楽しい旅ではありませんでした。

Mr. Avodarev 59:07
I was not absorbing what's really happening. Few minutes later, yes, I started to realize and I started to accept, yes, it is getting me to my destination safely. But the thing is, a lot of the vehicles around the Waymo vehicle understood that this is an autonomous vehicle and this is a very important factor.
私は実際に何が起こっているのかを吸収していませんでした。数分後、はい、私は気づき始め、受け入れ始めました、はい、それは私を無事に目的地に連れて行ってくれました。しかし、問題は、Waymoの車両の周りにいる多くの車両が、これが自律走行車であり、これが非常に重要な要素であることを理解していたということです。

Mr. Avodarev 59:30
Now, in the US, You don't have this mix of culture like what we have in Dubai and the UK, you will have a different situation. So each country has its own flavor when it comes to the mix of, let's say, driving cultures.
さて、アメリカでは、ドバイやイギリスのような文化のミックスはなく、状況は異なります。ですから、例えば、運転する文化の組み合わせに関しては、各国ごとに独自の特徴があります。

Mr. Avodarev 59:47
And this is something that needs to be taken into consideration. This is the reason why you need to test your community first. So don't go big bang, go gradually, put the safety driver, let people accept the concept of autonomous drive.
そして、これは考慮する必要があることです。これが、最初にコミュニティをテストする必要がある理由です。ですから、ビッグバンに行かず、徐々に行き、安全ドライバーを配置し、人々に自律運転の概念を受け入れさせてください。

Mr. Avodarev 01:00:01
Let the people around the vehicle understand that this is an autonomous vehicle. They need to know how to deal with situations. God forbid, if there is an accident, that might occur.
車両の周りの人々に、これが自律走行車であることを理解させてください。彼らは状況に対処する方法を知る必要があります。神は禁じられています、もし事故があれば、それは起こるかもしれません。

host 01:00:16
Thank you so much. Mr. Skora, can you expand upon the topic as well, specific to autonomous shuttles? So naturally I would feel slightly more safe and secure. And at the time of this show, perhaps that's not correct. No, no, I agree with you because the shuttle is going at a slower speed and makes it a little bit more safer.
どうもありがとうございます。スコラさん、自律型シャトルに特化したトピックについても詳しく説明していただけますか?だから当然、少しだけ安心感が増しました。そして、この番組の時点では、それは正しくないかもしれません。いやいや、シャトルはゆっくりとした速度で進んでいるので、少し安全になるので、私も同意します。

Mr. Sikora 01:00:46
Well, coming back to my experience, it's very similar. We just finished a project, a long project on the air side in Amsterdam, the airport, Skipper, where we had different use cases. The first use case was bringing employees from the entry gates to their workplaces.
さて、私の経験に戻ると、それは非常に似ています。アムステルダムの空路、空港、スキッパーでの長いプロジェクトを終えたばかりで、さまざまなユースケースがありました。最初のユースケースは、従業員を入場ゲートから職場に連れて行くことでした。

Mr. Sikora 01:01:18
And these were employees who are not very technical related. It was the cleaning area or the cleaning personalities. going to, and they started to be a little bit reluctant. But as we had a safety driver on board, we could tell them, well, how the vehicle is reacting, that the vehicle is constantly looking around the vehicle for obstacles, there's a perception system that relies on sense of fusion,
そして、彼らはあまり技術に関係のない従業員でした。それは掃除エリア、または掃除の性格でした。そうすると、彼らは少し気が進まなくなりました。しかし、セーフティドライバーが同乗していたので、車両がどのように反応しているか、車両が常に車両の周囲に障害物がないか見ていること、フュージョン感覚に依存する知覚システムがあることを伝えることができました。

Mr. Sikora 01:01:59
things like that. But telling them, in other words, that it's a safe ride. And from the start, they were very reluctant, and then it becomes a little bit more like a day -to -day usage to learn. The other use case was that we brought crew members from parked aircrafts to the crew center.
そんな感じです。しかし、言い換えれば、それは安全な乗り物だと彼らに伝えることです。そして、最初から彼らは非常に消極的でしたが、その後、それは少し日々の学習方法のようになります。もう1つのユースケースは、駐機中の航空機からクルーセンターにクルーを連れてきたことです。

Mr. Sikora 01:02:31
Absolutely. technical affected persons and they from the beginning they wanted to push the button to start the vehicle and they were very very excited about this right and it's absolutely different so there's within the population of a country there's differences and as well it's it was very important just to mention this that we informed the already existing drivers on the air side or everywhere that there's an autonomous vehicle coming if they don't know it then they cut our road and it ends up in an emergency brake or they are driving very close to us from behind so it's very important that everybody who is part of the traffic system knows about it and can accept it and then you have to educate the the riders as well as I mentioned otherwise I think the acceptance is is key for this and you won't get the acceptance.
そうですよ。技術的な影響を受けた人々、そして彼らは最初から、車両を始動するためにボタンを押したいと思っていました、そして彼らはこの権利に非常に興奮していました、そしてそれは絶対に異なるので、国の人口内には違いがあります、そしてまた、これに言及するだけで非常に重要でした、私たちはすでに存在するドライバーに、彼らがそうしない場合に自律走行車が来ることを知らせましたそれを知っている、そして彼らは私たちの道路を切断し、それは緊急ブレーキに終わるか、彼らは後ろから私たちのすぐ近くを運転しているので、交通システムの一部である誰もがそれについて知っていて、それを受け入れることができることが非常に重要です、そして、私が述べたように、ライダーを教育する必要がありますそうでなければ、私は受け入れがこれの鍵であり、あなたは受け入れを得ることができないと思います。

host 01:03:50
Absolutely thank you Dr. Mansour kind of like to talk about the auto manufacturers how do we get the auto manufacturers to participate more in connected vehicle an autonomous vehicle perhaps the fear of liability there are automobile manufacturers that are the technology standard it's available how do we how do we influence that?
マンスール博士は、自動車メーカーについて話すのが好きで、コネクテッドカー、自動運転車、おそらく責任の恐れ、利用可能な技術標準である自動車メーカーが存在する自動車メーカーについて話すのが好きです。

Professor R Mansour. 01:04:13
Yeah okay but first I want to comment on the ways the same topic actually RTA was actually Bioneer in fact they initiated I think the autonomous vehicle competition every year And, you know, mighty University of Dubai actually, we won, I think, the first version of, the second version of the autonomous vehicle.
ええ、わかりました、しかし、最初に私は同じトピックについてコメントしたいと思います、実際にはRTAは実際にバイオニアでした、彼らは毎年自動運転車の競争を開始し、そして、ご存知のように、強大なドバイ大学は、実際には、自動運転車の最初のバージョン、2番目のバージョンを勝ち取ったと思います。

Professor R Mansour. 01:04:44
Last year it was very interesting, which is very related to the topic that we are talking about, about the, you know, how could we make the people trust the autonomous vehicle, or use the autonomous vehicle.
昨年は非常に興味深く、私たちが話しているトピックと非常に関連していますが、それは、人々が自動運転車を信頼し、自律走行車を使用するためにはどうすればよいかということです。

Professor R Mansour. 01:04:58

So, last year the theme of the RTA autonomous vehicle competition was the user experience. So, and it was very nice, and my team actually participated, and we came up with a very nice solution. We've been shortlisted top six, so that's a good achievement from our university.
そのため、昨年のRTA自動運転車コンペティションのテーマはユーザーエクスペリエンスでした。ですから、それはとても素晴らしく、私のチームが実際に参加して、非常に素晴らしい解決策を考え出しました。私たちはトップ6の最終選考に残ったので、それは私たちの大学の良い成果です。

Professor R Mansour. 01:05:22
So, yes, I think user experience is very important. We need to develop this system autonomous. vehicle system that accept some information from the users, not just rely on the autonomous system. And that's what actually what we did in that sense.
ですから、ユーザーエクスペリエンスは非常に重要だと思います。このシステムを自律的に開発する必要があります。ユーザーからの情報を受け入れる車両システムは、自律システムに依存するだけではありません。そして、それがその意味で実際に私たちが行ったことです。

Professor R Mansour. 01:05:46
So I think this will increase the confidence and the trust to the autonomous vehicle. Yes, because I'm going to use the autonomous vehicle, but there's a way that I could prevent a disaster. This is what actually the main idea of user experience of first -year theme of the RTA.
ですから、これにより自動運転車への信頼と信頼が高まると思います。はい、自動運転車を使用するつもりですが、災害を防ぐ方法があります。これが、RTAの初年度のテーマのユーザーエクスペリエンスの主な考え方です。

Professor R Mansour. 01:06:10
Again, definitely technology needs to be advanced in the direction of autonomous vehicle, as I said, more reliable systems, definitely more use of AI, because when we talk about autonomous vehicle, we talk about big data.
繰り返しになりますが、私が言ったように、自動運転車の方向に技術を進めることは間違いなく必要です、より信頼性の高いシステム、間違いなくAIの使用を増やす必要があります。

Professor R Mansour. 01:06:32
A lot of information and this information cannot be analyzed unless we use AI models to analyze them efficiently. So it's a mix between the software and hardware.
多くの情報とその情報は、AIモデルを使用して効率的に分析しない限り、分析できません。つまり、ソフトウェアとハードウェアが混在しているのです。

host 01:06:49
Absolutely. I think that's a good opportunity for us to close out the guided discussion. I'd like to open it up to the audience for any questions to the panelists, any that you may have. I'd be happy to come to you with a microphone. Thank you.
そうですよ。これは、ガイド付きディスカッションを締めくくる良い機会だと思います。パネリストへの質問は、聴衆の皆さんにもお聞かせください。マイクを持ってお越しいただければ幸いです。ありがとうございます。

Questionor1 01:07:12
Thank you so much for the insightful session. I have a question to Dr. Wath. We are aware of the cybersecurity attacks that are related to AI models, such as the adversarial attacks, mislead or deceive the model to generate wrong outcomes. But when it comes to the unacceptable inability of the model, when it comes to the deep learning models, widely used in autonomous vehicles, who will ultimately give the autonomous vehicle the right to take a decision in certain situations, choosing between, for example, hitting two guys with one guy or an old guy and a small kid. So is that something that would be part of the international standards or the role of the authorities, which will be licensed?
洞察に満ちたセッションをありがとうございました。ワス博士に質問があります。私たちは、敵対的攻撃など、AIモデルに関連するサイバーセキュリティ攻撃、モデルを誤解させたり欺いたりして間違った結果を生み出すことを認識しています。しかし、モデルの許容できない無能さに関しては、自律走行車に広く使用されているディープラーニングモデルに関しては、最終的には自律走行車に特定の状況で決定を下す権利を与えます。たとえば、2人の男を1人の男とぶつけるか、老人と小さな子供を殴るかを選択します。では、それは国際基準の一部となるものなのか、それとも当局の役割の一部となるのか、それともライセンスされるものなのでしょうか?

Professor R Mansour. 01:08:15
Thank you very much, Dr. Raval, for this part of the question. Yes, we come back to the regulations. So I think that your question is strongly related to the regulations. So, with regulations, everything would be clear and definitely the point being raised by you is the ethical issue, ethical issues by AI model which is, I think, we work on this thing and we take it seriously.

ラバル博士、この質問の部分をありがとうございました。はい、レギュレーションに戻ります。ですから、あなたの質問は規制と強く関連していると思います。ですから、規制があれば、すべてが明確になり、間違いなく皆さんが提起しているのは、AIモデルによる倫理的な問題であり、私たちはこの問題に取り組み、真剣に受け止めていると思います。

Professor R Mansour. 01:08:48
Some say that, okay, the AI model will copy or follow the ethics being provided by the designer or the creator of the AI model. But this would be prevented or eliminated heavily by the regulations and that's why I mentioned earlier about explainable AI.
AIモデルは、AIモデルの設計者や作成者が提供する倫理を模倣したり、それに従うと言う人もいます。しかし、これは規制によって大幅に防止または排除されるため、説明可能なAIについて先に述べたのはそのためです。

Professor R Mansour. 01:09:13
With explainable AI, we could, as like, you know, regulatory authority, can we see, evaluate this AI model. And this is very important, Sir Mohammed, I think, that there should be some entity in the government that could give, like, you know, certifications.
説明可能なAIを使えば、規制当局のように、このAIモデルを見て評価することができます。そして、これは非常に重要なことだと思いますが、サー・モハメッドは、政府内に、例えば、認証を与えることができる何らかの機関が存在するべきだと考えています。

Professor R Mansour. 01:09:37
And this is very important certification to the AI model because the AI models are a lot, it would be a lot of hundred thousand or more of AI models. But we need certification and this certification could be, should be in, like, no local.
そして、これはAIモデルにとって非常に重要な認証であり、AIモデルはたくさんあり、数十万以上のAIモデルになります。しかし、私たちには認証が必要であり、この認証は、地元のものではないかもしれませんし、そうあるべきです。

Professor R Mansour. 01:09:54
For the way they have a certain certification entity that could certify the AI model that could be used for not only for autonomous vehicles, for any part of the system. Thank you very much for the question.
彼らは、自律走行車だけでなく、システムの任意の部分に使用できるAIモデルを認証できる特定の認証エンティティを持っています。ご質問ありがとうございます。

Questionor2 01:10:14
Thank you very much for your time today. I've got a quick question regarding supply chain security. Given the increasing reliance on software and hardware from various suppliers, the automotive and mobility industry, how might it be possible potentially to kind of ensure the security? of those third -party components for the classical kind of importing of technologies predicted to the automotive industry and even how would that be affected if a country has a strategy in assembling cars or getting into the automobile industry in terms of assembly let alone manufacturing as well. Thank you.
本日はありがとうございました。サプライチェーンのセキュリティについて簡単に質問があります。自動車業界やモビリティ業界など、さまざまなサプライヤーからのソフトウェアやハードウェアへの依存度が高まっていることを考えると、セキュリティを確保するにはどうすればよいのでしょうか?自動車業界に予測される技術の古典的な種類の輸入のためのこれらのサードパーティのコンポーネントのうち、さらには国が自動車を組み立てたり、組み立ての面で自動車産業に参入する戦略を持っている場合、それはどのように影響を受けるでしょうか。ありがとうございます。

Mr. Sikora 01:10:53
To be honest, the first step would be to ask for a certification related to cyber security. This is the first, then you might come up with the question how can you be sure that this is, then you need to do testing as well.
正直なところ、最初のステップはサイバーセキュリティに関連する認証を求めることです。これが最初で、次に、これが確実であることをどのように確認できるかという質問を思いつくかもしれません、その後、テストも行う必要があります。

Mr. Sikora 01:11:14
This is not only the functional testing but also the testing on potential potholes, potential open -attack holes. You need to check for a certain portion and to test it, otherwise I don't believe that there's so many options.
これは、機能テストだけでなく、潜在的なポットホール、潜在的なオープンアタックホールのテストでもあります。あなたは特定の部分をチェックし、それをテストする必要があります、そうでなければ私はそれほど多くの選択肢があるとは思わない。

Mr. Sikora 01:11:38
The other thing is what is general has to be done during the design of the vehicle is to separate safety critical functions from

functionality that has an interface to the tower or whatever, to separate different functions according to the importance for safety.
もう一つは、車両の設計中に一般的に行わなければならないことは、安全上重要な機能をタワーなどへのインターフェースを持つ機能から分離し、安全性の重要性に応じて異なる機能を分離することです。

Mr. Sikora 01:12:06
This is one thing as well, and based on AI or not, but in our case as well, based on AI doing sensor fusion, having redundancy and checking different parts from different vendors as well. So this should end up in the same reaction of the vehicle if you change the vendors, but otherwise I don't have an idea how to overcome this situation.
これも一つのことであり、AIに基づいているかどうかは別として、私たちの場合も、AIがセンサーフュージョンを行い、冗長性を持ち、異なるベンダーのさまざまな部品をチェックすることに基づいています。したがって、ベンダーを変更した場合、これは車両と同じ反応で終わるはずですが、そうでなければ、この状況をどのように克服するかがわかりません。

Questionor3 01:12:38
Thank you. Thank you so much for this well -experienced panelist and the discussion. My question is to Mr. Robert and I remember I left ITS 2014 in Detroit for the same question. Don't you think the gap between the manufacturing of infrastructure and from your experience being in the field of manufacturing the vehicles as autonomous is one of the the risk or challenges that creating this safety or secret issue. For example we do hear about V2X but the examples that we see today with liver 4 or liver 3 .5 or whatever to those vehicles is only depending on the car technology only without any interconnecting with the infrastructure. Let me just give you an example. The security or safety of the passengers versus the pedestrian. If there is an infrastructure saying to the car that there is pedestrian on the line corner, this will take an action. But we're not seeing this on a radio. Way more Tesla, others are doing it their own. When I ask the infrastructure guys the same question they say, it is the carbon factor who doesn't want to take our information. So how to resolve this issue?
ありがとうございます。経験豊富なパネリストとディスカッションをありがとうございました。私の質問はロバートさんへのもので、私も同じ質問のためにデトロイトのITS 2014を去ったことを覚えています。インフラの製造と、自動運転車として車両を製造する分野での経験との間のギャップが、この安全性や秘密の問題を生み出すリスクや課題の1つだと思いませんか。例えば、V2Xという言葉はよく耳にしますが、今日、肝臓4や肝臓3.5などの車両に見られる例は、インフラとの相互接続がなく、自動車技術のみに依存しています。例を挙げましょう。乗客と歩行者のセキュリティまたは安全性。ラインコーナーに歩行者がいると車に言っているインフラがある場合、これはアクションを取ります。しかし、これはラジオでは見られません。テスラの方がはるかに多く、他の人は自分でやっています。インフラの人たちに同じ質問をすると、私たちの情報を受け取りたくないのは炭素要因だ、と彼らが言うのです。では、この問題を解決するにはどうすればよいでしょうか?

Mr. Sikora 01:14:05
Tough question. I can just answer from the vehicle manufacturer for short. So what we are trying to get is a complete perception of the environment. This includes vulnerable services like cyclists or cars.
難しい質問です。私は簡単に自動車メーカーから答えることができます。ですから、私たちが得ようとしているのは、環境の完全な認識です。これには、自転車や車などの脆弱なサービスが含まれます。

Mr. Sikora 01:14:27
and pedestrians as well. It includes even dogs driving around. And the bad thing is it includes as well the flying birds, which in many situations leads to an emergency stop. You know that. I think we would be very open to establish an interface to, to, if vulnerable bird users can provide information where they are, and there are actually at the moment standardization efforts in place to do that via a cell phone.
そして歩行者も。犬が走り回っているところも含まれます。そして悪いことに、それは飛んでいる鳥も含んでいるので、多くの状況で緊急停止につながります。そのことを知っていますよね。脆弱な鳥のユーザーがどこにいても情報を提供できる場合、私たちは非常にオープンなインターフェースを確立することができると思いますし、実際に現在、携帯電話を介してそれを行うための標準化の取り組みが行われています。

Mr. Sikora 01:15:08
Everybody, nearly everybody has a cell phone at the moment. And he could, this person could as well distribute collective awareness messages like be continuous messages. And if it's common to do that, then we would be happy to include it into our sensor fusion system.
今は、誰もが、ほぼ全員が携帯電話を持っています。そして、彼は、この人は、継続的なメッセージのように、集合的な意識のメッセージを配布することもできました。そして、それが一般的であるならば、私たちはそれを私たちのセンサーフュージョンシステムに含めることを嬉しく思います。

Mr. Sikora 01:15:30

But not only rely on this information, but on others as well. This is again one thing that I have to answer you, Christian, I'm sorry. Thank you. Looks like we don't have any other questions, so we'll go ahead and wrap up, and I've got some closing remarks.

しかし、この情報だけでなく、他の情報にも頼っています。これもまた、クリスチャン、ごめんなさい、あなたに答えなければならないことの一つです。ありがとうございます。他に質問はなさそうですので、最後にお話しします。

Mr. Sikora 01:15:53

So first and foremost, I want to thank our panelists, Mr. Williams, and our panelists.

何よりもまず、パネリストの皆様、ウィリアムズさん、そしてパネリストの皆様に感謝したいと思います。