

Introduction to Industry 4.0 and Industrial Internet of Things
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 45

Advanced Technologies: Software-Defined Networking (SDN) in IIoT – Part 1

In this particular module I am going to highlight 2 important advanced concepts which are advanced in the sense that you know you may or may not use them for building your IIoT for a specific industrial problem, but these will help you to do efficient network setup for efficient network management and so on and also for securing the system. These are important, these are not mandatory, but are definitely important and I would recommend that one should consider these technologies for implementation in a real IIoT setup that is being made.

So, these 2 technologies are number 1 the software defined networks and number 2 the security; security is more common which is more applicable usefulness of securities quite imminent, but SDN is something whose benefits will be clearer to you in this particular lecture once we go through all the different concepts that we are going to.

So, what is this SDN, what is software defined networks and where does it position itself in the IIoT context? Software defined networks basically targets to have efficient and more effective representative network management in the IIoT setting. It is not necessary that SDN has to work only with IIoT, but because this particular course focuses on IIoT we are going to talk about SDN in the context of IIoT, but SDN applies for any kind of networks and also for networks such as your traditional internet, other different types of wireless networks and definitely for industrial IoT and IoT in general.

So, efficient and effective network management how it is going to be done, if we are talking about IIoT specifically the nature of traffic the requirements from the organizations these basically are non static, these basically change with time the traffic, the nature of traffic, the requirements of the traffic, the requirements from the clients, the specific installations the machinery everything is dynamic they change with time.

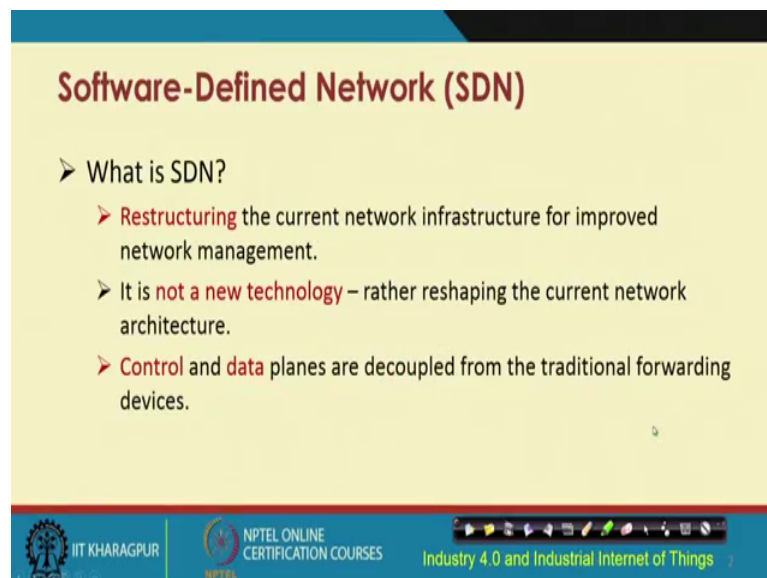
So, if we are talking about network management static traditional network management techniques are not very suitable to cater to the requirements of dynamism. They could

indeed be used, but you know if we are talking about autonomous deployments, autonomous setups and so on. It is important to cater to the dynamic requirements as much autonomously as possible, take for instance the routing tables, routing in traditional network. Routing in a traditional network basically you have routing tables which are stored which are pre-configured in different different routers, switches and so on.

These routing tables will basically help the data packets that are coming to these devices to know where they are going to go to. So, and these rules basically are fixed rules which are embedded in each of these different devices the routers, switches and so on. But if the traffic requirements change, if the overall requirements of the system changes, if the system architecture changes over time, then static rule based routing mechanisms are not very suitable this is just an example that I just gave you.

And you can extrapolate it to cater to the other different types of requirements scenarios and so on so, for which you need to have dynamic mechanisms in place. So, SDN is one such technology which can help you to address the requirements of dynamism that are there in most of this industrial communication settings.

(Refer Slide Time: 04:47)



Software-Defined Network (SDN)

- What is SDN?
 - **Restructuring** the current network infrastructure for improved network management.
 - It is **not a new technology** – rather reshaping the current network architecture.
 - **Control** and **data** planes are decoupled from the traditional forwarding devices.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things

So, what is this SDN? In SDN we are typically talking about decoupling of the data plane from or the decoupling of the control plane from the data plane.

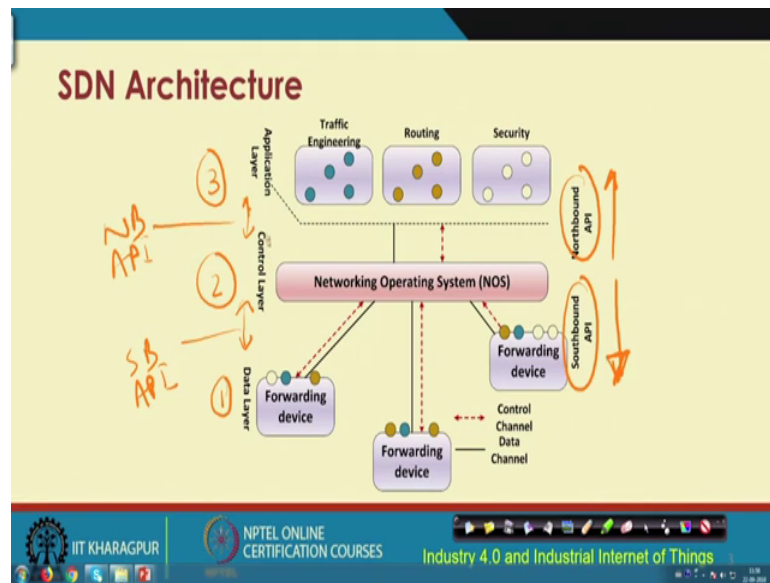
So, earlier traditionally in most of these switches, routers that are used in the internet conventionally used to have everything together. The control mechanism the data everything is basically stored p configured static in each of these individual network equipment like your router, switches and so on. In SDN what we are talking about is how you can separate out the control from this individual data that are stored in each of these different different network equipments and have a separate layer which is the control layer having an entity a network entity which is termed as the controller.

So, that controller is the one which is going to control each of these different network entities which are there like switches, routers etcetera and this controller entity the network entity controller basically is going to help in controlling each of these different devices which are part of the data plane. So, what is this SDN, it is the restructuring of the current network infrastructure for improved network management.

So, when we talk about restructuring as this particular term the qualifier suggests that it is not a new technology, but a technology that will help you to reengineer to reshape to relook at the current network the conventional network architecture and provide an efficient mechanism of doing things.

So, how it is done as I told you earlier it can be done by separating out the control plane from the data plane a process of decoupling that will have to happen and by which the traditional forwarding devices will only take care of what they are instructed to do by the controller the control plane equipment.

(Refer Slide Time: 07:05)



So, holistically this is how this SDN architecture is going to look like. So, this SDN architecture irrespective of whether it caters to the IIoT or IoT traffic or not, is going to have 3 different layers broadly 1 is your data layer, 2nd is the control layer and 3rd is the application layer.

So, we have 3 different layers, layer 1 devices are like forwarding devices like your routers etcetera these different forwarding devices, layer 2 device is the controller which basically also takes care of the network operating system which runs the network operating system. And then you have the applications which are running on the very top in the layer 3 this is this application layer where your business logic your different applications are running.

So, basically you have 3 different layers. So, the one switcher below these layers which are below the control the controller or the control layer this basically is known as the South bound API, once which are above are known as the North bound API. So, there are 2 APIs right application programming interface one interface between this control layer and the application layer.

So, this is one interface over here and this is another interface. So, this interface is known as the North bound API and this particular interface is known as the South bound API. So, this South bound API in other words basically concerns the interface between

the control layer and the data layer whereas, the Northbound API concerns the interface between the control layer and the application layer.

(Refer Slide Time: 09:10)

The slide is titled "SDN Components/Attributes" and lists the following components:

- Application programming interfaces (APIs)
 - Southbound API
 - Northbound API
- Logically centralized controller
- Forwarding devices
- Protocol – **OpenFlow**
- Applications

The slide footer includes the IIT KHARAGPUR logo, NPTEL ONLINE CERTIFICATION COURSES logo, and the text "Industry 4.0 and Industrial Internet of Things".

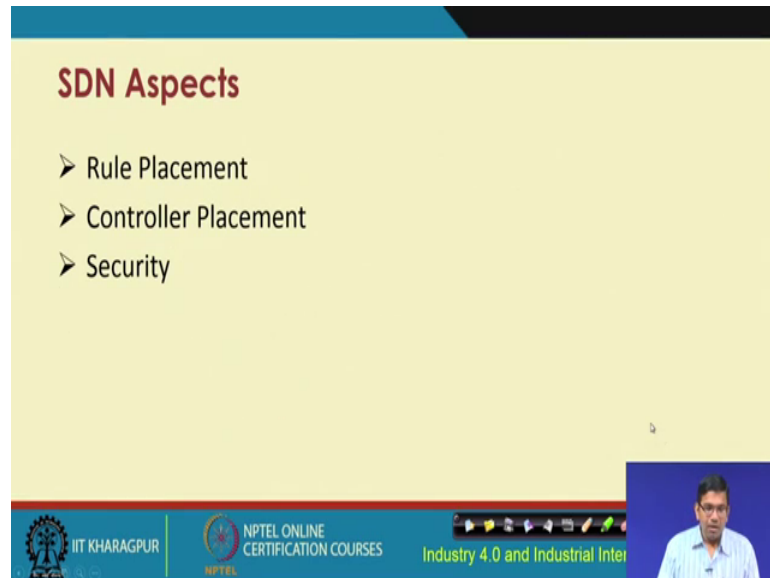
So, there are different components of the SDN Northbound and Southbound APIs are the ones that I just mentioned likewise there is this controller which is a logical centralized entity which is basically controlling this different data layer devices. There are forwarding devices in the data layer which basically takes care of mere forwarding based on the rules that are basically implemented in them that are configured in them. You also have to support this entire stuff you have to have some protocol which is going to help you to do whatever I just explained earlier.

So, there is a very popular protocol which is known as the open flow protocol which is specifically designed to cater to the requirements and the necessities of supporting SDN in a network software defined networks basically will be supported by this open protocol. The protocol started from the 1 dot 1 version and currently it is at 1 dot 5.

So, open flow 1.5 is the protocol that is open flow protocol that is the latest one which could be used and each of these different protocols and its different versions 1 dot 1, 1 dot 2 till 1 dot 5 has its own individual features. But holistically open flow as a whole will cater to the configuration of SDN in a particular network and on the top you have these different applications so, these are these different components of SDN. So, these apply as I said earlier to any kind of network where internet wireless or IoT or IIoT, but

IoT or IIoT has its own specific requirements and the configuration of the deployment of SDN for IoT, IIoT is something that is nontrivial.

(Refer Slide Time: 11:06)



The slide is titled "SDN Aspects" and lists three key areas: Rule Placement, Controller Placement, and Security. It is part of an NPTEL online course from IIT Khharagpur, specifically for "Industry 4.0 and Industrial Inter". A small video inset shows the presenter.

SDN Aspects

- Rule Placement
- Controller Placement
- Security

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Inter

So, before we discuss about those non trivialities let us talk about some of these different aspects. So, in SDN we need to understand few different concepts which will make us to understand further how SDN can cater to the requirements of IIoT. Number 1 is rule placement, second is controller placement and third is security, rule placement, controller placement and security are the 3 most important concepts that one should know in SDN.

So, let us try to go through each of these there are different different research papers that talk about different ways of rule placement, different ways of controller placement, different security mechanisms and so on, but we will go through some of these very naive high level views of each of these different concepts to make us understand what these are.

(Refer Slide Time: 11:55)

Rule Placement

- Forwarding devices forward an incoming traffic based on the control logic defined by the SDN controller.
- The control logic is placed at the devices in the form of flow-rule.
- Ternary content addressable memory (TCAM) available at the devices is used to place the flow-rules.
- TCAM is limited – limited number of flow-rules can be placed.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things

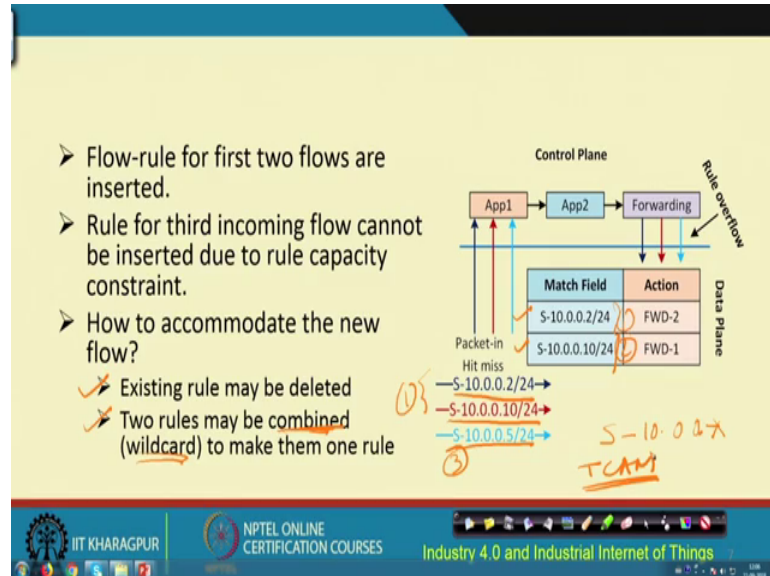
So, in the rule placement basically what we are talking about is that we have different forwarding devices that forward the incoming traffic based on certain control logic that is again defined by the SDN controller. And this control logic is basically placed at the devices; that means, in the data layer in the form of something known as the flow rule and it is this flow rule that we are talking about in this particular context.

Before we talk any further I should also tell you something else, these flow rules are basically stored in a memory in each of these devices which is known as the TCAM memory the full form of which is Ternary Content Addressable Memory. That are there the TCAM memory are there in each of these devices; that means, the data plane devices; that means, your router or the forwarding devices you have all these TCAM memory that are there which will store the different flow rules.

Now, this TCAM memory is very small and consequently this TCAM memory in each of these forwarding devices will store only a limited number of flow rules. So, this only a limited number of flow rules can be stored and that makes the life challenging about how you are going to design your flow rules and so on, because you have very limited space in the TCAM which can store your flow rules. If that was not there you could have if that constant was not there you could have a bunch of different flow rules all being stored in the TCAM memory for further use, but because that constant is there you need to now

know how you are going to design your flow rules, where you are going to place, how you are going to place and so on of these different rules.

(Refer Slide Time: 13:43)



So, let us now try to understand further how this TCAM and this 4 rule placement is going to work together what is this constant all about and we have to try to appreciate how this constant is going to bring in these different different issues which will have to be addressed.

So, let us say that you have all these different flows that are coming right. So, let us say that first you have 2 different flows like the ones that are shown over here, you have 2 different flows; you have 2 different flows like the ones let us say that these 2 flows have already come in. So, the flow rule for the first two flows are already inserted because that was not already there so, it is already inserted in your TCAM.

So, then corresponding actions for these different different flow rules are also mentioned in that data plane. So, basically you have for each of these flow rules you have the corresponding actions that are also specified. So, if certain traffic comes next so, what is going to happen is this matching is going to be done with this particular flow rule and based on this particular matching if the matching happens, then the corresponding action that is specified against these flow rules are going to be; are going to be taken so, these actions are going to be taken.

Now, let us say that you have a third incoming flow that comes this is this third one let us say that we have to deal with this third one so, first and second already dealt with stored over here. So, one and 2 already store now the third one comes. So, let us say that this particular TCAM memory can store only 2 flow rules, the third one comes and you will have to be either inserted to give the constraint to specify that constraint in this particular table or how do you deal with it; how do you deal with it. So, how do you accommodate this new flow?

There are 2 ways, one way is that you delete one existing rule and you insert the third one the other possibility is that you have to combine. So, you can using some wild card or other mechanisms you can have combined rules which will cater to multiple such rules together which will combine multiple rules together. For example, over here you can have is S 10 dot 0 dot 0 dot 2 here also you have S 10 dot 0 dot 0 dot 10. So, you can have a wild card and you could have something like S 10 dot 0 dot 0 dot star which will match both, but then although you can combine in the using a wild card like star etcetera you could combine these two in the form of one rule, but then that will also not make it very specific right.

So, those constants are also there, but you know certain cases you know this kind of combination will make sense and one could use. So, you we what we have seen is that TCAM memory has its own different constraints, we could only store few rules in it and if you have a additional rule coming in which cannot be stored, then it has to be handled in a certain way wild card mechanism is one, but then it has its own disadvantages.

(Refer Slide Time: 17:08)

Controller Placement

- How many controllers required?
- What should be there placement – flat, hierarchical, etc.
- What about fault-tolerance – backup controller?

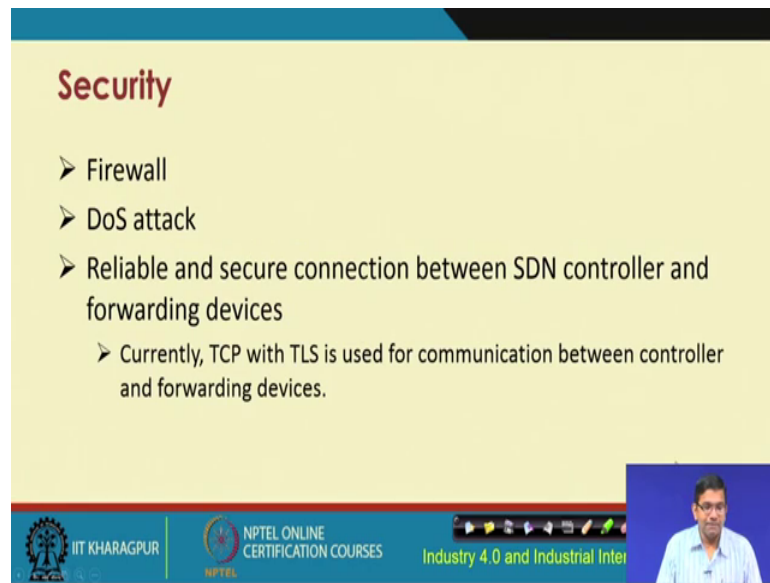
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Inter

So, let us look further. So, that was the rule placement and one problem with rule placement like this there are so many different problems these different research papers that talk about rule placement in SDN deal with and they identify the problems they solve the those problems and so on, but I think it is sufficient in a short lecture like this to know only what the issue main issue is and what are the different aspects of it.

The next issue is the controller placement, in controller placement we are typically talking about issues of dealing with identifying the number of controllers that might be required in a particular setting, identifying what should be there to be placed? How you are going to place it? Which architecture will be followed?

Whether it is going to be flat architecture, hierarchical architecture or other architectures that might be used to place the controller? And whether we are going to have some kind of fault tolerance in the event that some entity may be the main controller fails? Whether we are going to have fault tolerance to adopt a backup controller to be also in place which will take over if the main controller fails? So, all of these different controller placement issues are the common ones that are researched in the literature and different different solutions are provided.

(Refer Slide Time: 18:29)



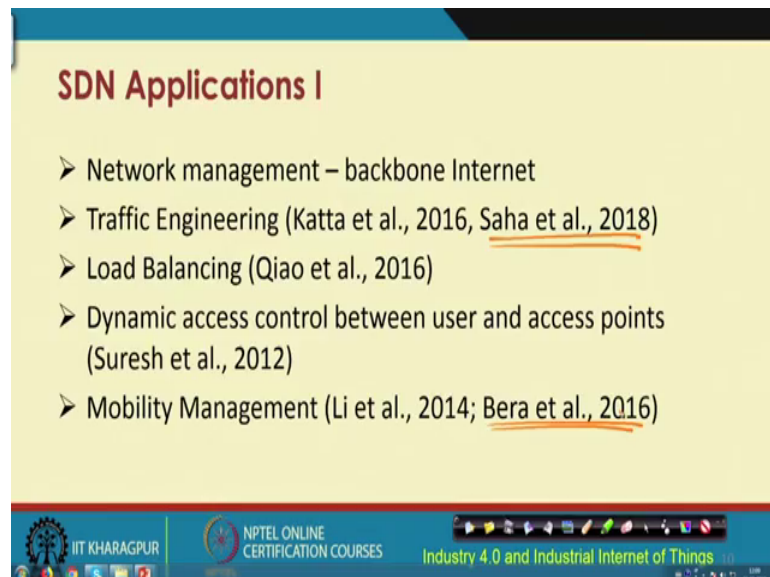
Security

- Firewall
- DoS attack
- Reliable and secure connection between SDN controller and forwarding devices
 - Currently, TCP with TLS is used for communication between controller and forwarding devices.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Inter

Security issues like you know installing firewalls, dealing with denial of service attacks, offering reliable secure connection between the controller and the forwarding devices in the data layer, these are the some of these different security issues that are also of concern in the context of SDN.

(Refer Slide Time: 18:50)



SDN Applications I

- Network management – backbone Internet
- Traffic Engineering (Katta et al., 2016, Saha et al., 2018)
- Load Balancing (Qiao et al., 2016)
- Dynamic access control between user and access points (Suresh et al., 2012)
- Mobility Management (Li et al., 2014; Bera et al., 2016)

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things

Different applications serving different different requirements such as network management for backbone internet, traffic engineering, load balancing, dynamic access control between the user and the access points, mobility management, these are some of

the issues that are researched and there are different solutions to them. I have cited some of these different literatures in case you are interested to know about in detail about any of these different issues their corresponding applications in SDN and so on.

Then these are some of these different research literature that one could go through these are some of these different papers that belong to us we are the ones who have authored these papers in our research group. So, you could go through these there are many other papers on SDN that we have authored in case you are interested you are encouraged to go through my Google scholar profile you will be able to go through the you will be able to find the corresponding literature the works that we have done on SDN. And if you are interested further you can go through them and if you are in doubt you could connect with me regarding any of these different papers that we have on SDN.

(Refer Slide Time: 20:01)



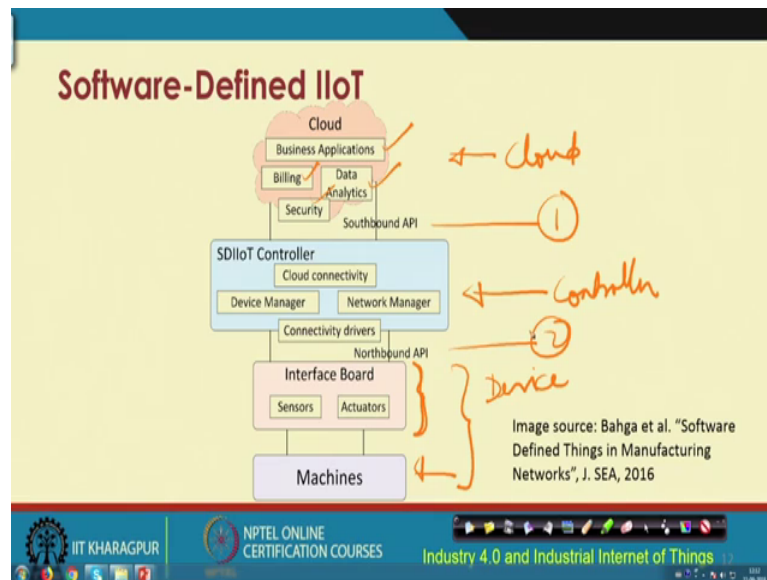
SDN Applications II

- WSN Management (Galluccio et al., 2015; Bera et al., 2016)
- IoT Applications (Bera et al., 2017)
- IIoT Applications (Wan et al., 2016)

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things

Different other issues such as the issues of management or sensor network management application level issues IIoT, IoT and so on, these are some of these papers again that belong to our research group and you are encouraged to go through them along with the other research papers that I have listed over here in these two slides.

(Refer Slide Time: 20:24)



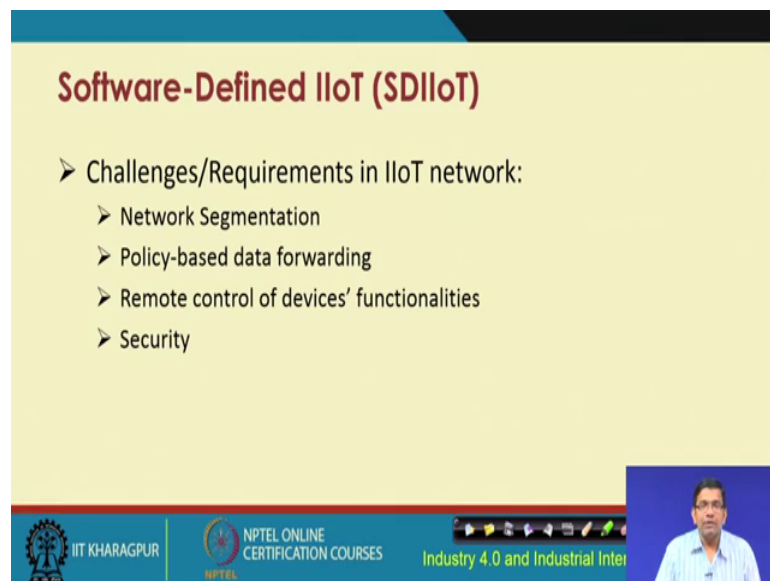
So, let us now get into the issue of SDN for IoT. So, far what I have made you understand is what SDN is and what is the overall architecture of SDN, what are these different components of SDN, what are these different API is the northbound API and the southbound API and so on. And the different protocols that will have to be used in order to deal with you know with SDN because SDN has its own different characteristics features and requirements so, you need to have specific protocols to deal with it.

The open flow versions 1 dot 1 to 1 dot 5 these different versions of the open flow protocol is a popular one that is used for catering to the requirements of SDN. So, let us now look at IIoT, catering to the IIoT scenarios, industrial IoT, industrial machinery, machinery fitted with different sensors, actuators and so on and software defined IIoT what is this architecture. So, this is this architecture that I have taken from this particular difference that you see in front of you.

So, basically what you have in a software defined IIoT scenario at the very bottom is the layer which deals with these machines which are fitted with the different sensors, this is your machines, these machines could be any industrial machinery, manufacturing machinery, powered machinery and so on. So, any machinery basically which has these different devices such as sensors, actuators and so on, these are fitted these sensors, actuators etcetera these are fitted through this interface layer, interface board having these sensors, actuators on top of these actual physical machines.

And then you have this controller these are basically your devices, device layer, this is your control layer, controller and then you have on top you have these the cloud which basically caters to these business applications business logic you know pricing billing analytics and so on security and so on. So, this particular API is your Southbound API over here and this is your Northbound API so, these two APIs are over here catering to these different requirements.

(Refer Slide Time: 22:47)



Software-Defined IIoT (SDIIoT)

- Challenges/Requirements in IIoT network:
 - Network Segmentation
 - Policy-based data forwarding
 - Remote control of devices' functionalities
 - Security

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Inter

So, there are different challenges or requirements in IIoT network, challenges with respect to network segmentation, challenges with respect to having policy based data forwarding, remote control of different devices and their functionalities and offering security, security is there all through. So, basically security issues I am not going to go through in detail, but the mind you that security is very important and it is even more important in the context of IIoT and particularly SDN, you know SDN implemented on IIoT.

(Refer Slide Time: 23:20)

Network Segmentation

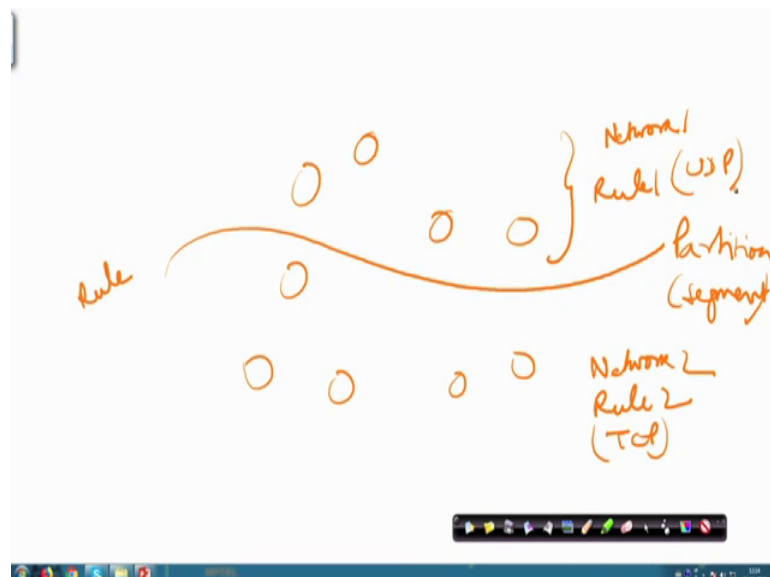
- Data from IloT system is typically follows UDP service.
- Streaming the **UDP data over TCP/IP may reduce network performance.**
- If want to use the **same/common network for all applications,** network **architecture and forwarding policies need to be changed.**
- For example, a subnetwork is responsible for forwarding IloT traffic, and other one is responsible for traditional Internet traffic.

- **SDN is capable of creating subnetworks according to rule-based traffic forwarding.**

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things

So, what is this network segmentation? So, network segmentation we are talking about segment is segmenting the network dynamically with the help of these different rules to have one part of the network follow certain requirement and the other part the segment other segments of the network follow other requirements and rules. So, let me just show you what I mean by this.

(Refer Slide Time: 23:49)



So, what we are talking about in this context is let us say that you have a certain network like this. So, we are talking about in network segmentation having you know let us say

that coming up with certain rule which will partition this network or segment this particular network into 2 dynamically based on a certain policy or a certain rule. So, rule based partitioning it is going to happen and it is going to happen dynamically. So, that one part of the network this network partition 1 and network partition 2 these are going to work together, but will follow different rules this will follow let us say rule 1 and this will follow rule 2.

So, rule 1 could be like at the transport layer this could be following let us say UDP where as this one this part of the network part 2 will follow maybe TCP this is just an example, but you know you could have different other policies implemented in the different parts of the network and this is very very important in the context of IIoT. The reason is that in IIoT you have a large industrial setting and in this large industrial setting consisting of largely different types of machinery not all of which are homogeneous all of which are catering to different different requirements and so on.

Some machinery might be catering to real time ultra real time requirements whereas, other parts of the other machinery and other parts of the system then other parts of the network might be catering to other non real time requirements and so on. So, basically implementing segmenting this network dynamically based on certain rules, based on certain policies and having them run different different protocols, different different policies etcetera is very important in a industrial or manufacturing power plant manufacturing setting.

(Refer Slide Time: 25:49)

Policy-based Data Forwarding

- Several sensors/actuators would be placed to monitor/actuate real-time status of industrial equipment.
- Forwarding policies may need to change dynamically depending on real-time situation.
- For example, temperature data may have higher priority compared to humidity, and vice-versa, in different time periods. How to meet such requirements dynamically?
- Rule-based forwarding policies in SDN would be capable of meeting such requirements of IIoT.

Bera et al., "Soft-WSN: Software-Defined WSN Management System for IoT Applications", *IEEE Systems Journal*, 2018.

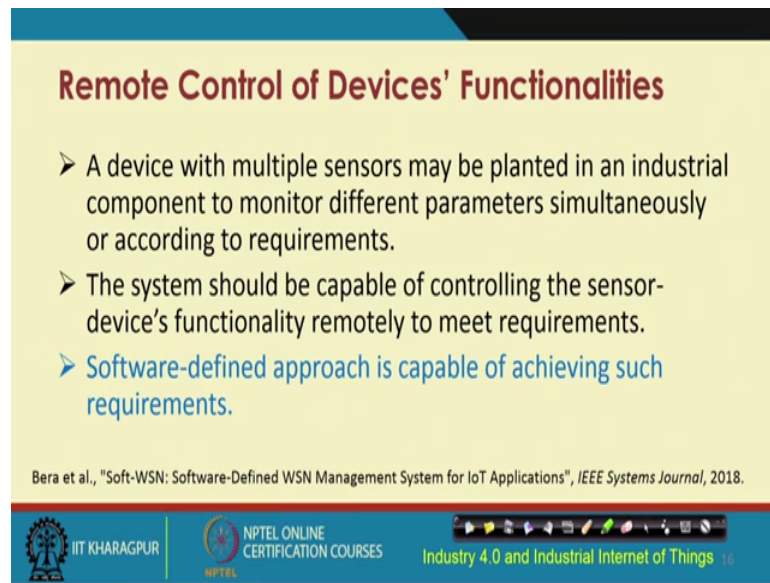
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things

So, policy based data forwarding is the second one. So, you here we are talking about you know different you know in a context of IIoT we are talking about the use of sensors and actuators again and they will have to be placed to monitor or actuate real time status of certain industrial requirement and these forwarding policies will need to be implemented and they will you know. So, in many cases they will change dynamically depending on the requirements that the real time situation that is there.

So, these will have to change for example, temperature data may have higher priority compared to humidity data or vice versa and in different parts or different periods of implementation different time periods basically these requirements may also change. In certain the certain parts of the network at certain points will have higher priority let us say to the temperature data.

Whereas, in the other instances of the time domain basically it might so happen that the humidity will have more priority over the temperature and so on to dynamically catered cater to this kind of requirements changing requirements and so on, you know SDN is useful and this is even particularly useful for IIoT requirements of this particular sort there are example of which I just give you. So, rule based forwarding policies in SDN would be able to meet the dynamic change in the requirements of IIoT.

(Refer Slide Time: 27:21)



Remote Control of Devices' Functionalities

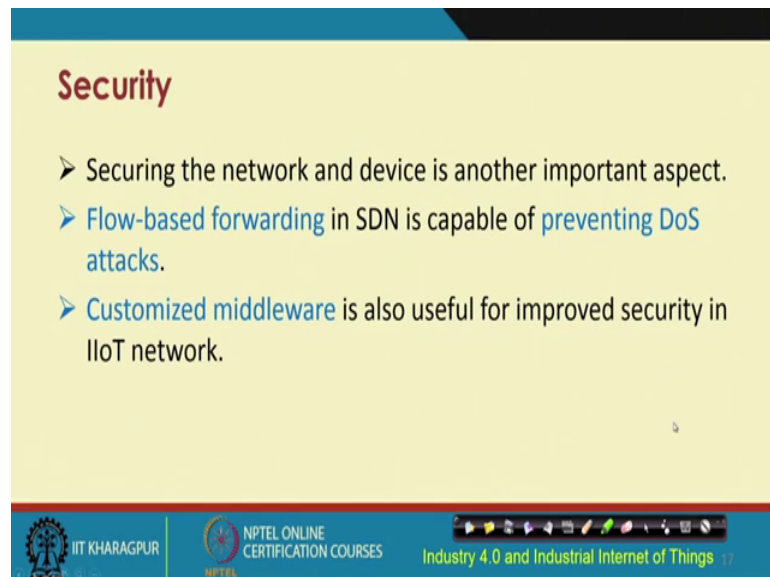
- A device with multiple sensors may be planted in an industrial component to monitor different parameters simultaneously or according to requirements.
- The system should be capable of controlling the sensor-device's functionality remotely to meet requirements.
- **Software-defined approach is capable of achieving such requirements.**

Bera et al., "Soft-WSN: Software-Defined WSN Management System for IoT Applications", *IEEE Systems Journal*, 2018.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 16

Remote control of you know the devices functionalities is very important remote activation remote control of these different devices is important and SDN can cater to this particular requirement in a dynamic fashion as and when and the requirement changes it can be done so, these things are very important.

(Refer Slide Time: 27:40)



Security

- Securing the network and device is another important aspect.
- **Flow-based forwarding** in SDN is capable of **preventing DoS attacks**.
- **Customized middleware** is also useful for improved security in IIoT network.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 17

Security as I told you before you know we are talking about the security of an SDN enabled with you know SDN enabled on top of IIoT. So, flow based forwarding has its own security vulnerabilities and also different DoS attacks can be form can be performed

and we can think of these different vulnerabilities where the dos attacks can be performed in the case of use of SDN and so on.

So, taking care of these issues implementing security protocols in the controller for instance is very important so, to get taking care of all these different issues is very important. So, you need to have a security layer basically implemented or it can be implemented vertically across all these different layers this is very important from the point of view of implementation of security either horizontally or vertically across the different layers of SDN for IIoT.

(Refer Slide Time: 28:35)

Things to consider for designing SDIIoT System

- Low-latency virtualization
 - Dynamic capacity adjustment based on demand
 - Easy movement of software components among servers
- Deterministic networking
 - Logically centralized view of the network
 - Rule-based (priority) forwarding to enable deterministic forwarding of traffic over network – so that events are processed in order

Source: <https://industrial-automation.cioreview.com/cxinsight/the-future-of-industrial-internet-of-things-is-softwaredefined-nid-23984-cid-173.html>

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 13

So, there are different requirements which will have to be taken into account to build SDN enabled IIoT systems. So, for example, low- latency virtualization is a very important requirement. So, here actually software defined also brings into picture the necessity of virtualization network virtualization, storage virtualization and so on. So, low latency; that means, very little less time we will have to cater to these virtualization requirements, because you are dealing with industrial machinery operating in very high speeds throwing large amount of data actuating in very high speed and so on.

So, low latency is very important; that means, in very less time the things are going to be done low latency virtualization; that means, virtualization in very less time least time virtualization will have to be done in order to cater to all these high speed requirements, you know real time requirements and so on. Deterministic networking is very important

here it is very important in SDIIoT scenarios to have the logical centralized view of the network, logical instantiation of the physical network and so on and rule based priority forwarding has to be implemented to enable deterministic forwarding of traffic over the network so that the events are processed in order.

(Refer Slide Time: 29:55)

Things to consider for designing SDIIoT System (contd.)

- High availability
 - Fault-tolerance feature of SDN controller to enable new servers or software to deal with faults
 - Carrier grade telecommunication NFV is capable of meeting such requirements
- Robust security
 - Centralized view of the devices and events should be present
 - Each component of IIoT system should be monitored – which will help us to prevent unwanted access of the system

Source: <https://industrial-automation.cioreview.com/cxinsight/the-future-of-industrial-internet-of-things-in-softwaredefined-nid-23984-cid-173.html>

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Inter | NPTEL

High availability is very important, fault tolerance feature is very important, we are talking about industrial machinery dealing with carrier grade telecommunication equipments, protocols and so on.

So, high availability with fault tolerance ensuring there is least downtime if at all there is any these are very important considerations of SDIIoT. Security I have time in again talked about security, security issues, robust security mechanisms taking care of all of these different issues of SDN and SDNO for IIoT is very important.


(Refer Slide Time: 30:27)

Things to consider for designing SDIIoT System (contd.)

- Up-to-date applications
 - The open architecture of devices should enable administrators to run up-to-date applications
 - Cost-effective, and secure management is possible by using the up-to-date applications

Source: <https://industrial-automation.cioreview.com/cxoinsight/the-future-of-industrial-internet-of-things-is-softwaredefined-nid-23984-cid-173.html>

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Inter



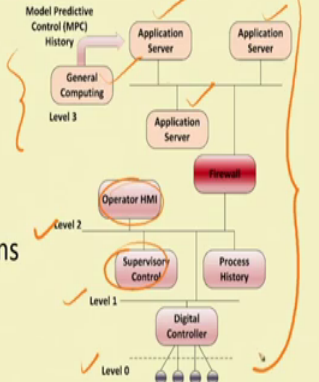
Applications up-to-date applications having open architecture of devices running different administrators specific requirements and up and making them up to date, in a cost effective secure manner is also very important for SDIIoT.

(Refer Slide Time: 30:45)

Current Practice: Automation

- Level 0 – Sensors
- Level 1 – Digital controllers
- Level 2 – Supervisory control, process history
- Level 3 – Computation, applications

Image source: Redrawn from http://blogs.windriver.com/wind_river_blog/2016/11/software-defined-infrastructure-in-industrial-iiot-how-it-works.html

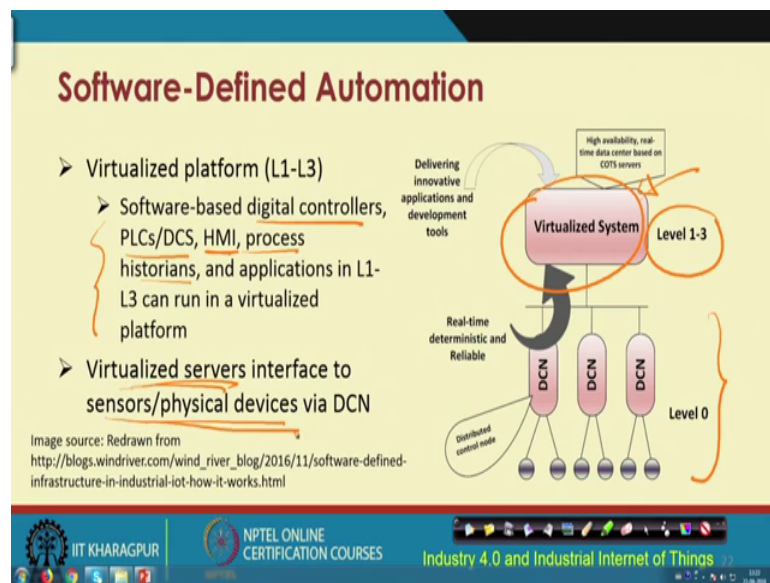


IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things

So, if we look at the current state of practice in the case of automation in industries. So, this is a global view an architectural view of you know of automation as it currently stands now. So, basically you will have in the case of automation in these settings you are going to have different levels right. So, you have level 0 you are going to have level 0

sensors basically the you know having different sensor equipments level 0. Level 1 is going to be the digital controller and the controller devices and so on. Level 2 is going to be the supervisory control like SCADA, PLC, HMI and so on and so forth. And level 3 is going to be dealing with all these different applications, computation, applications computation business logic, implementation, analytics and so on, this is the typical layered architecture of automation as it stands now.

(Refer Slide Time: 31:49)



Now if you want to implement SDIIoT on these kind of settings you are going to have something like that you have this is the holistic pictorial view of software defined IIoT or software defined automation. So, unlike in the previous scenario what we are going to have over here is something like this you are going to have levels 1 2 3 from before in this virtualized system.

So, basically these levels 1 2 3 will deal with stuff like you know software defined digital controllers, software defined digital controllers, software defined PLCs, software defined data acquisition systems, software defined HMI process control and so on. And so these are going to be software defined virtualized systems virtualized instances and so on and in level 0 you are going to have these virtualized servers that will interface with the sensors and the physical devices via the data center networks.

(Refer Slide Time: 32:48)

References

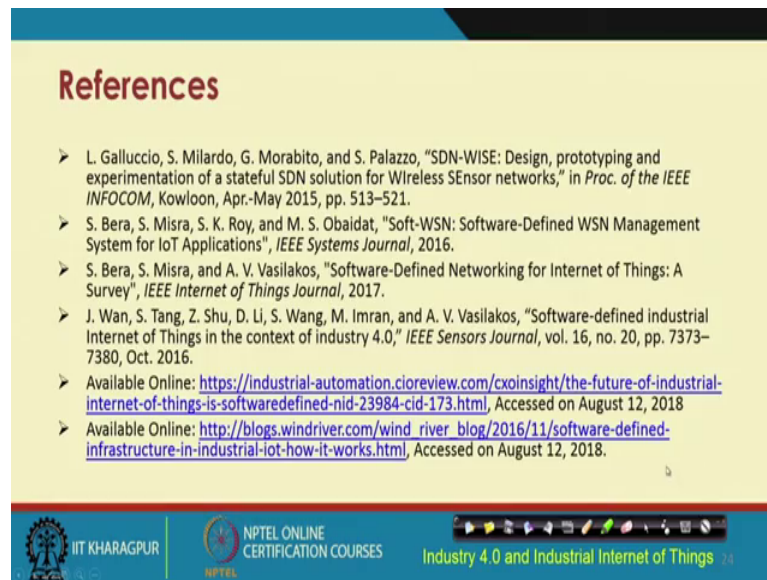
- N. Katta, O. Alipourfard, J. Rexford, and D. Walker, "CacheFlow: Dependency-Aware Rule-Caching for Software-Defined Networks," in *Proc. of the Symposium on SDN Research (SOSR)*, no. 6, CA, USA, Mar. 2016.
- S. Qiao, C. Hu, X. Guan, and J. Zou, "Taming the Flow Table Overflow in OpenFlow Switch," in *Proceedings of the ACM SIGCOMM*, Florianopolis, Brazil, Aug. 2016, pp. 591–592.
- L. Suresh, J. Schulz-Zander, R. Merz, A. Feldmann, and T. Vazao, "Towards programmable enterprise WLANs with Odin," in *Proc. of the ACM Workshop on HotSDN*, Helsinki, Finland, Aug. 2012, pp. 115–120.
- H. Li, P. Li, and S. Guo, "MoRule: Optimized rule placement for mobile users in SDN-enabled access networks," in *Proc. of the IEEE GLOBECOM*, TX, Dec. 2014, pp. 4953–4958.
- S. Bera, S. Misra, and M.S. Obaidat, "Mobility-Aware Flow-Table Implementation in Software-Defined IoT", in *Proc. of the IEEE GLOBECOM*, 2016.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 23

So, with this we come to an end of this particular part of the software defined networks for IIoT, we have gone through the different examples of the use of a software defined networks for IIoT the different requirements the challenges and so on. We have also gone through the overall architecture of SDN and thereafter how it applies to catering to the requirements of automation in most of these different advanced manufacturing industries where automation is required and so on.

And we have also finally, looked at the overall architecture of how you can transform the software defined how you can transform automation architecture that is typically encountered in the IIoT settings in these industries or the manufacturing plants and so on to the automation software defined automation architecture where you are going to have the logical view the virtual virtualized instances of all these controllers the overall you know SCADA controller in the controller devices and so on and also the virtualized instances of these different servers at the bottom and so on. So, you are going to have reduced number of layers in the virtualized or software defined automation architecture.

(Refer Slide Time: 34:12)



References

- L. Galluccio, S. Milardo, G. Morabito, and S. Palazzo, "SDN-WISE: Design, prototyping and experimentation of a stateful SDN solution for Wireless Sensor networks," in *Proc. of the IEEE INFOCOM*, Kowloon, Apr.-May 2015, pp. 513–521.
- S. Bera, S. Misra, S. K. Roy, and M. S. Obaidat, "Soft-WSN: Software-Defined WSN Management System for IoT Applications", *IEEE Systems Journal*, 2016.
- S. Bera, S. Misra, and A. V. Vasilakos, "Software-Defined Networking for Internet of Things: A Survey", *IEEE Internet of Things Journal*, 2017.
- J. Wan, S. Tang, Z. Shu, D. Li, S. Wang, M. Imran, and A. V. Vasilakos, "Software-defined industrial Internet of Things in the context of industry 4.0," *IEEE Sensors Journal*, vol. 16, no. 20, pp. 7373–7380, Oct. 2016.
- Available Online: <https://industrial-automation.cioinsight.com/cxoinsight/the-future-of-industrial-internet-of-things-is-softwaredefined-nid-23984-cid-173.html>, Accessed on August 12, 2018
- Available Online: http://blogs.windriver.com/wind_river_blog/2016/11/software-defined-infrastructure-in-industrial-iiot-how-it-works.html, Accessed on August 12, 2018.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 24

These are some of these references which have been given to you as usual for you know growing your curiosity further in order to understand these concepts in further depth if you are further interested to know them in detail. So, these are these different references and with this we come to an end of this part of the lecture on software defined IIoT.

Thank you.