Mine Automation and Data Analytics

Prof. Radhakanta Koner

Department of Mining Engineering

IIT (ISM) Dhanbad

Week-6

Lecture-27

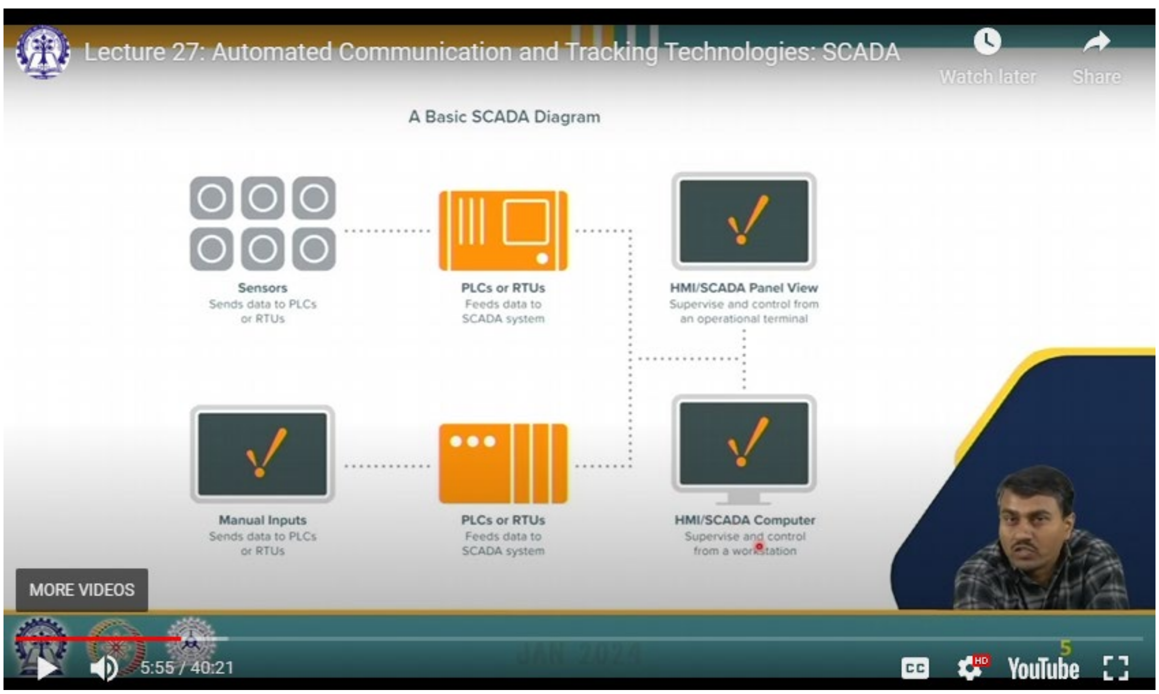
Automated Communication and Tracking Technologies: SCADA

Welcome back to my course, Mine Automation and Data Analytics. Today, in this lesson, we will introduce a new concept that is SCADA. The SCADA framework is very much in use in the industrial process control and data acquisition for establishing more control over different processes that operate in the industrial chain. So basically, in the 1960s and 70s, this technology was developed, and in the age of industry 4.0 and mining 4.0, that has been redeveloped, and that is the whole about this lesson we will cover.

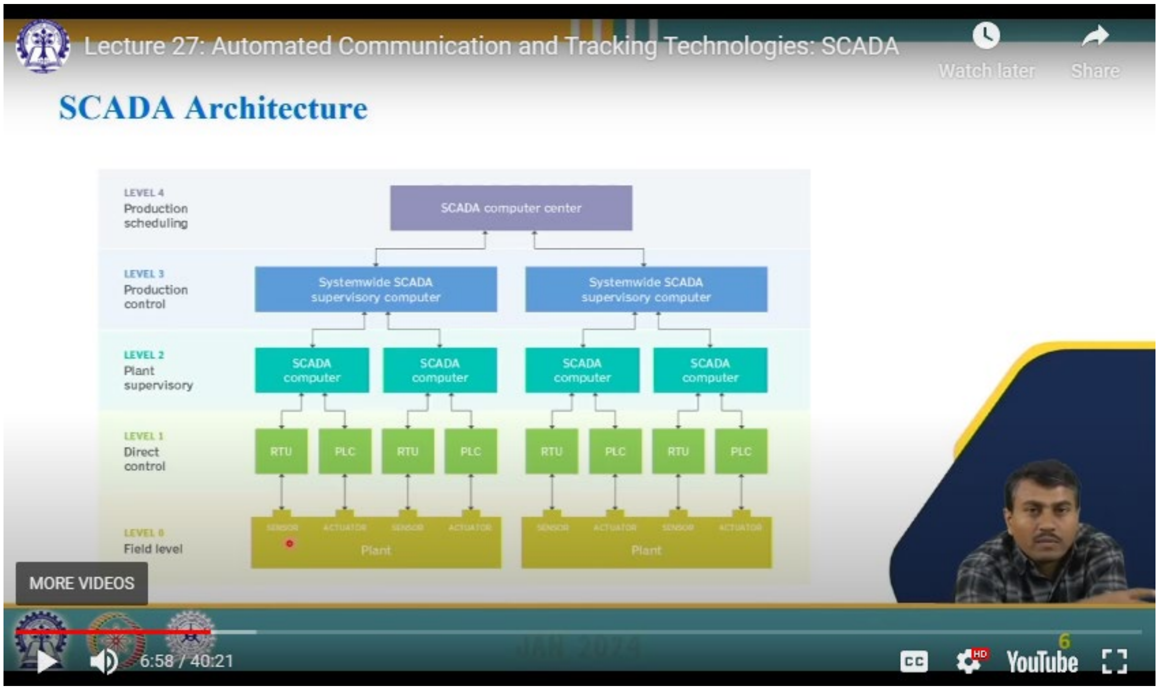
So, in this lesson, we will cover the following. We will discuss on the SCADA, what SCADA is all about and what is the architecture that this SCADA framework follows. Then, how this SCADA evolved over the time since 1960s and 70s and how it is now giving service in the industrial process automation. And different components that comprises the SCADA, different software and hardwares and the SCADA communication protocol, very important in the context of industry 4.0 also. This communication is playing a very important role and due to the cyber security issues, vulnerability issues, there are a lot of work going on in this communication protocol. We will discuss on that. Then the fundamental of control of SCADA system, how the control is established in a SCADA framework, what is the originating point of control. So that part we will discuss over. There are three kinds of basic control that we will cover in this lecture.

So, SCADA is basically a supervisory control and data acquisition system. And this system comprises of hardware and software together. And that basically allows smooth functioning in the industrial process. And there are a lot of advantages also. So let us see what are the controls and advantage that these SCADA can give us. So, it can control the industrial process locally or at remote locations. So direct control in the local region or a distance control through the remote control system, through the wireless and the LAN network. It can monitor the data, it can monitor the process, it can gather, it can collect the data, and it can process the data in real time. That is one of the beautiful features of this SCADA system. It can directly interact with the device such as sensors, valves, palm, and more through human-machine interface software. And whatever the machines are operating, it can establish a direct control through the network, through the different gateway, and through the actuator, it can basically actuate the desired action on the process. It has a very beautiful feature that is it records an event log file, what the process undergoes. So, it is very much helpful to diagonize the fault in the system. And also based on this log file, we can further optimise the process.

So, this is basically the general description about the SCADA framework. Here is the sensors; you can see sensors that sensor gathers information about the environment about the process, and these sensors are connected to the PLC as well as the RTU, remote terminal unit. There are also parts that manual inputs, there are some points that manual work is going on, so that is also can be connected to the RTU and PLC, Programmable Logical Controller. So, these PLC and RTU basically establish a direct connection with the sensor at the bottom level. Now, it is connected through the network protocol, and that network is also connected with the human-machine interface, that is, the SCADA panel view, and that is also connected with the SCADA computer or workstation. So here, it basically supervises, and it basically establishes control over the process, and it monitors the process very well. So, these are basically the overall framework: it is at the bottom, it is at the middle, and this is at the top.



SCADA architecture. As we have seen in the last slide, the sensors are connected to the PLC and RTU, and PLC and RTU are connected to the HMI and the SCADA computer. So, these particular pictures are defined clearly the five levels that the SCADA framework has.



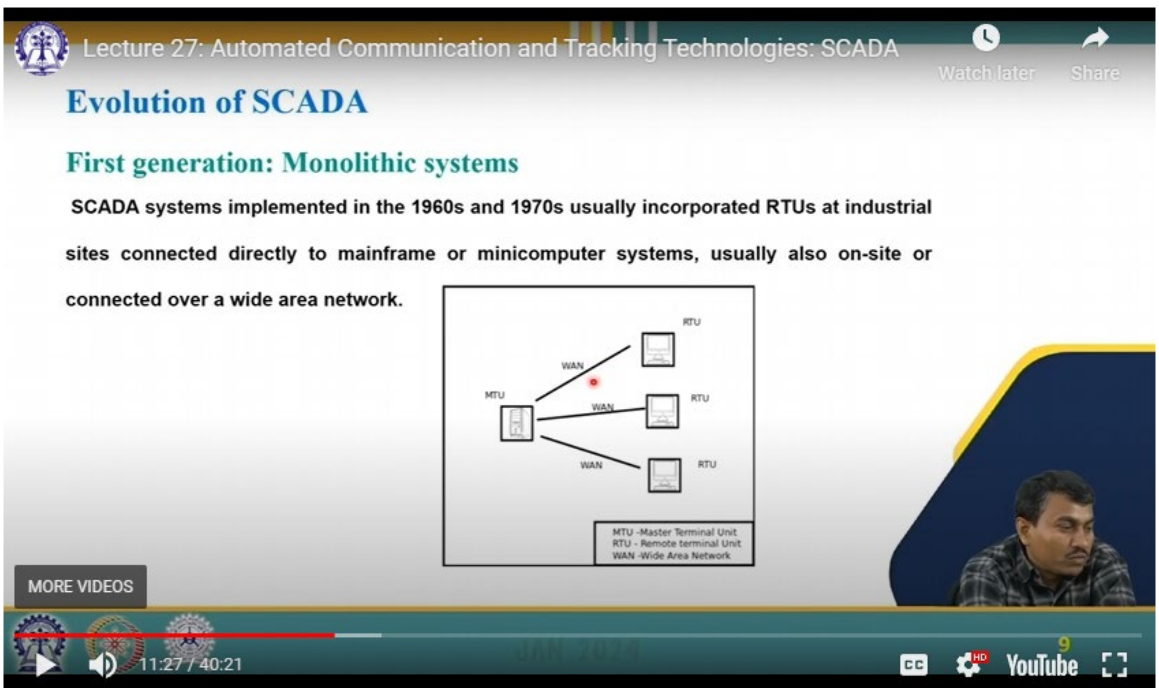
Level 0, that is, field level, at the bottom level, at the industrial field level, and at the site level. So, there are plans, and there is different work going on on the plan. So here at multiple points, sensors and actuators are located. Sensors are located and installed to get physical information about the environment. An actuator is installed at different points, at different instruments, to actuate the desired action on the process.

So, these are connected with the RTU and PLC, and that goes to the next level, that is a direct control. So, level 1 is in direct connection with the field level, and it establishes direct control. So, through RTU, it gets the data, and then through the PLC, it basically sends the command, the desired action, to the actuator. So, through that, this level 1 establishes a direct control over the process. Now this is the level 2, that is the planned supervisory.

So, this is basically get the data from the level 1, and based on the necessity, it basically sends the instruction to the controller, what kind of control is necessary. So, this is at the planned level, so SCADA computer does that. Now the, level 3, the production control, looking after overall process of the production. Here is a system-wide SCADA supervisory computer that connects multiple units within the plant, and instructs whenever necessary instruction is required to be sent to the controller and actuator, and time to time it can intercept in the process. And finally, that is the SCADA computer center, it is basically the above, that basically look after the production scheduling, business management and business intelligence. So, everything finally goes to the level 4.

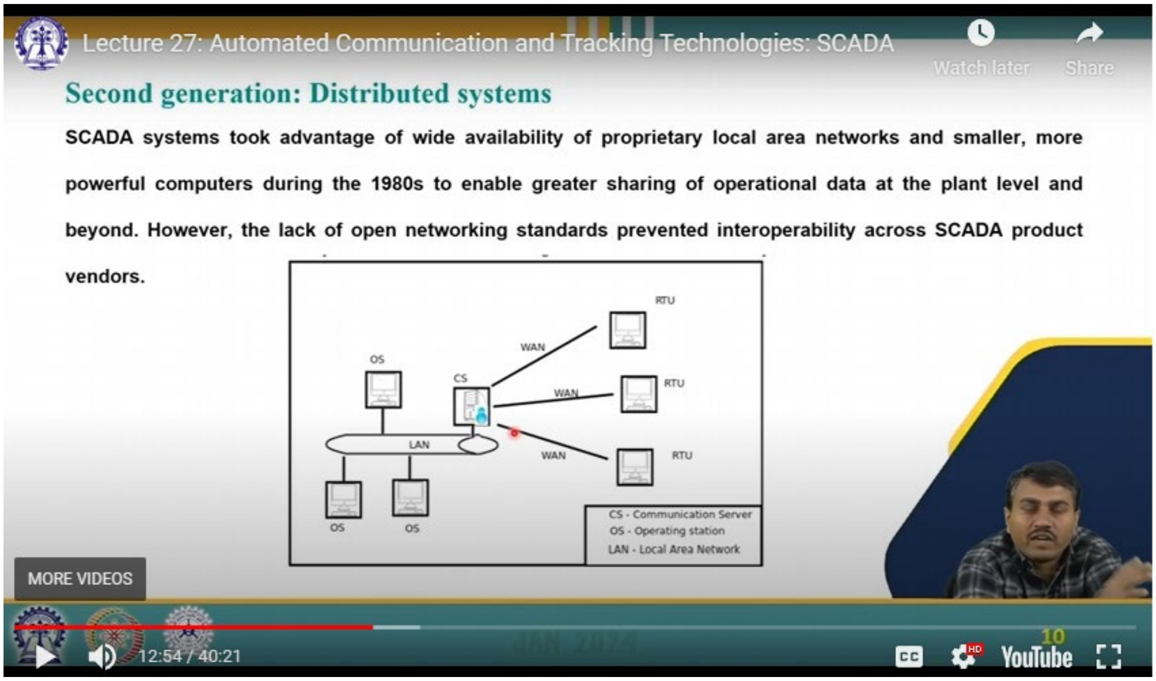
Level 0, the field level, includes the field devices, such as sensors used to forward data relating to the field process and actuators used to control processes. Level 1, the direct control level includes local controller, such as PLC and RTU, remote terminal units that interface directly with field devices, including accepting data as input from the sensor and sending command to the field device actuators. Level 2, the planned supervisory level includes local supervisory system that aggregate data from level controller and issue commands for those controller to carry out. Level 3 is basically at the production control level, it includes system-wide supervisory system that aggregate data from level 2 systems, to produce ongoing reporting to the production scheduling level, as well as other site or region-wide functions like alerts and reporting. Level 4, this basically the production scheduling level, this include business system used to manage the ongoing process in the industry.

Evolution of SCADA, as I said there is a long history of evolution of SCADA, let us go through that. First generation monolithic system. So, the SCADA system was initially implemented in 1960s and 70s, and it basically incorporated the remote terminal units at industrial site, connected directly to the mainframe or minicomputer system, and usually also onsite or connected over a wide area network. So, this is basically the framework.



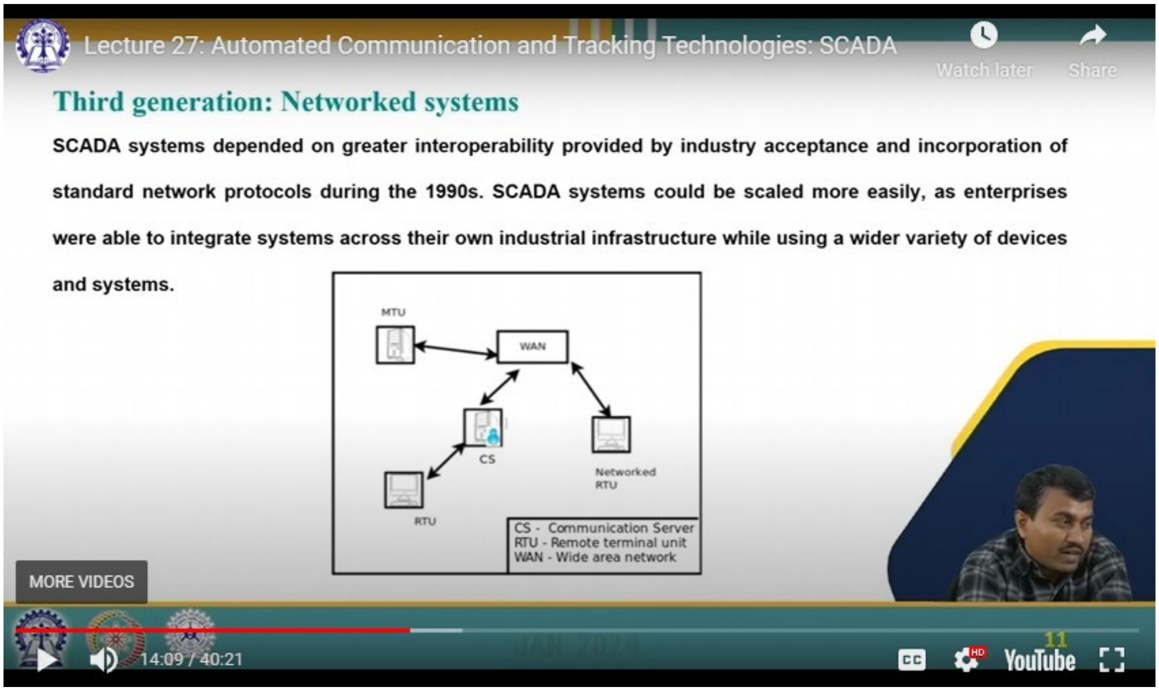
So, RTU is connected through the wide area network to the master terminal unit. And master terminal unit have a direct connection with the remote terminal unit. So, control was easier because at those days complexity in the industrial process was not so. So, that was a good system in the 1960s and 70s. This complexity increase over the evolution of and development of different technology and different process that basically give rise to the distributed system.

So, this system took the advantages of wide availability of the proprietary local area network and smaller and more powerful computers during the 1980s, to enable greater sharing of operational data at plant level and beyond. So here you can see the RTU is connected with the wide area network to the LAN and to the communication server. And there are different operating systems are working on these machines. Those are also connected with the LAN. So, but, here there are some issues of interoperability across different SCADA products.

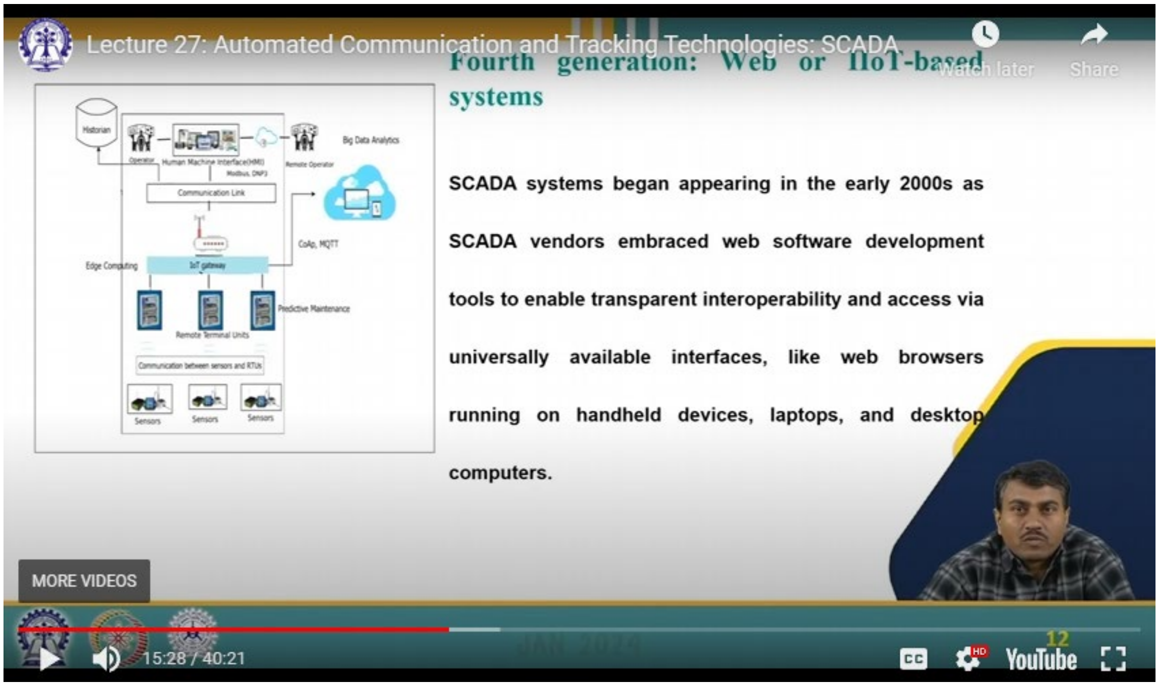


So, it because of the technical limitation in the 1980s. So, it basically lacks these network standard and later on it basically developed and nowadays it is very smooth.

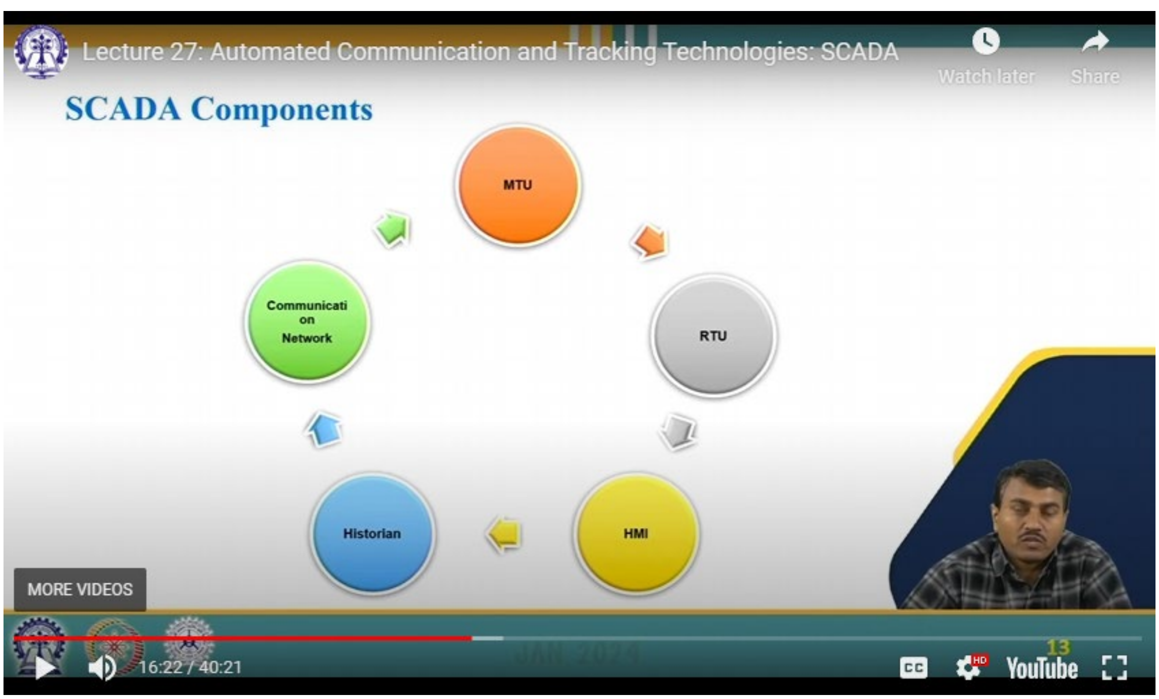
Third generation network system. So, this system basically depends on greater interoperability provided by industry acceptance and incorporation of standard network protocol during the 1990s. And the SCADA system could be scaled more easily as enterprises were able to integrate system across their own industrial infrastructure, while using wider variety of devices and systems. Here, you can see the network remote terminal unit came into the picture and the remote terminal unit at the site. This is the server, communication server. This is connected with the wide area network and it is connected finally to the master terminal unit. So, greater interoperability is established in this third generation.



The fourth generation is industrial internet of things based system. This is the latest system. This is basically developed in the early 2000s. So here you can see these are the sensors at the bottom level and it has established communication between the sensors and RTU. And the remote terminal unit is connected through the internet of things gateways, communication system. There are also wireless communication system as well. And through the communication link it is connected with the HMI, Human Machine Interface through the different network protocol. And there are some historian database that are operated and these data are also in the cloud and they are also have the big data analytics and the remote operator. So, these SCADA system basically embrace web software development tools to enable transparent interoperability and access via universally available interfaces. Like web browsers running on handheld devices, laptops and desktop computers.

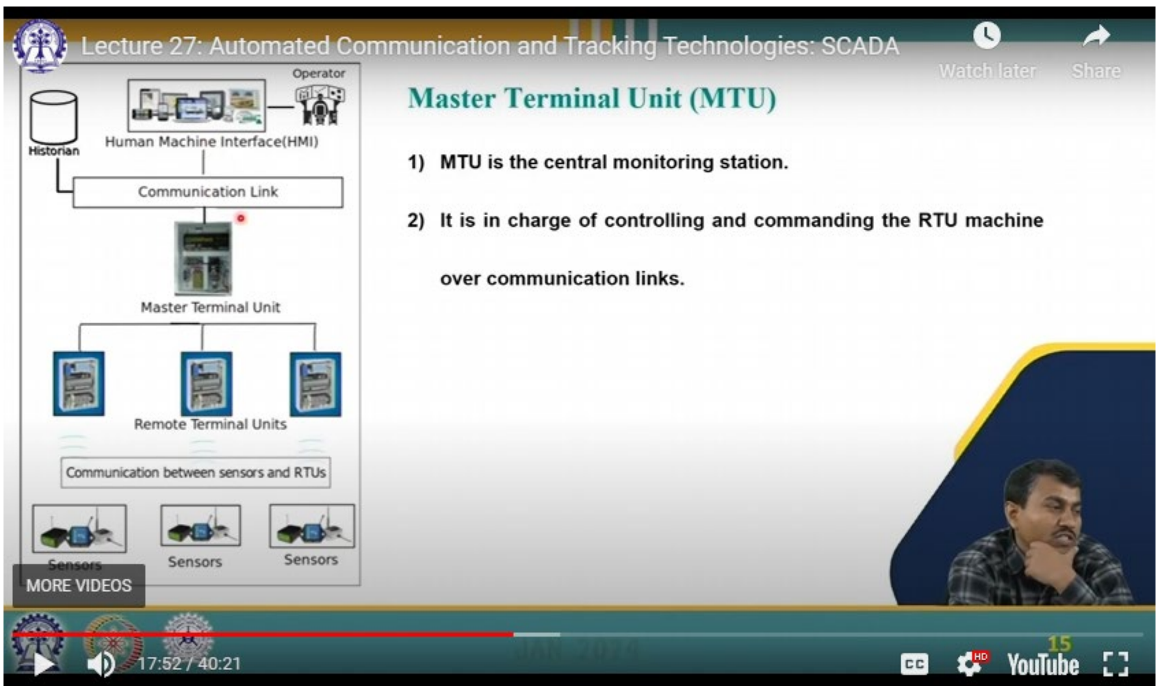


SCADA components. So, this is master terminal unit, then the remote terminal unit, then the human machine interface, then the historian that, is the database and the communication network. So, these are the five vital components of the SCADA. And out of these, in the context of the industry 4.0, communications plays a very important role for remote interoperability and, remote connection and remote control. And also in the context of industry 4.0, the cyber security that it has to ensure that no third party or undesirable interference by the third party over the network.



We have to ensure that. So, for that different kind of protocol, different kind of encryption are developed so that we can keep this kind of system secured and safe. The next topic, remote terminal units. RTU is responsible for collecting real time data and information from sensors that are connected to the physical environment using link LAN or wide area network. The RTU is forward information to the master terminal unit and these are additionally in charge of conveying the present status of data of physical devices associated with the system.

Master terminal unit. So, this master terminal unit is the overall in charge of this process control. So, the MTU is the central monitoring station, and it is in charge of controlling and commanding the remote terminal unit machine over communication links. So here you can see the master terminal unit is connected to all the remote terminal units and remote terminal units are in communication with the sensors and RTU and the actuators.



So, this basically oversees the process, and through the communication links, it basically sends the data to the human machine interface so that the operator can see the supervisory office, the control tower can see everything what is going on, and it is connected with the database historian and can monitor the data, collect the data, store the data for future processing. And here is the operator; the operator is working through the human-machine interface. So, it is also respond to messages from RTU and processes and store them for succeeding communications.

Human-machine interface. HMI provides a communication interface between SCADA hardware and software components. It is responsible for controlling SCADA operational information. For example, controlling, observing and communicating between several remote terminal units in the form of text, statistics or other comprehensible content.

Central database or historian. Historian is used for accumulating two-way communication data, events and alarm between the SCADA control center. And it can be described as a centralized database or a server located at distance location. The historian is queried to populate the graphical trends on the human machine interface. Communication link. This communication link and communication network is very important. The communication network provides communication service between various components in the SCADA network framework. The medium utilized can be either wireless or wired. Presently, wireless media is generally utilized as it interfaces geologically circulated areas and less available zones to communicate effortlessly.

SCADA communication protocol. Modbus. This Modbus transmission protocol developed by the Gold Modicon for their Modicon programmable controller in the 1970s. Later on this was taken over by the SCADA electrical. And most commonly used protocol for connecting electronic devices due to being openly published and easy to use. So, it becomes a very standard protocol in the industrial process. So, user used for interaction between the MTU and the RTU.

Modbus transmission control protocol. This is another version enhanced variation or another variant of the earlier one. This focus on the reliable communication over the internet and the intranet. Modbus plus protocol proposed to overcome master terminal vulnerabilities issues.

Distributed network protocol. Distributed network protocol or in abbreviation DNP is based on the enhanced performance architecture EPA model. Which is a streamlined type of open systems interconnection layer architecture developed by Harris distributed automation product. This OSI have seven layers in the network and this is very popular network protocol. DNP3 protocol was developed to achieve open standards based interoperability between RTU, MTU and programmable logic controllers. Core component of the DNP3 protocol include data link layer, convention, transport function, application convention and data link library. User layer is added to the EPA architecture responsible for task such as multiplexing, data fragmentation, prioritizing and error checking.

IEC 608705 protocol. International electro technical commission IEC 608705 protocol also follows the enhanced performance architecture model EPA model. An additional top layer representing the application layer is included in the EPA architecture to indicate functions related to the telecontrol framework. The variation of telecontrol framework such as T101, T102, T103 and T004 define diverse specification object, data objects and functions code at application convention level. For efficient transmission, the DNP3 layer stack adds a pseudo transport layer, but it is not utilized in IEC 608705.

Foundation field bus protocol. Foundation field bus protocol utilizes a four-layer stack comprising the user, application, data link and physical layers. The foundation field bus architecture follows the OSI layer model, with the user layer added as an additional top layer of the application layer. The user layer serves as a gateway between software programs and field devices, facilitating easy process integration. Foundation field bus offers features such as multifunctional devices, open standards and decreased wire cost, setting it apart from other protocols. Apart from these traditional communication protocol, in industrial internet of things CADAA uses the ZigBee.

ZigBee is an IEEE 802.15.4 based communication protocol. It was developed by ZigBee Alliance and standardized in 2003, and later revised in 2006. The communication range of ZigBee is small between 10-to-100-meter line of sight depending on environmental characteristics. ZigBee architecture comprises three layers of devices, fully functional devices that is FFDs which act as routers, reduce functional devices RFDs and a coordinator. ZigBee NML wireless personal area network, WIPAN, provides a communication protocol with low power digital radios. It operates as a low data rate, low power, low communication range wireless ad-hoc network secured by 128 bit symmetric encryption key with a data rate of 250 kilobytes per second.

Bluetooth low energy BLE. This BLE aims to decrease power consumption compared to classic Bluetooth technology. And the BLE shares the same protocol stack as classic Bluetooth but support quick transfer of small data packet with 1 Mbps data rate. It does not support data streaming. BLE follows a master-slave architecture where the master act as a central device connecting to multiple slaves making the devices more efficient. The energy is conserved by keeping the slave node in sleep mode by default and waking them periodically to send data packets to the master node and receive control packet from slave node. BLE is reported to be 2.5 times more energy efficient than ZigBee.

LoRa. This is basically for long range. So LoRa, a long range communication protocol was initially developed by Cecilia of Green Bowl, France and later acquired by Simtech in 2012. It supports long range communication up to 10 km and data rates less than 50 kilobytes per second while maintaining low power consumption. LoRa is particularly suitable for non real-time application that requires fault tolerance. It operates in the physical layer combined with long range wide area network LoRa wire WAN in the upper layer.

Fundamental of control. So, SCADA system make extensive use of electronic technology. The technology cycle are very short, and recommendation regarding specific types of hardware, software, communication protocol, etc. needs to be upgraded as and when technology advances.

General control. Control consists of monitoring the state of critical parameter, detecting when it varies from the desired state, taking action to restore it. So control can be discrete or analog, manual or automatic and periodic or continuous. So, the process variable is the parameter that is to be controlled. Process variable may be temperature, ventilation flow. So device that measure process variable are transducer or sensors. The set point is the desired value of the process variable. The control output. The process variable is the parameter that is to be controlled. Example of process variable in deep metal mine system are temperature, humidity, air velocity. To be controlled, the process variable must be capable of being measured and that measurement convert into signal that can be acted on by the controller.

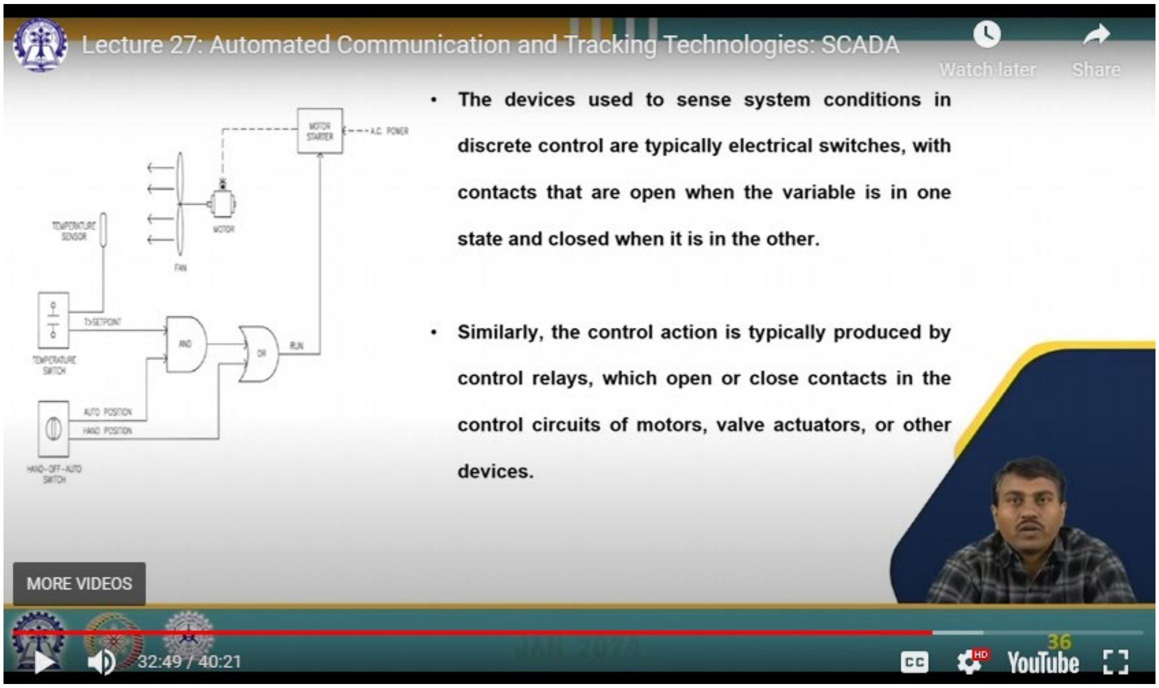
Device that measures process variable are transducer or sensor. In many cases, the process variable sensor consists of a direct measurement device called an element and a separate signal processor called a transmitter. An example of this would be temperature measurement using a resistive temperature detector as the element and a temperature transmitter, which converts the varying resistance value of RTD into a current or voltage proportional to the temperature.

The set point is the desired value of the process variable. Normally, preset into the control system by an operator or derived as an output of another control conclusion, the error signal is the difference between the process variable and the set point and is the basis of control action. The controller is the device that processes the error signal, determines the required action control required and provide a control output to the process.

The control output usually must act on the system through another device to affect the desired control action, such as varying the position of the ball, the speed of the motor or the current through a heating element. The device that convert the control output into a control action is the actuator.

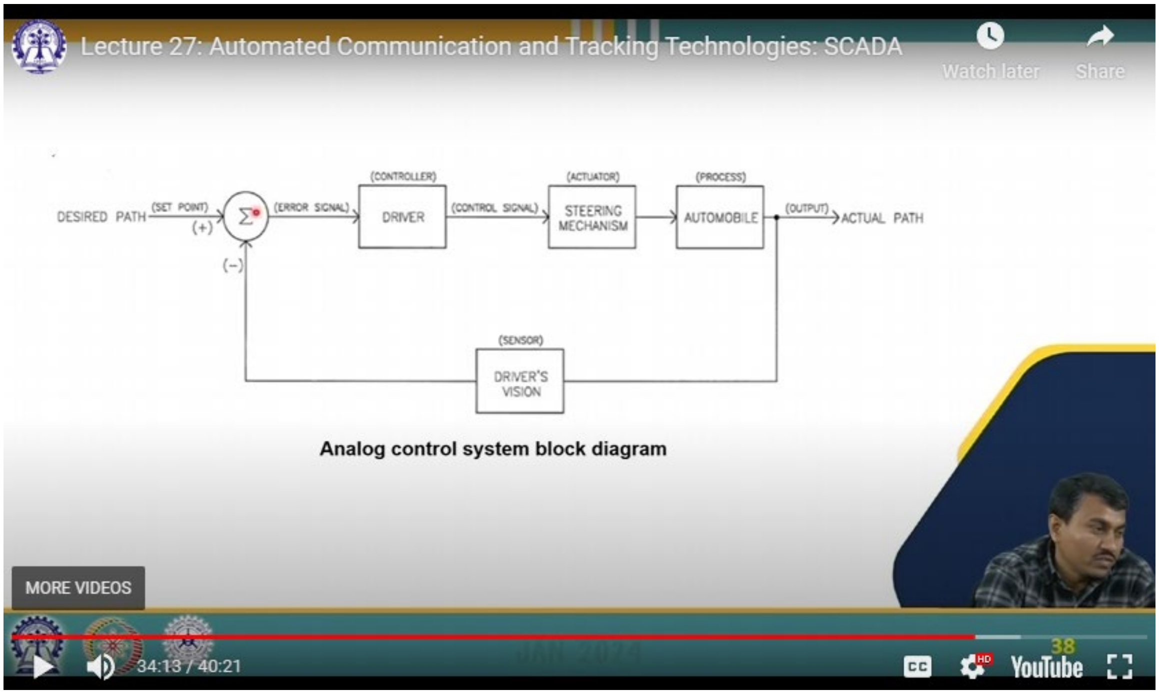
Discrete control. A discrete control deals with system in which each element can only exist in certain defined states. An example of discrete control would be starting an exhaust fan when the temperature in a space exceed a preset value. And stopping the fan when temperature falls below a lower preset value. So the temperature, the process variable, is either within the acceptable range or outside of it. The fan control relay actuator is either on or off. So, this type of control is implemented with a logic diagram and circuit. In discrete control, even through some of the parameter actually have a continuous range of values. The only information used by the control system is whether their value is greater than, less than or equal to some desired value.

So, this is basically the system. Here the fan is connected in the network and through the motor connection, electrical connection is there. It is connected to the AND and OR gateway. Here is the switch and here is the temperature sensor. So based on the temperature sensor data, it will decide on whether it will continue the switch on condition or switch off because temperature now goes below to the preset value.



If the temperature goes up, now the fan is on. So, this is controlled by this gateway. So the device used to sense system condition in discrete control are typically electrical switches with contact that are open when the variable is in one state and closed when it is in other state. Similarly, the control action is typically produced by control relay which open or close contact in control circuit of motors, valve actuators or other devices.

Analog control. Analog control deals with the system in which a variable can have a continuous range of values rather than simply a discrete state. So basic analog control consists of process of measuring the actual output of a system, comparing with the desired value of that output and taking control action based on the difference to cause the output to return to the desired value. So, this process can be as simple as a driver of an automobile comparing the speedometer reading process variable to the speed limit set point and adjusting the position of an accelerator pedal control action to speed up or slow down the vehicle accordingly. So here it is the desired path. Here it is the set point and here the error signal generated if it is speed up and goes below or based on that if it is below then accelerate, if it is up then de-accelerate.



So, this is the error signal generated. So, this is the driver, this is the controller, this is the control signal on the steering actuating, this is the automobile, the process, this is the output, the actual path. So here there is a driver vision sensors so that basically gives the feedback time to time whether we are in the speed limit or not and if required action or control to de-accelerate or de-accelerate.

Classes of analog controller. Analog controller can be classified by the relationship between the error signal input to them and the control action they produce. First one is the proportional P controller. Controllers in a proportional control system generate an output proportional to the error signal. An essential feature of P control is the error signal must remain non-zero to prompt a control action because if there is no difference, there is no proportion, so proportion control cannot work when there is zero error. So consequently P control alone cannot restore the process to the set point after an external disturbances. The steady state offset a non-zero error signal inherent in P controller is a defining characteristic. The adjustable parameter determining the proportionality of the controller's response is known as the gain. Higher gain result in larger control action for a given error signal and faster system response.

Proportional plus integral. Controllers in proportional integral control system generates a control action proportion to the error signal plus integral of that error signal. The addition of the integrator enables the controller to eliminate steady state offset and return the process variable to the set point value. The adjustable parameter controlling the integration constant of the PI controller is known as the reset as it effectively reset the error signal to zero. An engine governor operating in asynchronous mode maintaining a constant RPM over the full load range utilize PI control to achieve this control behavior.

Proportional plus integral plus derivative that is PID controller. Controllers in proportional integral derivative control system incorporates a component of control action proportional to the derivative of the error signal representing the rate of change of error signal. So this control mode enables the controller to anticipate change in the process variable by increasing the control action for rapid changes which is particularly beneficial for system requiring fast response time or those inherently unstable without control. The adjustable parameter controlling the derivative component in a PID controller is known as the rate.

Control loops. The complete control scheme required to control a single process variable or a group of related process variable is called a control loop. The control loop include the relevant part of the process, the process variable sensors and associated transmitter, input signals, the controller, the control output signal and the actuator. The process of adjusting the gain, reset, rate parameter to obtain effective stable response of the system to change in the set point or external disturbance is called loop tuning and is an essential aspect of control system startup and commissioning.

Types of controller. Controls can be implemented using either individual stand alone controller known as single loop controller or by combining multiple control loops into a larger controller. Single loop controller have provision for a process variable input signal, a control output signal, set point adjustment, tuning of PID control parameters and typically include some type of display of the value of the process variable and the set point.

These are the references.

So let me conclude in few sentences what we have covered in this lesson. So, we have provided an overview of supervisory control and data acquisition systems. We have explored the structural framework of the SCADA system, including hardware and software components. We basically discussed the evolution of SCADA over 1960s to today's time. We have discussed the key element that comprises the SCADA system such as sensor, actuator and control interfaces. We have explored the various protocols used for communication between different SCADA components. We have introduced the basic principle and methodologies involved in controlling SCADA system for monitoring and management purposes.

Thank you!