Nicola Tavares: Welcome to the ITS Standards Training.

Ken Leonard: ITS standards can make your life easier. Your procurements will go more smoothly and you will encourage competition but only if you know how to write them into your specifications and test them. This module is one in a series that covers practical applications for acquiring and testing standards-based ITS systems. I'm Ken Leonard the director of the U.S. Department of Transportation's Intelligent Transportation Systems Joint Program Office. Welcome to our ITS Standards Training program. We're pleased to be working with our partner the Institute of Transportation Engineers to deliver this approach to training that combines web-based modules with instructor interaction to bring the latest in ITS learning to busy professionals like yourself. This combined approach allows interested professionals to schedule training at your convenience without the need to travel. After you complete this training we hope you'll tell your colleagues and customers about the latest ITS standards and encourage them to take advantage of these training modules as well as archived webinars. ITS Standards Training is one of the first offerings of our updated professional capacity training program. Through the PCB program we prepare professionals to adopt proven and emerging ITS technologies that will make surface transportation safer, smarter, and greener. You can find information on additional modules and training programs on our website at www.pcb.its.dot.gov. Please help us make even more improvements to our training modules through the evaluation process. We will look forward to hearing your comments and thank you again for participating and we hope you find this module helpful.

Nicola Tavares: Throughout the presentation this "Activity" slide will appear indicating there is a multiple choice pop quiz following this slide. The presentation lecture will pause at each quiz section to allow you to use your computer mouse to select your answer. There is only one correct answer. Selecting the submit button will record your answer and the clear button will remove answer if you wish to select another answer. You will receive instant feedback on your answer choice. Please help us make even more improvements to our training modules by completing the post-course feedback form.

This Module is A304b: Specifying Requirements for Field Management Stations – Part 1 Object Definitions for Signal System Masters Based on NTCIP 1210 Standard

Your instructor Patrick Chan has been involved with the development of ITS standards since the year 2000. He was involved with the editing the recommended standard version of NTCIP 1210, which is this module. He is also involved with other ITS standards,

including NTCIP 1203 and the TMDD Standard. Patrick has 23 years of ITS experience, including 4 years with a public agency.

Patrick Chan: So we'll start off first by reviewing the target audience for this course, so the participant can self-assess whether they should participate in the whole course of not. Traffic engineering staff which may include specification writers who are responsible for specifying and implementing field master controllers for a traffic signal system. Traffic management center operation staff who uses the system but who may wish to better understand what capabilities of the field master is supported by the standard. System developers who are responsible for development and implementing field master controllers for a traffic signal system. And private and public sector users which include device manufacturers who are responsible for providing the software systems and the field master controllers that uses the NCTIP 1210 standard. This is a recommended curriculum path. The NTCIP 1210 standard was developed following a systems engineering process. So the graphic shows the recommended sequential curriculum path leading up to this module. Many of the concepts that will be discussed in this module has already been introduced in one of the modules in the curriculum path but this module just brings all of these concepts all together and specific to the requirements supported by the NTCIP 1210 standards. The curriculum path starts with I101 using ITS standards and overview, so it provides an entry overview of the ITS standards. A101 introduction to acquiring standards based ITS systems. A102 which is introduction to the user needs identification. Followed by A201 details on acquiring standards based ITS systems and C101 which is the introduction to the communications protocols and their uses in ITS applications. And there was also A304A which is part one of this module which is understanding the user needs for the field management stations, field masters, for snow system masters based on this standard and then this is the part two where we're going to specify requirements for these field management stations based on the NTCIP 1201 standard. This is a similar slide but in a textual format. If the participant is not familiar with any of the topics covered in these courses, it is recommended that the participant take those courses first prior to completing this course. There's also some assumptions that the participant should have some basic knowledge of how American style traffic signal operations work such as what the components of a typical signalized intersection is, the logic for selecting local signal timing pattern, and the logic for selecting signal timing patterns for system in general. This slide is the learning objectives for this course. Upon completing the course the participants should be able to describe the requirements that are supported in the NTCIP 1210 standard. Use the protocol requirements list, the PRL, to specify a NTCIP signal system master interface. In the previous module we used the PRL to identify the user needs, the features that are supported by the standard. But now we're going to go over uses to specify to requirements. How to achieve interoperability,

interchangeability using the requirements traceability matrix. That's one of the matrices that's included-- that are part of the NTCIP 1210 standard. Understand the NTCIP 1210 SNMP interface and dialogs. Dialogs being a sequence of events on data exchanges that occur between two components. And who they're going to incorporate requirements that are not covered by the current standard. So you may have a requirement that the standard doesn't support so how do we incorporate that requirement into your procurement, your specification?

Patrick Chan: So we start off with learning objective number one, describe the requirements in NTCIP 1210. What we're going to do in the next couple of slides is to review the components and the structure of the NTCIP 1210 standard. Use the PRL to trace from the user need to requirements. And just go over the organization and the composition of requirements within the standard. First we're going to review the architecture of a typical signal traffic control system that uses it with a field master. So we can see where the NTCIP 1210 standard is used. This slide shows the basic components of the traffic signal system with field master. The 1210 standard deals with really the interface between a traffic management system, which is usually in a traffic operation center, for example. Or it could be actually a field computer, let's say there's a maintenance personnel that has a field computer, but the standard really covers the interface-- describes interface between this traffic management center, or excuse me, traffic management system or a field computer with the signal system master, which we also call the SSM or the field master. So the NTCIP 1210 really deals with the management of the signal system master. There's another NTCIP standard called NTCIP Total Two that deals with the interface between the field master and the local controller, which we call the signal system local. So looking at this you'll realize that there is a relationship between the NTCIP 1210 and NTCIP 1202, but the focus of this module is just the NTCIP 1210 interface. To give a little history, a little bit more information where the standard is, the current standard, that's the current version of the standard that's available on the NTCIP.org website is version 1.53. Version 1.53 has been approved. So it's considered a recommended standard but has not been published yet. This approved version is available, I mentioned, on the NTCIP.org website for free until the published version is available. Once the published version is available that version should be available also at the NTCIP website. As it indicates, it was approved earlier about a year ago in early 2013. As for the published version, as of this point it's already been sent to the publishers, but it's just not currently available. But we do expect it to be available in early 2014. The participants should be aware, though, that the standard has not yet been deployed, even though we've approved the standard no one has, that we are aware of, has actually used NTCIP 1210 standard. And early deployments of standards often reveal issues, not all of the time, but often reveal issues and whoever is deploying it right now early on should be prepared for such issues. We definitely still encourage someone to deploy the NTCIP 1210 so we can determine what the issues are, if any, and so we can make additional refinements to the standard. The standard has gone to a peer review

process, so there's a level of confidence we have in the standard, but we just need someone to take the first step. To date, we are aware of some potential issues and those issues will be discussed in this course. Those that are seeking to deployment equipment conformance standards should work with U.S. DOT, other industry experts and the standards development organizations so that the industry can benefit from whatever lessons learned you may discover when you implement this standard. And we'll talk a little bit more about how to get in contact with these industry experts and U.S. DOT at the end of this course. This slide shows the table of contents for the NTCIP 1210 standards so that the user can get a familiarity with the overall flow of the structured standard, because the standard does follow system engineering process. This similar outline is used by all of the system engineering process based standards. Some highlights section one is general, just provides introduction to the standard. It defines the scope of the standard and provides some definitions. Section 2 is the concept of operations or the ConOps which defines the user needs that are addressed by the standard. Section 3, takes the same user needs from the ConOps and develops functional requirements, defines functional requirements. This section includes the protocol requirements list that we talked about earlier, which maps the user needs to requirements that are necessary to satisfy those user needs. They form a requirement definition also found in section three. This is a key menu of options that are used in the procurement specification, the PRL. And it was discussed in the previous module A304a and we'll just take it to the next level, discuss a little more further in detail in this module. Sections four through six represent the design content for the standard. Section 4 presents the standard sequence of data exchanges at the events, which we call dialog, that to occur between the traffic management system and the field master. Section 5 contains the objects, and the objects represent individual pieces of data that are referenced by the dialogs in section 4. And section 6 has the block objects which are defined groups of objects that provide a more bandwidth efficient means for exchanging large sets of data. These block objects are really important for systems that have older communication systems, communication networks such as dial up telephone lines running at let's say 1200 baud. So we have to address those older communication systems. So block objects give us a way to do that. The requirements traceability matrix make up Annex A which maps each requirement that's defined in section three to a specific design usually consisting of a dialog and list of objects. Annex B represents an alternative way to look at some of the requirements and object ranges. So just a different view of looking at the requirements. And Annex C represents some of the internal logic on how the field master should work. What the standard does not have, it does not contain any standard test cases for testing conformance to the standard. So you go ahead and deploy your standard, you'll have to create your own test cases, you have to develop them for your deployment. Those deploying the standards should investigate any developments to see if any other projects have already developed test procedures that can be reused for your project. This slide shows a snapshot of a small portion of the NTCIP 1210 PRL table. In the previous module A304a understanding user needs it discussed how to use the table to user needs for a project. So now we're going to

take it to the next step and discuss how you can use the table to select requirements for your project. The first column of the PRL represents the user need. Includes first the identifier which is the clause within the standard where the user need is formally defined. The second column indicates the name of the user need that's being referenced. To find what exactly this user need is we have to go to clause 2.5.1.1 in the standard and we present it here. So this is the formal definition of the user need 2.5.1.1. The title is configure cycle timers and unit backup time and the user need is the system owner needs to be able to determine the capabilities of the SSM. The system owner may need to configure the SSM to operate cycle timers for synchronizing the SSLs, the local controllers, directly used in the sync pulse. Notice the text will typically identify the need, in this case configure the SSM cycle timers and provide a justification to synchronize the SSL's. But it doesn't really precisely define any measure of requirements that is we can't determine from the user need the details on how we measure if the requirements or the user need has been properly satisfied. Thus, we developed requirements to provide us that extra detail. So going back to the PRL, the PRL is going to list the requirements that provide the details of the user need under the under need. So here's the user need and we see that this user need has two requirements. The third column of the PRL represents the requirements identifier, the clause, within the standard where the requirement is formally defined. And the fourth column indicates the name of the requirement that's being referenced. So the PRL shows that if you select a user need, that these are the requirements that are related to that user need. User need may be related to multiple requirements and those requirements would be listed below them as shown here. And the requirement may trace to multiple user needs so that requirement will appear multiple times in a table each time under the user need that that's going to trace to. So looking at the 2 requirements, for that user need, so we'll look at the 3.4.2.2.1 and we repeat it here, determine SSLs currently connected. Notice that the formal definition provides precise and measurable requirements about defining precisely how they will be achieved, meaning we don't define well, how are you going to do it? What technology are going to do to fulfill this requirement? So the first one the SSM shall allow a TMS to determine the SSLs currently connected to the SSM. And the second requirement the SSM shall allow the TMS to configure the specific time-of-day used for the calculation of the cycle timers from the SSM. Let's take a second, this slide to define how requirements are written in the standard. Each of the requirements generally follows a structure as follows, an actor. So each requirement will have an actor that identifies who or what does an action. It will define the action. It identifies what's about to happen. The target identifies who or what is receiving the action. Optionally, we also may have a constraint where we identify how to measure success or the failure of the requirement and localization which identifies circumstances to which the requirement applies. So we follow the structure throughout the standard, so that way we can minimize any ambiguities in the standard. As an example, this is an example of a requirement that's contained in NTCIP 1210. The actor in this case is the TMS. Note, that there's been-- some people contend that the actor's actually something else. But we'll say that the actor in this case is the TMS because it

initiates the action to determine from the information located in the target, the SSM, and the SSLs connected to it. So we have an actor. We have an action to determine. And we have the target the SSM and the SSLs. And we actually have a constraint here that says they are currently connected to the SSM. So if one of the SSLs is currently offline because we're doing construction so why while we're doing construction around that area we disconnect the SSL or maybe the communication line is broken, the SSM won't report that to the TMS. It's only those SSLs that are currently connected to the SSM. So this is just an example of what a requirement in 1210 looks like. This slide and the next slide provide a little bit more detail about the requirements that are defined in the standard. This slide provides an overview of the operational requirements included in the standard. Essentially, they are general requirements that define the basic characteristics of exchanging information and security between a traffic management system and the field master of the SSM. 3.3.1 covers requirements for making requests to the field master whether to get information or to set information. 3.3.2 are requirements for managing the logged data in the SSM such as retrieving the log, clearing the log, et cetera. 3.3.3 is managing the access to the information stored on the SSM. So that's the operational requirements. This slide represents in 3.3.4, represents a top level outline for the data exchange requirements. So this is the data that we get exchanged between the traffic management system and the field master. As with many of the NTCIP standards, most of these requirements have been divided into three groups representing system configuration, configuring your devices, system operations for in this case for SSM sending timing plans, controlling the timing plans. And system monitoring which is monitoring the operation of the devices checking the status. In addition though NTCIP 1210 has an additional group of requirements that contains all of the system detector requirements and that's the first one 3.4.1. collect system detector data. It should be noted that the actual organization of the data exchange requirements are not important. What is important is that traceability to the user needs. And we'll go through these choices later in this course. You may also note that NTCIP 1210 does not contain a section for backwards compatibility requirements. This is because this is the first version of the standard and there are no backwards compatibility issues at least for the standard to address. So while your project may still need to consider the needs and requirements for backwards compatibility with your existing proprietary equipment you may have there are now backwards compatibility issues with the standard. So we've reached our first activity which is actually a poll. There's a couple of them throughout the course and the purpose of these polls is to review our understanding of some of the key concepts that we have learned so far in the course. So the first poll is which of the following is not a major group of requirements in NTCIP 1210? And you can use the participant student supplement to help you with this, answer this question. The choices are collect system detector data, manage the SSM configuration, monitor the SSM operation, or backwards compatibility requirements. So which of the following is not a major group requirement in the NTCIP 1210 standard? So let's review our answer. The correct answer is actually D, because backwards compatibility requirements since this is the first version of NTCIP 1210 there

are no backwards compatibility requirements that we have to be concerned about. The standard of support question have requirements for collecting system detector data and monitoring these system detectors. There are requirements that allow monitoring and adjusting the configuration of your SSM, your field master. And there are requirements for monitoring alarms and monitoring your field master device status. So this is the end of the slides for the learning objective number one which is describing the requirement in NTCIP 1210. So what we've done so far, we've reviewed the components and structure of NTCIP 1210. We've used the PRL to trace user needs requirements and we went over to the organization and the requirements that are in the NTCIP 1210 standard.

Patrick Chan: Moving to learning objective number two which is to use the PRL to specify an SSM interface, single system master interface. So what this objective covers is the remainder of the PRL. We've only covered part of the PRL in the first module A304a. So now we're going to step through the process of preparing a PRL to include in the specification. So in these next slides we're going to explain how to use optional requirements constraints and predicates within a PRL. Specify conformance criteria for functional requirements within the PRL. And finally, we're going to talk about how to use the PRL in the specification. Returning to actually the PRL, the fifth column of the PRL defines the conformance for the user need or requirement reference by the row. If you see the letter M, M stands for mandatory, while O indicates optional. Mandatory means that the item must be supported by any implementation that once claimed conformance to the next hierarchical item, while optional means that the item does not have to be supported to claim conformance to the next hierarchical item. This means if the user need is selected to be supported, the user need in this case is configure cycle timers and unit backup time, then any requirements underneath there with conformance M must be supported. So to satisfy this user need to 2.5.1.1 it is mandatory that this requirement be fulfilled, determine SSLs currently connected. On the other hand, if it's optional that means you may include this requirement but it's not mandatory that this requirement be fulfilled so that the user need is satisfied. Notice that if the user need is optional and it's not selected, then all of the requirements that traces this user need do not have to be supported. So this is optional. This user need was optional. You can support these requirements underneath it but you're not required to. Note that this user need configure cycle timers, unit backup time as mandatory. So there's no higher level of user needs with this conformance statement. So this is mandatory. This supporting this user need is mandatory. It's to claim conformance to the standards. So to claim conformance to the standard you have to support this user need because it's mandatory. In addition to the basic mandatory and optional options, M&O, the conformance column must also indicate an option group by indicating an O followed by a decimal point followed by a group number and then followed by a parenthetical phrase that defines the rules for this optional group. This information inside the parenthesis indicates the minimum number, in this case one, and a maximum number. There is no maximum, that's indicated by the star (*), that must be selected for the group. In this example this slide shows that there are two user

needs threshold configuration, threshold selection and configuration signature selection where the conformance group 1, optional conformance group 1. Option 1. And that at least one of these options that's indicated by one must be supported. It must be selected in order to be conformant. So the one after the open parenthesis indicate that you have to support at least one of these options. The star indicates that you may select as many as you want, so you can select them all, if you like. So let's say I have an SS field master I'm putting in a new system, this says that I must either at least support threshold selection or signature selection. I'm also allowed to select both, but I must select at least one of them to claim conformance to the standard. Moving on, another notation that may appear in the conformance column is a predicate followed by a colon followed by one of the conformance symbols this notation that the indicated conformance only applies if the predicate conditions are true. The predicate is a term defined by a separate table presented just prior to the PRL, in this case threshold, this threshold predicate references clause 2.5.1.2.5.2 and a signature references clause 2.5.1.2.5.3 which happens to be the user needs discussed in the previous slide. So I'm going to go back so this is the threshold predicate and this one is the signature predicate. So if the user were to select the threshold selection user need that's represented by the threshold predicate. And that means if I select the threshold selection then this requirement becomes mandatory. If I were on the other hand to select the signature selection then the signature-- this requirement it becomes mandatory if I were to select a signature predicate, the signature selection. If I select both, then both of these actually one for the threshold, one of the signature, both requirements become mandatory. So that's conformance. The sixth column support allows the user to indicate what an implementation supports or a project requires. So far, we've been talking about writing a specification, what requirement does an agency or user need, does an agency like to see in his specification? The PRL table can also be used by a device manufacturer to indicate this is my standard product and these are all of the user needs and requirements in the standard that I support. So this PRL table can be used two different ways. One by the agency to indicate this is what I want, these are the requirements user needs that I want. And it can also be used by device manufacturer, let's say your vendor who provides the traffic management system to indicate this is what my product currently supports. I support these user needs. I support these requirements. So the support column for 1210, NTCIP 1210 contains either yes I support it, or no I do not support this requirement or user need. So the final column is called additional specifications and we left it in the column to indicate and provide some additional information that might be useful to the agency or for agency to fill in themselves. It's used to indicate additional project specification and/or notes. The PRL in some cases contains texts in this column when the developers of the standard believe that an issue was important enough that we added some text in, but it cannot be necessarily standardized across our projects. This is usually true with performance issues as shown here. The developers of the standard have determined that we need to include some place in the standard, the definition of what the response start time is for requests. Meaning by the time, let's say in my SSM, we seize a request, what's the allowable

response time, how soon after I receive the request do I have to start setting my answer? So that it won't be like oh I received a request but the master goes I'll send back an answer two or three minutes later. So this phrase prevents that. But the value of it is going to vary depending on how you operate your system, such as what kind of communications line-- what your communications network is. So the default value is actually 2000 milliseconds or 2 seconds but we allow this value to be customized for each project. So for this example project we're going to put in 500 milliseconds. Note that the default is not necessarily a recommendation; it's just intended to provide an unambiguous interpretation in the clause in case this specification, your specification fails to specify a value. So if there's no value there, the standard says use 2 seconds, 2.0 seconds. But if there's a value in this case 500 milliseconds use the 500 milliseconds. The contents of what's additional in the additional certification column is not limited to standardized text. Any agency can add their own specification in this column or anywhere else for that matter. But just be aware that please do it carefully to avoid creating a specification that requires a custom solution. Any addition should be designed to address potential concerns or issues or to support actual user needs whether they're defined by the standard or some other user need that the standard doesn't support. To assist agencies as much as possible, we've included some additional samples specifications wording to go underneath additional specifications in the participant student supplement. These weren't included in the standard. It wasn't quite an error, we just didn't include it, but we have some examples of some additional specifications that you may wish to include if you're creating a spec for your agency. So we do encourage you to go through the student supplements and that was included with this module if you're creating a specification, just to get ideas on where else you may want to specify additional requirements. So we've reached our second poll. The poll is where is a list of potential issues and sample specifications to consider for NTCIP 1210 deployments? Where can they be found? So the answer choices are A, in the user need section, the standard. B, in the requirement section of the standard. C, in the participant student supplement. Or D answers A and B and the user needs and the requirement section of the standard. So, again, where is the list? Can a list of potential issues and sample specifications to consider for NTCIP 1210 deployments, where can they be found? So let's review the answers. The correct answer is in the participant student supplement. So we've included in the student supplement a list of some of the potential issues that we are aware of at this time with the standard, again the potential. And we've also included some sample texts for additional project specifications that you may wish to include when you're completing your PRL. They're not really in the user needs section of the standard, the user needs section only defines potential needs of the stakeholders. The requirements section only gives requirements with little to no guidance on additional specifications. And so since A and B were incorrect D is also incorrect.

Patrick Chan: The next couple of slides we're going to go through a case study. What, again, this is not a real life example because no one, that we are aware of, has actually

deployed NTCIP 1210, but we wanted to show an example of how you would complete a PRL for a specification. For this example, for this case study we're going to use the exact same example that we used in module A304a. So in this example Suburbanville wants to upgrade its old closed-loop system so that supports ITS standards. They want to deploy regional masters to control normal operations. They want to be able to monitor detailed operations or local controls when needed. Time-of-day, be able to select time of day patterns, signal patterns based on time-of-day. They may want to use a signature selection for traffic responsive operations. And they may like to get instant notification of any unusual traffic conditions. Before we start filling out the PRL, though, we should mention a couple of general statements that you may wish to include in your procurement spec. Require support of all values for all NTCIP objects unless otherwise noted. So this is very important that your procurement, the specification supports the full range of values indicated in the standards so that you may conform it to the standard. There is some text on how to do this in the student supplement. And specific grain specifications are discussed on the following slide. So there's a couple of slides where a couple of areas where the standard is silent about the range but we want to put in some values for it to better define your system so that you get the system that you're looking for. Define response start time. The response start time which we talked about briefly which is when the time a component receives a request to the time it begins sending a response, it's not explicitly defined in NTCIP 1210. It is defined, however, in NTCIP 1103 which is a normative standard. However, so not to be ambiguous you may want to include a definition in your procurement specs and in language, again in the student supplement that we provided for clarification. And include a filled out version of the PRL. And in the next level of slides I will show you how we do that step by step. So a sign at the very top up here of the PRL, the first user need that we encountered in the PRL is the mandatory need to provide live data. All of the requirements that trace user need are marked mandatory. So we reflect all of these, yes, under the support column. Next, we'll fill out the additional specifications column. So we'll use values of 500 milliseconds for both requirements. The response start time we'll define it as 500 milliseconds. For requirements 3.3.3.2 configure access, we want to be a little bit more specific about the number of access levels that will be supported. If you were to look at the requirement it only says states that you'll support, at least one user level in addition to the administrator unless specified. So let's say in our case study we want to support at least three access levels. So we'll add that statement to the additional specification. The SSM shall support at least three access levels in addition to the administrator access level. The next user need is to provide offline log data which is mandatory and all of the requirements that are traced to it are mandatory. So we're going to select them all. We also discussed in the student supplement that we should probably define in detail the performance of the size of this event logging functions. So what we're doing to do in the next couple of slides we'll specify some range specifications for the event log. So we're going to size out what size event log we want for our implementation. But before we go through the details of specifying the event log, we really need to understand how the event logging mechanism

works. So the next three or four slides will through the event log, we'll go through a quick example so the participant can think about what information will you want to record in our field master SSM. One of the key things that we might be interested in knowing in the event log is when did the event occur? Such as when a timing pattern change occurs, since this is an offline log, the log accommodates this by providing a time stamp in UTC time so there's the date, hours, minutes and seconds. We may also be interested I knowing additional event specific information. So for an SSM, we may be interested in knowing the ID, identifier, of the new signal timing pattern that was activated. So this information is user configurable, and is stored in the value field at the table. In this context, we know that 16 is the timing pattern ID that we changed to at midnight January 1, 2013. Of course, our field master is likely to simultaneously manage multiple coordinated sections, each section choosing their own signal timing pattern. Thus for the new selection that meaning on the next question that we have is what section did the signal timing pattern change occur when it changed to pattern 16? This can be accomplished through the ID column of the event log. Note that this ID is not strictly the ID at the section of the section number, but it's an event identifier because the event logging mechanism is very generic, the standard event logging mechanisms used for all the NTCIP field devices. So this same structure can be applied for signal controllers, all dynamic message signs. It is also possible to have multiple events occur at the same time. So there might be another role of data where in this case, the signal timing pattern changed to pattern five, but let's say in section three, really event identifier three. So we followed this data so the next question is how do we retrieve the data from the table? So we need a way to reference each role in the table and this information is stored in the number column, which essentially is a sequential number, with the most recent events always being row one shifting everything down so that all of the rows, that the most recent event is event one. The second most recent event is always row two. The standard requires that new events are added as row one and other events are shifted downwards, that way the traffic management system can always pull the table for the first few rows in the table and be confident that it's getting the latest events that occurred that's been logged in the event log. But the user may also want to capture other types of events as well such as the communications status, such as when a controller goes offline or comes online. This information can be stored in the same log as well and it's fully configurable by the user. In this case, the log entry for tech communication status would look very similar. The time would be recorded the same way. However, in this case, the questions may be different. So what is the new status? Is it responding or not responding? So while we get the time stamp, the value is going to be different depending on what we're looking for. Likewise, the event ID represents the ID to configure the event, where the event 0.7 might be the on change event for intersection communication status. So that might be an event ID 27. So it might be in section three, for example, but it's identified as 27. And, again, how do we retrieve the data? So we use the number column, again, to reference a specific row. Again, the log knows that the newest event is in row one. Now, we may also want to distinguish these communication status events from the previous events which is

the signal timing patterns. So the standard allows us to separate two different types of events into different classes in order to better manage the information so we add a class number. So class one event which in this case are my communication status, while class two events are my signal time and patterning events. So now we can quickly search the event log for say just the most recent signal time and pattern changes which are event class two and then see what the latest changes the most current events were for signal time plan changes only. So this is the entirety of how the event login mechanism works generically. Again, we used to seeing event login mechanism for all of the NTCIP devices. Now, that we understand how the event logging mechanism works we can consider the various sizing ranges that we want to require for our device. So to answer that we ask ourselves a series of questions including one, how many event classes do I need? So how many types of groups of events do I want to manage? In our example, we've identified at least two, one for communication status and another for signal timing pattern changes. How many event types IDs do I need? In this case, we have to ask how many section IDs do I have to manage in addition to how many intersection types will I have to manage. Be aware the event ID values cannot overlap between two classes so that just adds the number of event types. How many events should be stored per event class? In this case, in our example, we've only had two events, but this value to be used really depends on how you operate your system. If we only had two events per class, then you have to ask the question is it okay if a third event occurs that the earliest event drops off. It's no longer in the event log. So probably not. You have to consider that event logs are often used for trouble shooting. So you have to ask yourself, did we store enough events to be able to troubleshoot the system after a certain period of time, let's say through a weekend if you don't have maintenance over the weekend. And the final question is how many objects should their controller be able to monitor? In this case, in our example, we only monitored intersection communication status and this timing pattern number. But in theory this should be able to monitor any object that is specified by the standard. The final question is on this slide is what type of events are to be monitored? In our examples, we've monitored only on change events. That means any time the communication status changes for a section or any time a signal timing pattern changes for a section we want to be able to log it. But we can also monitor or record other types of events. For example, we can monitor when the value goes above or below a value such as when a value reported by a system detector goes above or below a threshold value. The hysteresis, for example, the occupancy, it records when a value goes above a maximum or below a minimum value. So you might say they report the log when the occupancy reported by the system detector goes outside of a defined range. Periodic events, for example, report the traffic volumes measured by the traffic detectors every 60 seconds. There's also a bitwise type logic where when a specific bit is set then log the event. This is really particularly important for diagnostic events where a bit can mean different things such as a short alarm status object for an intersection set. The next user need that we encounter in the PRL is the mandatory need to connect communications networks. All of the requirements here that are traced to this user need are also marked mandatory. So we'll select all of

these support, all of these requirements as a user needs. However, just be aware that there may be potential issues in the design of this feature that may affect interoperability and we'll discuss this later in the course. It's also mentioned and discussed in the student supplement. So be careful when deploying this feature, this mandatory feature and make sure you understand it. The next user need that we encounter is the optional need to support legacy communications network. This user need was put into really support older systems that you slow down with communications lines between the traffic management system and the field master. Again, for example, let's say dialup telephone lines, that you have 1200 baud modems. There's nothing in our example to indicate that this user need is required so we'll just select no. But, however, if we did select this user need, notice that the first three requirements are mandatory while the forth one is optional. The next user need we encounter in the PRL is the mandatory need to configure timers and unit backup time. Most of the requirements related to this need are mandatory so we'll just go ahead and select those. The optional needs all relate to the optional ability of the field master to send out sync pulses to coordinate the local controllers. So let's just talk about this a little bit as a background. A sync pulse is a pulse issued by the field masters to all the local controllers in its zone so that all of the local controller can synchronize their operations on that sync pulse. It's really used for older systems because the older systems have clocks that are probably drift a lot, that aren't that accurate. Now modern controllers we use clock synchronization. Typically, we synchronize the clock once a day. The clocks are more accurate. We synchronize once a day using some kind of common time source, whether it be WWV or the Eastern Grid. And this is typically what we do these days for modern controllers. But for the older controllers, we need to be able to support sync pulses. So we also talking about ranges, some of the requirements talk about being able to manage sections, manage the number of SSLs, manage the number of patterns. So we want to be able to specify the ranges for each of these, specify how many sections we think we're going to need to support for our system, specify how many local controllers do we think we need to support for our system and specify a number signal timing patterns that we want our system to support. So all of these values are depending on the system and how you manage your system. So now that we've talked a little about all of that, let's go back to the PRL and fill it out. So we're assuming that our modern controllers do not need a sync pulse so we're going to select no for these three optional requirements, while these three optional requirements are related to having a sync pulse. And we'll also fill out some range specifications for the first three requirements to ensure that the system we're procuring fully supports our operational needs requirement. So the SSM shall support at least 16 local controllers. The SSM shall support at least three patterns for each section. And the SSM shall support at least three sections. The next user need that we encounter is the mandatory need to manage section definition set. So if we're managing the sections for our field masters so all of the requirements related to this need are also mandatory so we'll go ahead select those. The next user need is to be able to implement a manually selected plan to override the plan selection. There's only requirement for this user need and the user need is mandatory so we'll go ahead and select both. Next user need is the

mandatory need to implement plan based on a traffic management system command. So, again, all of these requirements related to this need including the need itself are mandatory so we'll go ahead and select those. And the next user need that we encounter is the need to implement plan based on the timebase schedule. All of these requirements, again, are related to this need, are mandatory. So we'll go ahead and select those. But as we discuss in the student supplement you may want to specify ranges for the schedule. So before we do that, we need to understand how the time based schedule works. So the next couple of slides we'll review how the generic timebase control schedule works. And, again, this is generic to all NTCIP devices. All of the NTCIP devices use the scheduler the same way. So the scheduler, the scheduling logic begins by defining a day plan. The day plan works by determining what month it is, what day of the week it is, and what day of the month it is. So if three values in all three columns are true, then that particular day plan would apply. There will be times when multiple rules evaluate it to be true; in which case, the most specific rule is applied. So, for example, the rule for the Fourth of July falling on a Monday would overrule the weekly Monday rule. So this table really defines the standard schedule with all of the major holidays and it may look like this example so we'll go through it. The first entry is that this is true for all months. If it's a Monday to Friday, no matter what date it is, or what day of the month it is it will be day plan one. The second one, depending, no matter what month it is, no matter what day of the month it is, for Saturday and Sunday, we'll run day plan two. However, if the day is January 1 it doesn't matter what day it is, we want to run the day plan three which might be a holiday schedule. So every January 1 we want to run day plan three. However, sometimes January 1 might fall on a Saturday or a Sunday so that Friday if it falls on a Saturday or that Monday if January 1 falls on a Sunday we felt that you may want to run a holiday schedule for that day also. So we need to handle that condition. So the conditions are if the day is December 31 and it's a Friday, still run the holiday schedule because that will be to observe New Year's Day. If it's January 2 and it lands on a Monday, go ahead and also run the day plan number three on a holiday schedule. The next one is Martin Luther King Day. Martin Luther King Day is always the third Monday of January. So we handle that by saying January on a Monday, and if it's between January 15 to January 21 which is the possible days that it could be to be the third Monday of January then run day plan three and so on and so forth. So the last two it says, well, we may have a special holiday schedule for December. So in December if it's a Monday to Friday, no matter what day of the month it is, go ahead and run day plan four. And December, no matter what Saturday, Sunday, it is, if it's a Saturday or Sunday no matter what day of the month it is, go ahead and run day plan five. So this is the number of scheduled entries will depend on your operations. You should always allow some room for growth even though we've only defined 18 different entries for our table, we'll require let's say 32 entries for our table, and you'll see that, how we fill that in a couple of slides. So that's the day plan schedule. Let's look at how-- let's look within the day plan itself. So after you figure out how many day plans your operations need to support, you have to ask, how many events do you need to support during the day for the day plan? Each event results in an action. So let's go to

this. So event one might be a five o'clock in the morning let's go ahead and run the A.M. rush hour plan. And then at the second event, might be oh, for day plan one is at ten o'clock let's go ahead and get out of the rush hour plan and run a midday plan. Event three, maybe at 3:00 P.M. let's run a school day plan because all of the kids are getting out of school so you may have a special plan for that. And then day event four at four o'clock let's start running the P.M. rush hour plan. And then the fifth event might be at 10:00 P.M. at night, our rush hour is over so let's just start running our night plan, which would be action number five. So for our example, we'll assume, again, we want to provide room for growth. We'll assume that we'll require a day plan and that there are eight events for each day plan. Notice that in the previous table, the last column was something that says action. So what is an action? An action can be a task or one or more tasks that you want to perform at that time. So action two, for example, shows that if we implement action two we want to actually implement two different tasks. There might be one task for different one or multiple sections or maybe one or more multiple intersections. But the effect can be enabling or disabling a single timing pattern or it might be enabling or disabling a special function. To figure out the size of the table you'll need you'll have to have an idea of how you may want to configure your system with some wiggle room. So in our example, we'll assume we want to support 32 different actions with up to four tasks per action. So that means for each action I might be able to control four sections, for example, or four intersections. Another feature that we want to review is local time and Daylight Savings Time. So if you recall from the event log every time it's defined by the local time which may also require for Daylight Savings Time. Figuring our Daylight Savings Time is difficult and varies widely throughout the world. So the NTCIP standard supports Daylight Savings Time by having its own table. Most countries there's only one entry needed for Daylight Savings Time, but there actually are a couple of countries that may have multiple Daylight Savings Time events. So we're allowed to have more than one entry in the table. So going through this table, we only have one entry, Daylight Savings Time. Daylight Savings Time begins the second Sunday of March after March 1. So after March 1, Daylight Savings Time begins the second Sunday of March. The reason why we have the one is in some countries, there are some areas in the world where Daylight Savings Time doesn't occur until some other Sunday, let's say the first Sunday or the 15th day of the Monday; that's why we had this particular value. And Daylight Savings Time begins at 7200 seconds or in this case 2 hours so for our example 2:00 A.M. Daylight Savings doesn't begin until after 2:00 A.M. So again, we start off. It's the second Sunday after March 1 at 2:00 A.M. When does it end? Well, it ends at the first Sunday after November 1 at 2:00 A.M., again 7200 seconds. And the adjustment is 3600 seconds or 1 hour which is equivalent to one hour. So the Daylight Savings Time adjustment is one hour. So this is how you fill out the Daylight Savings Timetable. So now that we've talked about the timebase schedule and the Daylight Savings Time, let's go back to our PRL table and fill out the additional specification. The SSM shall support at least 32 timebase table entries, 8 day plans, 8 events per day plan, 32 field master actions in the action table while supporting 4 events per action and 1 daylight savings schedule. So, again, this

additional specification will just help clarify what you would like to see in your system. Generally, it won't be a problem with vendors, but you just want to be unambiguous as possible. The next user need we encounter in the PRL is the mandatory need to configure traffic responsive mode. All of these requirements related to this need are mandatory so we'll go ahead and select those. However, again, there is a range specification that we can include or in this case, assign system detectors. So let's look at an example. The number of system detectors that need to be supported can be defined in the PRL. In this figure, we show five system detectors, three on the main line, one, two, three and two on the side cross street. So we show five system detectors, but for growth we may want to specify the system supports at least eight system detectors. Again, it depends on your system. So here's the PRL with the sample text filled in. SSM shall support at least eight system detectors. Moving on to the next user need the system configured threshold selection. Our project description did not require threshold selection. We select a signature selection for this project. Again, we could select both. We're allowed to. But we didn't select this need or any of the requirements underneath it for our example. However, if we had selected the need we would have selected all of the mandatory requirements underneath it and for these optional we would have chosen yes or no for these three optional requirements. Again, we could fill out some of the requirements at performance specifications for some of this, for some of those requirements. So we can define the minimum number of detectors per group, the number of levels that need to be supported for split cycle offset. So as your detector values change or cycle split offsets will change so you can specify how many levels of each you would like to support. The optional requirements you may be concerned about traffic backups for your system. So the standard does allow you to specify your system needs to support these options to override the signal timing plans based on backup queues, occupancy values levels, or non-arterial detector levels. The next user need is the optional need to configure signature selection. Our project description for our example specifically required signature selection so we'll go ahead and select this user need. And because we selected this user need we must select the mandatory requirements there underneath it. So that's these two requirements. Again, we can specify ranges for these requirements with signature selections. So the implementer has to determine for its agency based on its operations and its needs, how many signatures it wishes to support and how many signature detectors needs to be supported for each signature. We're not going to show the sample text for that particular user need, plus I think you got the basic idea by now. Next user need we encounter is the mandatory need to configure a plan selection mode schedule, which is selecting the method for selecting timing plans so we'll select that user need. And there's only one requirement, which is also mandatory so we'll go ahead and select that two. The next user need is synchronize clocks of SSLs. So this user need is mandatory and so are all of the requirements underneath it. So we'll select this user need and all of the requirements. The next user need is the condition or optional need to configure cycle length by plan. We had previously decided that sync pulses were not needed for our project so we'll select no for this user need. But if were to select yes, then this

requirement would become mandatory also. So we'll have to select yes for that also but since we select no we don't have to select yes for this requirement. The next user need is the need to manage alarms, all of the requirements. Well, the user need is mandatory, all of the requirements are mandatory so we'll go ahead and select that. The same with loss of control of SSL, the user need is mandatory and so are the requirements, so we'll go ahead and select those. And failed system detectors, all of the-- well, the user need is mandatory so we'll go ahead and select that. This is a conditional so if we had selected the threshold option, then we would have to select yes for that. But because we did not select it we'll select no for this requirement. And signature, we did select the signature selection previously. So because of that, this requirement because it's mandatory so we'll go ahead and select yes and support this requirement. Other alarms within SSL, again, the user need is mandatory and there's only one requirement which is also mandatory, so we'll select that also. Forward SSM alarms and events, again, user need is mandatory and so is all of the requirements underneath it so we select yes for that. And manage system display data, all of the requirements are mandatory as is the user need. We'll fill out the additional specification that's 500 milliseconds. Previously, we had actually already selected current traffic responsive comparison so we'll go ahead and select that also. Monitor traffic conditions, all of the requirements related to this need is yes so we'll go ahead and select those since this user need is mandatory. And finally, managed SSLs, this is actually an optional user need. So we'll go ahead and select no for this case as to make it simpler. So if you select "No" none of these requirements will become mandatory so we don't have to select those requirements. So this is an example of how we complete a PRL. We've reached our next poll. So the poll asks when should a requirement with a conformance statement Threshold:M, threshold mandatory, so the predicate is threshold, be selected? You can look at NTCIP 1210 Clause 3.2.3.2. Or the participant student supplement on page two to help you with this poll. We've reprinted the predicate table here for you. So, again, when should a requirement with a conformance Threshold:M be selected? Your choices are only when user need 2.5.1.2.5.2 is selected. Always. Only when requirement 3.4.4.1.4.2 is selected. Or D, only when requirement 3.4.3.5.3.5 is selected. So go ahead and fill out the poll. So the correct answer is actually A, only when user need 2.5.1.2.5.2. is selected. That was the purpose of the predicate table. The predicate table says the threshold is predicated only when something is true. So threshold pointed to user need 2.5.1.2.5.2 so when user need 2.5.1.2.5.2. is true then this requirement comes into play. And since there was Threshold:M it means that well since we selected this user need that particular requirement is now mandatory. So the correct answer is A. It is not B. The predicate means that support is conditional on another selection. It is not C. If you look at requirement 3.4.4.1.4.2 you'll see that's Threshold:M also and that doesn't make sense because then it will be a circular logic that this requirement is true when the condition is true also which the circular in nature. So that doesn't make sense. And requirement 3.4.3.5.3.5 as a requirement under user need threshold selection. So even though it's an optional requirement so that don't make sense

because the conformance may be mandatory even if this override threshold is not selected.

Patrick Chan: So the next couple of slides what we'll do is now that we've completed the PRL the next couple of slides we'll talk about how to include the PRL as part of your specification. Note that the PRL is only part of one interface specification, your NTCIP interface. It only defines the data requirements for NTCIP interface. When combined with the communication specification which we talked about in Module C101 introduction to the communications protocols and their users in ITS applications, together with this completed PRL for 1210 they form interface specification. A deployment may need multiple interface specifications. So you may have a traffic management system but in addition to controlling and monitoring field masters they may control and monitor other devices, such as a local intersection which uses a different standard, NTCIP 1202 or let's say a dynamic metro sign. So you may have different interface specifications for each of those types of devices, one for the field master, this one, one for DMS, and one for traffic signal controllers. You may also need to support legacy protocols which may be a current vendor's proprietary communications protocol and data requirements swapping out controllers of field masters from existing one to a new one is generally prohibitively expensive. So if you've got a large system you can't do it all at once. Or you might be lucky and you may have the funds to do it but often we don't have enough funds to change out the whole system. So what many HC's do is procure the system in phases and when they procure the new system these new controllers or field masters will support both the current vendor's proprietary protocol but also support NTCIP. So when you first install the system you use the old proprietary protocols. And then once it's a sufficient number or a critical mass or critical, you have the new controllers installed in the right places, you can switch over to the NTCIP protocols for those controllers. It might be simply a switch that's in the field masters or it might be just changing out the firmware. Note, I talked about phased deployment of devices. You can also do something similar when you replace your TMC software. Your TMC, traffic management system may support your current vendors proprietary protocol but when you purchase replacement it should also support NTCIP interface, so that as you purchase new controllers with the NTCIP interface, your new traffic management system will be able to manage and communicate with the new controllers while also controlling, operating and controlling and monitoring your current controllers. Consistency, notice that the interface specifications are not standalone items but are a part of your overall specifications. So, for example, when an interface requires clock synchronization there is an implicit specification that the device supports a clock. So the hardware and software specifications that go along with your overall specifications should also specify the parameters of this clock. It's also possible that maybe your current system doesn't have clocks right now but in the future you do plan to add clocks to your new controllers, to your new systems so you may think ahead and it's like well, I don't have it now. I don't have this feature right now but I do plan to use it in the future. So I'll go ahead and procure it. But the point of this slide is just

make sure you're consistent throughout the different specifications. There's some sample text in the participant student supplement about how to use the PRL in the specification. So we'll go over some of those briefly here on this slide. You want to introduce the PRL in these specifications, so the proposers reading the spec understand how to use and read the PRL. In theory the proposer should understand it all ready, but just clarify that the PRL is part of just specification. The PRL is actually copyrighted by the standards development organizations which that makeup NTCIP. So just add a copyright disclaimer on the PRL. And refer this to the supplement for additional text, including additional specifications as we've shown when we walked through the PRL we do have some additional-- we do have some sample text to try and clarify the standard and make your specification as tight as possible. So do review that student supplement. So just to summarize what we've learned in learning objective number two. We used the PRL to specify an SSM interface. We talked about the use of optional requirements, constraints of predicates within the PRL. We've specified some performance criteria for some of the functional requirements. We specified limits and ranges for other functional requirements within the PRL. And we've talked about how to use the PRL, how to include it in your specification.

Patrick Chan: Learning objective three, achieve interoperability and interchangeability. So the next couple of slides we're going to talk about how to use the requirement traceability matrix, how it traces to a single design, how to use a PRL and a requirements traceability matrix to prepare for interoperability and how to use the PRL and requirements traceability matrix to compare for interchangeability. First, the requirements traceability matrix for the standard can be found in Annex A. What the requirements traceability matrix does is it maps out all of the requirements that's supported by the standard to a specific design, to a single design. Note, there are some potential issues in the current version of the standards and early deployments should coordinate with other experts. But let's continue. And we'll discuss some of those issues later in the module. Let's first review, I'll go over the requirements traceability matrix. The first column of the matrix presents the requirements identified which is the number of the calls within the standard where the requirement is formally defined. The second column indicates the name of the requirement that is being referenced. So we've done that earlier, so we'll just continue on. The third column represents the clause reference of the associated dialog. Each requirement should only trace to one dialog. In other words, there's only one standardized design for any given requirement. And by having that one standard design, that's what provides support of interoperability and interchangeability. Each dialog defines a sequence of events that must be supported. It might be exchange of information. It also may contain other rules on how the standardized design should be implemented. The fourth and fifth column of the requirements traceability matrix define the clause references and the names of the associated objects. Single requirements will often trace to multiple objects and a single object often traces to multiple requirements. But note, for example, note that requirement 3.3.1.6 here references a group of associated objects called the 5.7

group. The rules in the dialog 4.2.13 will tell you how to use the associated rules in the 5.7 group, how they should be used in the dialog. So early deployment should be careful to precisely define what objects may be implemented for their projects to avoid ambiguity. But the dialogs, usually, tell you exactly within that group how each object is to be used. There is a many-to-many relationships between requirements and objects as I briefly mentioned before. Requirements can relate to multiple objects and/or dialogs. But in addition, the object or dialogs can be traced back to multiple requirements. So you may have different requirements pointing to the same dialog. But the same dialog may point to multiple requirements. The sixth column provides comments that are informational in nature and do not relate to conformance. So they're really there for reference and may provide some useful information. If there's nothing there don't worry about it. In this case, this is just clarifying that this requirement is related to traffic management system communicating to a local controller using the field master as a pass-through. So, again, the requirements traceability matrix provides exactly one design for any requirement and thereby allows a given feature to interoperate and be interchangeable. In other words, all systems to conform to the standard, all systems shall fulfill the requirement the exact same way. The standard says this is how you shall do it to fulfill the requirement to conform to the standard. By conforming to the standard we achieve interoperability. So we'll discuss how now. First of all the requirements traceability matrix provides interoperability at an individual requirement level. Well, let's go back. Let's talk a little bit more about the interoperability. The interoperability is really the ability of different components or for the purpose of this module different implementations from different vendors whether it be a field master or a traffic management system, to exchange information, to use the information that has been exchanged. Interoperability is a key objective for using the standards. And interoperability reduces risk and by extension costs. An example of interoperability is Wi-Fi. Along with other standards such as Internet protocols, when we have Wi-Fi it doesn't matter whose hotspot you're at, whether it's at McDonald's, Starbucks or airport or what laptop you're using whether it's Dell or Lenovo, by conforming to the Wi-Fi standard, the Internet standard, HTTP, the mail protocols, and other standards, NTCIP users will be able to connect to the Internet and get their mail. The idea is similar with NTCIP at the traffic management system and devices uses the same standard it doesn't matter whose field master you try and share information with or whose traffic management system vendor you're trying to use, you'll be able to share the information. So the requirements traceability matrix provides interoperability at an individual requirement level. So for each requirement, it doesn't have to be double standard, but for each requirement we define by a single design how we support interoperability. This is how we shall do it. This is what I'm going to provide you. This is what you're going to receive from me and this is the sequence. The PRL on the other hand indicates what requirements are supported or required by the implementation whether it be the traffic management system or the field master. A comparison of the PRLs for each component, the TMS or the field master will provide a quick determination of interoperability. So based on these requirements if I look into the PRL you can see oh

my traffic management system supports these user needs and these requirements and comparing it to the field master's PRL you'll see what user needs and requirements it will support. So if both the traffic management system and the field master support the same feature then interoperability is provided for that feature. But let's go through some of the other scenarios. If the traffic management system supports it but the SSM does not, well, the traffic management system can still use other features, typically, as long as the feature doesn't change the mode of the device, for example, into a mode that the SSM does not support it by the standard. And typically a TMS can still use the same feature. They can still operate with that feature of other devices. So I may not be able to interoperate for that feature with one SSM but if another SSM from a different vendor supports it I'll be able to interoperate with that SSM, that vendor B's SSM. Another scenario is that the field master supports it but the traffic management system does not. So in that case that feature that the SSM supports can be used by other future TMS's. Or maybe it could be supported potentially be used manually meaning, for example, a field maintenance laptop. So we have a maintenance laptop, a field personnel is out there and if that laptop software supports it then that laptop software they're interoperable with the field master. This is for in comparison to PRLs also allow quick determination of interchangeability. Interchangeability is the ability to replace one component with another from a different manufacturer. So the closer that the two PRLs from the two vendors match, the more likely these two different field masters will be interchangeable. So they're both pieces of equipment from two different vendors, both supported feature. The equipment is interchangeable for that feature. The new equipment supports it but the old one doesn't, well, it might be because the new equipment is interchangeable with other equipment from other vendors. And it might be because there's a new feature that you've added as part of your procurement but if the old equipment supports it but the new one does not well it might be because the feature simply wasn't supported by the old equipment. Or maybe the reason why the new one doesn't need it is because the new equipment doesn't support it is because maybe it didn't require any specification. It may have been a feature that the old system didn't use so now it's fine that the new equipment doesn't support that feature. So we've reached another poll. And the poll asks what does the following table mean? So this is a snapshot of the requirements traceability matrix. We have requirement 3.4.1.1 assign system detectors. It points to a dialog 4.2.1 and 5 different objects. So what does the following table mean? A, all of the objects must be supported. B, at least one of the objects must be supported. C, all of the objects must be supported if the requirement is supported. D, at least one of the objects must be supported if the requirement is supported. So we'll pause right here. So the correct answer is actually C. So this is kind of tricky. It says all of the objects must be supported if the requirement is supported. If you don't support that requirement, if that requirement is not specified in your specifications then those objects don't necessarily have to be supported. They may be supported anyway as a result of a different requirement but it doesn't mean it has to be supported for this particular requirement. So the correct answer, again, is C all of the objects must be supported if the requirement is supported. A is

incorrect because the objects only have to be supported. The requirement has been selected in the PRL. Again, they still might be supported anyway as a result of a different requirement that happens to point to the same objects but not for this requirement. At least one of the objects must be supported which is incorrect. If the requirement is selected all of the indicated objects must be supported. And D is incorrect, if at least one of the objects must be supported that's not true. It's not one of the objects must be supported if the requirement is supported. All of the objects must be supported. So let's summarize learning objective number three. We've achieved interoperability, interchangeability through the requirement traceability matrix which traces requirements to a single design. So the standard defines for each requirement. To fulfill the requirement this is the design you must support. The PRL and the RTM allows of easy checks and interoperability. And the PRL and RTM allows for easy checks for interchangeability.

Patrick Chan: Learning objective number four is to understand the NTCIP 1210 dialogs. So what we'll do is we'll examine one of the dialogs of the SSM. And we'll also examine one of the other dialogs that exchange information to an SSL via the SSM. This is a typical NTCIP dialog that's defined in section four of the standard. Notice that many of the dialogs are just simple gets or sets coupled with a response. This one happens to contain a get coupled with a loop that repeatedly sets objects. So for this dialog 4.2.1 the first thing we do is get the maxSensorSources. So we get how many sensors are supported by this field master. And then for each sensor we're going to set a value. Set this sensorSourceintersection, sensorSourceDetNumber, sensorSourceVolumeFactor and sensorSourceOccWeighting. This is what the RTM looks like for a particular requirement which in this case is 3.4.1.1. assign system detectors. Notice that all of the objects that appear here were also shown in the previous sequence diagram. Notice the difference, the RTM provides traceability and says this is the dialog and the objects that must be supported while the dialog in the sequence diagram previously shows what the sequencing of events, what it's going to get-- what's the sequence of events that occurred to fulfill this requirement? A get response, a set of response. One of the user needs that are supported by NTCIP 1210 is the ability to support a pass-through capability so that a traffic management system can deliver send data directly to the local controller. So the master operates as an intermediary rather than the data. So this was the user need and the requirements that define that. The SSM needs to provide the ability to connect communication networks. And the SSM shall provide a pass-through capability for the TMS, traffic management system, to deliver data to the local controller. Note, there are some potential issues as we mentioned earlier. So we'll spend a little time in the following slides to talk about ways to get around the potential issue. This slide is a sequence diagram. It's time going down. So time increases as we go down. This slide kind of explains the standardized designing for the design for connected networks. So to understand the potential issues associated with this feature, we need a basic understanding how this routing works for this requirement. So this slide visually describes how the routing has been designed. First up here the TMS sends a get message route it

to assure that the SSM will support the number of routing message desired. And in response, the SSM will send back a response confirming. The intent of this dialog was to A, allow a TMS to get a set command device including to identify the SSL number. The command is intended for looking at the indication of the frequency once per second, once per minute, one time, et cetera. So it sends it to the SSM and the SSM responds back that yeah, I've received it or maybe I didn't. The next step, then that configuration forces the SSM, the master to forward that command to the SSL. The SSL then responds back like okay, here's my response. So the SSM sends the command to response. The response on the SSL will be stored within the SSM in the SSL response field. Then at a later time which is undefined, it's really at the convenience of the traffic management system when it thinks it's an appropriate time, the traffic management center will poll the master to get that information back from the masters which is to get back the response that originated in the local controller. So that's the intent of this dialog. Some potential catches we do not define or the standard does not define exactly what goes-- what the message is, the format of the message is that the field master has passed through to the local controller from the traffic management system. It could be SNMP request. It could be STMP request. It could be any message conforming to another standard, let's say NTCIP 1210. It could be a message in proprietary format. The standard is silent about that. And, in reality, the SSM doesn't need to understand what's in the content of the message because it's just a pass-through. But it is important that the SSL understand what the message is requesting. The other catch that potentially causes the problem is the sslResponse contains all responses from the SSL. You can interpret this to mean that this is the last packet received from the local controller which could be a response to the command, the command from the traffic management system. It could be a response to some other command. It could be a response to some automated request from the field master. Or it could be just some unsolicited report from the local. So it's not clearly defined. We're unsure what's in that response because 1210 is really interface standard. So the standard doesn't define what the field master does with the response he receives from the SSL. So one can argue that this feature of the standard is not reliable for exchanging information. Again, because it's an interface standard we don't control what the traffic management system should-- when it should poll the field master to get the response that's the word in the field master. When you design the field master, you can probably define it, say hey, this is what I want you to do with it when I use a pass-through but it's not defined in the standard. If you define it within the field master elsewhere, not in the interface specification you can possibly avoid this problem. But the concern is as currently designed by the standard the actual response may be overridden before the traffic management system can retrieve the information. Again, we don't control when the traffic management system will poll the field master to get the response back. So potential workarounds around this since the requirement is that it's a pass-through we couldn't really use IP routing. It's for communications. It's a much more reliable way of exchanging data with the local controller though it does require more bandwidth. With IP you have direct routing which is much faster so you can get that information faster. But there's a

caveat that you've got to have the bandwidth to support IP communications. If IP routing is not a viable solution, then there is some standardized predefined commands, specifically six that the traffic management system can issue directly to the local controller via the field master. So you just tell the field master go ahead and issue this command to the local controller. These commands are to set the time, set sync control, set the pattern, set the special functions, get the status and get the detector volume and occupancy. There's typically a traffic management system may wish to send other types of commands to do local controller, such as I want to download the signal timing pattern to the local controller but that's-- you can't use that direct command to the local controller via the field master. Third potential workaround if you don't have a high speed connection you need to send other commands. You can interpret the definition of all response mean that the most recent response as determined by the transport layer. This essentially requires the field master to process all of the responses, but they'll only really look at the first few bytes of the response message to identify if it's a response to do request from the traffic management system or if the information is intended for another application. If the information, the response from the SSL was intended for another application they could probably throw it out. But if it is a response to regional requests from the traffic management system it would probably just keep it and hope that the traffic management system gets the information-- both the SSMs get the information in time before it's overridden. Require the traffic management system to provide and include port numbers in the transport later. Port numbers are an option so if you require a traffic management system to send out port numbers, the local controller would be required to send back a response of a port number also that way as you send different requests you can send them to different port numbers. And an analogy is if you have a web browser with multiple windows open, when you send a request for information let's say refresh this webpage from one of the windows, your browser knows which port, which window it's requesting, who sent the request. And then when you get the response back on the new webpage it will refresh the webpage on the appropriate window. So then something similar would happen with the field master. Well, actually with the traffic management system the field master would only store response values that are directly associated with the command that was sent out based on the port number. And allow exchange of virtually any connection of data. While it appears that this solution will work, none of these solutions have really been peer reviewed or deployed, so again, you may wish to contact other experts to discuss this in a little bit more detail. And you can do that by contacting, you know, NTCIP coordinator. The second potential issue is the definition of the SSL number, the intersection number. It's defined as intersection number of the target SSL. But there's an implication that it might also be-- that's analogous to a drop number because the range of the object SSL number is from 0 to 63 with 63 defined as a broadcast address. So this appears to be-- to confuse this value with a drop number of a PMPP circuit. The most logical workaround to this ambiguity is to accept the literal interpretation and definition. The disadvantage of that is that your routing feature is limited to the 62 intersections-- excuse me, local controllers, but that's actually probably a fine reality. There's very few, if

any, field masters that control more than 62 local controllers. So that's to summarize from the what we learn about connecting the communication network feature. There is a potential issue that the response when we're using the pass-through feature that the response from the local controller can be overridden before it's read. There's three potential workarounds by using IP routing, using the command feature or do some transport layer processing. Another one is that the intersection number, the SSL number definition might be confusing between the intersection and the drop number. But if we just assume that intersection number limits support of the field master to the 62 intersections. So another poll, what type of messages does the standard allow to be sent to the local controller using the sslCommand feature? The potential answers are A, any of the thirteen standardized messages. B, any of the thirteen user defined messages. C, any message clearly defined in a specification or D virtually any packetized message. So which type of messages does the standard allow to be sent to the local controller using the sslCommand feature? So the answer to this is actually virtually any packetized message. Again, the standard is very silent on what gets transmitted when the field master is used as a pass-through. It can be an SNMP message. It could be a different standard. You might be able to use a 1202 data dictionary to send information directly from the traffic management system to the local controller. The standard is silent. A is incorrect, the standard does not have 13 messages. The reality is it really doesn't include messages. The standard doesn't support messages, any of the thirteen user defined messages. STMP defines thirteen user defined dynamic objects and those can be sent alone with any message. And any message clearly defined in its specification and that's incorrect, as we said. The routing feature is really silent so it allows any type of message to be sent. So just to summarize, learning objective number four we've discussed dialogs between the traffic management center and the field masters review dialog. And we've discussed routing between the traffic management system to the local controller using the field master as a pass-through.

Patrick Chan: Our final learning objective, number five incorporate requirements not covered by the standard. Conditions and context for extending the NTCIP 1210 standard will be discussed and we'll show an example-- present an example of how we can extend the standard. So the NTCIP standards allow for extensions to support operational or user needs that are not supported by the standards. Extensions generally had designs that are not recognized by a standard. And because of that by definition when you add an extension they are considered to be non-conformant though NTCIP does allows its use. The use of extensions really causes interoperability and interchangeability problems which are the very issue that the standards are intended to address and avoid. And while there are times that the extensions are justified and we'll talk about those, they really should only be done with proper consideration to costs involved. So, again, extending the standard complicates interoperability and interchangeability. Interoperability and interchangeability cannot be obtained with extensions unless all of these nine details are known meaning we know what the sequences are of data exchanges and what the rules

are that are defined by the dialog. And we have a clear understanding of what the objects are, what data is being exchanged in the extension. Extensions really are custom solutions. They increase specification costs, development costs, testing costs, integration costs. It takes a little longer to deploy the system and there's increased maintenance cost. And the concern really is that you still may end up with a proprietary solution. Extensions should only be considered when NTCIP features are inadequate to meet the needs. So there's a user need that your agency has that standard does not support and it's important to how you operate your system then yeah an extension should be considered and the benefits-- and you should do the extension when the benefits of the extension outweigh the added cost to build it, deploy it, maintain it, test it. Some key principles to follow when designing an extension. Appropriately integrate with NTCIP only deployments so don't add enumerations to standard objects. So if NTCIP object has a value of one to eight for the same object don't add a value nine. You're breaking conformance and you're creating interoperability problems. Create a new object that has that new value number nine that you want to support. Properly register the new objects on the OID tree to do that. Again, contact your NTCIP coordinator so that other people-- so other implementations are aware of what changes you made, what your extensions are. And allow the mode to have standard operations. So, for example, you adopt a traffic adaptive mode operation make sure that there's some way for you to switch back to a standard mode of operation such as timebase coordination that's supported by the standard. Try and minimize additional added complexity. So try to use the bulk of NTCIP design-- try to use the standard wherever possible before you minimize the use of extensions. So here's an example, of a user need that's not supported currently by the NTCIP 1210 standard. A TMS operator needs the SSM to override timing pattern selections based on the detection of ice in the area. The formation of ice on certain roadways can create traffic hazards that may warrant the prohibition of certain movements at intersections resulting in changed demand patterns on the roadway network. This feature allows the SSMs to ensure these conditions are handled smoothly. So we have a user need that says hey if we detect ice, we want to be able to change the signal timing pattern. So this user need may result in two different requirements that traces the user need. And this traceability should be shown in the table similar to a PRL. Notice the specification typically include configuring the system, the new feature, controlling the new feature and monitoring the new feature. But in this example we determined yeah we don't need a new requirement to control since it's kind of automatic. But we do have one requirement to configure the system, that's the first one X.2.1., the SSM shall allow the TMS to define which plan to use when ice is detected for more than one minute. And the second requirement so we can monitor it the SSM shall allow the TMS, the traffic management system, to determine whether ice is currently detected, how long it has been detected and whether the ice detection override plan is active. So we also want to know is the plan already active, this ice detection override plan for ice. For those requirements we'll create a requirement traceability matrix for these two custom requirements. So the first one configure ice detection override. Notice that this is a set command. This is generic set command so we're going to set an

object xxxIceDetectionOverridePattern to say hey run this pattern. I want to run pattern 16. So I would set the value to 16 so telling the field master run plan 16. The second requirement is to monitor so we'll get the values from the field master. The first one is has ice been detected or not? So this may be a yes or a no. The time the ice has been detected for. So it might be in seconds, so it's like oh we've detected ice for 150 seconds for example. And X.4.4. xxxiceDetectionOverrideActive, am I already running that override pattern right now? Is it in effect? This slide shows what a custom object for the customized user need might look like so this is xxxiceDetectionOverridePattern, which pattern am I going to run. It's an integer, so it supports values 1 to 255. The definition is the timing pattern that is to be activated when the ice detected is true. And the ice detected time is more than 60 seconds in the past. And the point of this slide is to emphasize that even for simple custom feature as detecting ice, it still takes a considerable amount of work to build out the custom-- to define the custom dialogs and the objects. So it really should only be done when there is a real need. It's not our goal at this time to explain how to define our object. We just want to explain that it does require some additional work. This is the slide that shows the custom object for the customized user need, what it might look like. So we've reached our final poll. And the question is which of the following is the best reason to extend the standard? The answer choices are A, there's an unmet need that justifies the added cost. B, the extender system uses a nonstandard design. C, you want to use your specification to favor a specific vendor. Or D, the standardized solution is overly complex for your simple needs. So the correct answer is actually A, unmet need justifies the cost. So there was some user need that wasn't satisfied by the standard and supporting that user need justifies the cost. So that answer is A. It isn't B. The existing system uses a nonstandard design, so essentially it's a proprietary design. So you do that will just prolong customization for another generation. So you're still going to have this customized approach for your new system. B to favor a specific vendor, we won't talk about that one. And standardized solution is overly complex. And we recognize-- so even though some of the solutions are complex the lifecycle cost of implementing a nonstandard solution are significant because, again, it's custom. You still have to maintain that custom design. So let's review what we've covered in learning objective number five. We've discussed the conditions and the context for extending the standard. And we've provided an example of how to extend the standard.

Patrick Chan: So the last couple of slides, we just wanted to review what we've learned in this module. The PRL can be used to trace user needs to requirements. The additional specification PRL column can be used to define additional performance and objet range specifications. The student supplement has a list of additional specifications that can be used for the PRL if you're writing a specification. The RTM traces each requirement to a single design solution, therefore providing for interoperability and potential interchangeability. NTCIP 1210 allows the traffic management system to send virtually any message to a local controller via the field master. And develop custom features

entails significant effort and risk. Here are some resources in case you wanted to learn more or you need additional information about any of the concepts we talked about today. The current version of the standard will be found at NTCIP.org. That's also how you can reach out to the NTCIP coordinator for assistance if you have any questions or comments. There's also an NTCIP guide which provides some background information about how the NTCIP family of standards work. And the IEEE 1233 which is a guide for developing system requirements specifications. This is a slide for questions. These are some frequently asked questions or questions that have been asked regarding the NTCIP 1210 standard. The first question is how do I get assistance if I want to deploy NTCIP 1210? Again, currently there are no deployments that we are aware that uses NTCIP 1210. So if you're deploying or you need assistance we would recommend contacting the NTCIP coordinator. And you can find that person, reach out by email at NTCIP.org. Where can I find out more information about the Daylight Savings Time? There is a concept-- the Daylight Savings Time is defined in a different standard, a normative standard called NTCIP 1201 global objects. And in one of the annexes there is a discussion on how Daylight Savings Time is supposed to work. When the final standard be published? For version one, it is currently at the publisher's, so we're hoping that the final version, public standard version will be available in early 2014. Can you give an example of a performance requirement for field masters? We have a couple of requirements, performance requirements scattered throughout the PRL. So one example is how quickly the response time for a component will respond to a request from another component. So that's an example of a performance requirement. A question that was asked, is this consistent with the systems engineering process for a traffic signal installation and system integration including the TMS interface? And the answer is actually yes. We use the system engineering process in the development of the standard. So we do have a concept of operations to help which is a good starting point to requirements and the design. Can you give us a link of the system engineering process relevant to the standard? I don't have the exact link but if you look at the NTCIP guide, NTCIP 1201 in the previous slide, there is a discussion in there, in the latest version, version four about how to use system engineering process. In addition, U.S. DOT has published a document about user system engineering process for ITS project. And so if you do a search for U.S. DOT systems engineering ITS you should be able to find that guidebook. Often also a source that's quoted is Caltrans, the state of California Department of Transportation has a system engineering handbook. I forget what version it is. But if you do a search for a system engineering ITS you'll be able to find that document. And finally, can you send us or give a link to download these slides and save for future reference? If you found this, the student supplement it should also be there, along with these slides. So it should be bcb.its.dot.gov, I believe. So this concludes our course today. Thank you very much for joining us. Hopefully it's been helpful. And this concludes the presentation. Thank you.

End of 2013_12_23_13.07_A304b_Final_Recording.wmv