INST 260 (Data Acquisition systems), section 3

Lab

Data acquisition and transport over Ethernet: *Question 111*, **completed objectives due by the end of day 6**

Exam

Day 6 – only a simple calculator may be used! **Complete mastery of these objectives due by the next exam date**

Specific objectives for the "mastery" exam:

- Electricity Review: Calculate and annotate voltages and currents in a DC series-parallel resistor circuit given source and resistor values
- Sketch proper wire connections for a data acquisition unit to measure an analog sensor signal
- Convert between different numeration systems (decimal, binary, hexadecimal, octal)
- Calculate ADC (analog-digital converter) input and output values given calibrated ranges
- Solve for a specified variable in an algebraic formula
- Determine the possibility of suggested faults in a simple circuit given measured values (voltage, current), a schematic diagram, and reported symptoms
- Motor/relay/3phase/PLC Review: Determine status of a relay logic circuit given a schematic diagram and switch stimulus conditions
- INST241 Review: Identify (American) wire colors for different thermocouple types
- INST250 Review: Convert between different pressure units (PSI, "W.C., bar, etc.) showing proper mathematical cancellation of units (i.e. the "unity fraction" technique)

Recommended daily schedule

Day 1

Theory session topic: IP, TCP, and UDP

Questions 1 through 20; answer questions 1-8 in preparation for discussion (remainder for practice)

Day 2

Theory session topic: HART and Modbus protocols

Questions 21 through 40; answer questions 21-29 in preparation for discussion (remainder for practice)

Day 3

Theory session topic: Digital network security

Questions 41 through 60; answer questions 41-46 in preparation for discussion (remainder for practice)

Day 4

Theory session topic: Digital network security (continued)

Questions 61 through 80; answer questions 61-66 in preparation for discussion (remainder for practice)

Day 5

Theory session topic: Review for exam

Questions 81 through 100; answer questions 81-90 in preparation for discussion (remainder for practice)

Feedback questions *(101 through 110)* are optional and may be submitted for review at the end of the day

Day 6

Exam

How To . . .

Access the worksheets and textbook: go to the *Socratic Instrumentation* website located at `http://www.ibiblio.org/kuphaldt/socratic/sinst` to find worksheets for every 2nd-year course section organized by quarter, as well as both the latest "stable" and "development" versions of the *Lessons In Industrial Instrumentation* textbook. Download and save these documents to your computer.

Maximize your learning: complete all homework *before* class starts, ready to be assessed as described in the "Inverted Session Formats" pages. Use every minute of class and lab time productively. Follow all the tips outlined in "Question 0" as well as your instructor's advice. Do not take constructive criticism personally. Make every reasonable effort to solve problems on your own before seeking help.

Identify upcoming assignments and deadlines: read the first page of each course worksheet.

Relate course days to calendar dates: reference the calendar spreadsheet file (`calendar.xlsx`), found on the BTC campus `Y:` network drive. A printed copy is posted in the Instrumentation classroom.

Locate industry documents assigned for reading: use the Instrumentation Reference provided by your instructor (on CD-ROM and on the BTC campus `Y:` network drive). There you will find a file named `00_index_OPEN_THIS_FILE.html` readable with any internet browser. Click on the "Quick-Start Links" to access assigned reading documents, organized per course, in the order they are assigned.

Study for the exams: Mastery exams assess specific skills critically important to your success, listed near the top of the front page of each course worksheet for your review. Familiarize yourself with this list and pay close attention when those topics appear in homework and practice problems. Proportional exams feature problems you haven't seen before that are solvable using general principles learned throughout the current and previous courses, for which the only adequate preparation is independent problem-solving practice every day. Answer the "feedback questions" (practice exams) in each course section to hone your problem-solving skills, as these are similar in scope and complexity to proportional exams. Answer these feedback independently (i.e. no help from classmates) in order to most accurately assess your readiness.

Calculate course grades: download the "Course Grading Spreadsheet" (`grades_template.xlsx`) from the Socratic Instrumentation website, or from the BTC campus `Y:` network drive. Enter your quiz scores, test scores, lab scores, and attendance data into this Excel spreadsheet and it will calculate your course grade. You may compare your calculated grades against your instructors' records at any time.

Identify courses to register for: read the "Sequence" page found in each worksheet.

Receive extra instructor help: ask during lab time, or during class time, or by appointment. Tony may be reached by email at `tony.kuphaldt@btc.edu` or by telephone at 360-752-8477.

Identify job openings: regularly monitor job-search websites. Set up informational interviews at workplaces you are interested in. Participate in jobshadows and internships. Apply to jobs long before graduation, as some employers take *months* to respond! Check your BTC email account daily for alerts.

Impress employers: sign the FERPA release form granting your instructors permission to share academic records, then make sure your performance is worth sharing. Document your project and problem-solving experiences for reference during interviews. Honor all your commitments.

Begin your career: participate in jobshadows and internships while in school to gain experience and references. Take the first Instrumentation job that pays the bills, and give that employer at least two years of good work to pay them back for the investment they have made in you. Employers look at delayed employment, as well as short employment spans, very negatively. Failure to pass a drug test is an immediate disqualifier, as is falsifying any information. Criminal records may also be a problem.

file `howto`

General Values, Expectations, and Standards

Success in this career requires professional integrity, resourcefulness, persistence, close attention to detail, and intellectual curiosity. If you are ever in doubt as to the values you should embody, just ask yourself what kind of a person you would prefer to hire for your own enterprise. Those same values will be upheld within this program.

Learning is the purpose of any educational program, and a worthy priority in life. Every circumstance, every incident, every day here will be treated as a learning opportunity, every mistake as a "teachable moment". Every form of positive growth, not just academic ability, will be regarded as real learning.

Responsibility means *ensuring* the desired outcome, not just *trying* to achieve the outcome. To be a responsible person means you *own* the outcome of your decisions and actions.

Integrity means being honest and forthright in all your words and actions, doing your very best every time and never taking credit for the achievement of another.

Safety means doing every job correctly and ensuring others are not endangered. Lab safety standards include wearing closed-toed shoes and safety glasses in the lab room during lab hours, wearing ear protection around loud sounds, using ladders to reach high places, using proper lock-out/tag-out procedures, no energized electrical work above 30 volts without an instructor present in the lab room, and no power tool use without an instructor present in the lab room.

Diligence in study means exercising self-discipline and persistence, realizing that hard work is a necessary condition for success. This means, among other things, investing the necessary time and effort in studying, reading instructions, paying attention to details, utilizing the skills and tools you already possess, and avoiding shortcuts. Diligence in work means the job is not done until it is done *correctly*: all objectives achieved, all problems solved, all documentation complete, and no errors remaining.

Self-management means allocating your resources (time, equipment, labor) wisely, and not just focusing on the closest deadline.

Communication means clearly conveying your thoughts and paying attention to what others convey, across all forms of communication (e.g. oral, written, nonverbal).

Teamwork means working constructively with your classmates to complete the job at hand. Remember that here the first job is *learning*, and so teamwork means working to maximize everyone's learning (not just your own). The goal of learning is more important than the completion of any project or assignment.

Initiative means recognizing needs and taking action to meet those needs without encouragement or direction from others.

Representation means your actions reflect this program and not just yourself. Doors of opportunity for all BTC graduates may be opened or closed by your own conduct. Unprofessional behavior during tours, jobshadows, internships, and/or jobs reflects poorly on the program and will negatively bias employers.

Trustworthiness is the result of consistently exercising these values: people will recognize you as someone they can rely on to get the job done, and therefore someone they would want to employ.

Respect means acknowledging the intrinsic value, capabilities, and responsibilities of those around you. Respect is gained by consistent demonstration of valued behaviors, and it is lost through betrayal of trust.

Punctuality and Attendance: late arrivals are penalized at a rate of 1% grade deduction per incident. Absence is penalized at a rate of 1% per hour (rounded to the nearest hour) except when employment-related, school-related, weather-related, or required by law (e.g. court summons). Absences may be made up by directing the instructor to apply "sick hours" (12 hours of sick time available per quarter). Classmates may donate their unused sick hours. Sick hours may not be applied to unannounced absences, so be sure to alert your instructor and teammates as soon as you know you will be absent or late. Absence on an exam day will result in a zero score for that exam, unless due to a documented emergency.

Mastery: any assignment or objective labeled as "mastery" must be completed with 100% competence (with multiple opportunities to re-try). Failure to complete by the deadline date caps your grade at a C−. Failure to complete by the end of the *next* school day results in a failing (F) grade for that course.

Time Management: Use all available time wisely and productively. Work on other useful tasks (e.g. homework, feedback questions, job searching) while waiting for other activities or assessments to begin. Trips to the cafeteria for food or coffee, smoke breaks, etc. must not interfere with team participation.

Orderliness: Keep your work area clean and orderly, discarding trash, returning tools at the end of every lab session, and participating in all scheduled lab clean-up sessions. Project wiring, especially in shared areas such as junction boxes, must not be left in disarray at the end of a lab shift. Label any failed equipment with a detailed description of its symptoms.

Independent Study: the "inverted" instructional model used in this program requires independent reading and problem-solving, where every student must demonstrate their learning at the start of the class session. Question 0 of every worksheet lists practical study tips. The "Inverted Session Formats" pages found in every worksheet outline the format and grading standards for inverted class sessions.

Independent Problem-Solving: make an honest effort to solve every problem before seeking help. When working in the lab, help will not be given unless and until you run your own diagnostic tests.

Teamwork: inform your teammates if you need to leave the work area for any reason. Any student regularly compromising team performance through absence, tardiness, disrespect, or other disruptive behavior(s) will be removed from the team and required to complete all labwork individually. The same is true for students found inappropriately relying on teammates.

Communication: check your email daily for important messages. Ask the instructor to clarify any assignment or exam question you find confusing, and express your work clearly.

Academic Progress: your instructor will record your academic achievement, as well as comments on any negative behavior, and will share all these records with employers if you sign the FERPA release form. You may see these records at any time, and you should track your own academic progress using the grade spreadsheet template. Extra-credit projects will be tailored to your learning needs.

Office Hours: your instructor's office hours are by appointment, except in cases of emergency. Email is the preferred method for setting up an appointment with your instructor to discuss something in private.

Grounds for Failure: a failing (F) grade will be earned in any course if any mastery objectives are past deadline by more than one school day, or for any of the following behaviors: false testimony (lying), cheating on any assignment or assessment, plagiarism (presenting another's work as your own), willful violation of a safety policy, theft, harassment, sabotage, destruction of property, or intoxication. These behaviors are grounds for immediate termination in this career, and as such will not be tolerated here.

file `expectations`

Program Outcomes for Instrumentation and Control Technology (BTC)

#1 Communication

Communicate and express concepts and ideas across a variety of media (verbal, written, graphical) using industry-standard terms.

#2 Time management

Arrives on time and prepared to work; Budgets time and meets deadlines when performing tasks and projects.

#3 Safety

Complies with national, state, local, and college safety regulations when designing and performing work on systems.

#4 Analysis and Diagnosis

Analyze, evaluate, and diagnose systems related to instrumentation and control including electrical and electronic circuits, fluid power and signaling systems, computer networks, and mechanisms; Select and apply correct mathematical techniques to these analytical and diagnostic problems; Select and correctly use appropriate test equipment to collect data.

#5 Design and Commissioning

Select, design, construct, configure, and install components necessary for the proper function of systems related to instrumentation and control, applying industry standards and verifying correct system operation when complete.

#6 System optimization

Improve technical system functions by collecting data and evaluating performance; Implement strategies to optimize the function of these systems.

#7 Calibration

Assess instrument accuracy and correct inaccuracies using appropriate calibration procedures and test equipment; Select and apply correct mathematical techniques to these calibration tasks.

#8 Documentation

Interpret and create technical documents (e.g. electronic schematics, loop diagrams, functional diagrams, P&IDs, graphs, narratives) according to industry standards.

#9 Independent learning

Select and research information sources to learn new principles, technologies, and techniques.

#10 Job searching

Develop a professional resume and research job openings in the field of industrial instrumentation.

file `outcomes_program`

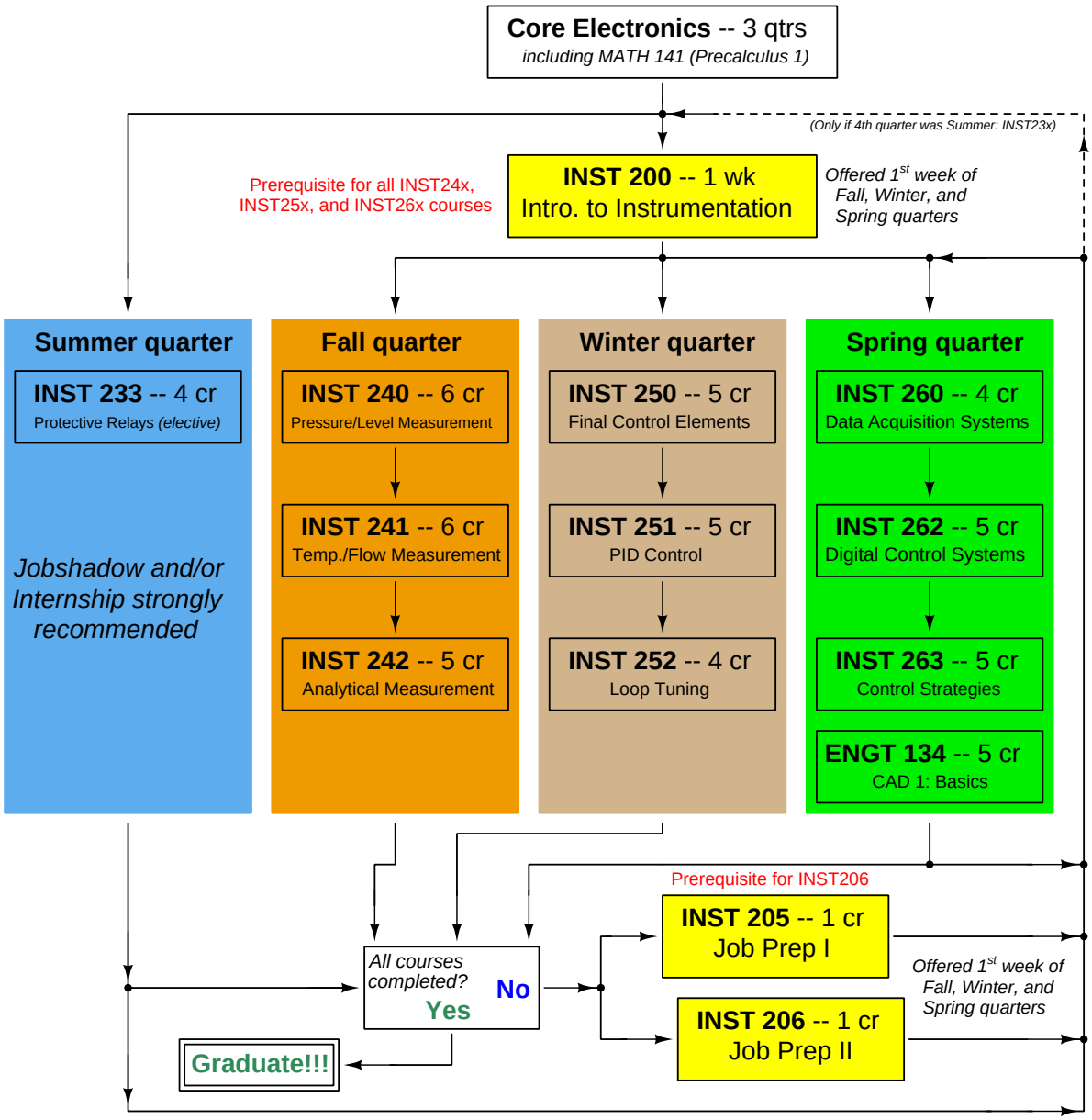
INST 260 Course Outcomes

Each and every outcome in this course is assessed at a mastery level (i.e. 100% competence)

- Calculate and annotate voltages and currents in a DC series-parallel circuit. [Ref: Program Learning Outcome #4]
- Sketch proper wire connections for a data acquisition unit to measure an analog sensor signal. [Ref: Program Learning Outcome #5]
- Convert between different numeration systems (decimal, binary, hexadecimal, octal). [Ref: Program Learning Outcome #4]
- Calculate ADC (analog-digital converter) input and output values given calibrated ranges. [Ref: Program Learning Outcome #7]
- Solve for specified variables in algebraic formulae. [Ref: Program Learning Outcome #4]
- Determine the possibility of suggested faults in simple circuits given measured values (voltage, current), schematic diagrams, and reported symptoms. [Ref: Program Learning Outcome #4]
- Demonstrate proper use of safety equipment and application of safe procedures while using power tools, and working on live systems. [Ref: Program Learning Outcome #3]
- Communicate effectively with teammates to plan work, arrange for absences, and share responsibilities in completing all labwork. [Ref: Program Learning Outcomes #1 and #2]
- Construct and commission a working data acquisition system consisting of a DAQ unit, signal wiring, Ethernet wiring and components, and a personal computer running DAQ software. [Ref: Program Learning Outcome #5]
- Generate accurate schematic diagrams documenting your team's DAQ system. [Ref: Program Learning Outcome #8]
- Design and build a circuit responding to changes in either light intensity or temperature. [Ref: Program Learning Outcome #5]
- Diagnose a random fault placed in another team's DAQ system by the instructor within a limited time using no test equipment except a multimeter and network diagnostic utilities on the personal computer, logically justifying your steps in the instructor's direct presence. [Ref: Program Learning Outcome #4]

file `outcomes_INST260`

Sequence of second-year Instrumentation courses



The particular sequence of courses you take during the second year depends on when you complete all first-year courses and enter the second year. Since students enter the second year of Instrumentation at four different times (beginnings of Summer, Fall, Winter, and Spring quarters), the particular course sequence for any student will likely be different from the course sequence of classmates.

Some second-year courses are only offered in particular quarters with those quarters not having to be in sequence, while others are offered three out of the four quarters and must be taken in sequence. The following layout shows four typical course sequences for second-year Instrumentation students, depending on when they first enter the second year of the program:

Possible course schedules depending on date of entry into 2nd year

file `sequence`

General tool and supply list

Wrenches

- Combination (box- and open-end) wrench set, 1/4" to 3/4" – *the most important wrench sizes are 7/16", 1/2", 9/16", and 5/8"; get these immediately!*
- Adjustable wrench, 6" handle (sometimes called "Crescent" wrench)
- Hex wrench ("Allen" wrench) set, fractional – 1/16" to 3/8"
- *Optional:* Hex wrench ("Allen" wrench) set, metric – 1.5 mm to 10 mm
- *Optional:* Miniature combination wrench set, 3/32" to 1/4" (sometimes called an "ignition wrench" set)

Note: *always maximize surface engagement on a fastener's head to reduce stress on that fastener. (e.g. Using box-end wrenches instead of adjustable wrenches; using the proper size and type of screwdriver; never using any tool that mars the fastener such as pliers or vise-grips unless absolutely necessary.)*

Pliers

- Needle-nose pliers
- Diagonal wire cutters (sometimes called "dikes")

Screwdrivers

- Slotted, 1/8" and 1/4" shaft
- Phillips, #1 and #2
- Jeweler's screwdriver set
- *Optional:* Magnetic multi-bit screwdriver (e.g. Klein Tools model 70035)

Electrical

- Multimeter, Fluke model 87-IV or better
- Assortment of alligator-clip style jumper wires
- Soldering iron (10 to 40 watt) and rosin-core solder
- Resistor, potentiometer, diode assortments (from first-year lab kits)
- Package of insulated compression-style fork terminals (14 to 18 AWG wire size, #10 stud size)
- Wire strippers/terminal crimpers for 10 AWG to 18 AWG wire and insulated terminals
- *Optional:* ratcheting terminal crimp tool (e.g. Paladin 1305, Ferrules Direct FDT10011, or equivalent)

Safety

- Safety glasses or goggles (available at BTC bookstore)
- Earplugs (available at BTC bookstore)

Miscellaneous

- Simple scientific calculator (non-programmable, non-graphing, no conversions), TI-30Xa or TI-30XIIS recommended. Required for some exams!
- Portable personal computer capable of wired Ethernet connectivity, Wi-Fi connectivity, displaying PDF documents, creating text documents, creating and viewing spreadsheets, running PLC programming software (MS Windows only), and executing command-line utilities such as `ping`.
- Masking tape (for making temporary labels)
- Permanent marker pen
- Teflon pipe tape
- Utility knife
- Tape measure, 12 feet minimum
- Flashlight

file `tools`

Methods of instruction

This course develops self-instructional and diagnostic skills by placing students in situations where they are required to research and think independently. In all portions of the curriculum, the goal is to avoid a passive learning environment, favoring instead *active engagement* of the learner through reading, reflection, problem-solving, and experimental activities. The curriculum may be roughly divided into two portions: *theory* and *practical*. All "theory" sessions follow the *inverted* format and contain virtually no lecture.

Inverted theory sessions

The basic concept of an "inverted" learning environment is that the traditional allocations of student time are reversed: instead of students attending an instructor-led session to receive new information and then practicing the application of that information outside of the classroom in the form of homework, students in an inverted class encounter new information outside of the classroom via homework and apply that information in the classroom session under the instructor's tutelage.

A natural question for instructors, then, is what their precise role is in an inverted classroom and how to organize that time well. Here I will list alternate formats suitable for an inverted classroom session, each of them tested and proven to work.

Small sessions

Students meet with instructors in small groups for short time periods. Groups of 4 students meeting for 30 minutes works very well, but groups as large as 8 students apiece may be used if time is limited. Each of these sessions begins with a 5 to 10 minute graded inspection of homework with individual questioning, to keep students accountable for doing the homework. The remainder of the session is a dialogue focusing on the topics of the day, the instructor challenging each student on the subject matter in Socratic fashion, and also answering students' questions. A second grade measures each student's comprehension of the subject matter by the end of the session.

This format also works via teleconferencing, for students unable to attend a face-to-face session on campus.

Large sessions

Students meet with instructors in a standard classroom (normal class size and period length). Each of these sessions begins with a 10 minute graded quiz (closed-book) on the homework topic(s), to keep students accountable for doing the homework. Students may leave the session as soon as they "check off" with the instructor in a Socratic dialogue as described above (instructor challenging each student to assess their comprehension, answering questions, and grading the responses). Students sign up for check-off on the whiteboard when they are ready, typically in groups of no more than 4. Alternatively, the bulk of the class session may be spent answering student questions in small groups, followed by another graded quiz at the end.

Correspondence

This format works for students unable to attend a "face-to-face" session, and who must correspond with the instructor via email or other asynchronous medium. Each student submits a thorough presentation of their completed homework, which the instructor grades for completeness and accuracy. The instructor then replies back to the student with challenge questions, and also answers questions the student may have. As with the previous formats, the student receives another grade assessing their comprehension of the subject matter by the close of the correspondence dialogue.

Methods of instruction (continued)

In all formats, students are held accountable for completion of their homework, "completion" being defined as successfully interpreting the given information from source material (e.g. accurate outlines of reading or video assignments) and constructive effort to solve given problems. It must be understood in an inverted learning environment that students *will* have legitimate questions following a homework assignment, and that it is therefore unreasonable to expect mastery of the assigned subject matter. What is reasonable to expect from each and every student is a basic outline of the source material (reading or video assignments) complete with major terms defined and major concepts identified, plus a good-faith effort to solve every problem. Question 0 (contained in every worksheet) lists multiple strategies for effective study and problem-solving.

Sample rubric for pre-assessments

- **No credit** = Any homework question unattempted (i.e. no effort shown on one or more questions); incomprehensible writing; failure to follow clear instruction(s)
- **Half credit** = Misconception(s) on any major topic explained in the assigned reading; answers shown with no supporting work; verbatim copying of text rather than written in student's own words; outline missing important topic(s); unable to explain the outline or solution methods represented in written work
- **Full credit** = Every homework question answered, with any points of confusion clearly articulated; all important concepts from reading assignments accurately expressed in the outline and clearly articulated when called upon by the instructor to explain

The minimum expectation at the start of every student-instructor session is that all students have made a good-faith effort to complete 100% of their assigned homework. This does not necessarily mean all answers will be correct, or that all concepts are fully understood, because one of the purposes of the meeting between students and instructor is to correct remaining misconceptions and answer students' questions. However, experience has shown that without accountability for the homework, a substantial number of students will not put forth their best effort and that this compromises the whole learning process. Full credit is reserved for good-faith effort, where each student thoughtfully applies the study and problem-solving recommendations given to them (see Question 0).

Sample rubric for post-assessments

- **No credit** = Failure to comprehend one or more key concepts; failure to apply logical reasoning to the solution of problem(s); no contribution to the dialogue
- **Half credit** = Some misconceptions persist by the close of the session; problem-solving is inconsistent; limited contribution to the dialogue
- **Full credit** = Socratic queries answered thoughtfully; effective reasoning applied to problems; ideas communicated clearly and accurately; responds intelligently to questions and statements made by others in the session; adds new ideas and perspectives

The minimum expectation is that each and every student engages with the instructor and with fellow students during the Socratic session: posing intelligent questions of their own, explaining their reasoning when challenged, and otherwise positively contributing to the discussion. Passive observation and listening is not an option here – every student must be an active participant, contributing something original to every dialogue. If a student is confused about any concept or solution, it is their responsibility to ask questions and seek resolution.

If a student happens to be absent for a scheduled class session and is therefore unable to be assessed on that day's study, they may schedule a time with the instructor to demonstrate their comprehension at some later date (before the end of the quarter when grades must be submitted). These same standards of performance apply equally make-up assessments: either inspection of homework or a closed-book quiz for the pre-assessment, and either a Socratic dialogue with the instructor or another closed-book quiz for the post-assessment.

Lab sessions

In the lab portion of each course, students work in teams to install, configure, document, calibrate, and troubleshoot working instrument loop systems. Each lab exercise focuses on a different type of instrument, with a limited time period typically for completion. An ordinary lab session might look like this:

(1) Start of practical (lab) session: announcements and planning
   (a) The instructor makes general announcements to all students
   (b) The instructor works with team to plan that day's goals, making sure each team member has a clear idea of what they should accomplish
(2) Teams work on lab unit completion according to recommended schedule:
   (First day) Select and bench-test instrument(s), complete prototype sketch of project
   (One day) Connect instrument(s) into a complete loop
   (One day) Each team member drafts their own loop documentation, inspection done as a team (with instructor)
   (One or two days) Each team member calibrates/configures the instrument(s)
   (Remaining days, up to last) Each team member troubleshoots the instrument loop
(3) End of practical (lab) session: debriefing where each team reports on their work to the whole class

Troubleshooting assessments must meet the following guidelines:

- Troubleshooting must be performed *on a system the student did not build themselves.* This forces students to rely on another team's documentation rather than their own memory of how the system was built.
- Each student must individually demonstrate proper troubleshooting technique.
- Simply finding the fault is not good enough. Each student must consistently demonstrate sound reasoning while troubleshooting.
- If a student fails to properly diagnose the system fault, they must attempt (as many times as necessary) with different scenarios until they do, reviewing any mistakes with the instructor after each failed attempt.

Distance delivery methods

Sometimes the demands of life prevent students from attending college 6 hours per day. In such cases, there exist alternatives to the normal 8:00 AM to 3:00 PM class/lab schedule, allowing students to complete coursework in non-traditional ways, at a "distance" from the college campus proper.

For such "distance" students, the same worksheets, lab activities, exams, and academic standards still apply. Instead of working in small groups and in teams to complete theory and lab sections, though, students participating in an alternative fashion must do all the work themselves. Participation via teleconferencing, video- or audio-recorded small-group sessions, and such is encouraged and supported.

There is no recording of hours attended or tardiness for students participating in this manner. The pace of the course is likewise determined by the "distance" student. Experience has shown that it is a benefit for "distance" students to maintain the same pace as their on-campus classmates whenever possible.

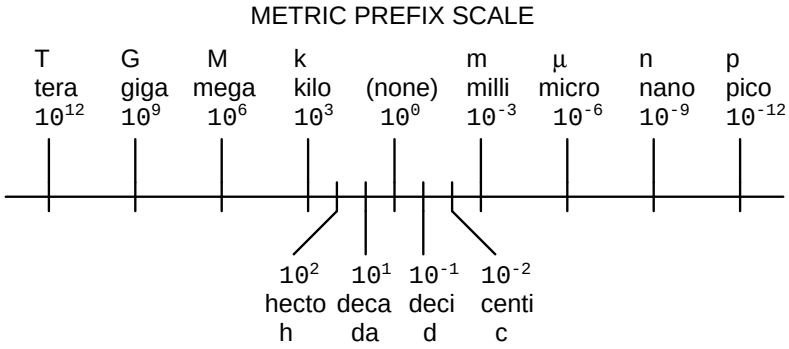
In lieu of small-group activities and class discussions, comprehension of the theory portion of each course will be ensured by completing and submitting detailed answers for *all* worksheet questions, not just passing daily quizzes as is the standard for conventional students. The instructor will discuss any incomplete and/or incorrect worksheet answers with the student, and ask that those questions be re-answered by the student to correct any misunderstandings before moving on.

Labwork is perhaps the most difficult portion of the curriculum for a "distance" student to complete, since the equipment used in Instrumentation is typically too large and expensive to leave the school lab facility. "Distance" students must find a way to complete the required lab activities, either by arranging time in the school lab facility and/or completing activities on equivalent equipment outside of school (e.g. at their place of employment, if applicable). Labwork completed outside of school must be validated by a supervisor and/or documented via photograph or videorecording.

Conventional students may opt to switch to "distance" mode at any time. This has proven to be a benefit to students whose lives are disrupted by catastrophic events. Likewise, "distance" students may switch back to conventional mode if and when their schedules permit. Although the existence of alternative modes of student participation is a great benefit for students with challenging schedules, it requires a greater investment of time and a greater level of self-discipline than the traditional mode where the student attends school for 6 hours every day. No student should consider the "distance" mode of learning a way to have more free time to themselves, because they will actually spend more time engaged in the coursework than if they attend school on a regular schedule. It exists merely for the sake of those who cannot attend during regular school hours, as an alternative to course withdrawal.

file `distance`

- **Metric prefixes**
- Yotta = 10^{24} Symbol: Y
- Zeta = 10^{21} Symbol: Z
- Exa = 10^{18} Symbol: E
- Peta = 10^{15} Symbol: P
- Tera = 10^{12} Symbol: T
- Giga = 10^{9} Symbol: G
- Mega = 10^{6} Symbol: M
- Kilo = 10^{3} Symbol: k
- Hecto = 10^{2} Symbol: h
- Deca = 10^{1} Symbol: da
- Deci = 10^{-1} Symbol: d
- Centi = 10^{-2} Symbol: c
- Milli = 10^{-3} Symbol: m
- Micro = 10^{-6} Symbol: μ
- Nano = 10^{-9} Symbol: n
- Pico = 10^{-12} Symbol: p
- Femto = 10^{-15} Symbol: f
- Atto = 10^{-18} Symbol: a
- Zepto = 10^{-21} Symbol: z
- Yocto = 10^{-24} Symbol: y



- **Conversion formulae for temperature**
- ^{o}F = (^{o}C)(9/5) + 32
- ^{o}C = (^{o}F - 32)(5/9)
- ^{o}R = ^{o}F + 459.67
- K = ^{o}C + 273.15

Conversion equivalencies for distance

1 inch (in) = 2.540000 centimeter (cm)

1 foot (ft) = 12 inches (in)

1 yard (yd) = 3 feet (ft)

1 mile (mi) = 5280 feet (ft)

Conversion equivalencies for volume

1 gallon (gal) = 231.0 cubic inches (in^3) = 4 quarts (qt) = 8 pints (pt) = 128 fluid ounces (fl. oz.) = 3.7854 liters (l)

1 milliliter (ml) = 1 cubic centimeter (cm^3)

Conversion equivalencies for velocity

1 mile per hour (mi/h) = 88 feet per minute (ft/m) = 1.46667 feet per second (ft/s) = 1.60934 kilometer per hour (km/h) = 0.44704 meter per second (m/s) = 0.868976 knot (knot – international)

Conversion equivalencies for mass

1 pound (lbm) = 0.45359 kilogram (kg) = 0.031081 slugs

Conversion equivalencies for force

1 pound-force (lbf) = 4.44822 newton (N)

Conversion equivalencies for area

1 acre = 43560 square feet (ft^2) = 4840 square yards (yd^2) = 4046.86 square meters (m^2)

Conversion equivalencies for common pressure units (either all gauge or all absolute)

1 pound per square inch (PSI) = 2.03602 inches of mercury (in. Hg) = 27.6799 inches of water (in. W.C.) = 6.894757 kilo-pascals (kPa) = 0.06894757 bar

1 bar = 100 kilo-pascals (kPa) = 14.504 pounds per square inch (PSI)

Conversion equivalencies for absolute pressure units (only)

1 atmosphere (Atm) = 14.7 pounds per square inch absolute (PSIA) = 101.325 kilo-pascals absolute (kPaA) = 1.01325 bar (bar) = 760 millimeters of mercury absolute (mmHgA) = 760 torr (torr)

Conversion equivalencies for energy or work

1 british thermal unit (Btu – "International Table") = 251.996 calories (cal – "International Table") = 1055.06 joules (J) = 1055.06 watt-seconds (W-s) = 0.293071 watt-hour (W-hr) = 1.05506 x 10^{10} ergs (erg) = 778.169 foot-pound-force (ft-lbf)

Conversion equivalencies for power

1 horsepower (hp – 550 ft-lbf/s) = 745.7 watts (W) = 2544.43 british thermal units per hour (Btu/hr) = 0.0760181 boiler horsepower (hp – boiler)

Acceleration of gravity (free fall), Earth standard

9.806650 meters per second per second (m/s^2) = 32.1740 feet per second per second (ft/s^2)

Physical constants

Speed of light in a vacuum (c) = 2.9979×10^8 meters per second (m/s) = 186,281 miles per second (mi/s)

Avogadro's number (N_A) = 6.022×10^{23} per mole (mol^{-1})

Electronic charge (e) = 1.602×10^{-19} Coulomb (C)

Boltzmann's constant (k) = 1.38×10^{-23} Joules per Kelvin (J/K)

Stefan-Boltzmann constant (σ) = 5.67×10^{-8} Watts per square meter-Kelvin^4 ($W/m^2 \cdot K^4$)

Molar gas constant (R) = 8.314 Joules per mole-Kelvin (J/mol-K)

Properties of Water

Freezing point at sea level = $32^oF = 0^oC$

Boiling point at sea level = $212^oF = 100^oC$

Density of water at 4^oC = 1000 kg/m^3 = 1 g/cm^3 = 1 kg/liter = 62.428 lb/ft^3 = 1.94 $slugs/ft^3$

Specific heat of water at 14^oC = 1.00002 calories/g·^oC = 1 BTU/lb·^oF = 4.1869 Joules/g·^oC

Specific heat of ice $\approx$ 0.5 calories/g·^oC

Specific heat of steam $\approx$ 0.48 calories/g·^oC

Absolute viscosity of water at 20^oC = 1.0019 centipoise (cp) = 0.0010019 Pascal-seconds (Pa·s)

Surface tension of water (in contact with air) at 18^oC = 73.05 dynes/cm

pH of pure water at 25^o C = 7.0 (*pH scale = 0 to 14*)

Properties of Dry Air at sea level

Density of dry air at 20^oC and 760 torr = 1.204 mg/cm^3 = 1.204 kg/m^3 = 0.075 lb/ft^3 = 0.00235 $slugs/ft^3$

Absolute viscosity of dry air at 20^oC and 760 torr = 0.018 centipoise (cp) = 1.8×10^{-5} Pascal-seconds (Pa·s)

file `conversion_constants`

Question 0

How to get the most out of academic reading:

- Outline, don't highlight! Identify every major idea presented in the text, and express these ideas in your own words. A suggested ratio is one sentence of your own thoughts per paragraph of text read.
- Articulate your thoughts as you read (i.e. "have a conversation" with the author). This will develop *metacognition*: active supervision of your own thoughts. Note points of agreement, disagreement, confusion, epiphanies, and connections between different concepts or applications.
- Work through all mathematical exercises shown within the text, to ensure you understand all the steps.
- Imagine explaining concepts you've just learned to someone else. Teaching forces you to distill concepts to their essence, thereby clarifying those concepts, revealing assumptions, and exposing misconceptions. Your goal is to create the simplest explanation that is still technically accurate.
- Create your own questions based on what you read, as a teacher would to challenge students.

How to effectively problem-solve and troubleshoot:

- Rely on principles, not procedures. Don't be satisfied with memorizing steps – learn *why* those steps work. Each step should make logical sense and have real-world meaning to you.
- Sketch a diagram to help visualize the problem. Sketch a graph showing how variables relate. When building a real system, always prototype it on paper and analyze its function *before* constructing it.
- Identify what it is you need to solve, identify all relevant data, identify all units of measurement, identify any general principles or formulae linking the given information to the solution, and then identify any "missing pieces" to a solution. Annotate all diagrams with this data.
- Perform "thought experiments" to explore the effects of different conditions for theoretical problems. When troubleshooting, perform *diagnostic tests* rather than just visually inspect for faults.
- Simplify the problem and solve that simplified problem to identify strategies applicable to the original problem (e.g. change quantitative to qualitative, or visa-versa; substitute easier numerical values; eliminate confusing details; add details to eliminate unknowns; consider simple limiting cases; apply an analogy). Remove components from a malfunctioning system to simplify it and better identify the nature and location of the problem.
- Check for exceptions – does your solution work for *all* conditions and criteria?
- Work "backward" from a hypothetical solution to a new set of given conditions.

How to manage your time:

- Avoid procrastination. Work now and play later, every single day.
- Consider the place you're in when deciding what to do. If there is project work to do and you have access to the lab, do that work and not something that could be done elsewhere (e.g. homework).
- Eliminate distractions. Kill your television and video games. Turn off your mobile phone, or just leave it at home. Study in places where you can concentrate, like the Library.
- Use your "in between" time productively. Don't leave campus for lunch. Arrive to school early. If you finish your assigned work early, begin working on the next assignment.

Above all, cultivate persistence, as this is necessary to master anything non-trivial. The keys to persistence are (1) having the desire to achieve that mastery, and (2) realizing challenges are normal and not an indication of something gone wrong. A common error is to equate *easy* with *effective*: students often believe learning should be easy if everything is done right. The truth is that mastery never comes easy!

file `question0`

Checklist when reading an instructional text

"Reading maketh a full man; conference a ready man; and writing an exact man" – Francis Bacon

Francis Bacon's advice is a blueprint for effective education: reading provides the learner with knowledge, writing focuses the learner's thoughts, and critical dialogue equips the learner to confidently communicate and apply their learning. Independent acquisition and application of knowledge is a powerful skill, well worth the effort to cultivate. To this end, students should read these educational resources closely, write their own outline and reflections on the reading, and discuss in detail their findings with classmates and instructor(s). You should be able to do all of the following after reading any instructional text:

☑ Briefly OUTLINE THE TEXT, as though you were writing a detailed Table of Contents. Feel free to rearrange the order if it makes more sense that way. Prepare to articulate these points in detail and to answer questions from your classmates and instructor. Outlining is a good self-test of thorough reading because you cannot outline what you have not read or do not comprehend.

☑ Demonstrate ACTIVE READING STRATEGIES, including verbalizing your impressions as you read, simplifying long passages to convey the same ideas using fewer words, annotating text and illustrations with your own interpretations, working through mathematical examples shown in the text, cross-referencing passages with relevant illustrations and/or other passages, identifying problem-solving strategies applied by the author, etc. Technical reading is a special case of problem-solving, and so these strategies work precisely because they help solve any problem: paying attention to your own thoughts (metacognition), eliminating unnecessary complexities, identifying what makes sense, paying close attention to details, drawing connections between separated facts, and noting the successful strategies of others.

☑ Identify IMPORTANT THEMES, especially GENERAL LAWS and PRINCIPLES, expounded in the text and express them in the simplest of terms as though you were teaching an intelligent child. This emphasizes connections between related topics and develops your ability to communicate complex ideas to anyone.

☑ Form YOUR OWN QUESTIONS based on the reading, and then pose them to your instructor and classmates for their consideration. Anticipate both correct and incorrect answers, the incorrect answer(s) assuming one or more plausible misconceptions. This helps you view the subject from different perspectives to grasp it more fully.

☑ Devise EXPERIMENTS to test claims presented in the reading, or to disprove misconceptions. Predict possible outcomes of these experiments, and evaluate their meanings: what result(s) would confirm, and what would constitute disproof? Running mental simulations and evaluating results is essential to scientific and diagnostic reasoning.

☑ Specifically identify any points you found CONFUSING. The reason for doing this is to help diagnose misconceptions and overcome barriers to learning.

General challenges following a tutorial reading assignment

- Summarize as much of the text as you can in one paragraph of your own words. A helpful strategy is to explain ideas as you would for an intelligent child: as simple as you can without compromising too much accuracy.
- Simplify a particular section of the text, for example a paragraph or even a single sentence, so as to capture the same fundamental idea in fewer words.
- Where did the text make the most sense to you? What was it about the text's presentation that made it clear?
- Identify where it might be easy for someone to misunderstand the text, and explain why you think it could be confusing.
- Identify any new concept(s) presented in the text, and explain in your own words.
- Identify any familiar concept(s) such as physical laws or principles applied or referenced in the text.
- Devise a proof of concept experiment demonstrating an important principle, physical law, or technical innovation represented in the text.
- Devise an experiment to disprove a plausible misconception.
- Did the text reveal any misconceptions you might have harbored? If so, describe the misconception(s) and the reason(s) why you now know them to be incorrect.
- Describe any useful problem-solving strategies applied in the text.
- Devise a question of your own to challenge a reader's comprehension of the text.

General follow-up challenges for assigned problems

- Identify where any fundamental laws or principles apply to the solution of this problem, especially before applying any mathematical techniques.
- Devise a thought experiment to explore the characteristics of the problem scenario, applying known laws and principles to mentally model its behavior.
- Describe in detail your own strategy for solving this problem. How did you identify and organized the given information? Did you sketch any diagrams to help frame the problem?
- Is there more than one way to solve this problem? Which method seems best to you?
- Show the work you did in solving this problem, even if the solution is incomplete or incorrect.
- What would you say was the most challenging part of this problem, and why was it so?
- Was any important information missing from the problem which you had to research or recall?
- Was there any extraneous information presented within this problem? If so, what was it and why did it not matter?
- Examine someone else's solution to identify where they applied fundamental laws or principles.
- Simplify the problem from its given form and show how to solve this simpler version of it. Examples include eliminating certain variables or conditions, altering values to simpler (usually whole) numbers, applying a limiting case (i.e. altering a variable to some extreme or ultimate value).
- For quantitative problems, identify the real-world meaning of all intermediate calculations: their units of measurement, where they fit into the scenario at hand. Annotate any diagrams or illustrations with these calculated values.
- For quantitative problems, try approaching it qualitatively instead, thinking in terms of "increase" and "decrease" rather than definite values.
- For qualitative problems, try approaching it quantitatively instead, proposing simple numerical values for the variables.
- Were there any assumptions you made while solving this problem? Would your solution change if one of those assumptions were altered?
- Identify where it would be easy for someone to go astray in attempting to solve this problem.
- Formulate your own problem based on what you learned solving this one.

Questions

Question 1

Read and outline the introduction to the "Internet Protocol (IP)" section of the "Digital Data Acquisition and Networks" chapter in your *Lessons In Industrial Instrumentation* textbook.

After closely reading and outlining a text, you should be ready to share the following with your classmates and instructor:

(1) Your written summary of all major points of the text, expressed as simply as possible in your own words. A "Table of Contents" format works well for this.
(2) Active helpful reading strategies (e.g. verbalizing your thoughts as you read, simplifying long sentences, working through mathematical examples, cross-referencing text with illustrations or other text, identifying the author's problem-solving strategies, etc.).
(3) General principles, especially physical laws, referenced in the text.
(4) Questions of your own you would pose to another reader, to challenge their understanding.
(5) Ideas for experiments that could be used to either demonstrate some concept applied in the text, or disprove a related misconception.
(6) Any points of confusion, and precisely why you found the text confusing.

file i04444

Question 2

Read and outline the "IP Addresses" subsection of the "Internet Protocol (IP)" section of the "Digital Data Acquisition and Networks" chapter in your *Lessons In Industrial Instrumentation* textbook.

After closely reading and outlining a text, you should be ready to share the following with your classmates and instructor:

(1) Your written summary of all major points of the text, expressed as simply as possible in your own words. A "Table of Contents" format works well for this.
(2) Active helpful reading strategies (e.g. verbalizing your thoughts as you read, simplifying long sentences, working through mathematical examples, cross-referencing text with illustrations or other text, identifying the author's problem-solving strategies, etc.).
(3) General principles, especially physical laws, referenced in the text.
(4) Questions of your own you would pose to another reader, to challenge their understanding.
(5) Ideas for experiments that could be used to either demonstrate some concept applied in the text, or disprove a related misconception.
(6) Any points of confusion, and precisely why you found the text confusing.

file i04445

Question 3

Read and outline the "Subnetworks and Subnet Masks" subsection of the "Internet Protocol (IP)" section of the "Digital Data Acquisition and Networks" chapter in your *Lessons In Industrial Instrumentation* textbook.

After closely reading and outlining a text, you should be ready to share the following with your classmates and instructor:

(1) Your written summary of all major points of the text, expressed as simply as possible in your own words. A "Table of Contents" format works well for this.
(2) Active helpful reading strategies (e.g. verbalizing your thoughts as you read, simplifying long sentences, working through mathematical examples, cross-referencing text with illustrations or other text, identifying the author's problem-solving strategies, etc.).
(3) General principles, especially physical laws, referenced in the text.
(4) Questions of your own you would pose to another reader, to challenge their understanding.
(5) Ideas for experiments that could be used to either demonstrate some concept applied in the text, or disprove a related misconception.
(6) Any points of confusion, and precisely why you found the text confusing.

file i04446

Question 4

Read and outline the "Command-Line Diagnostic Utilities" subsection of the "Internet Protocol (IP)" section of the "Digital Data Acquisition and Networks" chapter in your *Lessons In Industrial Instrumentation* textbook.

After closely reading and outlining a text, you should be ready to share the following with your classmates and instructor:

(1) Your written summary of all major points of the text, expressed as simply as possible in your own words. A "Table of Contents" format works well for this.
(2) Active helpful reading strategies (e.g. verbalizing your thoughts as you read, simplifying long sentences, working through mathematical examples, cross-referencing text with illustrations or other text, identifying the author's problem-solving strategies, etc.).
(3) General principles, especially physical laws, referenced in the text.
(4) Questions of your own you would pose to another reader, to challenge their understanding.
(5) Ideas for experiments that could be used to either demonstrate some concept applied in the text, or disprove a related misconception.
(6) Any points of confusion, and precisely why you found the text confusing.

file i04447

Question 5

Read and outline the "Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)" section of the "Digital Data Acquisition and Networks" chapter in your *Lessons In Industrial Instrumentation* textbook.

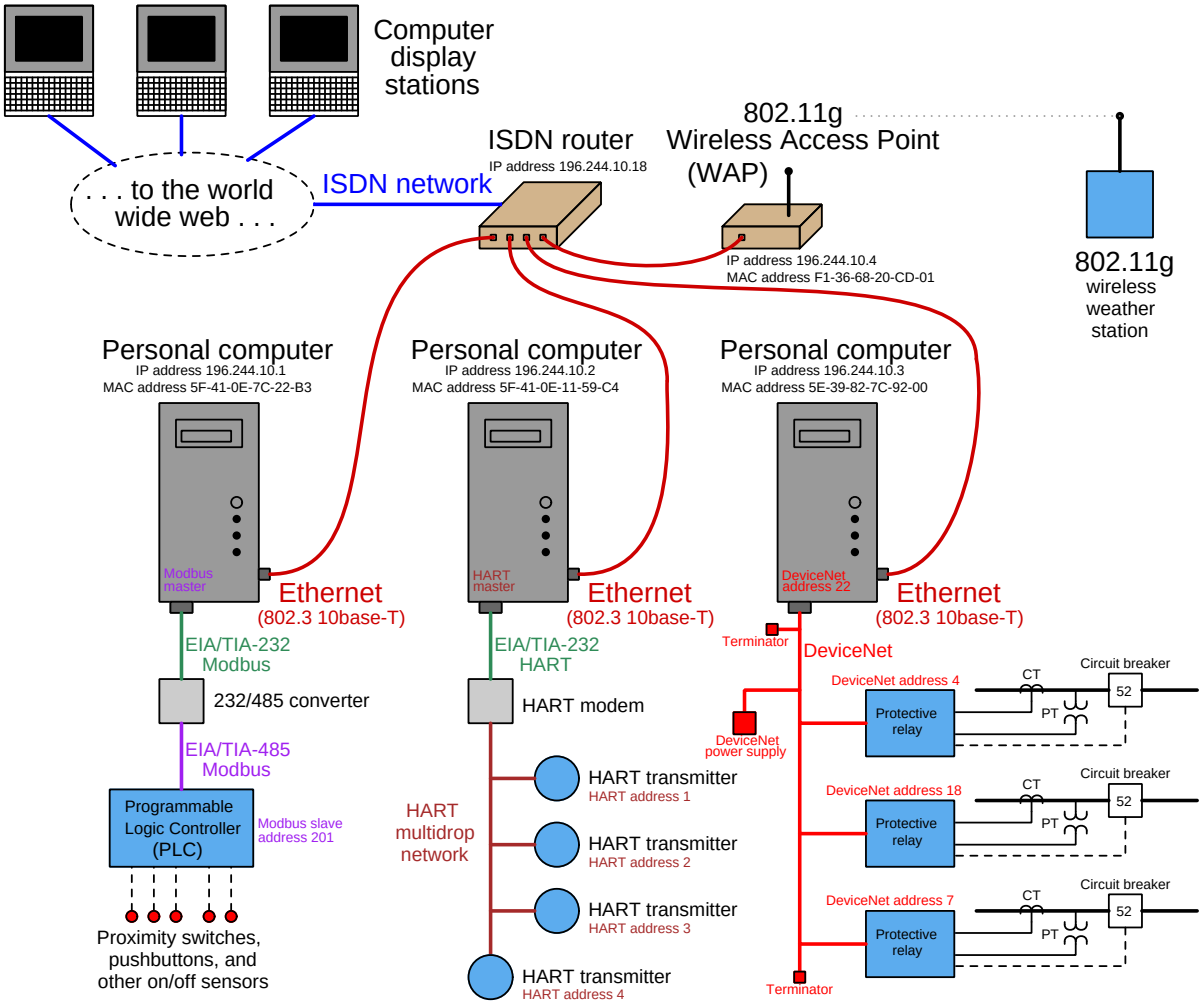
After closely reading and outlining a text, you should be ready to share the following with your classmates and instructor:

(1) Your written summary of all major points of the text, expressed as simply as possible in your own words. A "Table of Contents" format works well for this.
(2) Active helpful reading strategies (e.g. verbalizing your thoughts as you read, simplifying long sentences, working through mathematical examples, cross-referencing text with illustrations or other text, identifying the author's problem-solving strategies, etc.).
(3) General principles, especially physical laws, referenced in the text.
(4) Questions of your own you would pose to another reader, to challenge their understanding.
(5) Ideas for experiments that could be used to either demonstrate some concept applied in the text, or disprove a related misconception.
(6) Any points of confusion, and precisely why you found the text confusing.

file i04448

Question 6

Examine this network diagram of an industrial data acquisition system, comprised of different technologies for acquiring the data, but ultimately communicating to computer display stations located somewhere on the Internet (world wide web):



Identify some of the different OSI layer 1 (physical) network standards you see in this system, as well as OSI layer 2 (data link) addressing schemes. Then, explain how all this data, in all its different forms, gets shuttled over the same ISDN cable to the Internet using TCP/IP packets.

Suggestions for Socratic discussion

- Identify where the diagnostic utlility `ping` could be used to test nodes in this heterogeneous network.
- Identify where the diagnostic utlility `ping` could *not* be used to test nodes in this heterogeneous network.

file i02236

Question 7

One day a new instrument technician goes to connect a PLC (programmable logic controller) to an operator display panel and notices the communication ports on both the PLC and on the display panel are labeled *Modbus*, which the technician figures is some sort of networking standard. Upon inspection of the screw terminals the technician also notices the wiring is similar to RS-485 (EIA/TIA-485), with TD(+), TD(−), RD(+), and RD(−) terminals. Later on, when reading the user manuals for both devices, the technician notices the ports described as being "RS-485" as well as being "Modbus."

Asking a more experienced technician about this, the answer is that the ports are *both* EIA/TIA-485 and Modbus. These two network standards are not exclusive, but complementary.

Elsewhere in the world, a new computer network technician is going to download some software from a website, and notices it is possible to use either *HTTP* (Hyper-Text Transfer Protocol) or *FTP* (File Transfer Protocol) to do the job. Looking behind the computer, the technician notices a regular Ethernet cable (twisted-pair) plugged into the network port. Later, the technician asks someone more experienced, "Which network standard am I using when I download files, HTTP, FTP, or Ethernet?" The answer is similar to that given to the instrument technician: HTTP and FTP are alternatives to each other, both being complementary to Ethernet as parts of a complete protocol "pathway" from file to user. It is never a question of HTTP *or* Ethernet, just as it is never a question of Modbus *or* RS-485.

How would you explain either situation, using the OSI seven-layer model as a guide?

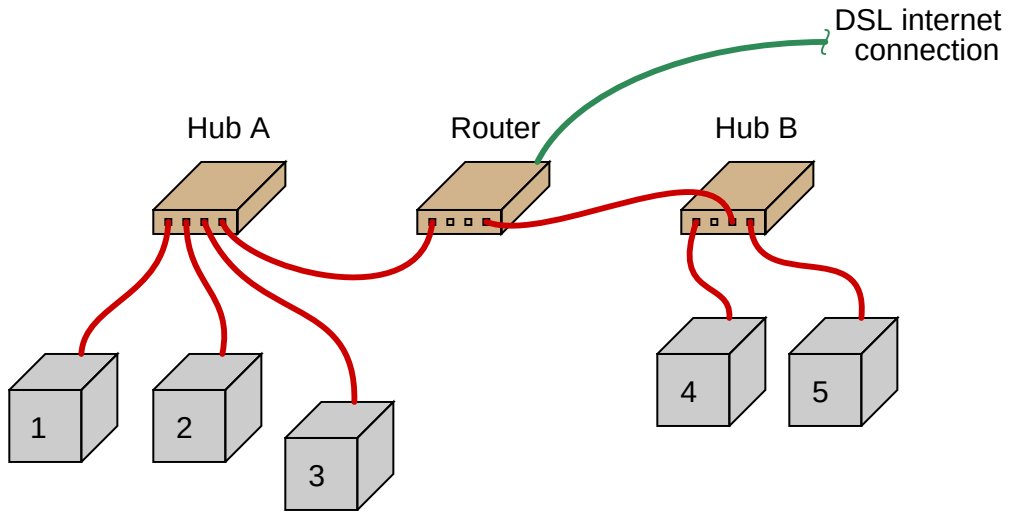
Suggestions for Socratic discussion

- A commonly-heard criticism of the OSI model is that "no communications standard fully agrees with it," i.e. no single standard has specifications in all seven layers of the model. Explain why this is not really a problem at all, and how it represents a fundamental misunderstanding of the OSI model.
- *ASCII* is a layer-6 standard for encoding alphanumeric text in digital form. Give an example where this standard works in conjunction with lower-level standards to communicate text data between two computers.
- *S-HTTP* is a layer-7 standard used for encrypting and decrypting digital data over networks. This is what you are using when you access a web page beginning with `https://`. Give an example where this standard works in conjunction with ASCII and other lower-level standards to securely communicate a credit card number between two computers during an online purchase transaction.

file i02237

Question 8

The following Ethernet network has a problem. Someone trying to access the Internet from personal computer #4 cannot do so, and has called you to troubleshoot the problem:



Your first diagnostic test is to "ping" computer #4 from computer #5, and you find that this test is successful. Your next test is to check Internet connectivity at computer #5 by "pinging" `http://www.google.com`, and you find that test is successful as well.

Identify the likelihood of each specified fault for this network. Consider each fault one at a time (i.e. no coincidental faults), determining whether or not each fault could independently account for *all* measurements and symptoms in this network.

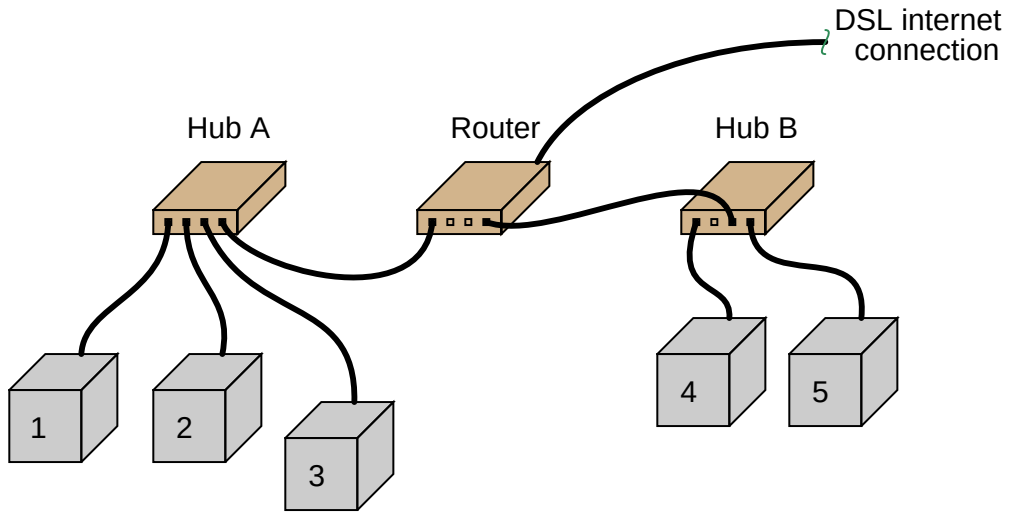
Fault	**Possible**	**Impossible**
Hub A failed		
Hub B failed		
Router failed		
Internet service provider failed		
Cable failed between computer #4 and Hub B		
Cable failed between Hub A and Router		
Cable failed between Hub B and Router		
Security settings (e.g. firewall) in computer #4		

Finally, identify the *next* diagnostic test or measurement you would make on this system. Explain how the result(s) of this next test or measurement help further identify the location and/or nature of the fault.

file i04461

Question 9

This Ethernet network has a problem in it somewhere:



- 1 can "ping" 3
- 4 can "ping" `www.google.com`
- 4 can "ping" 5
- 2 cannot "ping" `www.google.com`

An excellent diagnostic strategy is to trace paths of data flow in a complex system, looking for places of intersection. Successful paths prove all points along the pathway are functioning. Places of overlap between unsuccessful paths prove that section is suspect.

Apply this strategy to the problem at hand, and use the results to narrow the field of possible faults.

Also, identify a good "next ping" test to do.

file i02123

Question 10

The fourth version of the *IP* (Internet Protocol) standard, known as IPv4, specifies an address that is 32 bits wide. The address is usually expressed in the form of four "octets" translated into decimal form and separated by periods. Here is an example of an IPv4 address:

```
196.252.70.183
```

What are the largest and the smallest IPv4 addresses possible in this format? How many total unique addresses does this work out to be?

The next version of IP is version 6 (version 5 was experimental). IPv6 uses a 128-bit wide address. How many "octets" does it take to express an IPv6 address? How many unique addresses can be represented in the IPv6 field?

Suggestions for Socratic discussion

- Are there any special IP addresses reserved for specific purposes?
- How do the address spaces of IPv4 and IPv6 compare to that of Ethernet MAC address space?
- Why are IP addresses required in addition to Ethernet MAC addresses in a network where most devices are Ethernet-based?
- Explain what `192.168.25.7/24` means as an IP address.
- Explain what `192.168.25.7/8` means as an IP address.

file i02241

Question 11

When I first heard of the "Internet," I made the mistake of thinking it was a special cable stretching across vast portions of the world, dedicated to transporting web-page digital data. To my surprise, the essential thing that makes up the Internet is not a physical object at all, but rather a *network protocol* specifying how digital data may be transparently communicated across all manner of digital networks (dedicated cables, satellite links, fiber optics, radio, etc.). This protocol permits the exchange of data across an ad-hoc collection of networks between points far and wide. Without a platform- and network-independent protocol, Internet really would have to be a dedicated cable or radio link stretching across the United States in order for people across the country to digitally communicate.

This protocol comes in two parts: *TCP* and *IP*. Sometimes it is referred to as a single standard: *TCP/IP*. Explain what "TCP" and "IP" represent, and how these network protocols are independent of specific details such as cable type, data rate, "mark" and "space" voltage levels, and other parameters associated with digital network hardware.

Suggestions for Socratic discussion

- An alternative to TCP is UDP, often used in industrial Ethernet networks. Explain why UDP is more popular within industry, and how it differs from TCP.
- SCADA systems used for the monitoring and control of such things as pipelines and electric power transmission networks typically rely on their own dedicated communication channels rather than the "internet" to communicate digital data over long distances. Explain why.
- Suppose an instrument technician got bored and decided to build a SCADA system for her home. Using a PLC to acquire data from sensors installed throughout the house and also to control lights and valves, the technician is able to monitor her home from a "smart" phone with internet access. Identify some of the network standards that might be employed in this system to transfer data between the PLC and her phone.

file i02232

Question 12

Question 13

Question 14

Question 15

Question 16

Question 17

Question 18

Question 19

Question 20

Question 21

Read and outline the "Basic Concept of HART" subsection of the "HART Digital/Analog Hybrid Standard" section of the "Digital Data Acquisition and Networks" chapter in your *Lessons In Industrial Instrumentation* textbook.

After closely reading and outlining a text, you should be ready to share the following with your classmates and instructor:

(1) Your written summary of all major points of the text, expressed as simply as possible in your own words. A "Table of Contents" format works well for this.
(2) Active helpful reading strategies (e.g. verbalizing your thoughts as you read, simplifying long sentences, working through mathematical examples, cross-referencing text with illustrations or other text, identifying the author's problem-solving strategies, etc.).
(3) General principles, especially physical laws, referenced in the text.
(4) Questions of your own you would pose to another reader, to challenge their understanding.
(5) Ideas for experiments that could be used to either demonstrate some concept applied in the text, or disprove a related misconception.
(6) Any points of confusion, and precisely why you found the text confusing.

file i04462

Question 22

Read and outline the "HART physical layer" subsection of the "HART Digital/Analog Hybrid Standard" section of the "Digital Data Acquisition and Networks" chapter in your *Lessons In Industrial Instrumentation* textbook.

After closely reading and outlining a text, you should be ready to share the following with your classmates and instructor:

(1) Your written summary of all major points of the text, expressed as simply as possible in your own words. A "Table of Contents" format works well for this.
(2) Active helpful reading strategies (e.g. verbalizing your thoughts as you read, simplifying long sentences, working through mathematical examples, cross-referencing text with illustrations or other text, identifying the author's problem-solving strategies, etc.).
(3) General principles, especially physical laws, referenced in the text.
(4) Questions of your own you would pose to another reader, to challenge their understanding.
(5) Ideas for experiments that could be used to either demonstrate some concept applied in the text, or disprove a related misconception.
(6) Any points of confusion, and precisely why you found the text confusing.

file i04463

Question 23

Read and outline the "HART Multidrop Mode" subsection of the "HART Digital/Analog Hybrid Standard" section of the "Digital Data Acquisition and Networks" chapter in your *Lessons In Industrial Instrumentation* textbook.

After closely reading and outlining a text, you should be ready to share the following with your classmates and instructor:

(1) Your written summary of all major points of the text, expressed as simply as possible in your own words. A "Table of Contents" format works well for this.
(2) Active helpful reading strategies (e.g. verbalizing your thoughts as you read, simplifying long sentences, working through mathematical examples, cross-referencing text with illustrations or other text, identifying the author's problem-solving strategies, etc.).
(3) General principles, especially physical laws, referenced in the text.
(4) Questions of your own you would pose to another reader, to challenge their understanding.
(5) Ideas for experiments that could be used to either demonstrate some concept applied in the text, or disprove a related misconception.
(6) Any points of confusion, and precisely why you found the text confusing.

file i04464

Question 24

Read and outline the "HART Multi-Variable Transmitters and Burst Mode" subsection of the "HART Digital/Analog Hybrid Standard" section of the "Digital Data Acquisition and Networks" chapter in your *Lessons In Industrial Instrumentation* textbook.

After closely reading and outlining a text, you should be ready to share the following with your classmates and instructor:

(1) Your written summary of all major points of the text, expressed as simply as possible in your own words. A "Table of Contents" format works well for this.
(2) Active helpful reading strategies (e.g. verbalizing your thoughts as you read, simplifying long sentences, working through mathematical examples, cross-referencing text with illustrations or other text, identifying the author's problem-solving strategies, etc.).
(3) General principles, especially physical laws, referenced in the text.
(4) Questions of your own you would pose to another reader, to challenge their understanding.
(5) Ideas for experiments that could be used to either demonstrate some concept applied in the text, or disprove a related misconception.
(6) Any points of confusion, and precisely why you found the text confusing.

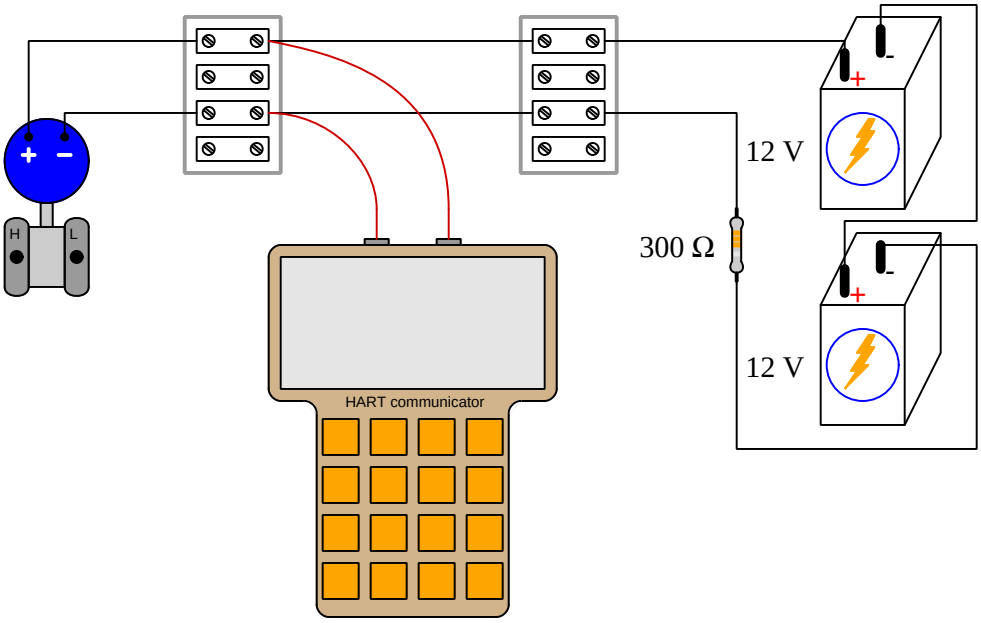
file i04465

Question 25

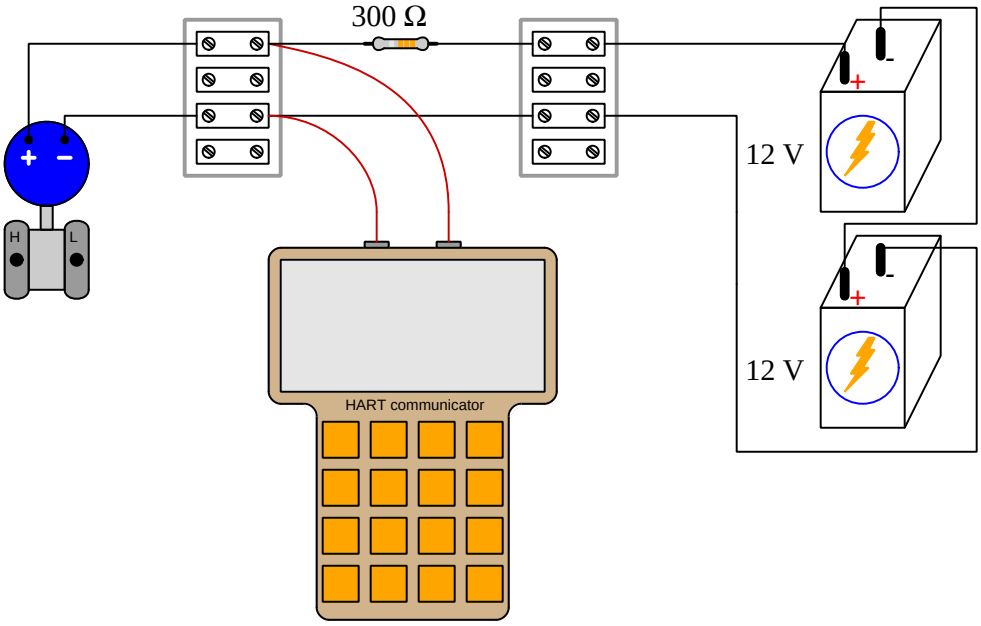
Identify whether or not the HART communicator will be able to communicate with the HART transmitter in each of these circuits, explaining why or why not for each case. Bear in mind the following facts about HART devices:

- HART uses a master/slave arbitration – slave devices only transmit in response to the master's request for information
- HART master devices output AC voltage signals (FSK tones) when transmitting
- HART slave devices output AC current signals (FSK tones) when transmitting
- All HART devices sense AC voltage signals (FSK tones) when receiving

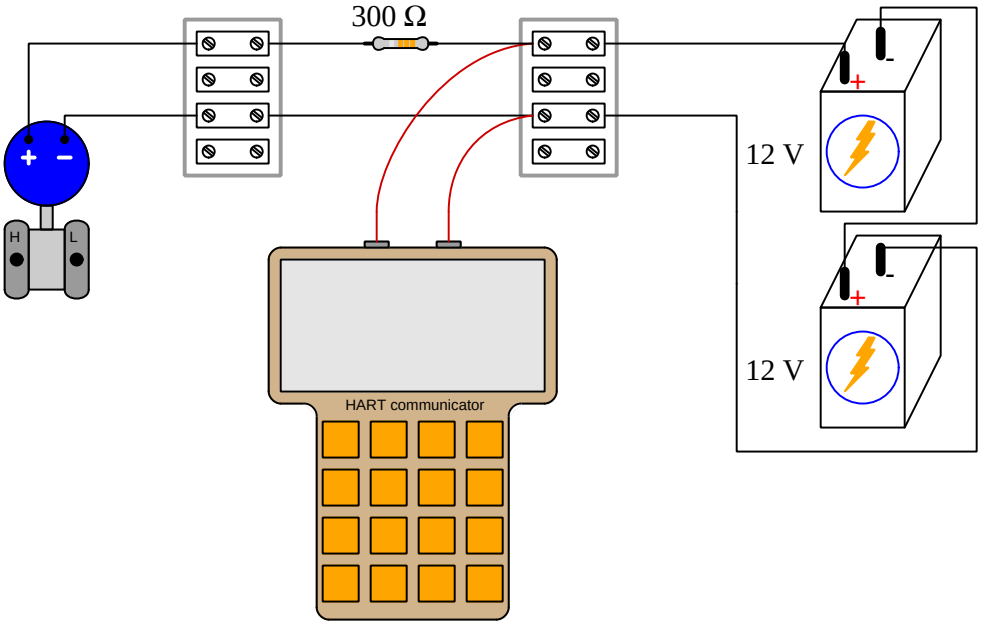
Circuit #1:



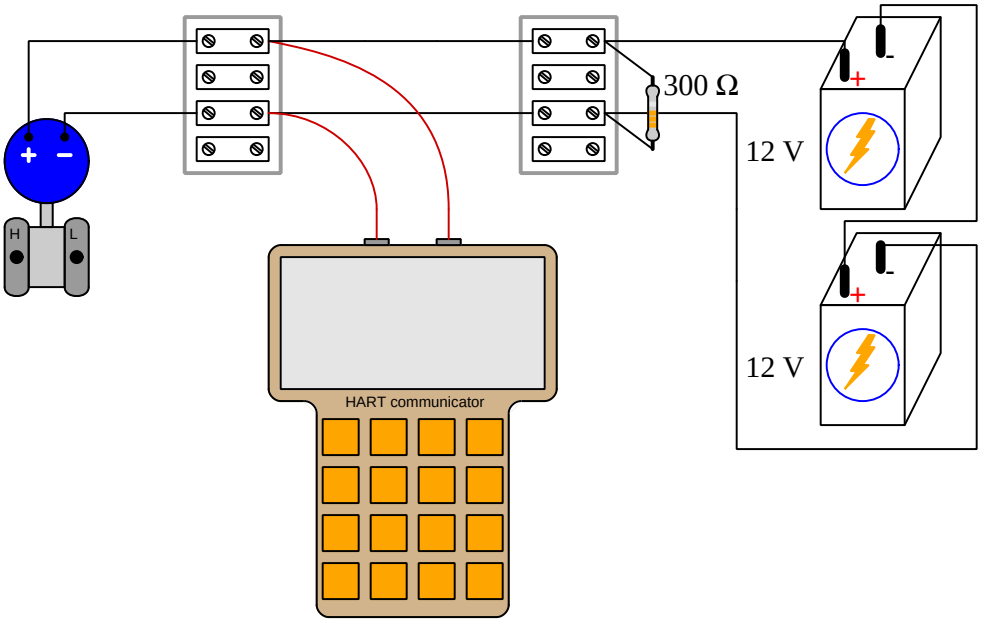
Circuit #2:



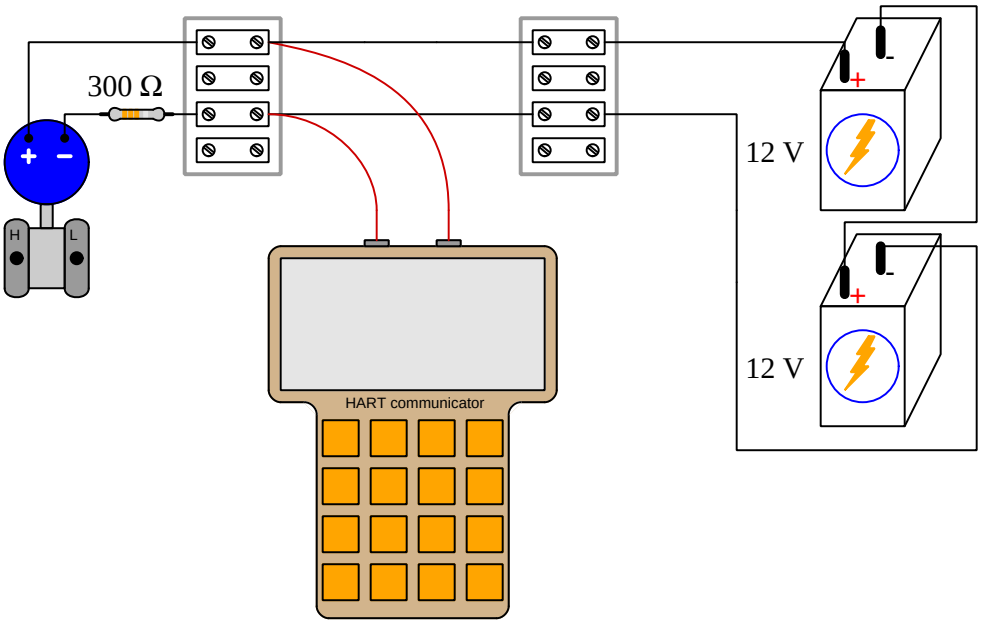
Circuit #3:



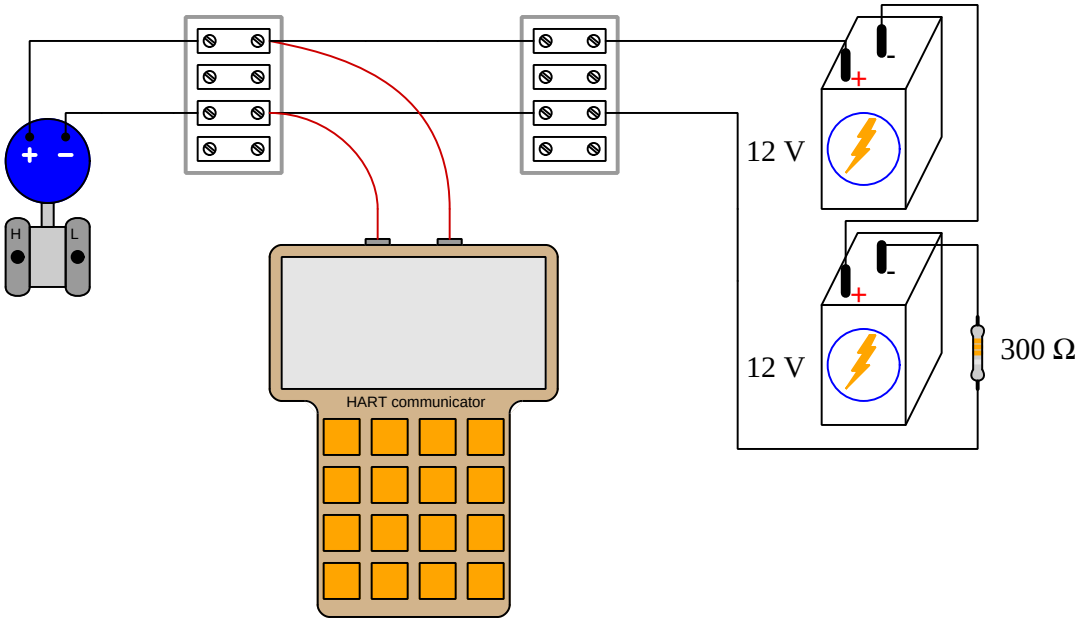
Circuit #4:



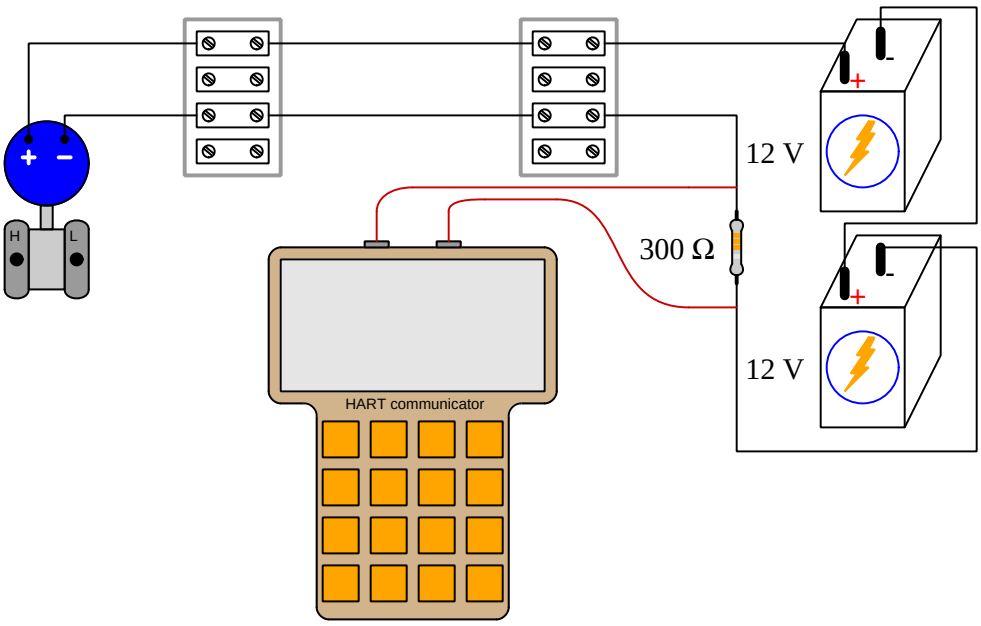
Circuit #5:



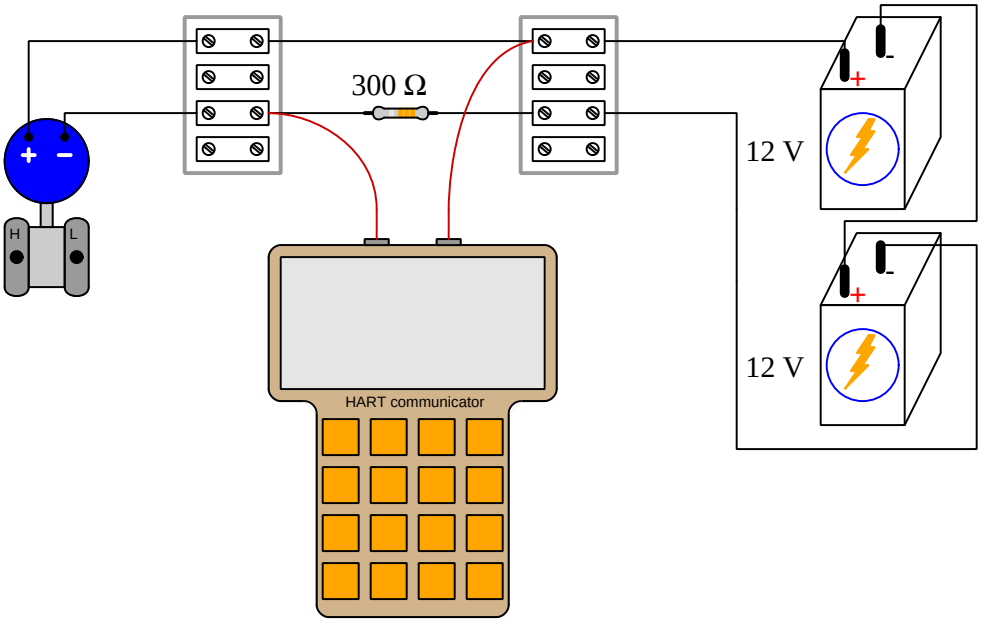
Circuit #6:



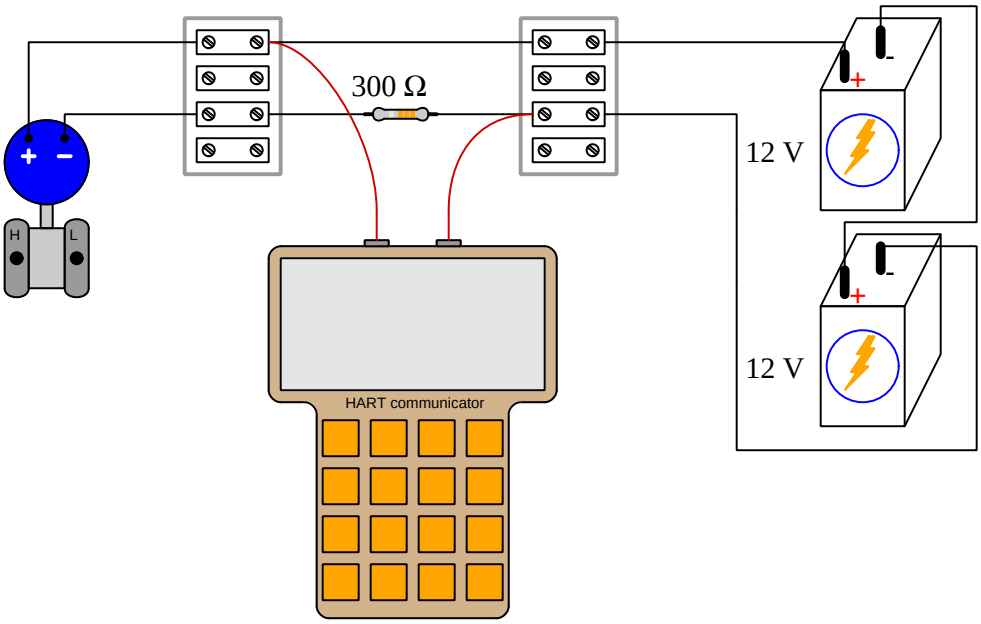
Circuit #7:



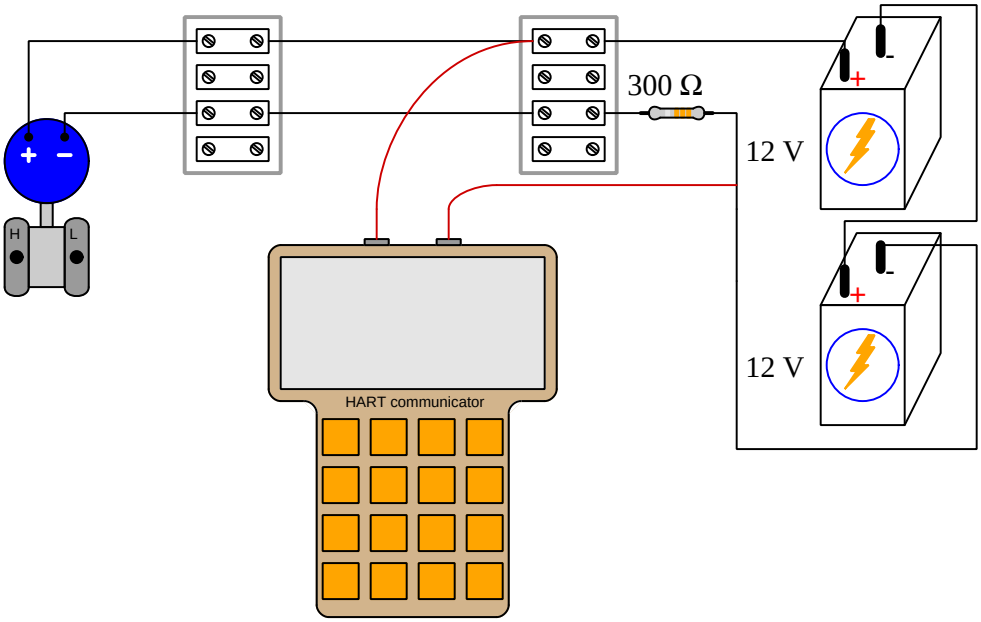
Circuit #8:



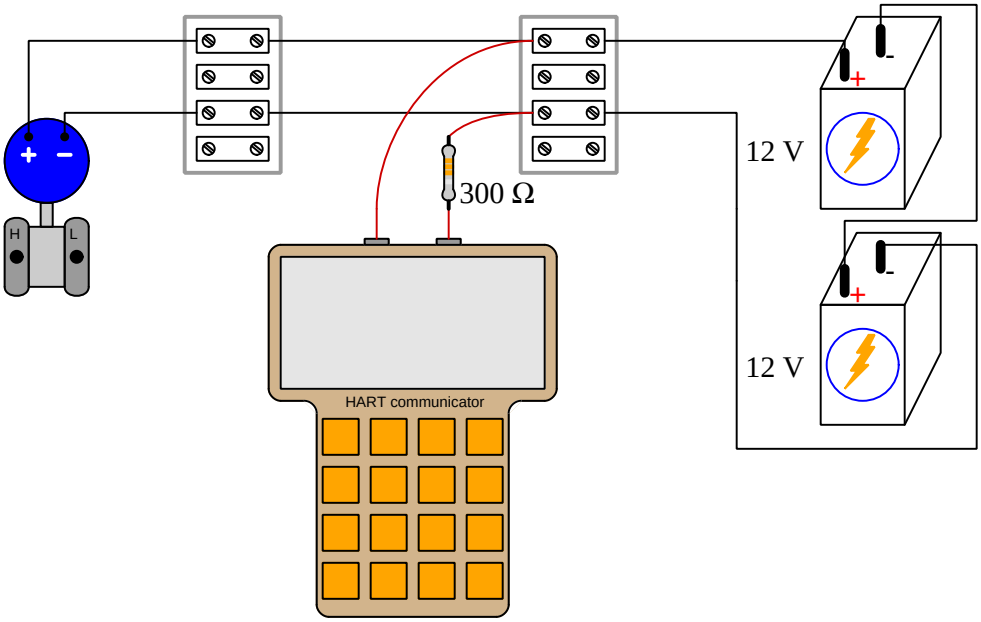
Circuit #9:



Circuit #10:



Circuit #11:



Suggestions for Socratic discussion

- Is the size of the resistor relevant? If the resistor happened to be a different value, would its placement in the circuit matter as much?

  file i03332

Question 26

Read and outline the introduction and the "Modbus Overview" subsection of the "Modbus" section of the "Digital Data Acquisition and Networks" chapter in your *Lessons In Industrial Instrumentation* textbook.

After closely reading and outlining a text, you should be ready to share the following with your classmates and instructor:

(1) Your written summary of all major points of the text, expressed as simply as possible in your own words. A "Table of Contents" format works well for this.
(2) Active helpful reading strategies (e.g. verbalizing your thoughts as you read, simplifying long sentences, working through mathematical examples, cross-referencing text with illustrations or other text, identifying the author's problem-solving strategies, etc.).
(3) General principles, especially physical laws, referenced in the text.
(4) Questions of your own you would pose to another reader, to challenge their understanding.
(5) Ideas for experiments that could be used to either demonstrate some concept applied in the text, or disprove a related misconception.
(6) Any points of confusion, and precisely why you found the text confusing.

file i04467

Question 27

Read the "Modbus Function Codes and Addresses" subsection of the "Modbus" section of the "Digital Data Acquisition and Networks" chapter in your *Lessons In Industrial Instrumentation* textbook.

After closely reading and outlining a text, you should be ready to share the following with your classmates and instructor:

(1) Your written summary of all major points of the text, expressed as simply as possible in your own words. A "Table of Contents" format works well for this.
(2) Active helpful reading strategies (e.g. verbalizing your thoughts as you read, simplifying long sentences, working through mathematical examples, cross-referencing text with illustrations or other text, identifying the author's problem-solving strategies, etc.).
(3) General principles, especially physical laws, referenced in the text.
(4) Questions of your own you would pose to another reader, to challenge their understanding.
(5) Ideas for experiments that could be used to either demonstrate some concept applied in the text, or disprove a related misconception.
(6) Any points of confusion, and precisely why you found the text confusing.

file i04468

Question 28

Read Appendix C of the Allen-Bradley "PowerFlex 4 Adjustable Frequency AC Drive user manual" (document FRN 5.xx), and answer the following questions:

Describe what a VFD (Variable Frequency Drive) is useful for. What, exactly, does it do in a control system?

What does this section have to say about the "+" and "−" wires for Modbus RS-485 devices?

Identify some of the commands for the AC motor drive accessible as individual bits in register 8192.

Identify the register within the AC motor drive holding the frequency "reference" (command) value. This is the numerical value commanding the motor how fast to spin. Is this numerical value specified in integer, fixed-point, or floating-point format?

Suggestions for Socratic discussion

- Based on your reading of this manual, is there any danger in accidently reversing the Modbus (RS-485) wire connections?
- The wiring diagram on page C-1 shows a 120 ohm termination resistor installed at the cable end. Can you think of any application where you might wish to use a different-value termination resistor on this network cable (i.e. something other than 120 Ω)?
- Page 1-9 of this manual describes a "reflected wave problem" that may manifest on long lengths of motor cable between the drive and the motor. Based on the description and the table of figures shown on that page, what does this problem consist of?
- Identify some of the error codes generated by this VFD which may be read via Modbus (held in register 8449).
- The network wiring diagram shown in figure C.1 shows an interesting method of grounding the shield conductor in each cable. Interpret this diagram, and then elaborate on alternative methods of shield grounding which would also work.

file i04469

Question 29

Read pages 4-46 through 5-8 of the Automation Direct "GS1 Series Drives user manual" (document GS1-M), and answer the following questions:

Describe what a VFD (Variable Frequency Drive) is useful for. What, exactly, does it do in a control system?

Identify the purpose of the "FA-ISONET" device referenced on pages 5-6 and 5-7.

Identify some of the status bits readable in register 48450 (2001 hex).

Identify the register within the AC motor drive holding the speed "reference" (command) value. This is the numerical value commanding the motor how fast to spin. Is this numerical value specified in integer, fixed-point, or floating-point format?

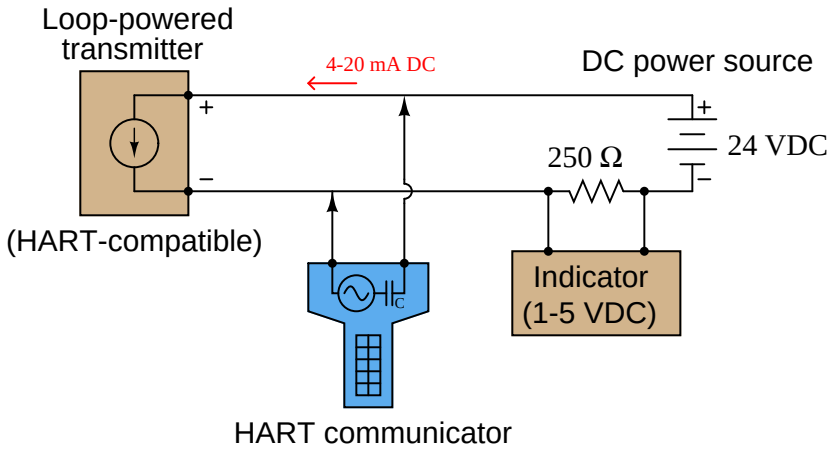
Suggestions for Socratic discussion

- Identify which layer of the OSI model the FA-ISONET device operates on.
- Can the Modbus bit rate of this VFD be arbitrarily set, or is it fixed at one communication speed?
- Identify which register(s) within the VFD you would have to write data into via Modbus in order to command the drive to "Run" and to "Stop".
- Explain the significance of the speed reference value residing in a register address beginning with "4" within the Modbus addressing scheme.

file i04470

Question 30

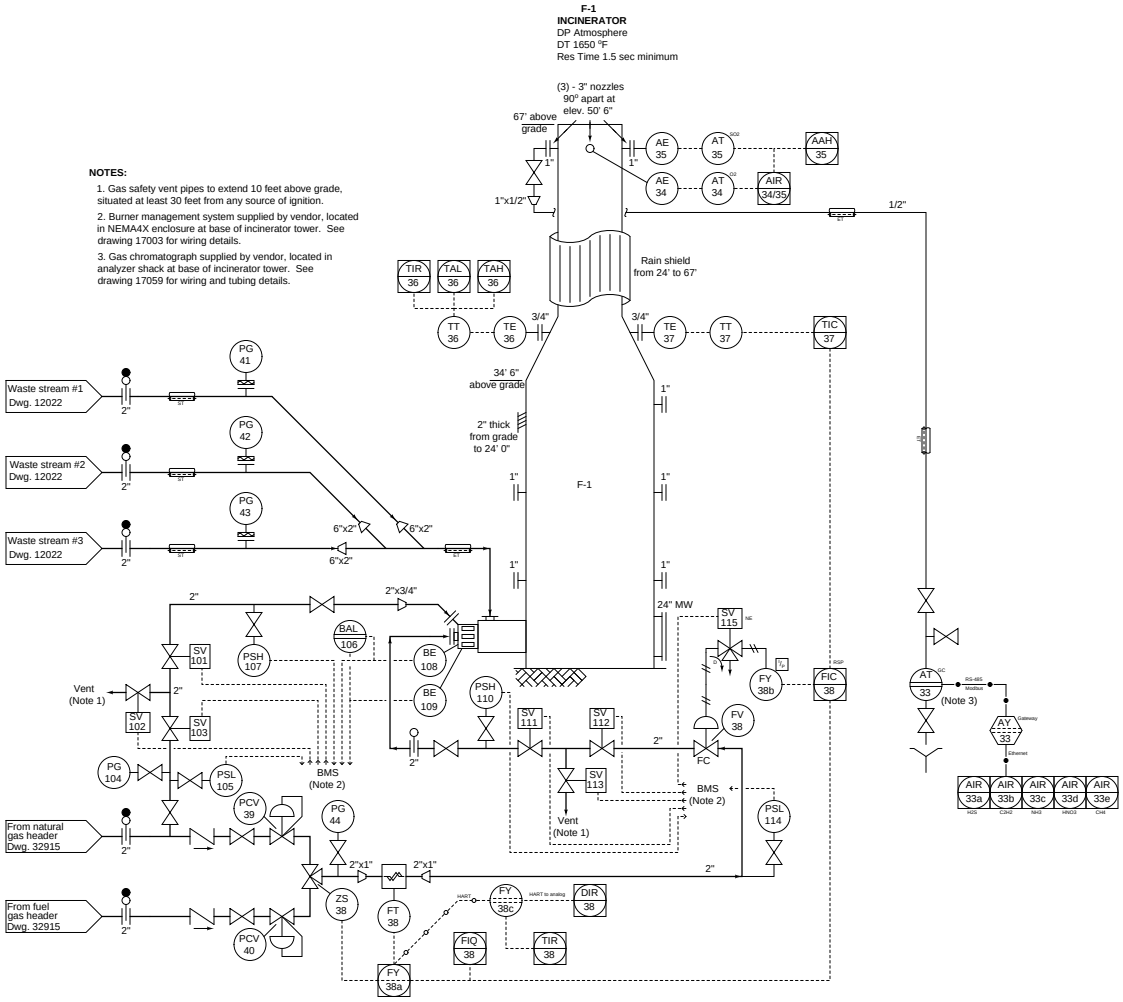
Suppose you were connecting a HART-compliant transmitter to an indicator that was intolerant of the high-frequency HART communication signals. Show where you would place a HART *filter* circuit in this 4-20 mA loop circuit to prevent those high-frequency signals from getting to the indicator, and also what that filter circuit would consist of:



file i01398

Question 31

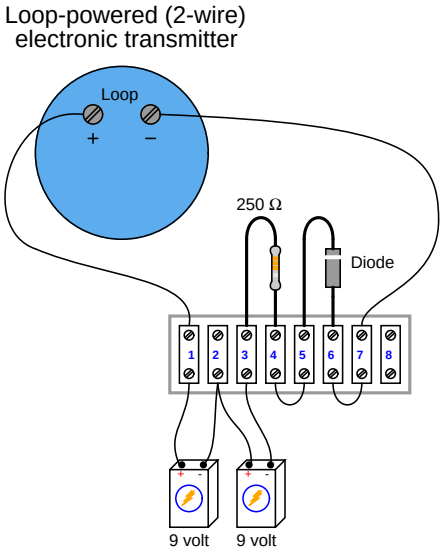
Identify where a HART multivariable transmitter is used in this incinerator process, and how the multiple variables are extracted from it to report on various indicating instruments:



file i01215

Question 32

Connect a "smart" (HART protocol) loop-powered to a DC voltage source, a 250 ohm resistor, and a diode as shown, using parts supplied by the instructor. All electrical connections must be made using a terminal strip (no twisted wires, crimp splices, wire nuts, spring clips, or "alligator" clips permitted):



After building your circuit, answer the following questions:

- Connect a HART communicator device in parallel with the transmitter, turn it on, and use it to access the transmitter's programmable parameters.
- Use a multimeter set to measure *AC* volts to detect HART communications in the circuit. What happens to the AC voltage measurement when the HART communicator is turned off? Is there any way to capture the peak HART signal values using your multimeter?
- Temporarily short past the resistor with a jumper wire and note whether or not this has any effect on the 4-20 mA analog current signal. Also note whether this elimination of the resistor has any effect on the ability of the transmitter to communicate using HART (digital) signals.

Suggestions for Socratic discussion

- It is possible to properly connect a HART communicator to a HART instrument and still not have it "talk." The communicator must also be programmed with a *Device Description* (DD) for the HART instrument in order to communicate and access all its parameters. Explain they purpose and rationale for Device Descriptions.

  file i03878

Question 33

Question 34

Question 35

Question 36

Question 37

Question 38

Question 39

Question 40

Question 41

Read and the "Lexicon of Cyber-Security Terms" section of the "Instrumentation Cyber-Security" chapter in your *Lessons In Industrial Instrumentation* textbook and answer the following questions:

- Explain the difference between a *LAN* and a *WAN*, giving practical examples of each.
- Describe the difference between an *active* attack and a *passive* attack.
- Explain what a "man in the middle" attack is, and give one practical example relevant to the field of instrumentation and control.
- Describe what a *denial of service* attack is.
- Three types of attacks related to passwords are described here: *password sniffing*, *dictionary attacks*, and *brute-force attacks*. Explain what these terms mean, and why an attacker might be inclined to use them.
- What is a "key" as it applies to the subject of *cryptography*?

Suggestions for Socratic discussion

- Formulate an analogy to explain common cyber-attacks using the US Postal Service as the "system," mail as the "data" communicated by the system, and postal customers as "users" of the system.
- What does it mean if a particular communications protocol exchanges passwords "in the clear" (sometimes referred to as *cleartext*), and why might this be a problem for network security?
- Identify ways to make passwords more resistant against dictionary-style attacks.

file i02720

Question 42

Read and outline the "Air Gaps" subsection of the "Design-Based Fortifications" section of the "Instrumentation Cyber-Security" chapter in your *Lessons In Industrial Instrumentation* textbook.

After closely reading and outlining a text, you should be ready to share the following with your classmates and instructor:

(1) Your written summary of all major points of the text, expressed as simply as possible in your own words. A "Table of Contents" format works well for this.
(2) Active helpful reading strategies (e.g. verbalizing your thoughts as you read, simplifying long sentences, working through mathematical examples, cross-referencing text with illustrations or other text, identifying the author's problem-solving strategies, etc.).
(3) General principles, especially physical laws, referenced in the text.
(4) Questions of your own you would pose to another reader, to challenge their understanding.
(5) Ideas for experiments that could be used to either demonstrate some concept applied in the text, or disprove a related misconception.
(6) Any points of confusion, and precisely why you found the text confusing.

file i02721

Question 43

Read and outline the "Firewalls" subsection of the "Design-Based Fortifications" section of the "Instrumentation Cyber-Security" chapter in your *Lessons In Industrial Instrumentation* textbook.

After closely reading and outlining a text, you should be ready to share the following with your classmates and instructor:

(1) Your written summary of all major points of the text, expressed as simply as possible in your own words. A "Table of Contents" format works well for this.
(2) Active helpful reading strategies (e.g. verbalizing your thoughts as you read, simplifying long sentences, working through mathematical examples, cross-referencing text with illustrations or other text, identifying the author's problem-solving strategies, etc.).
(3) General principles, especially physical laws, referenced in the text.
(4) Questions of your own you would pose to another reader, to challenge their understanding.
(5) Ideas for experiments that could be used to either demonstrate some concept applied in the text, or disprove a related misconception.
(6) Any points of confusion, and precisely why you found the text confusing.

file i02723

Question 44

Read the "Malicious Intrusion Threats" and "Defending Your Assets With Virtual Private Networking" sections of the "Securing SEL Ethernet Products With VPN Technology" Application Guide published by Schweitzer Engineering Laboratories (document AG2002-05) and answer the following questions:

Identify some vulnerabilities related to *passwords* used to authenticate access to computer systems.

Explain what a *network sniffer* can do, and how one might be used by a malicious party to infiltrate an industrial computer system.

Explain in your own words how Virtual Private Network (VPN) technology works with standard Internet Protocol (IP) to safeguard data communications over unsecure networks such as the Internet.

An essential component to a VPN is a *shared key*. Explain what this key is, and how it works to ensure security of the VPN.

Suggestions for Socratic discussion

- In the electric power industry, "smart" monitoring and control devices are often referred to as *IED*s (Intelligent Electronic Devices). For those who have studied protective relaying or other forms of electric power system instrumentation, identify some specific examples of IEDs, and also why a malicious party might wish to compromise one or more of them.
- What does it mean if a particular communications protocol exchanges passwords "in the clear" (sometimes referred to as *cleartext* or *plaintext*), and why might this be a problem for network security?
- Explain in detail what "tunneling" is in a digital network.
- Explain in detail how "keys" are handled between VPN devices to ensure security.
- Explain in detail how VPN works with IP (Internet Protocol) packets to provide security.
- Does VPN provide *confidentiality*, *integrity*, and/or *authentication*? Explain in detail.

file i00674

Question 45

Read selected portions of the "A View Through the Hacker's Looking Glass" paper written by Garrett Leischner and David Whitehead of Schweitzer Engineering Laboratories (document TP6237-01, April 2006) and answer the following questions:

In this paper, three different hypothetical attacks are described both from the attacker's perspective and the victim's perspective. For each of these three attacks, describe the *motive* behind each and the system *vulnerabilities* that were exploited.

Which of these attacks were *passive* and which were *active* in nature? Explain your reasoning in detail.

Summarize in your own words some of the simple measures any organization can take to better secure its digital systems.

Suggestions for Socratic discussion

- Describe some of the practical tips listed in this document for creating and remembering "strong" passwords. How do you think the "strength" of a password might be calculated?
- If the reference to a *red stapler* is not familiar to you, I will give you a new homework assignment: watch Mike Judge's hilarious comedy *Office Space*. This movie actually shows the kind of damage disgruntled technical workers can wreak, as well as lampoons some really bad (but all-too-common) management philosophies.

file i00959

Question 46

A very good place to start exploring computer security is with your own personal computer. Regardless of manufacturer or operating system, your own personal computer has vulnerabilities and protections related to data security. Here we will explore some of them.

How secure (i.e. difficult to guess) is your password? When you must change your password, how do you choose and remember a new one?

When you typically log into your computer, how much privilege do you have as a user on the operating system? All modern operating systems have the ability to grant different levels of read and write and execute access to different users depending on how those user accounts are set up. The most privileged level of access is often called "Administrator" (or "root" in Unix-based operating systems) in which that user is allowed to do anything at all, which is convenient when doing tasks such as installing new software, but represents a vulnerability in that any malicious access made under that user session enjoys the same unrestricted power (to do harm). Inspect the user accounts on your computer's operating system, and identify the level of privilege you typically use when logged on.

How does the anti-virus software work on your computer? That is, how does this software recognize threats and protect you against them?

Explain the difference between anti-virus software and firewall software.

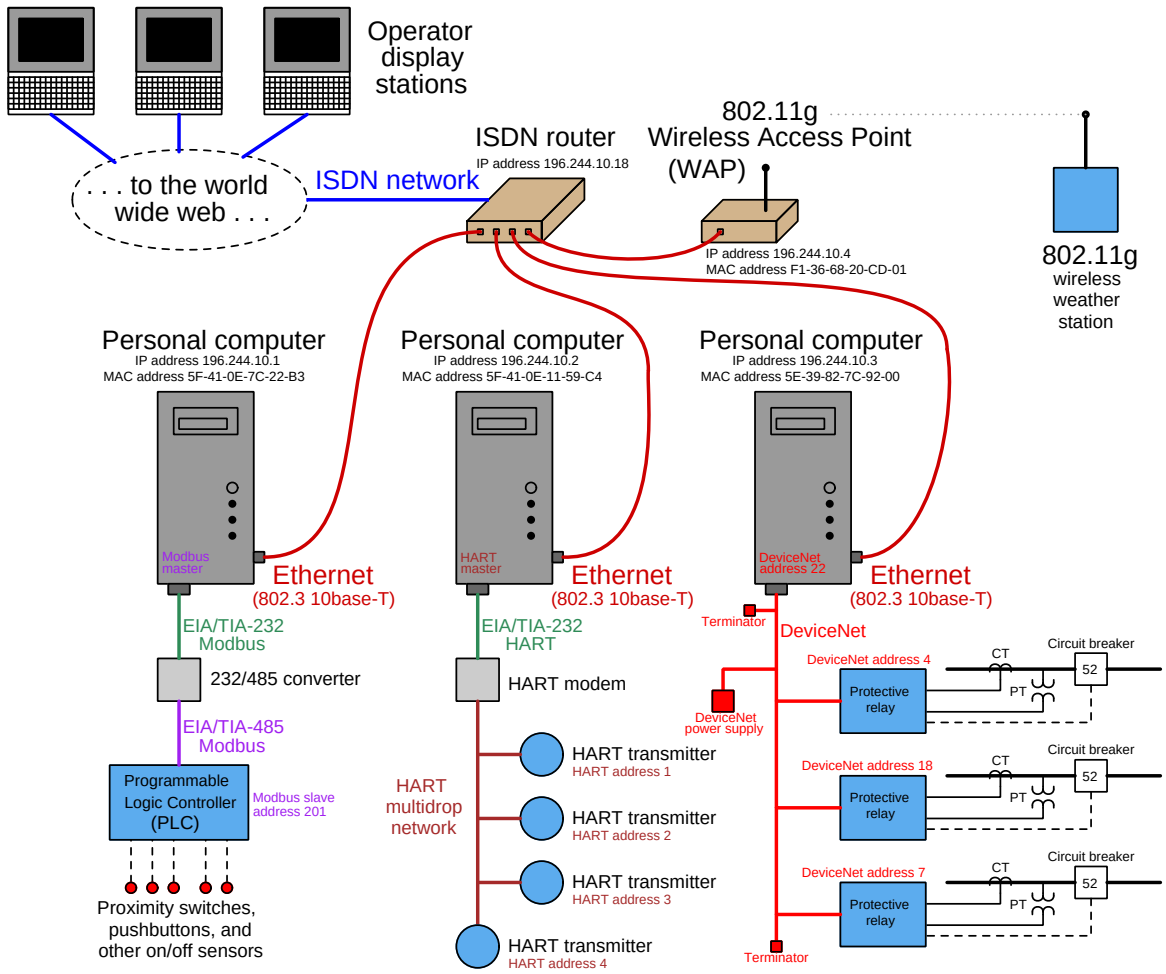
Identify how to disable your computer's wireless network access, and explain why that might be a good policy in certain situations.

Do you store personally important files on your computer, such as financial or legal records? If so, is that entirely necessary? Identify ways to maintain the security of those critical files if they need to be maintained in digital form.

file i02494

Question 47

Examine this illustration of an industrial computer system to identify any potential security vulnerabilities, and then recommend ways to fortify it from attack:



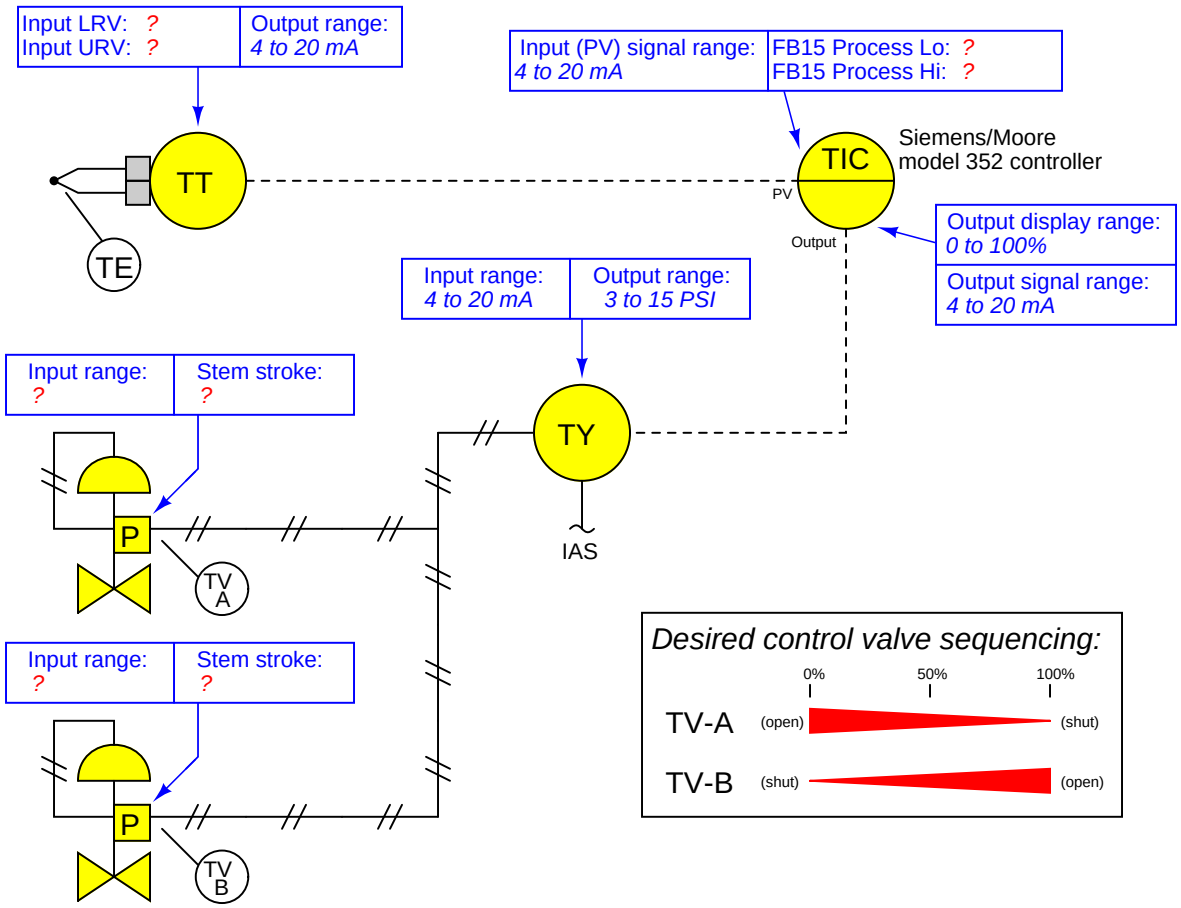
Suggestions for Socratic discussion

- Do you see any application for a *firewall* in this system? If so, where should that firewall be located?
- Do you see any application for a *VPN* in this system? If so, how should that VPN be implemented?
- A good strategy for formulating any security policy is to first identify all functions provided by the system, then identify all authorized users of the system, delineate which users get to access which functions, decide on security techniques for limiting access accordingly, and finally forbid all other uses of the system. Apply this strategy to the analysis of the system shown, and try to either identify those elements or formulate questions you would ask of the system's owner to identify those elements.

file i02454

Question 48

Suppose you are asked to configure the instruments in this temperature control loop to sense and display process temperature over a range of 200 to 1800 degrees Celsius, with the loop controller actuating two split-ranged control valves in a complementary sequence:



Write the proper range values inside the boxes near each instrument, showing the proper configuration for each instrument needed to achieve the desired result.

Suggestions for Socratic discussion

- Suppose the controller displayed a temperature of 1246 when the actual process temperature was 1265 ^{o}C. First, identify *two* possible locations in this loop for a calibration error that would account for this discrepancy. Then, assuming only one fault, explain how you could positively determine the location of this calibration error with a single diagnostic test.
- Suppose valve TV-A was 44% open and TV-B was 56% open when the controller output displayed 52%. First, identify *two* possible locations in this loop for a calibration error that would account for this discrepancy. Then, assuming only one fault, explain how you could positively determine the location of this calibration error with a single diagnostic test.

file i02078

Question 49

Read section 2 of the "Firewall and Proxy Server HOWTO for Linux" document written by Mark Grennan, and answer the following questions:

In your own words, describe what a *firewall* is with regard to computers.

Describe the author's advice for creating a *security policy* for any computer system.

This document describes two different kinds of firewalls: *filtering* firewalls and *proxy server* firewalls. Describe in your own words the differences between each firewall type.

Suggestions for Socratic discussion

- Explain what a "private LAN" is, and describe a practical example of one if you can.

file i03579

Question 50

Read selected portions of the "Guidelines for Writing RFC Text on Security Considerations" best practices paper (published by The Internet Society as `RFC 3552`) and answer the following questions:

Explain the difference between what this paper defines as an *active* attack versus a *passive* attack.

This paper describes one special form of active attack called *man-in-the-middle*. Explain how this sort of attack works, and give one practical example relevant to the field of instrumentation and control.

Two types of attacks related to passwords are described in this paper: *password sniffing* and *dictionary attacks*. Explain what these terms mean, and why an attacker might be inclined to use either of them.

Suggestions for Socratic discussion

- What does it mean if a particular communications protocol exchanges passwords "in the clear" (sometimes referred to as *cleartext*), and why might this be a problem for network security?
- Identify ways to make passwords more resistant against dictionary-style attacks.

file i00914

Question 51

Read selected sections of the "Guidelines on Firewalls and Firewall Policy" document written by Karen Scarfone and Paul Hoffman (NIST Special Publication 800-41, Revision 1), and answer the following questions:

Read the "Overview of Firewall Technologies" introduction and then explain in your own words what a *firewall* does to make a network more secure, and the methods by which it accomplishes this task.

Differentiate between these different firewall functions: *packet filtering*, *stateful inspection*, and *stateful protocol analysis* (otherwise known as *deep packet inspection*).

Suggestions for Socratic discussion

- Describe a scenario in which a data packet would get rejected by each type of firewall action described in this document.
- Explain what "packet fragmentation" refers to, and why a firewall programmed to exclude fragmented packets can actually cause certain security problems with Virtual Private Networking.
- What does a *proxy server* do, and how is this related to firewalls?

file i03323

Question 52

Question 53

Question 54

Question 55

Question 56

Question 57

Question 58

Question 59

Question 60

Question 61

Read and outline the "Demilitarized Zones" subsection of the "Design-Based Fortifications" section of the "Instrumentation Cyber-Security" chapter in your *Lessons In Industrial Instrumentation* textbook.

After closely reading and outlining a text, you should be ready to share the following with your classmates and instructor:

(1) Your written summary of all major points of the text, expressed as simply as possible in your own words. A "Table of Contents" format works well for this.
(2) Active helpful reading strategies (e.g. verbalizing your thoughts as you read, simplifying long sentences, working through mathematical examples, cross-referencing text with illustrations or other text, identifying the author's problem-solving strategies, etc.).
(3) General principles, especially physical laws, referenced in the text.
(4) Questions of your own you would pose to another reader, to challenge their understanding.
(5) Ideas for experiments that could be used to either demonstrate some concept applied in the text, or disprove a related misconception.
(6) Any points of confusion, and precisely why you found the text confusing.

file i02724

Question 62

Read selected portions of the "SEL-3610 Port Server, SEL-3620 Ethernet Security Gateway, and SEL-3622 Security Gateway" Instruction Manual published by Schweitzer Engineering Laboratories (document SEL-3610/SEL-3620/SEL-3622) and answer the following questions:

Both the SEL-3620 and SEL-3622 are modern network security devices intended for use on Ethernet-based data networks. Describe the three major digital data security features ("services") common to both of these devices.

The "security posture" of these devices when functioning as firewalls is *deny-by-default*. Explain what this phrase means, and why it is beneficial from a security perspective.

Examine the three firewall rules shown in Figure 6.1 (found on page 6.2) and explain what each of them does.

Note the IP addresses shown in the firewall rule list in Figure 6.1 (page 6.2), how each one is followed by a forward slash symbol and an integer number. What exactly does this number represent, and why is it significant in one of the rules that its value is 32?

Suppose the firewall were configured with two contradicting rules. Explain what would happen, and why this is.

The three possible actions this firewall may take in following a rule are: *Drop*, *Accept*, and *Reject*. Explain what each of these actions does.

file i02194

Question 63

Read the whitepaper entitled "Understanding Deep Packet Inspection (DPI) for SCADA Security" by Eric Byres of Tofino Security (document WP_INDS_TOF_514_A_AG) and answer the following questions.

Explain what criteria are typically used by a firewall to filter data in a communications network. Note: each rule for allowing data through a firewall is called an *Access Control List*, or *ACL*.

Explain why traditional IT (Information Technology) firewall rules are insufficient to protect against malicious packets from reaching control system hardware.

Explain what *DPI* is and how it provides better security for industrial protocols than a simple firewall.

Suggestions for Socratic discussion

- Figure 1 in this whitepaper shows "frame" diagrams of typical packets intercepted by a firewall. Examine these diagrams and explain how they reveal the layered nature of the OSI communication model.
- Traditional firewalls are fairly generic within the IT world, but DPI firewalls cannot be. Explain why a DPI firewall must be specifically configured for the control system it's intended to protect.

file i02217

Question 64

A Deep Packet Inspection (DPI) industrial firewall called the "Xenon" is manufactured by Tofino Security. Read portions of the *Tofino*^{TM} *Xenon Security Appliance* datasheet and explain how this firewall device "knows" how to filter specific message types in specific industrial data formats such as Modbus and OPC.

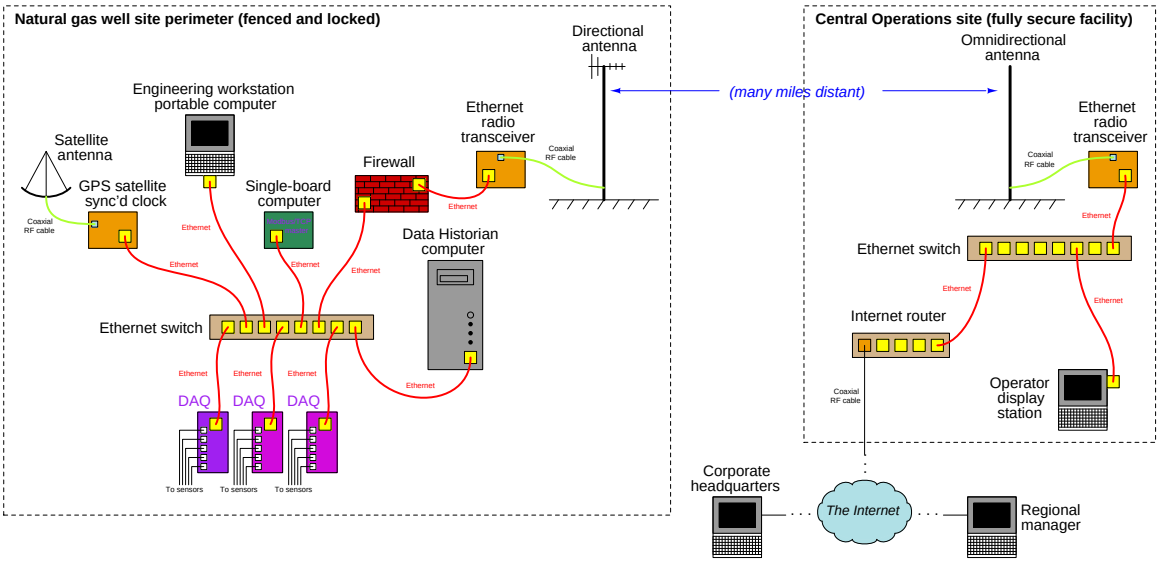
Suggestions for Socratic discussion

- Describe the difference between a traditional firewall and a DPI firewall, in terms of OSI layers.

file i02705

Question 65

The following diagram shows the components of a SCADA (Supervisory Control And Data Acquisition) system, used to collect process data from a remote natural gas well, archive that data over time, and make that archived data available to personnel at both a centralized operations site as well as to corporate and regional headquarters via the internet.



Basic system operation is as follows: the DAQ units receive analog and discrete inputs from a variety of sensors on the natural gas wellhead. The single-board computer uses Modbus/TCP to poll these DAQ units and read their input states, assigning tag names to all data, scaling the data (where applicable) to engineering units from the raw signal voltages (e.g. a 3 volt analog input signal becomes 450 PSI of gas pressure), and time-stamping each signal with a time value polled from the GPS clock (also via Modbus/TCP). A portable Engineering Workstation computer is used to edit and update software in the single-board computer as necessary, as well as perform diagnostic tests on the system. The Data Historian computer periodically reads the single-board computer's collated process data using SFTP (Secure File Transfer Protocol) and archives it in a database holding records for up to several years. Any other operations computer connected to this system (e.g. the Operator Display Station at the Central site, the Regional Manager's computer, Corporate Headquarters) has access to this archived data by reading database files off of the Historian computer.

Multiple natural gas wells are interconnected in the same way to the centralized operations site – the diagram only shows one gas well's communication network for simplicity.

Identify as many potential cyber-vulnerabilities evident in this system diagram as you can, explaining how hackers might gain unauthorized access to critical system functions.

Modify this system to include a DMZ for added security. Be as specific as you can in your modifications.

Suggest alterations (other than a DMZ) which could enhance the cyber-security of this SCADA system.

file i02191

Question 66

Explore the *firewall* settings on your personal computer, and identify some of the restrictions already set in it, as well as further restrictions you could set if you wished.

Suppose you will be using a laptop computer to perform maintenance work on a SCADA system, for example using the computer to make edit configuration settings in the SCADA controller. Will configuring that laptop computer's firewall to only allow these kinds of messages make the SCADA system more secure? Explain why or why not.

file i00661

Question 67

Read section 3 ("Techniques and Technologies for Defending High-Risk Network Links) of the "Defending Risky Electronic Access Points into a 'Closed' Industrial Control System (ICS) Network Perimeter" paper published by National Security Agency, and answer the following questions:

This paper frequently references *LAN* and *WAN*. What, exactly, do these two terms mean? If possible, relate them to networks you are working with in the lab.

This section of the paper describes three security measures applicable to many common digital data networks. Identify each of the three suggested actions, and explain the purpose of each.

Explain in detail what a *DMZ* is, and how it differs from the use of a single *firewall* in a network system.

Another term used within this paper is that of a *stateful firewall*. The word "stateful" refers to the firewall device keeping track of the state of communication between two or more devices. For example, a stateful firewall will only allow communication that is solicited (e.g. a web server responding to a query from a web browser). Explain how a stateful firewall provides an extra measure of security compared to a stateless firewall.

Suggestions for Socratic discussion

- Identify a way in which a hacker might be able to defeat a DMZ set up between an enterprise network and a control system network.
- This document makes mention of *proxy servers*. Discuss what a "proxy" is in the computer networking sense of the word, and how this relates to network security.

file i03111

Question 68

Question 69

Question 70

Question 71

Question 72

Question 73

Question 74

Question 75

Question 76

Question 77

Question 78

Question 79

Question 80

Question 81

Describe your recent learning experiences succinctly enough to be included as a line-item in your résumé. Identify how this learning has made you more marketable in this career field. Be as specific as you can, and feel free to include non-technical as well as technical learning in your description (e.g. project management, organization, independent research, troubleshooting, design, software applications, electric circuit analysis, control theory, etc.)!

Identify any knowledge and/or skill areas in which you would like to become stronger, and describe practical steps you can take to achieve that goal. Don't limit yourself to just technical knowledge and skills, but consider behavioral habits (e.g. patience, attention to detail, time management) and general academic abilities (e.g. reading, writing, mathematics) as well. If you find yourself struggling to achieve a goal, don't just say "I'll work harder" as your plan of action – identify something *different* you can do to achieve that goal.

Note: your responses to these questions will not be shared in Socratic discussion with classmates without your consent. Feel free to maintain these as private notes between yourself and your instructor.

A helpful guide to traits and skills valued by employers are the "General Values, Expectations, and Standards" pages near the beginning of this worksheet. Another is the "So You Want To Be An Instrument Technician?" career guide.

file i00999

Question 82

Read the "Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies" report written by David Whitehead, Kevin Owens, Dennis Gammel, and Jess Smith of Schweitzer Engineering Laboratories (document TP6774-01, October 2016) and answer the following questions:

How did hackers (a.k.a. "malicious actors") gain *initial* access into the computer systems of the Ukrainian power system?

Describe simple steps that could have been taken to foil this initial phase of the attack.

How much advance planning did the hackers engage in prior to the attack?

Explain what a *VPN* is, and how hackers were able to establish one into the network of the electrical utility.

Once full access was gained to the computer systems, what exactly did the hackers do to create a power outage?

After the hackers had created power outages, what additional steps did they take to interfere with the restoration of power?

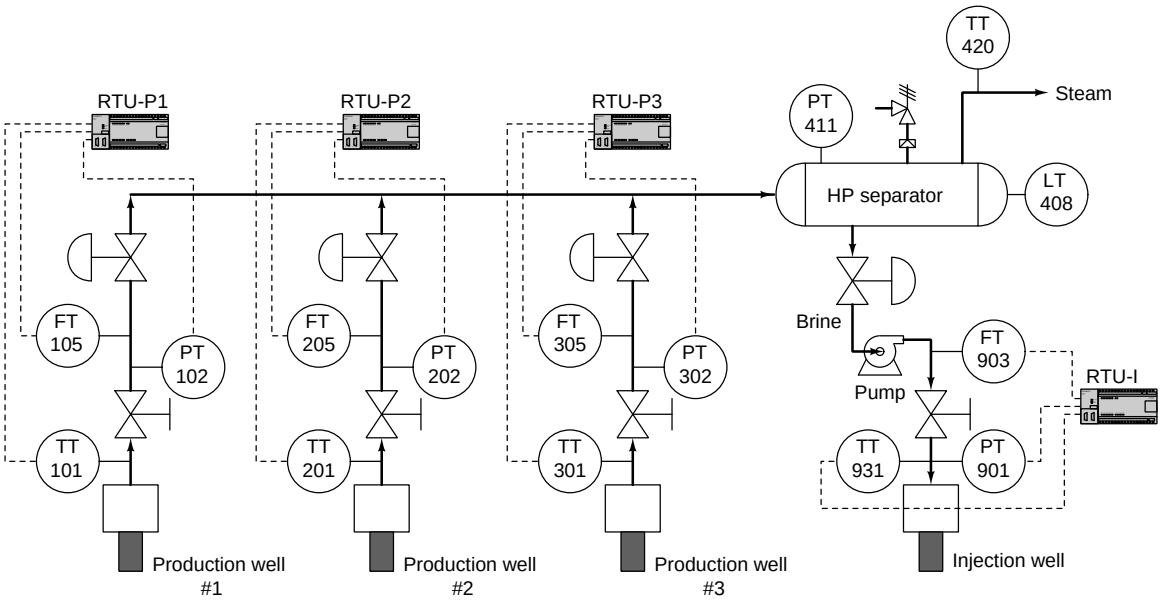
Suggestions for Socratic discussion

- One of the vulnerabilities of the utility computer networks is that they lacked *multi-factor authentication*. What does this phrase mean, and how would its implementation have made this attack more difficult to implement?

file i04466

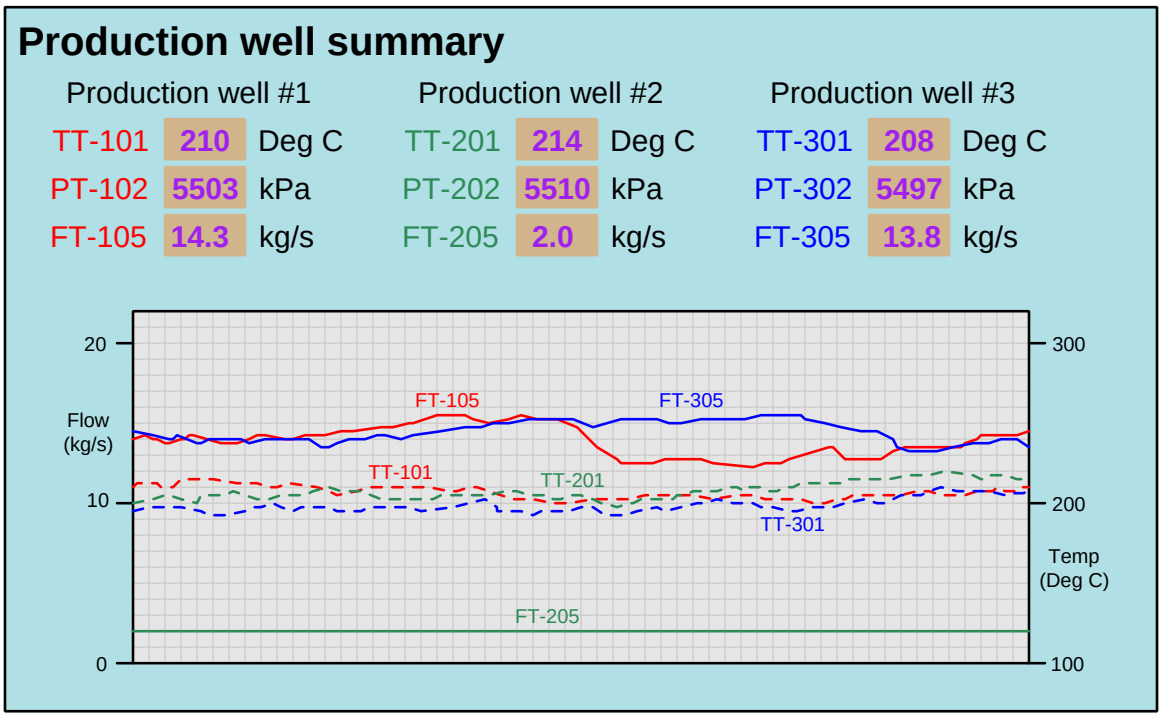
Question 83

Geothermal power plants rely on multiple "production wells" drilled deep into the earth to extract hot, pressurized water which is then flashed into steam and used to drive steam turbine engines to generate electricity. The following PFD shows three production wells extracting fluid and one injection well returning water back into the earth to be re-heated. The rest of the geothermal power plant piping is not shown in this diagram for simplicity's sake:



The SCADA system at this power plant uses Siemens brand Remote Terminal Units (RTUs) to collect data at each wellhead. These units communicate over fiber-optic cables to computers located inside the main control room where human operators monitor and control the process.

The SCADA system monitoring the wells is giving some strange indications, as evidenced by the HMI (Human-Machine Interface) graphic display inside the operator control room:



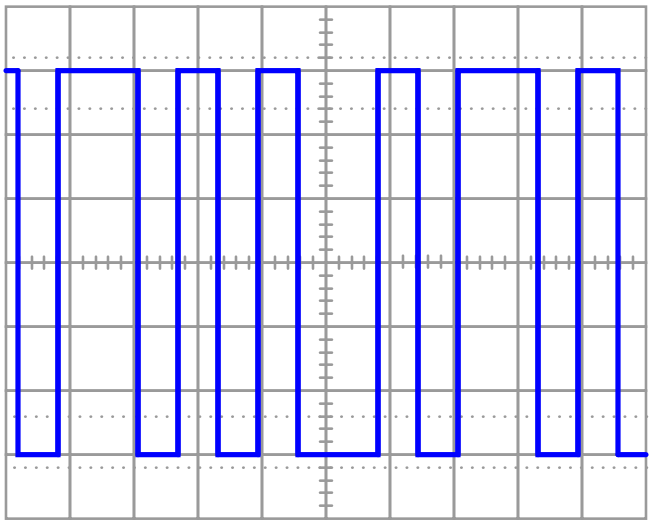
Determine the nature and location of the fault as best you can. If there are multiple possible problems, list them and then identify diagnostic tests you could use to eliminate possibilities from that list.

file i01187

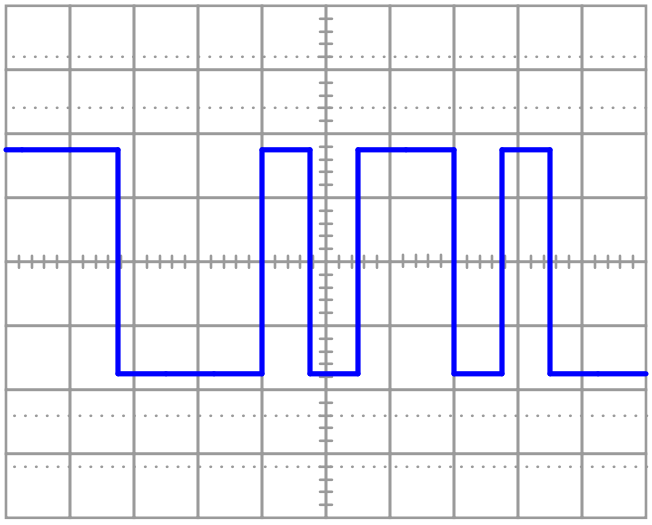
Question 84

Decode the following serial data streams, each one encoded using a different method:

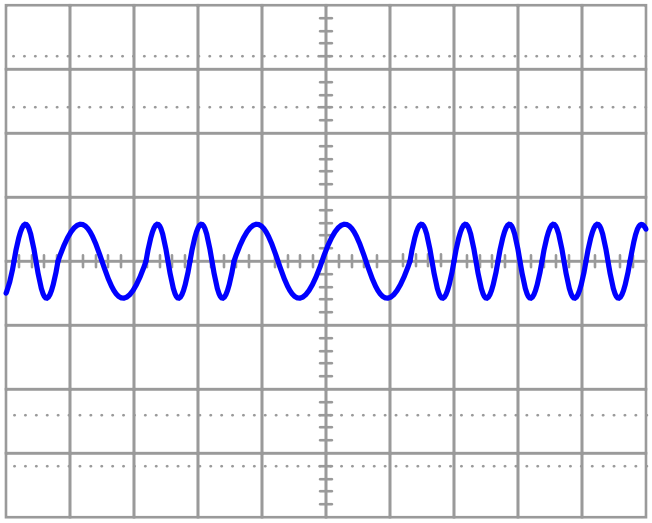
(Manchester encoding)



(NRZ encoding)



(FSK encoding)



Suggestions for Socratic discussion

- Students often experience confusion interpreting data streams when viewed like this, especially Manchester-encoded data. One problem-solving strategy that works well to help interpret waveform patterns is to *work the problem backwards*. Start with a known data stream (binary 1's and 0's) and then sketch a waveform representing that data stream. Do this for several different data streams, experimenting with different pattern combinations of 1's and 0's (repeating bits versus alternating bits, etc.), and then examine the waveforms you sketched to see what general principles you might apply to reliably interpret any data stream encoded in that manner.
- A necessity for proper interpretation of NRZ datastreams is proper measurement of pulse width. Suggest a way to do this when the pulse don't evenly line up with divisions on the oscilloscope screen.
- Explain how these three different encoding methods provide an excellent contrast between *bit rate* and *baud*. Which form of encoding has the greatest bits/second to baud ratio? Which form of encoding has the least bits/second to baud ratio?

file i00883

Question 85

Here is an oscilloscope's view of an eight-bit data stream sent asynchronously with no parity bit, using *NRZ* (Non-Return to Zero) encoding:

Identify the binary data represented by this waveform.

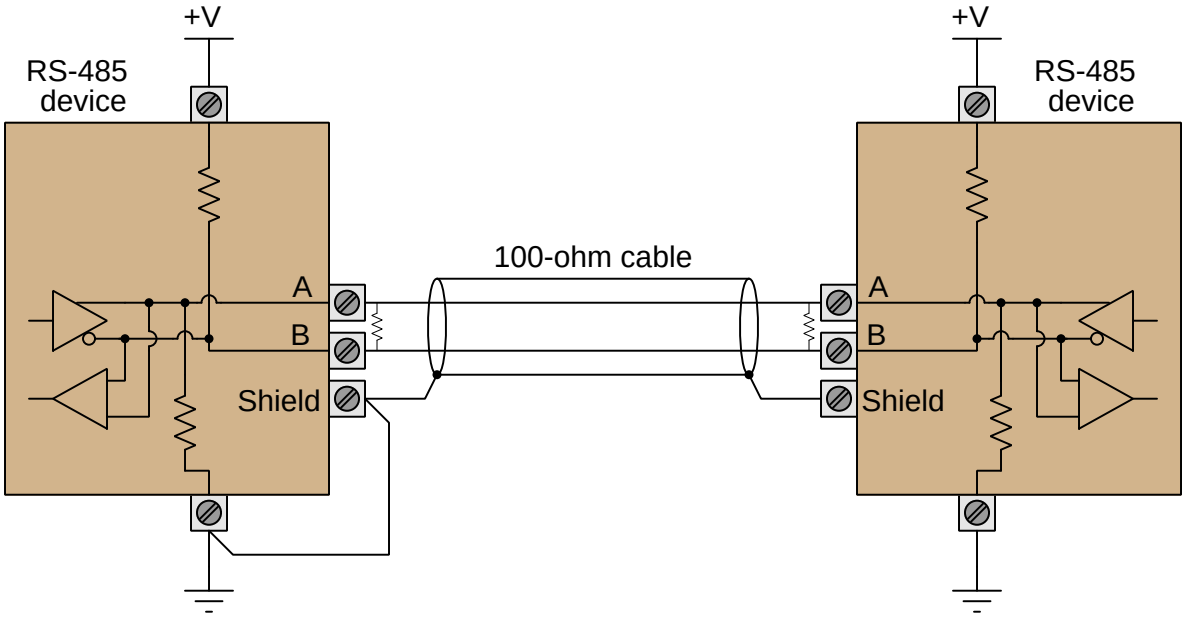
Suggestions for Socratic discussion

- Explain why it is absolutely vital to know the data frame contains eight data bits and no parity, when interpreting this waveform.
- Describe a practical method for determining the width of each bit in this waveform.
- Re-draw this NRZ waveform assuming it was sent with an "odd" parity bit.
- Re-draw this NRZ waveform assuming it was sent with an "even" parity bit.

file i02369

Question 86

Terminating resistors are not always necessary in EIA/TIA-485 networks, but when they are it is important to ensure their presence does not compromise biasing. Explain how termination resistors may adversely affect the biasing of a EIA/TIA-485 network, based on what you see in this schematic:



Calculate the "idle" voltage for this data network, assuming termination resistors of 100 Ω each, bias resistors of 1k Ω each, and a 15 volt power supply at each end. Does this meet the standard for a EIA/TIA-485 network?

Suggestions for Socratic discussion

- Are terminating resistors always needed in an EIA/TIA-485 network? If not, what applications can do without them?
- Demonstrate how to *estimate* numerical answers for this problem without using a calculator.
- Based on the information given in this problem, can we ascertain the characteristic impedance of the cable used in this system? Why or why not?
- If the cable used in this system is replaced by one having significantly greater length but possessing the same characteristic impedance rating as before, will the terminating resistor values need to be altered? Why or why not? If the resistor values do need to be changed, will they need to be larger (more ohms) or smaller (less ohms) than they are now?

file i02198

Question 87

An analog-to-digital converter (ADC) has a calibrated input range of 0 to 5 volts, and a 12-bit output. Complete the following table of values for this converter, assuming perfect calibration (no error):

Input voltage (volts)	Percent of span (%)	Counts (decimal)	Counts (hexadecimal)
1.6			
		3022	
	40		
			A2F

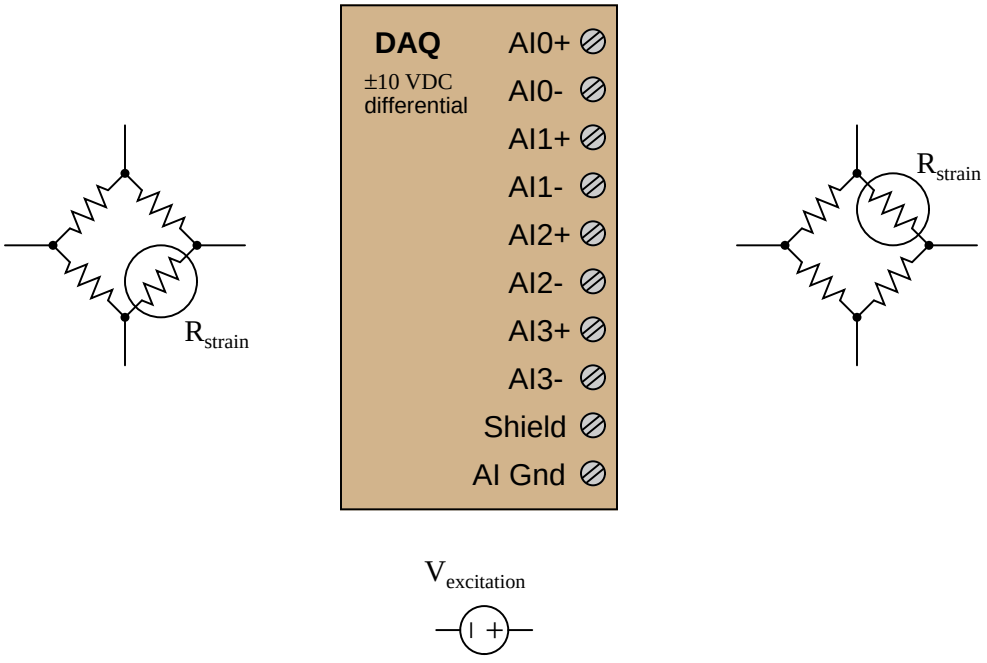
Suggestions for Socratic discussion

- Calculate the resolution of this ADC in *percent* of full-scale range. In other words, what is the smallest percentage of input signal change it is able to resolve?

file i03822

Question 88

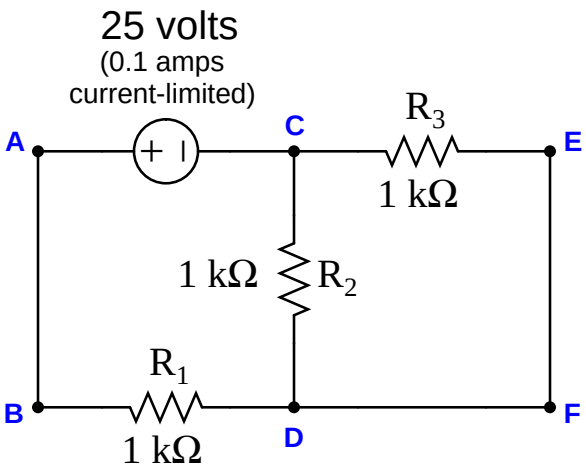
Sketch connecting wires to allow this data acquisition unit (DAQ) to sense strain using quarter-bridge strain gauge circuits on input channels #2 and #3, such that increasing tension on the strain gauge (increasing gauge resistance) generates a more *positive* signal voltage on each channel:



file i04586

Question 89

Suppose an ammeter inserted between test point **D** and the nearest lead of resistor R_1 registers 25 mA in this series-parallel circuit:



Identify the likelihood of each specified fault for this circuit. Consider each fault one at a time (i.e. no coincidental faults), determining whether or not each fault could independently account for *all* measurements and symptoms in this circuit.

Fault	Possible	Impossible
R_1 failed open		
R_2 failed open		
R_3 failed open		
R_1 failed shorted		
R_2 failed shorted		
R_3 failed shorted		
Voltage source dead		

This question is typical of those in the "Fault Analysis of Simple Circuits" worksheet found in the *Socratic Instrumentation* practice worksheet collection, except that all answers are provided for those questions. Feel free to use this practice worksheet to supplement your studies on this very important topic.

Suggestions for Socratic discussion

- Identify a good diagnostic "next step" to narrow the scope of the problem and ultimately locate the one fault in this circuit.

file i04490

Question 90

The `grades_template` spreadsheet provided for you on the Y: network drive allows you to calculate your grade for any course (by entering exam scores, attendance data, etc.) as well as project to the future for courses you have not yet taken. Download the spreadsheet file (if you have not done so yet) and enter all the data you can for grade calculation at this point in the quarter.

Also, locate the pages in your course worksheet entitled "Sequence of Second-Year Instrumentation Courses" to identify which courses you will need to register for next quarter.

If this is Fall, Winter, or Spring quarter, plan a time to complete your *Capstone Assessment*. This is a timed exercise where you must commission a feedback control system for a working process. It is permissible to do this during a scheduled lab period, but of course you should confer with your lab teammates before reserving a time to do this. Otherwise, you may check with your instructor to find a suitable date and time to reserve for completing this mandatory exercise.

Details about the Capstone Assessment are found in the very last question of this worksheet. Pay close attention to the objectives specific to this quarter's study, and to any previous quarters you have completed. Capstone Assessments are *cumulative*, meaning the objectives accumulate for each quarter of study you have completed. Concepts you must know well to successfully complete a Capstone Assessment include: *4-20 mA loop circuit function, correctly identifying voltage polarities and current directions for DC sources and loads, setting loop controller parameters (e.g. controller action, PV scaling), and how to access equipment manuals within the electronic Instrumentation Reference.* Take time between now and your first Capstone attempt to master these things!

Lastly, prepare to comment on your job-search process to date. Where have you applied for jobs so far? Which industries most interest you, and why? Which employers have you researched, and what have you discovered so far? Which areas of the world are you interested in living and working? Which resources are you using to identify open positions (e.g. job search websites, classified advertisements, cold-calling specific employers)? Are there any places you would like to intern at in order to gain specific experience prior to employment?

If an employer were to interview you today, how would you describe your knowledge and skill set? What do you have listed on your resume that *demonstrates* (and not just claims) your work ethic and expertise?

Suggestions for Socratic discussion

- If you do not yet have enough data to calculate a final grade for a course (using the spreadsheet), experiment with plugging scores into the spreadsheet to obtain the grade you would like to earn. How might this be a useful strategy for you in the future?
- Why do you suppose this spreadsheet is provided to you, rather than the instructor simply posting your grades or notifying you of your progress in the program courses?
- Identify any courses that are *elective* rather than required for your 2-year AAS degree.

file i02659

Question 91

A numeration system often used as a "shorthand" way of writing large binary numbers is the *octal*, or base-eight, system. Based on what you know of place-weighted numeration systems, describe how many valid ciphers exist in the octal system, and the respective "weights" of each place in an octal number.

Also, perform the following conversions:

- 35_8 into decimal:
- 16_{10} into octal:
- 110010_2 into octal:
- 51_8 into binary:

Suggestions for Socratic discussion

- If binary is the "natural language" of digital electronic circuits, why do we even bother with other numeration systems such as hex and octal?
- Why is octal considered a "shorthand" notation for binary numbers?

file i02166

Question 92

A numeration system often used as a "shorthand" way of writing large binary numbers is the *hexadecimal*, or base-sixteen, system.

Based on what you know of place-weighted numeration systems, describe how many valid ciphers exist in the hexadecimal system, and the respective "weights" of each place in a hexadecimal number.

Also, perform the following conversions:

- 35_{16} into decimal:
- 34_{10} into hexadecimal:
- 11100010_2 into hexadecimal:
- 93_{16} into binary:

file i02167

Question 93

Suppose the analog-to-digital converter in an instrument has 12 bits of resolution to represent an analog voltage input range of 0 to 5 volts DC. Determine the digital "count" value of this ADC (expressed in binary form) given a 3.6 volt input signal.

Count = _____

file i03795

Question 94

Suppose the analog-to-digital converter in an instrument has 12 bits of resolution to represent an analog voltage input range of 0 to 5 volts DC. Determine the digital "count" value of this ADC (expressed in binary form) given a 2.1 volt input signal.

Count = _____

file i03796

Question 95

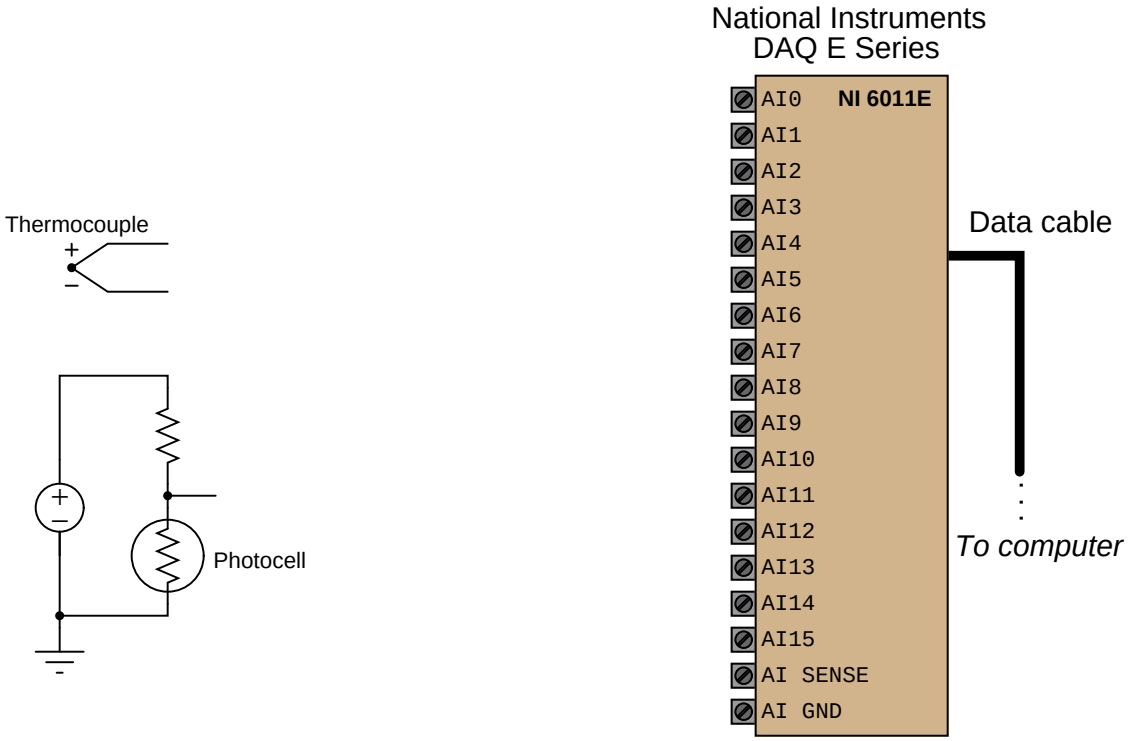
Suppose the analog-to-digital converter in an instrument has 12 bits of resolution to represent an analog voltage input range of 0 to 5 volts DC. Determine the digital "count" value of this ADC (expressed in binary form) given a 1.4 volt input signal.

Count = _____

file i03797

Question 96

Identify suitable input terminals, proper modes, and necessary connecting wires to allow this National Instruments E-series data acquisition unit (DAQ) to sense the two voltage sources shown:



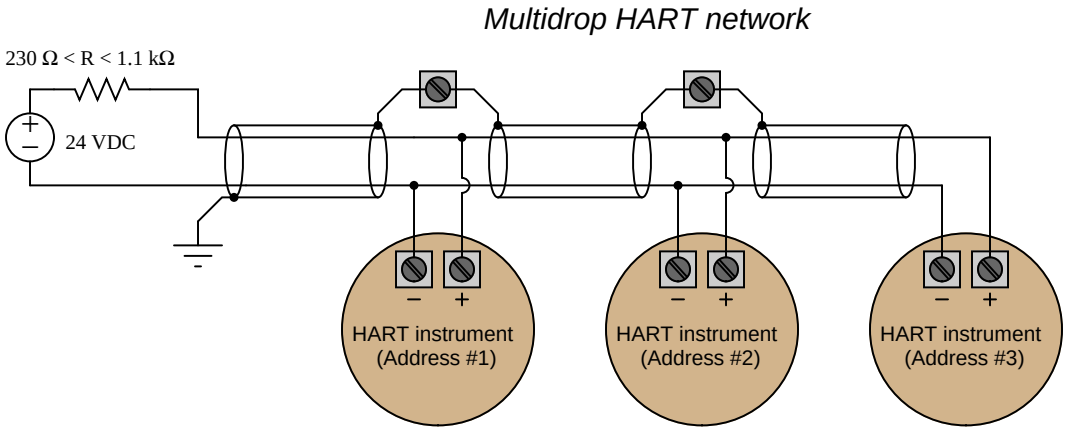
The available modes for the input channels are RSE, NRSE, and DIFF:

Channel	Mode	First terminal	Second terminal
0			
1			

file i01686

Question 97

HART instruments have the capability of operating as purely digital devices, with no analog current signal output. When multiple HART devices are operated like this, paralleled on a common network cable, it is called *multidrop mode*:



Answer the following questions about "multidropped" HART instruments:

- Explain why multidrop HART mode precludes the use of 4-20 mA as a signaling standard. In other words, explain why the option of "multidropping" HART instruments is an *all-or-nothing* choice, rendering the loop current signal meaningless with regard to process measurements.
- Explain why each HART instrument in multidrop mode requires a unique "address" number assigned to it, and identify how many (maximum) different addresses may exist in a HART multidrop network.
- Explain why "burst mode" cannot be used with multidrop HART instruments, and then identify applications where burst mode *would* be useful.
- Finally, identify at least three different places in this network where a HART modem or handheld communicator could be connected to establish communication with the devices.

Suggestions for Socratic discussion

- How much total current would you expect to measure in a multidrop HART network?
- What is the maximum number of HART devices that may be multi-dropped?

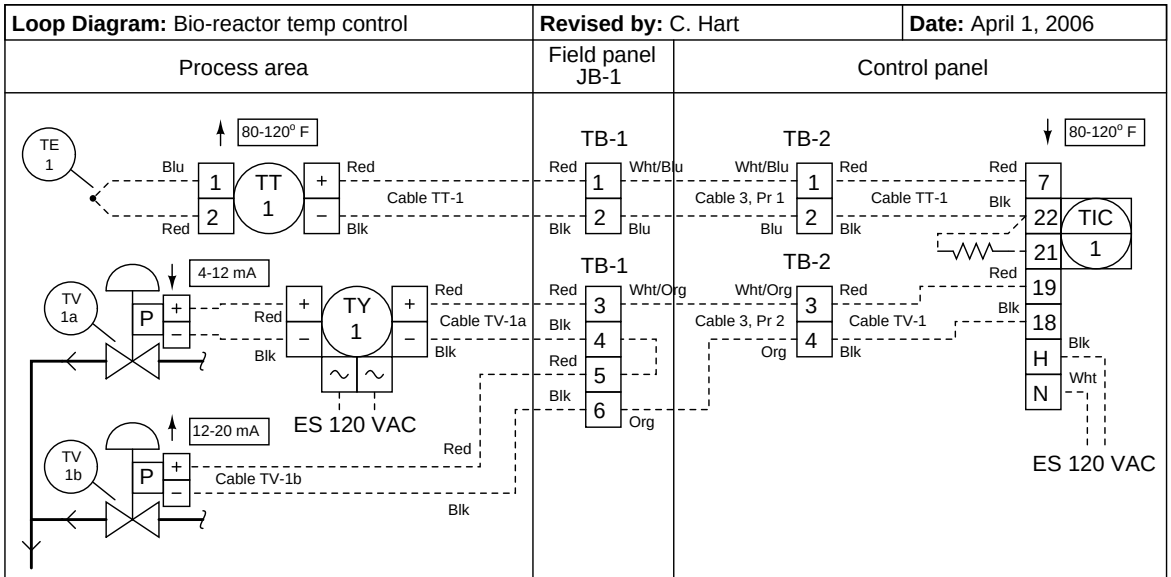
file i02229

Question 98

"Smart" control valve positioners are devices that take a 4-20 mA DC analog current signal and very precisely position the valve stem according to that signal. Since smart positioners contain microprocessors, they are more than capable of communicating via a digital network standard such as HART.

A problem may arise, though, if we try to connect more than one HART-capable valve positioner in the same 4-20 mA current loop, such as when we wish to *split-range* two or more control valves. This is where multiple control valves actuate over different portions of the 4-20 mA range, for example a heating valve that operates from 4 to 12 mA and a cooling valve that operates from 12 to 20 mA. In a traditional (analog) split-range control valve system, the I/P transducers would simply be connected in series so that the same current flowed through both I/P coils, driving both control valves. With HART-capable positioners, though, we might not want the devices to be connected directly in series, because then there may be a conflict of HART signals when we just wish to "talk" with one of the devices.

Explain how this problem is overcome in the following split-range control valve system:



Tag number	Description	Manufacturer	Model	Calibration	Notes
TE-1	Thermocouple	Omega		Type T	Ungrounded tip
TT-1	Temperature transmitter	Rosemount	3144	80-120°F 4-20 mA	
TIC-1	Controller	Siemens	PAC 353	1-5 V 80-120°F	Reverse-acting control
TY-1	HART isolator	Action Instruments	AP4830-2000	n/a	
TV-1a	Control valve	Fisher	Easy-E	4-12 mA	DVC6000 smart positioner
TV-1b	Control valve	Fisher	Easy-E	12-20 mA	DVC6000 smart positioner

Suggestions for Socratic discussion

- If we were to connect a HART communicator device to terminals 3 and 4 of TB-1, which control valve would we be communicating with?
- Which valve carries the cooling fluid and which valve carries the heating fluid in this temperature control system?

file i02230

Question 99

Calculate the resistance between points **A** and **B** (R_{AB}) for the following resistor networks:

Figure 1

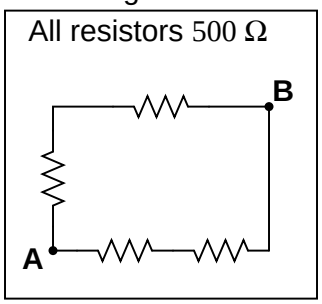


Figure 2

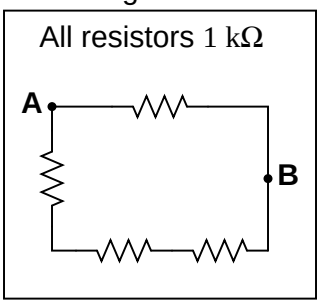


Figure 3

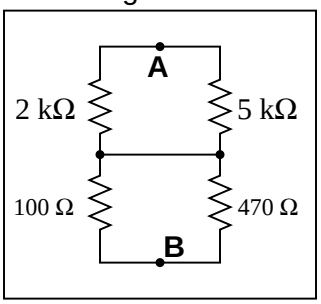


Figure 4

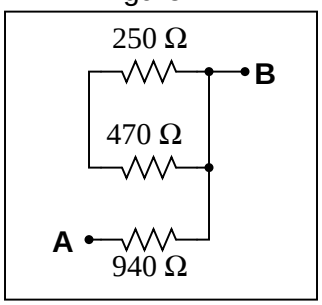


Figure 5

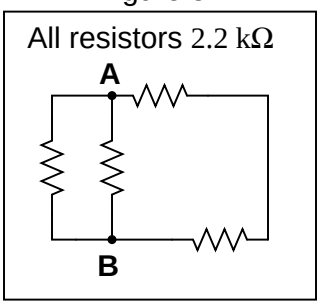
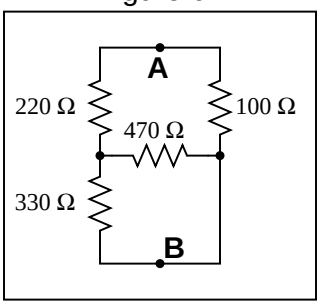


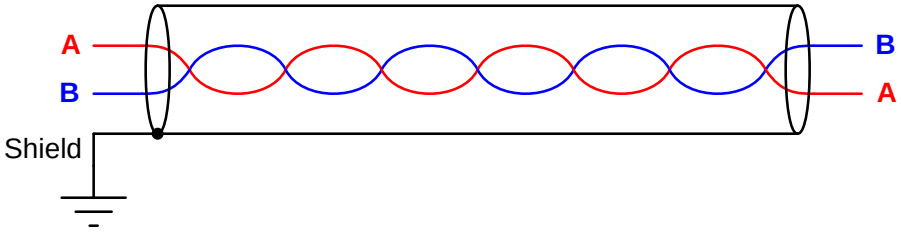
Figure 6



file i00597

Question 100

Industrial signal cables are often comprised of *twisted, shielded wire pairs*. Both the twisting of the wire pairs and the shielding encapsulating the pairs works to protect the signals from corruption due to external noise. One of these techniques guards against interference from stray electrical fields while the other guards against interference from stray magnetic fields. Identify which does which, and explain why.



Furthermore, explain how a multimeter set to measure AC voltage (ideally, AC millivolts) could be used to detect the presence of *electric* field-induced noise anywhere along the cable's length. Also, explain how a multimeter set to measure AC millivoltage could be used to detect the presence of *magnetic* field-induced noise anywhere along the cable's length.

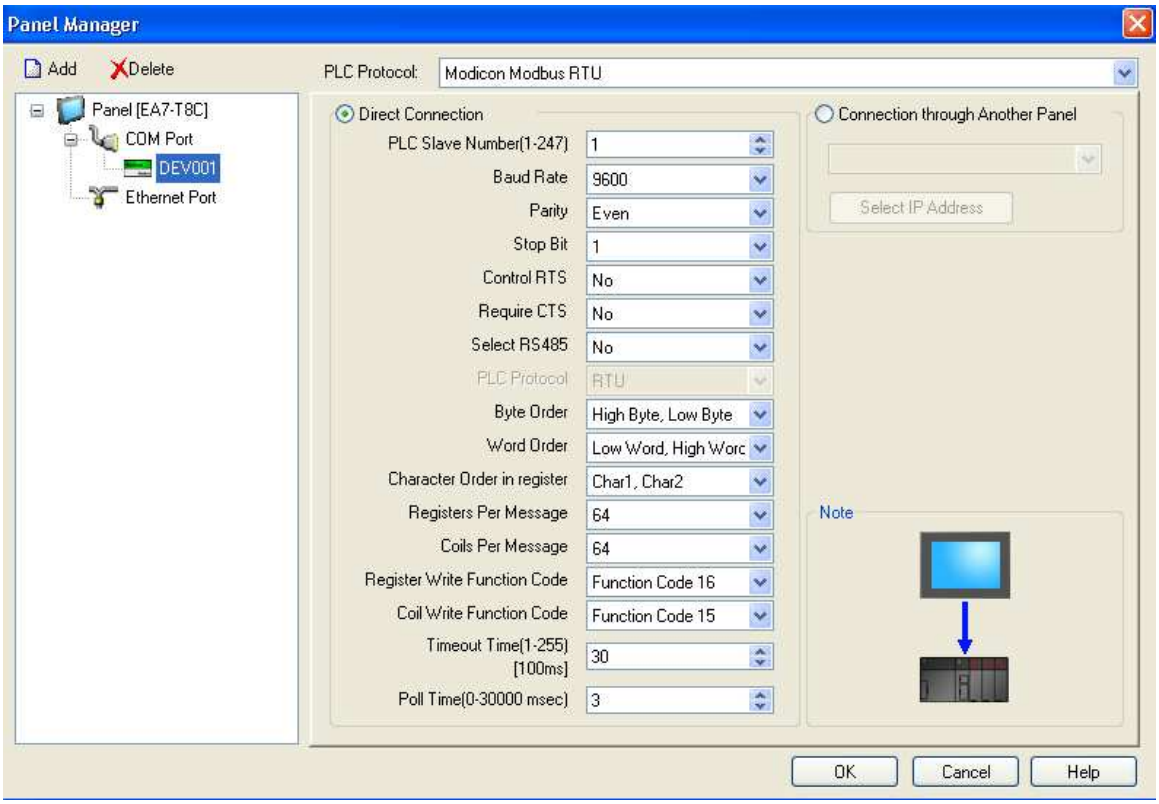
Suggestions for Socratic discussion

- Identify what would cause a *ground loop* to form in this cable, why that would be a bad thing, and how we may avoid it.
- Is the *rate of twist* of the wire pair relevant to noise immunity? If so, which would be better – a cable with a "slow" twist or a cable with a tightly-twisted wire pair?

file i02192

Question 101

The following screen capture shows the configuration window for an HMI panel, providing serial communication parameters for it to exchange data with a Modbus device:



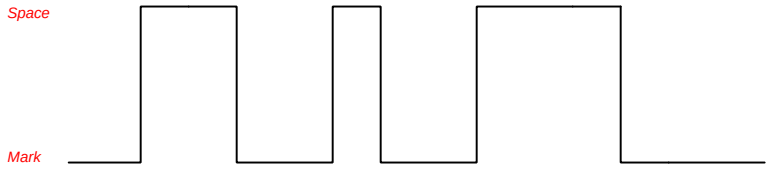
Identify the purpose for the "Control RTS" and "Require CTS" parameters, both of which happen to be de-activated (set to "No").

Two options exist for Modbus Register Write function codes: 06 and 16. Likewise, two options exist for Modbus Coil Write function codes: 05 and 15. Explain the difference between each option, and why one setting might be more useful than the other.

file i00718

Question 102

Here is an oscilloscope's view of an ASCII character sent asynchronously with 8 data bits, odd parity and 1 stop bit ("8-O-1"), using *NRZ* (Non-Return to Zero) encoding:



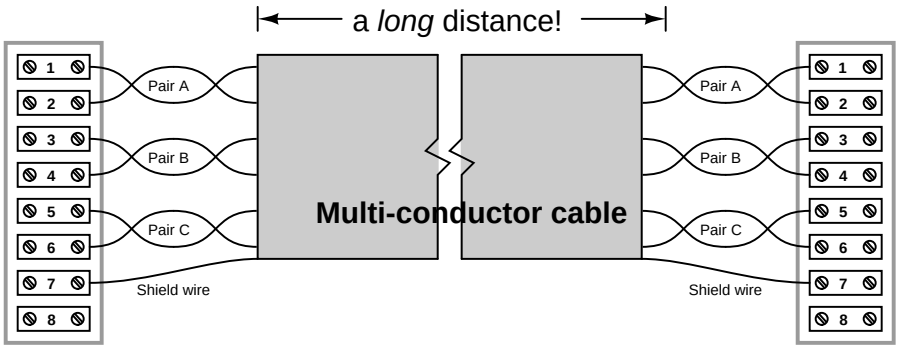
Answer the following questions:

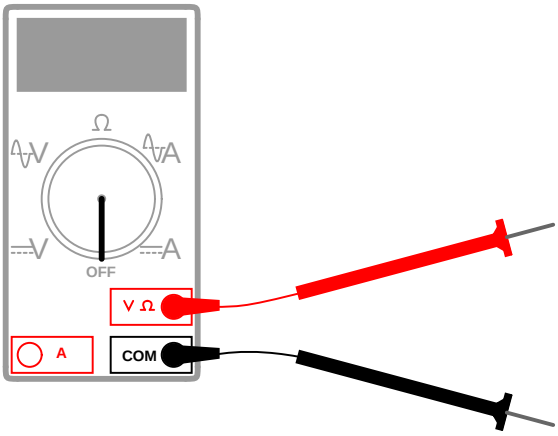
- Identify the *Start* bit in this frame
- Identify the *Stop* bit in this frame
- Identify the *Parity* bit in this frame
- Identify the *Data field* in this frame
- Identify any portions of the waveform where the NRZ signal is *idle*
- Identify the ASCII character represented by the data in this frame
- Determine whether or not the parity is valid

file i03194

Question 103

Suppose you are asked to check the integrity of a multi-conductor signal cable run between two locations. The cable has six signal conductors in it plus a shield, each one terminated at a terminal block at each end:



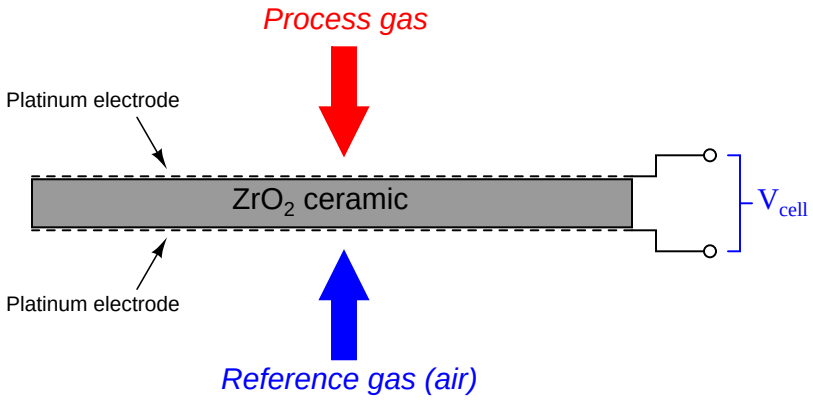


Faults you are looking for include *open* conductors, as well as *shorts* between conductors and/or shorts to ground. Devise a series of tests you could perform with nothing but a multimeter to comprehensively check the electrical integrity of this cable.

file i00734

Question 104

The *Nernst equation* finds application in many different chemical analyzer technologies. One of these analytical technologies is *oxygen concentration* in mixed gas streams, such as the exhaust from a combustion process where oxygen content is usually maintained at about 2% (instead of the normal 20.9% oxygen concentration of Earth's atmosphere). A common oxygen sensor is made of a "sandwich" of platinum electrodes on either side of a solid zirconium oxide membrane. One side of this electrochemical cell is exposed to the exhaust gas (process), while the other side is exposed to heated air which serves as a reference:



Voltage output by the cell is predicted by the Nernst equation:

$$V = \frac{RT}{nF} \ln\left(\frac{C_1}{C_2}\right)$$

Where,

V = Voltage produced across membrane due to ion exchange, in volts (V)
R = Universal gas constant (8.315 J/mol·K)
T = Absolute temperature, in Kelvin (K)
n = Number of electrons transferred per ion exchanged (2, for oxygen atoms)
F = Faraday constant, in coulombs per mole (96,485 C/mol e^-)
C_1 = Concentration of oxygen in ambient air (20.9%)
C_2 = Concentration of oxygen in exhaust gas

Suppose a DAQ module were connected to one of these oxygen-sensing cells, and you needed to enter a formula into the DAQ software to translate voltage into oxygen concentration. Manipulate the Nernst equation to solve for the concentration of oxygen in the exhaust gas from the measured voltage:

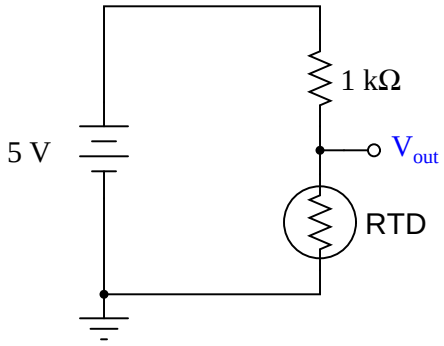
$C_2 =$

file i00929

Question 105

Write an equation describing the output voltage as a function of temperature, assuming the RTD (Resistive Temperature Detector) has a resistance predicted by the following formula:

$$R_{RTD} = 100(1 + 0.00392T)$$

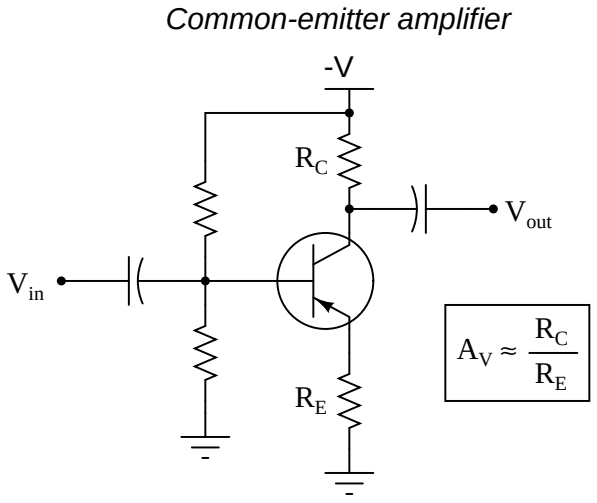


$V_{out} = f(T) =$

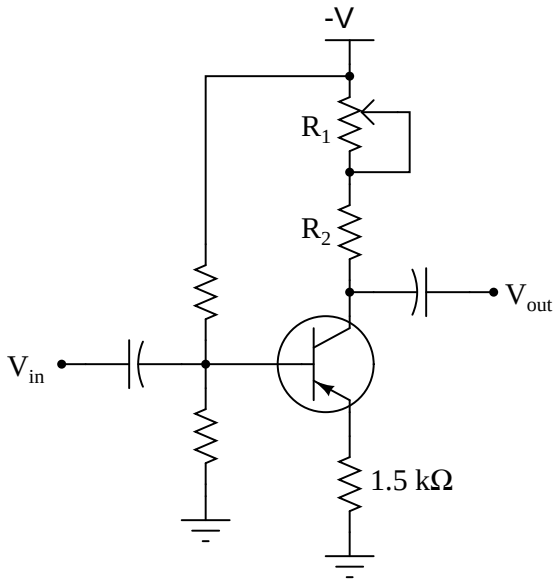
file i00536

Question 106

The voltage gain of a common-emitter transistor amplifier is approximately equal to the collector resistance divided by the emitter resistance:



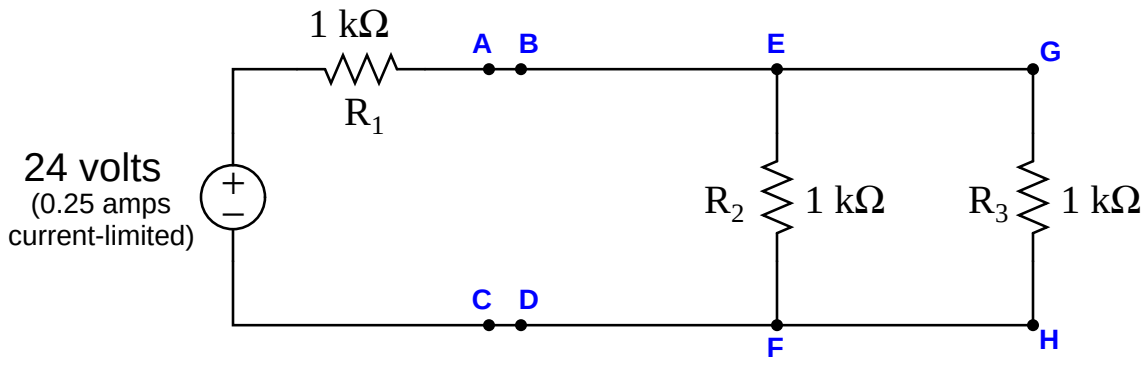
Knowing this, calculate the necessary resistance values for the following fixed-value resistor (R_2) and potentiometer (R_1) to give this common-emitter amplifier an adjustable voltage gain range of 2 to 8:



file i03519

Question 107

Suppose a voltmeter registers 0 volts between test points **A** and **C**, but measures 24 volts between those same two test points after the connection has been broken between points **C** and **D**:



Identify the likelihood of each specified fault for this circuit. Consider each fault one at a time (i.e. no coincidental faults), determining whether or not each fault could independently account for *all* measurements and symptoms in this circuit.

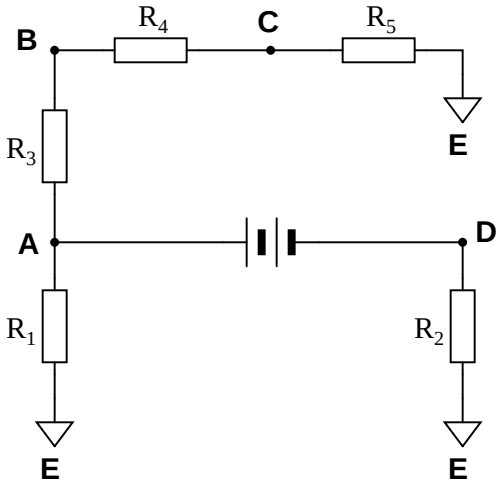
Fault	**Possible**	**Impossible**
R_1 failed open		
R_2 failed open		
R_3 failed open		
R_1 failed shorted		
R_2 failed shorted		
R_3 failed shorted		
Voltage source dead		

Finally, identify the *next* diagnostic test or measurement you would make on this system. Explain how the result(s) of this next test or measurement help further identify the location and/or nature of the fault.

file i00171

Question 108

Determine what will happen to the following voltage drops (between specified test points in the circuit) if the resistance of resistor R_3 happens to decrease:

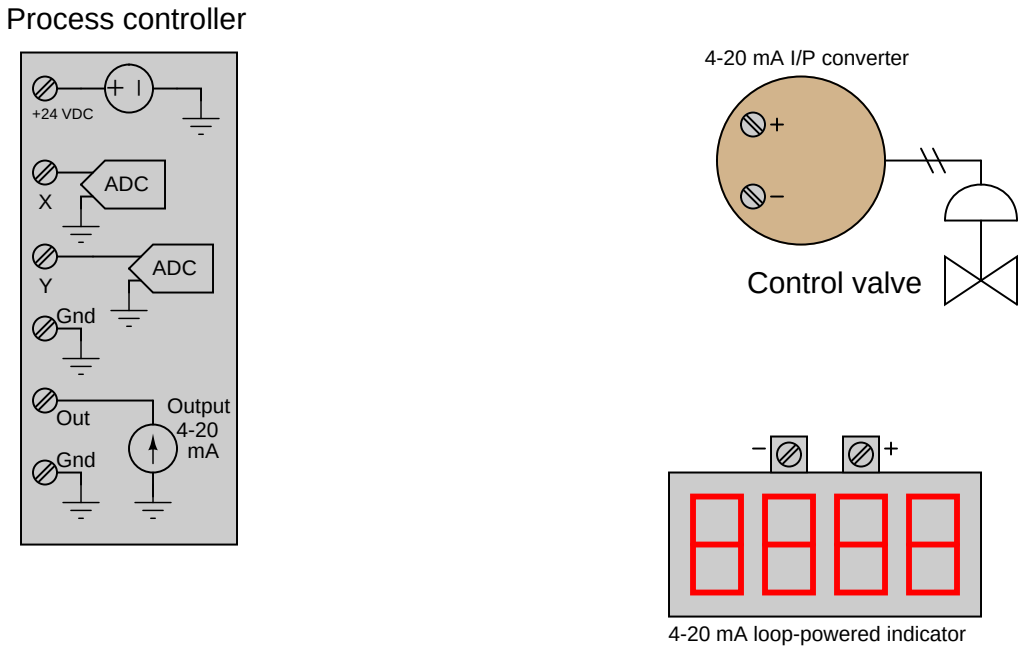


- V_{AC} = (*increase*, *decrease*, or *stay the same*)
- V_{BE} = (*increase*, *decrease*, or *stay the same*)
- V_{AD} = (*increase*, *decrease*, or *stay the same*)
- V_{CD} = (*increase*, *decrease*, or *stay the same*)

file i02914

Question 109

Shown here is a process controller, an I/P transducer, and a loop-powered indicator:

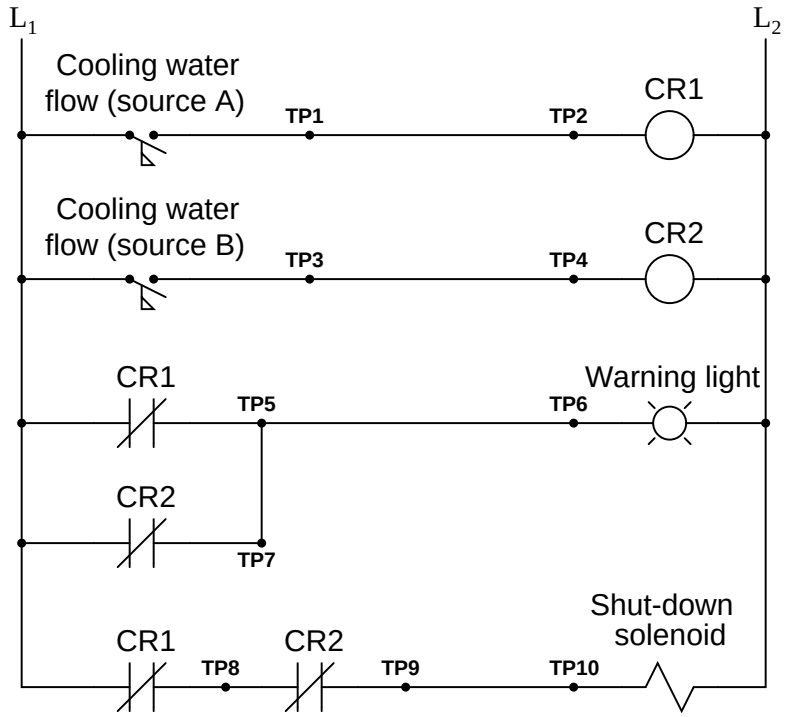


Show how the controller would connect to drive the I/P transducer and also provide a 4-20 mA DC input signal to the loop-powered indicator such that the indicator will show the percentage signal output to the I/P transducer (i.e. the approximate valve position).

file i02529

Question 110

A water-cooled generator at a power plant has two sources of cooling water flow, each source equipped with a flow switch that returns to its normally-open status if the water flow through the pipe stops. If either water source ceases supplying cooling water to the generator (for whatever reason), that flow switch will de-actuate and turn the warning light on. This is all that is required, as the generator will still receive adequate cooling from only one source. If both water sources cease supplying water, however, a "trip" solenoid will energize to shut down the generator before it overheats:



One day the warning light comes on, but there is still cooling water flowing to the generator so it does not shut down. You are asked to determine what the problem is, while maintaining the system in an operating condition (i.e. you are not allowed to shut off control power or do anything else that might shut down the generator).

First, assess whether or not the following diagnostic test would provide any useful information about the fault: *suppose a technician connects an AC voltmeter between terminals TP6 and L2.* Will this test provide information to help us diagnose the nature and/or location of the fault? Why or why not?

Next, propose a diagnostic test that would definitely provide useful information about either the location or the nature of the fault in this system. Your proposal must identify the meaning of at least one possible result of the test (e.g. *"If I jumper terminals X and Y together and I measure a decrease in source voltage, it means the fault must be a short somewhere in branch A-B-C of the circuit"*). Remember that the best diagnostic test is one that yields definitive answers no matter what its result might be. Directly checking a suspected component is *not* a good diagnostic test, unless there are simply no other options!

file i03199

Question 111

Lab Exercise – introduction

Your task is to build, document, and troubleshoot a telemetry system consisting of an analog sensor connected to a data acquisition (DAQ) module, which then sends the data over Ethernet to some form of digital display console (e.g. a personal computer running appropriate software, an HMI panel, etc.). Temperature and pressure are suggested process variables to measure. Electric current (measured using a shunt resistor or a current transformer) is another excellent process variable to measure, and this works well to introduce the specialized topic of electric power metering and protection. Other process variables are open for consideration, though.

The following table of objectives show what you and your team must complete within the scheduled time for this lab exercise. Note how some of these objectives are individual, while others are for the team as a whole:

Objective completion table:

Performance objective	Grading	1	2	3	4	Team
Team meeting and prototype sketch (do *first!*)	mastery	–	–	–	–	
Circuit design challenge	mastery					– – – –
Final documentation and system inspection	mastery					– – – –
Demonstrate IP "ping" utility	mastery	–	–	–	–	
Demonstrate use of a "knockout punch" tool	mastery	–	–	–	–	
Accurate measurement of variable ($\pm$ 1% of span)	mastery	–	–	–	–	
Data communicated via Ethernet	mastery	–	–	–	–	
Troubleshooting	mastery					– – – –
Safety and professionalism	deduction					
Lab percentage score	proportional					– – – –
Decommission and lab clean-up	(ungraded)	–	–	–	–	

The "proportional" score for this activity is based on the number of attempts require to master each objective. Every failed attempt is marked by a 0, and every pass by a 1. The total number of 1 marks divided by the total number of marks (both 1's and 0's) yields a percentage value. Team objectives count as part of every team member's individual score. The *Safety and professionalism* deduction is a flat -10% per instance, levied on occasions of unprofessional or unsafe conduct.

It is essential that your team plans ahead what to accomplish each day. A short (10 minute) team meeting at the beginning of each lab session is a good way to do this, reviewing what's already been done, what's left to do, and what assessments you should be ready for. There is a lot of work involved with building, documenting, and troubleshooting these working instrument systems!

As you and your team work on this system, you will invariably encounter problems. You should always attempt to solve these problems as a team before requesting instructor assistance. If you still require instructor assistance, write your team's color on the lab whiteboard with a brief description of what you need help on. The instructor will meet with each team in order they appear on the whiteboard to address these problems.

Lab Exercise – objectives and expectations

Each objective is assessed at the *mastery* level, which means it is not complete until it meets *all* expectations. Re-tries are allowed, but failed attempts will be recorded and factored into your score for this lab exercise.

Team meeting and prototype sketch

Read the lab exercise documentation and discuss with your teammates the objectives to be achieved and the time allotted to do so. Formulate a plan to achieve these objectives and draft a prototype design for the system you intend to build. Then, meet with your instructor to present your team's action plan and prototype design. *This prototype sketch should be annotated with all expected physical parameters (e.g. voltage polarities, current directions, fluid pressures, etc.).* Be prepared to answer all manner of questions about your team's goals, planned schedule of work, available resources, and prototype design, including analysis of the design for specific faults and condition changes. Do not begin construction until your design has been analyzed and approved! Note that multiple meetings may be required if the instructor's assistance is needed to select components influencing your design.

Circuit design challenge

Design and build either a light-sensing or temperature-sensing circuit from components meeting criteria randomly specified by the instructor, using a digital multimeter (DMM) to record either minimum or maximum signal levels.

Final loop diagram and system inspection

Create a complete loop diagram of your team's completed system according to the ISA 5.1 standard, then show that the constructed system meets or exceed all standards described in the lab exercise documentation.

Demonstration of IP "ping" utility

Correctly use the `ping` command-line utility to test connectivity between two or more IP-networked devices.

Demonstrate use of a "knockout punch" tool

Safely use a "knockout punch" tool to punch a hole in sheet metal suitable for connection to an electrical conduit fitting.

Accurate measurement of variable

Demonstrate that your data acquisition system accurately registers the process variable to within $\pm$ 1% of span over the entire measurement range. This will require you to enter a mathematical formula into the DAQ polling software to convert the "raw" voltage signal into a value representing the real process variable value.

Data communicated via Ethernet

Demonstrate that your data acquisition system communicates data over an Ethernet network.

Troubleshooting

Logically diagnose the nature and location of a fault placed in a working system that your team did not build. This will be limited in time, with each student passing or failing individually.

Lab Exercise – objectives and expectations (continued)

Lab percentage score

Successful completion of the lab exercise requires demonstrated mastery of all objectives. A percentage value is based on the number of attempts required to achieve mastery on these objectives: the number of objectives divided by the number of total attempts equals the percentage. Thus, a perfect lab percentage score is possible only by completing all objectives on the first attempt. Marks given for team objectives factor into each individual's score. If one or more members of a team repeatedly compromise team performance, they may be removed from the team and required to complete remaining lab exercises alone.

Deductions from this percentage value will be levied for instances of unsafe or unprofessional conduct (see below), the final result being the lab percentage score.

Safety and professionalism (deduction)

In addition to completing the specified learning objectives in each lab exercise, each student is responsible for abiding by all lab safety standards and generally conducting themselves as working professionals (see the *General Values, Expectations, and Standards* page near the beginning of every worksheet for more detail). Expectations include maintaining an orderly work environment and returning all tools and test equipment by the end of every school day (team), as well as following clear instructions (e.g. instructions given in equipment manuals, lab documentation, verbally by the instructor), communicating with teammates, formulating a plan to complete the lab project in the allotted time, and productively managing time. As with the other objectives, chronic patterns of poor performance in this domain may result in the offending student being removed from the team. Deductions to the lab percentage score will *not* be made for performance already graded such as tardiness and attendance.

General format and philosophy

This lab exercise is *project-based:* the instructor serves as the project engineer, while each student's role is to implement the standards set for the project while budgeting time and resources to complete it by the deadline date. Students perform real work as part of the lab exercise, managing their work day and functioning much the same as they will on the job. The tools and equipment and materials used are all industry-standard, and the problems encountered are realistic. This instructional design is intentional, as it is proven effective in teaching project management skills and independent working habits.

When you require the instructor's assistance to answer a question or to check off an objective, write your name (or your team's name) on the lab room whiteboard. Questions take priority over checkoffs, so please distinguish questions from other requests (e.g. writing a question-mark symbol "?" after your name makes this clear). **There will be times when you must wait for extended periods** while the instructor is busy elsewhere – instant service is an impossibility. Adequate time *does* exist to complete the lab exercise if you follow all instructions, communicate well, and work productively. Use all "down time" wisely: filling it with tasks not requiring the instructor's assistance such as other lab objectives, homework, feedback questions, and job searches.

Remember that the lab facility is available to you at all hours of the school day. Students may perform non-hazardous work (e.g. circuit work at less than 30 volts, documentation, low air pressures, general construction not requiring power tools) at *any time during the school day* without the instructor's presence so long as that work does not disturb the learning environment for other students.

DO NOT TAKE SHORTCUTS when completing tasks! Learning requires focused attention and time on task, which means that most 'shortcuts" actually circumvent the learning process. Read the lab exercise instructions, follow all instructions documented in equipment manuals, and follow all advice given to you by your instructor. Make a good-faith effort to solve all problems on your own *before* seeking the help of others. Always remember that this lab exercise is just a means to an end: no one *needs* you to build this project; it is an activity designed to develop marketable knowledge, skills, and self-discipline. In the end it is your *professional development* that matters most, not the finished project!

Lab Exercise – team meeting, prototype sketch, and instrument selection

An important first step in completing this lab exercise is to **meet with your instructor** as a team to discuss safety concerns, team performance, and specific roles for team members. If you would like to emphasize exposure to certain equipment (e.g. use a particular type of control system, certain power tools), techniques (e.g. fabrication), or tasks to improve your skill set, this is the time to make requests of your team so that your learning during this project will be maximized.

An absolutely essential step in completing this lab exercise is to work together as a team to **sketch a prototype diagram** showing what you intend to build. This usually takes the form of a simple electrical schematic and/or loop diagram showing all electrical connections between components, as well as any tubing or piping for fluids. This prototype sketch need not be exhaustive in detail, but it does need to show enough detail for the instructor to determine if all components will be correctly connected for their safe function.

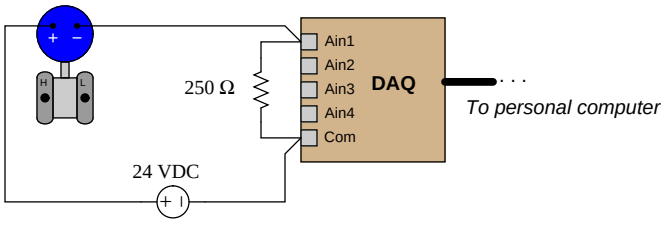
You should practice good problem-solving techniques when creating your prototype sketch, such as consulting equipment manuals for information on component functions and marking directions of electric current, voltage polarities, and identifying electrical sources/loads. Use this task as an opportunity to strengthen your analytical skills! Remember that you will be challenged in this program to do all of this on your own (during "capstone" assessments), so do not make the mistake of relying on your teammates to figure this out for you – instead, treat this as a problem *you* must solve and compare your results with those of your teammates.

Your team's prototype sketch is so important that the instructor will demand you provide this plan before any construction on your team's working system begins. *Any team found constructing their system without a verified plan will be ordered to cease construction and not resume until a prototype plan has been drafted and approved!* Similarly, you should not deviate from the prototype design without instructor approval, to ensure nothing will be done to harm equipment by way of incorrect connections. Each member on the team should have ready access to this plan (ideally possessing their own copy of the plan) throughout the construction process. Prototype design sketching is a skill and a habit you should cultivate in school and take with you in your new career.

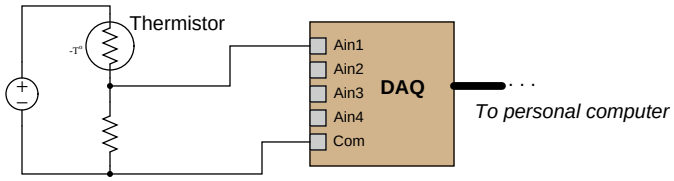
Each lab team locker has its own data acquisition unit (DAQ), and other DAQ units are available from the instructor. You will need to install software on a personal computer in order for that computer to gather analog data from the DAQ unit.

It is recommended that you test your DAQ before connecting it to any external circuitry. For a simple test of an analog input, set your multimeter to "Diode Test" so that it outputs a small voltage, then connect your meter leads to one of the analog input channels on the DAQ: the software should register a small voltage on that channel, letting you know the DAQ is functioning.

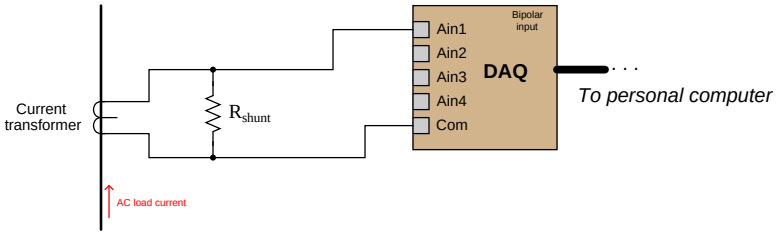
You will need to choose a suitable sensor to connect to one of the DAQ analog inputs. For greatest accuracy, I recommend using a standard 4-20 mA loop-powered pressure or temperature transmitter, with a 250 ohm resistor connected to the DAQ so it can read a 1-5 volt signal:



You are also welcome to be more creative and build yourself a simpler analog sensing circuit such as this:



The challenge with a circuit such as this is that it will *not* output a signal that is linearly proportional to temperature like the loop-powered transmitter will. In order to make this work, you will have to program a formula into the DAQ software to "linearize" the voltage signal into a proportional temperature value. This will require extra work on your part to characterize the sensor, then develop a formula describing the signal voltage value as a function of the measured variable. You may find a computer spreadsheet program to be helpful, plotting a curve of voltage versus sensor stimulus (e.g. temperature), then using the curve-fitting utility in the spreadsheet to develop an equation relating voltage to the measurement.



If you choose to build a system to measure AC current using a current transformer (CT, shown above), you will need to select a suitable shunt resistor to drop voltage generated by current output by the CT. This is done by researching the "burden" rating of the CT, which will tell you how large that load resistor may be. CTs act as current sources, and so "want" to drive a low-resistance load (e.g. an ammeter to measure the CT secondary current). However, the DAQ needs to see a strong enough voltage drop across the shunt resistor to use a reasonable percentage of its range, in order to make good use of its resolution. *If you build this circuit, you must be sure to do so in a way that the CT's secondary winding will never become open-circuited when load current goes through it! Open-circuited current transformers are capable of generating dangerously high voltages!!!*

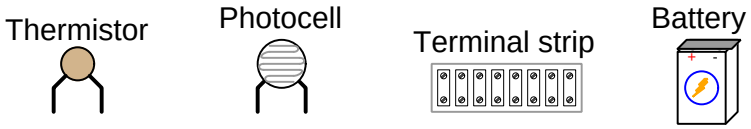
For any application, it is extremely important to check the input ratings of your DAQ unit to ensure they are appropriate for the measurement task, and also check to see that the *absolute maximum* ratings are such that the DAQ will not become damaged in the event of any single-component failure. For example, if your DAQ happens to have an absolute maximum input voltage rating of 20 volts and your circuit could potentially apply 24 volts to the DAQ input in the event of a particular component fault, it means you must re-design your circuit to prevent this ever from happening.

Planning a functioning system should take no more than an hour if the team is working efficiently, and will save you hours of frustration (and possible component destruction!).

Lab Exercise – circuit design challenge

Build a simple circuit using either a light sensor (photocell) or a temperature sensor (thermistor) connected to a fixed-value resistor and a battery such that a variable output voltage will be generated as the sensor is stimulated. Your circuit must either make the voltmeter indication increase with increasing sensor stimulus (more voltage for more light or heat – direct action), or do the exact opposite (reverse action), as specified by the instructor. You will also need to demonstrate how to record and display the lowest and highest voltages output by this circuit using your digital multimeter's "min/max" recording function function. All electrical connections must be made using a terminal strip (no twisted wires, crimp splices, wire nuts, spring clips, etc.) "Alligator" clips are permitted for making connections to battery terminals only.

This exercise tests your ability to properly identify the operating characteristics of a light or temperature sensor, properly size a resistor to form a voltage divider circuit with the sensor, properly connect a voltmeter into the circuit to achieve the specified response direction, properly use a DMM to capture minimum and maximum voltage values, and use a terminal strip to organize all electrical connections.



The following components and materials will be available to you: assorted CdS **photocells** and **thermistors** ; **terminal strips** ; lengths of **hook-up wire** ; **battery**. You must provide resistor(s), your own tools, and digital multimeter (DMM) as well as a copy of this page for your instructor to mark objectives.

SEQUENCE: (1) Instructor chooses criteria; (2) You build and test circuit without any power sources at all; (3) Instructor provides battery and observes you energizing the circuit for the very first time; (4) You demonstrate to the instructor that the circuit fulfills its intended function. (5) You demonstrate how to capture the minimum or maximum value using your DMM.

Sensor type (instructor chooses): ____ Photocell ____ Thermistor

Meter response (instructor chooses): ____ Direct ____ Reverse

Captured value (instructor chooses): ____ $V_{minimum}$ ____ $V_{maximum}$

Lab Exercise – building the system

The Instrumentation lab is set up to facilitate the construction of working instrument "loops," with over a dozen junction boxes, pre-pulled signal cables, and "racks" set up with 2-inch vertical pipes for mounting instruments. The only wires you should need to install to build a working system are those connecting the field instrument to the nearest junction box, and then small "jumper" cables connecting different pre-installed cables together within intermediate junction boxes.

After getting your prototype sketch approved by the instructor, you are cleared to begin building your system. All wire connections should be made using terminal blocks. No twisted or taped wire connections will be allowed.

You will need to configure the DAQ software to "scale" the 1-5 VDC signal into an actual measurement of your process variable (e.g. temperature, pressure). A requirement of this lab is that the DAQ software accurately register the process variable you are measuring, rather than merely displaying a voltage value from the sensor.

The DAQ provided in your team's tool locker is equipped with its own Ethernet port, which means you may use any Ethernet-equipped personal computer to run the DAQ software and poll data from the DAQ unit over the lab's Ethernet network. For those teams interested in learning Modbus programming and familiar with programming the lab's caSCADA system(s), I recommend writing C-language code to poll data from a Modbus-compliant DAQ and executing that code in any computer with a C compiler. Examples of Modbus programming using the `libmodbus` library are shown in the Modbus section of the *Lessons In Industrial Instrumentation* textbook.

Your chosen system may require its own electrical enclosure to house the DAQ and/or other components, not already a part of the lab's permanently-installed loop system. If you need to punch a hole in the side of a custom enclosure as part of your system, you must use a special tool called a *knockout punch* to make these holes (rather than use a hole saw on a drill). The Greenlee company manufactures a line of knockout punches called the *Slug Buster*, which you may wish to research in preparing to use this tool.

Common mistakes:

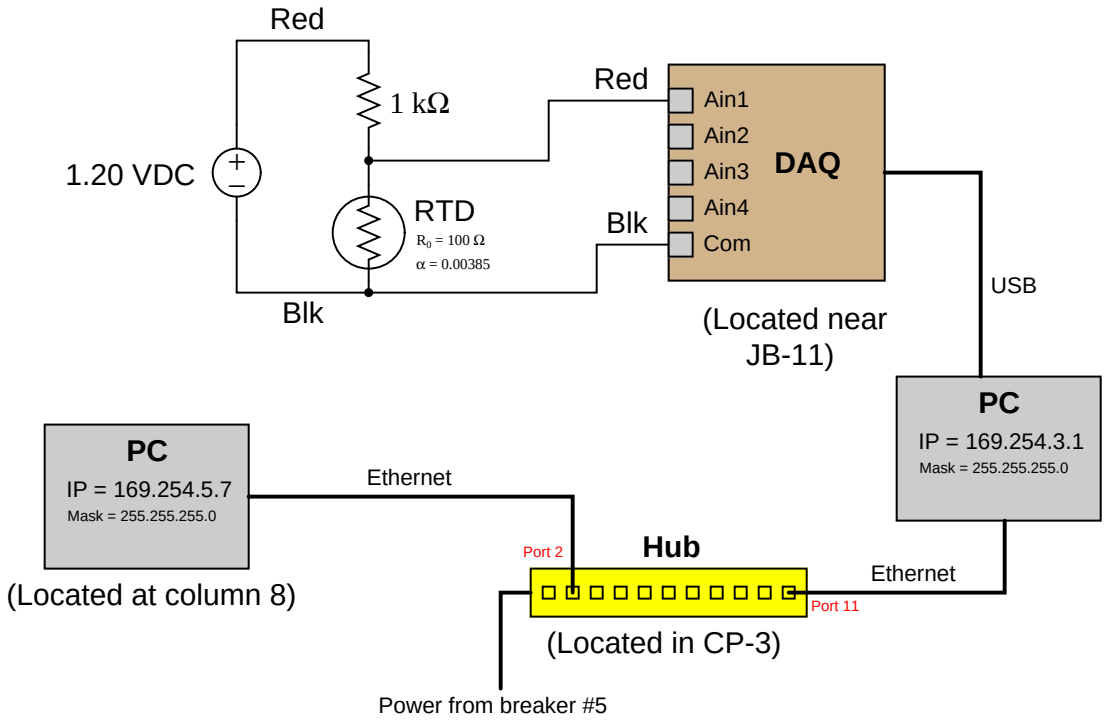
- Starting to build the circuit before planning its construction on paper with a proposed circuit sketch.
- Failing to heed signal voltage limits for the DAQ analog input channels. *Be careful not to over-power the DAQ with signal voltages exceeding its measurement limits!*
- Failing to tug on each and every wire where it terminates to ensure a mechanically sound connection.
- Students working on portions of the system in isolation, not sharing with their teammates what they did and how. It is important that the whole team learns all aspects of their system!

Building a functioning system should take no more than one full lab session (3 hours) if all components are readily available and the team is working efficiently!

Lab Exercise – documenting the system

Each student must sketch their own *system diagram* for their team's data acquisition system. This will not be an ISA-standard loop diagram, but rather a combination of schematic diagram (showing the sensor and DAQ connections) and block diagram (showing the computer Ethernet network complete with IP addresses). Your diagram must be *comprehensive* and *detailed*, showing every wire connection, every cable, every terminal block, range points, network addresses, etc.

An example system diagram is shown here:



Note that if using an Ethernet-equipped DAQ unit, the DAQ will be able to plug directly into the Ethernet hub without need for an intermediary computer (e.g. 169.254.3.1 shown in this diagram.)

When your entire team is finished drafting your individual diagrams, call the instructor to do an inspection of the system. Here, the instructor will have students take turns going through the entire system, with the other students checking their diagrams for errors and omissions along the way. During this time the instructor will also inspect the quality of the installation, identifying problems such as frayed wires, improperly crimped terminals, poor cable routing, missing labels, lack of wire duct covers, etc. The team must correct all identified errors in order to receive credit for their system.

After successfully passing the inspection, each team member needs to place their system diagram in the diagram holder located in the middle of the lab behind the main control panel. When it comes time to troubleshoot another team's system, this is where you will go to find a diagram for that system!

Common mistakes:

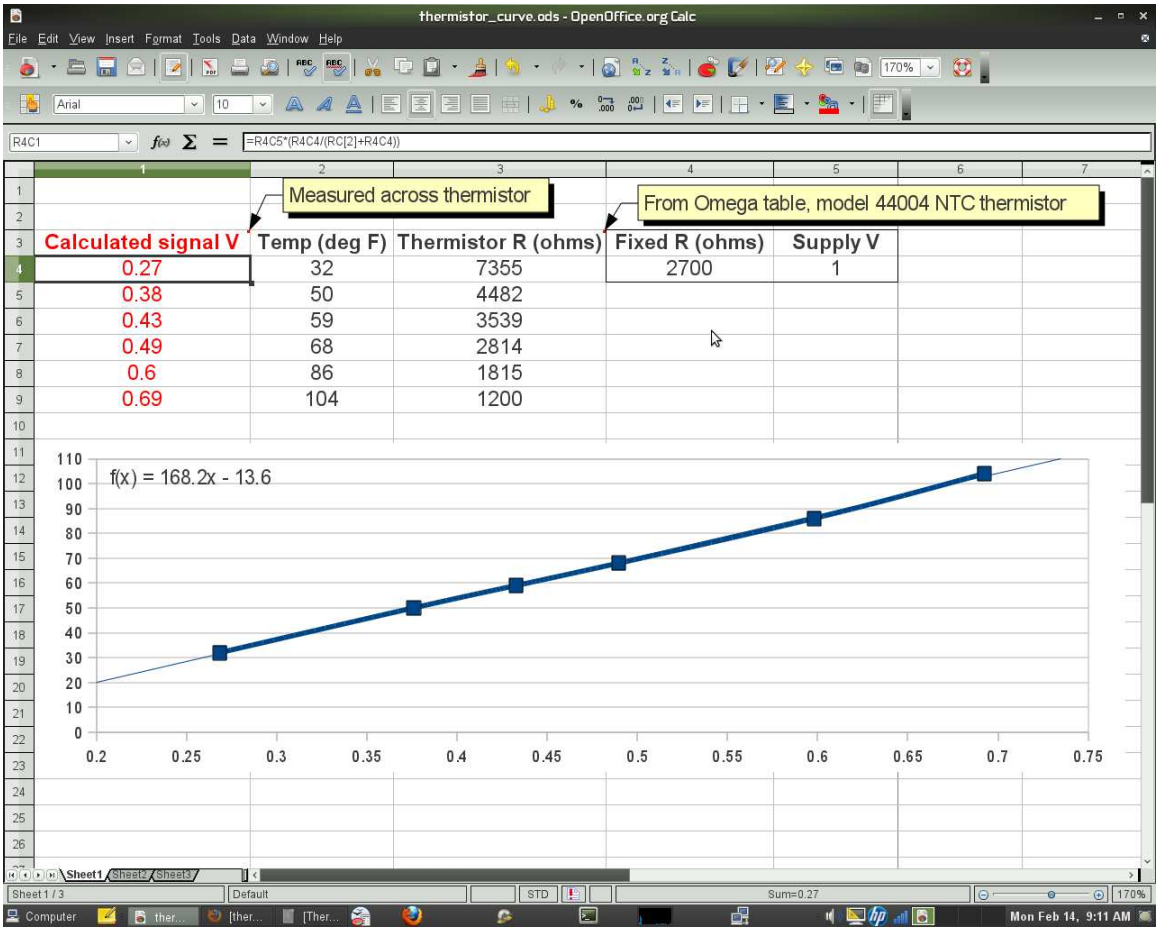
- Forgetting to label all signal wires.
- Forgetting to note all wire colors.
- Forgetting to put your name on the diagram!
- Basing your diagram off of a team-mate's diagram, rather than closely inspecting the system for yourself.
- Not placing instruments in the correct orientation (field instruments on the left, control room instruments on the right).

Notes on DAQ signal scaling/linearization

Each team must configure their DAQ system to accurately report the measured variable in appropriate units of measurement. The measurement accuracy will be checked by the instructor by applying random stimuli to the sensor while the team verifies the remote indication (on a computer connected through the network to the DAQ module). DAQ polling software contains a provision for entering your own mathematical scaling formula to perform this function.

If your system uses a loop-powered 4-20 mA transmitter, the only DAQ configuration you will need to do is "scale" the DAQ so that it converts the linear 1-5 VDC signal into a linear representation of the measured variable. However, you will need to rely on those teammates who have taken the INST24X courses to calibrate the transmitter so that it accurately outputs the 4-20 mA signal.

If your system reads a raw voltage signal from a resistive sensor in a bridge or other voltage-divider network, you will need to program the DAQ software to "linearize" the signal so that it will register the actual process variable and not just a plain signal voltage. The following screenshot shows how a computer spreadsheet may be used to generate a linearizing equation from published sensor data:



In this particular example, the sensor is a negative temperature coefficient (NTC) thermistor, model 44004, manufactured by Omega. The formula entered into cells R4C1 through R9C1 calculates the voltage dropped across a fixed resistor (2700 Ω) connected in series with the thermistor and powered by a 1 volt DC source, using the voltage divider equation ($V_R = V_{source}\frac{R}{R_{total}}$). The thermistor resistance values seen in column 3 were taken from an Omega-published table for the model 44004 thermistor. A "scatter" plot graphs temperature as a function of voltage, and a "trendline" plotted by the spreadsheet program attempts to match the data points to a mathematical formula. In this particular case, the fitted formula happens to

be Temp = 168.2 * (Voltage) − 13.6. It is this formula you must enter into the DAQ software, so it knows how to translate the measured voltage signal into a temperature value.

If the sensor you choose does not have a data table describing its characteristics, you may generate your own by subjecting it to known stimuli and measuring its resistance at those known values. Then, you may use a spreadsheet to plot the voltage response and derive an equation to fit the data.

Another huge advantage of using a computer spreadsheet to model the signal voltage as a function of temperature is that it allows you to "experiment" with different values of fixed resistance, to see the effect it has on linearity. By entering a new fixed-resistor value into the spreadsheet, you may immediately see the effect that value change has on the curvature of the scatter plot, as well as the effect it has on the signal voltage strength.

Common mistakes:

- Choosing a poor-accuracy calibration standard (e.g. trying to calibrate your $1500 precision Rosemount pressure transmitter to ± 0.1 PSI using a $30 pressure gauge that only reads to the nearest 5 PSI!).
- Improperly configuring the spreadsheet scatter plot to generate a fitted equation (e.g. having variables on wrong axes)

Characterizing your sensor and scaling the DAQ software should take no more than one full lab session (3 hours) if the team is working efficiently!

Lab Exercise – Ethernet data transfer

An essential part of this lab exercise is to have the acquired data transported over an Ethernet network. Each team's tool locker DAQ is equipped with an Ethernet port, and software is freely available for polling data over Ethernet using any personal computer. You are encouraged to install this free software on your own laptop PC and experiment with it independent of your teammates. Part of the capstone challenge at the end of every quarter (for those students who have completed this course) will include use of a DAQ on your own personal computer.

If you are familiar with C-language programming, there is a free C library called `libmodbus` which may be used to write your own data polling software to acquire data from any Modbus-compliant DAQ unit. Examples of Modbus programming using the `libmodbus` library are shown in the Modbus section of the *Lessons In Industrial Instrumentation* textbook. Writing your own polling code is fairly advanced DAQ usage, but is certainly within the capabilities of any student who has programmed any of the lab's caSCADA systems. A convenient computing platform to use for this code-writing is a Raspberry Pi, a single-board computer running the Linux operating system that is available for very modest cost.

Another Ethernet-related objective in this lab exercise is using the `ping` utility to test for network connections. When two personal computers have been successfully connected to a common Ethernet network, you should be able to "ping" one computer from the other by invoking the `ping` utility with the IP address of the destination computer as an argument to the `ping` command. The ping query and response is part of the ICMP (Internet Control Message Protocol) specified in RFC 792. You may run the `ping` command from a command-line window on a Microsoft Windows operating system. More detailed instructions on the use of `ping` may be found in your *Lessons In Industrial Instrumentation* textbook.

A successful "ping" from one computer to another is a *necessary* condition for remote viewing of that computer's display, but it is not a *sufficient* condition. That is to say, although a computer that refuses to "ping" is definitely not ready to be logged into remotely, a computer that does "ping" without trouble may not necessarily be ready for remote login. Getting a successful "ping" from a computer is merely the first step in establishing full communication with it.

If a "ping" attempt proves unsuccessful, it means something is inhibiting communication between that device and the computer you're using to issue the ping. A good test to do in this circumstance is try "pinging" other devices on that same network. Any successful ping attempts will definitively prove OSI layers 1, 2, and 3 are all functional between those two points, since "ping" requires those three layers to function. Once you know which portion(s) of the network are functional, you may narrow the field of fault possibilities.

Network functions above OSI layer 3 (e.g. "firewall" software running on personal computers) are capable of inhibiting communication between devices on the lab's Ethernet network, including "ping" messages. For example, a firewall configured with a rule to drop or reject any ICMP communications will block all "ping" queries. If you decide to connect your own personal computer (laptop) to the lab's Ethernet network, you may find it easier to temporarily disable all security features on your personal computer to enable free and open communication between your computer and all other devices on the network. Just be sure to re-enable the security features when you are done, so your computer will not be unprotected the next time you connect to the Internet!

Lab Exercise – troubleshooting

The most important aspect of this lab exercise is *troubleshooting*, where you demonstrate your ability to logically isolate a problem in the system. All troubleshooting must be done on a system you did not help build, so that you must rely on others' documentation to find your way around the system instead of from your own memory of building it. Each student is given a limited amount of time to identify both the location and nature of the fault. All troubleshooting activities must be proctored by the instructor to assess proper diagnostic reasoning and technique.

The standard procedure involves a group of no more than four students troubleshooting the same faulted system, with the builders of that system playing the role of operators. All troubleshooters are given a two-minute period to individually identify a plausible fault based on observable symptoms and submit it in writing to the instructor for assessment. Those students whose faults are indeed plausible advance to the next round, where each one takes turns making diagostic tests on the system. One minute is given to each student for devising this test, but no time limit is placed on the execution of that test. Whenever someone decides enough data has been collected to pinpoint the location and nature of the fault, they declare to have reached a conclusion and submit to the instructor in writing for assessment.

Individual troubleshooting with a five-minute time limit is also an acceptable format, but this generally only works with small class sizes.

Failure to correctly identify both the general location and nature of the fault within the allotted time, and/or failing to demonstrate rational diagnostic procedure to the supervising instructor will disqualify the effort, in which case the student must re-try with a different fault.

A standard multimeter is the only test equipment allowed during the time limit. No diagnostic circuit breaks are allowed except by instructor permission, and then only after correctly explaining what trouble this could cause in a real system.

The instructor will review each troubleshooting effort after completion, highlighting good and bad points for the purpose of learning. Troubleshooting is a skill born of practice and failure, so do not be disappointed in yourself if you must make multiple attempts to pass! One of the important life-lessons embedded in this activity is how to deal with failure, because it *will* eventually happen to you on the job! There is no dishonor in failing to properly diagnose a fault after doing your level best. The only dishonor is in taking shortcuts or in giving up.

Common mistakes:

- Attempting to *visually* locate the fault.
- Neglecting to take measurements with your multimeter.
- Neglecting to check other measurements in the system (e.g. pressure gauge readings).
- Incorrectly interpreting the loop diagram (e.g. thinking you're at the wrong place in the system when taking measurements).
- Incorrect multimeter usage (e.g. AC rather than DC, wrong range, wrong test lead placement). This is especially true when a student comes to lab unprepared and must borrow someone else's meter that is different from theirs!

The purpose of every troubleshooting exercise is to foster and assess your ability to intelligently diagnose a complex system. Finding the fault by luck, or by trial-and-error inspection, is no demonstration of skill. Competence is only revealed by your demonstrated ability to logically analyze and isolate the problem, correctly explaining all your steps!

Troubleshooting takes a lot of lab time, usually at least two 3-hour lab sessions for everyone in a full class to successfully pass. Budget for this amount of time as you plan your work, and also be sure to take advantage of your freedom to observe others as they troubleshoot.

Lab Exercise – decommissioning and clean-up

The final step of this lab exercise is to decommission your team's entire system and re-stock certain components back to their proper storage locations, the purpose of which being to prepare the lab for the next lab exercise. Remove your system documentation (e.g. loop diagram) from the common holding area, either discarding it or keeping it for your own records. Also, remove instrument tag labels (e.g. FT-101) from instruments and from cables. Perform general clean-up of your lab space, disposing of all trash, placing all tools back in their proper storage locations, sweeping up bits of wire off the floor and out of junction boxes, etc.

Leave the following components in place, mounted on the racks:

- Large control valves and positioners
- I/P transducers
- Large electric motors
- Large variable-frequency drive (VFD) units
- Cables inside conduit interconnecting junction boxes together
- Pipe and tube fittings (do not unscrew pipe threads)
- Supply air pressure regulators

Return the following components to their proper storage locations:

- Sensing elements (e.g. thermocouples, pH probes, etc.)
- Process transmitters
- "Jumper" cables used to connect terminal blocks within a single junction box
- Plastic tubing and tube fittings (disconnect compression-style tube fittings)
- Power cables and extension cords
- Adjustment (loading station) air pressure regulators

Finally, you shall return any control system components to their original (factory default) configurations. This includes controller PID settings, function block programs, input signal ranges, etc.

file i00350

Question 112

Capstone Assessment (end of quarter)

This performance assessment tests your mastery of many important instrumentation concepts. You are to automate a pre-built process based on prototype diagrams you sketch of all instrument connections, and demonstrate the automatic control of this process. All this must be done individually with no assistance from anyone else, within one continuous time block not to exceed three hours. You may refer to manufacturer documentation and/or textbooks, but not to personal notes, while building your loop.

You are entirely responsible for figuring out how the process works and what you must do to control it, based on your inspection of it after it has been selected for you. This includes identifying the process variable, the final control element, any loads, instrument model numbers, and locating manufacturer's documentation for the instrumentation.

You may perform the assessment activity at any time in the quarter. Successful completion counts as the "mastery" portion of the course exam(s). There will be no grade penalty for repeated attempts, however successful completion of this activity is required to pass the course.

In addition to exhibiting a steady-state control in automatic mode (i.e. the process variable follows changes made to the setpoint and settles at or near the setpoint value without oscillation after some time), the process must also meet the following criteria based on courses you have completed:

- If you have passed or are currently taking the *INST241* course, your transmitter and controller must be properly configured to register the process variable (in engineering units, not percent) over a range specified by the instructor. Note: if the transmitter is analog rather than "smart," the instructor will have you determine its "As-Found" range and direct you to range the loop controller to match the transmitter rather than calibrate the analog transmitter to a specified range.
- If you have passed or are currently taking the *INST252* course, the controller must be tuned for robust response to perturbations (changes) in either setpoint or load as selected by the instructor at or near a setpoint value also specified by the instructor. "Robust" control is defined here as the controller compensating for perturbations as quickly as possible without creating any process variable oscillations (i.e. a *critically damped* response). It will be your decision to use P, I, D, or any combination thereof in the controller's tuning.
- If you have passed or are currently taking the *INST260* course, you must connect a data acquisition unit (DAQ) to record a variable in the process selected by the instructor and display a trend graph and/or a scaled representation of the measured variable on a personal computer networked to the DAQ. For example, if you are instructed to display the controller's output value using the DAQ, the display should register on a scale of 0% to 100% just like the controller's output is ranged from 0% to 100%. If the DAQ needs to show the process variable, it must register that variable in the same range as the transmitter. If your DAQ provides a trend graph, the vertical scale markings of that trend graph must be similarly ranged.

Given the time constraint of this assessment, you will not be required to cut and fit flexible conduit to the field instruments. All other wiring must be neatly installed so as to avoid creating safety hazards (tripping, etc.) and confusion for other students assembling their loops.

Limited availability of components and physical space in the lab means that only a few students will be able to work on this assessment at once, so plan on attempting this *well before* the final due date!

Capstone assessment check-list (listed in sequential order) Name: _____

Bring a printed copy of this check-list with you when beginning the capstone assessment! Remember that you must work independently once the instructor assigns you a vest to wear. Any consultation with classmates, use of personal notes, or deviation from your approved diagram(s) will result in immediate disqualification, which means you must take everything apart and re-try the capstone assessment on a different process. Any damage done to the process or instrumentation will similarly result in disqualification, and you must repair the damage prior to re-trying the capstone assessment. You are allowed to use manufacturer documentation, as well as any documentation provided by the instructor (e.g. textbooks).

No teamwork is allowed while wearing the vest!

Selection	(Instructor writes/checks)
Instructor assigns a vest for you to wear	
Instructor selects a process for you to automate	
Instructor selects process variable range (*INST241 only*)	
Instructor selects setpoint/load & SP value (*INST252 only*)	@ SP =
Instructor selects DAQ variable to measure (*INST260 only*)	
Instructor selects controller – **label with your name!**	
Instructor verifies no wiring connected to the process	

The time clock starts now! **Start time:** _____

Criterion	(Instructor verifies)
You sketch basic loop diagram – instructor verifies correctness	
You sketch DAQ connection diagram – instructor verifies correctness	

Now you may begin wiring and configuring the components

Criterion	(Instructor verifies)
Steady-state control in automatic mode	
Controller correctly registers the process variable (*INST241 only*)	
Controller responds robustly to perturbations (*INST252 only*)	
DAQ measurement correctly scaled and/or graphed (*INST260 only*)	

The time clock stops now! **Stop time:** _____

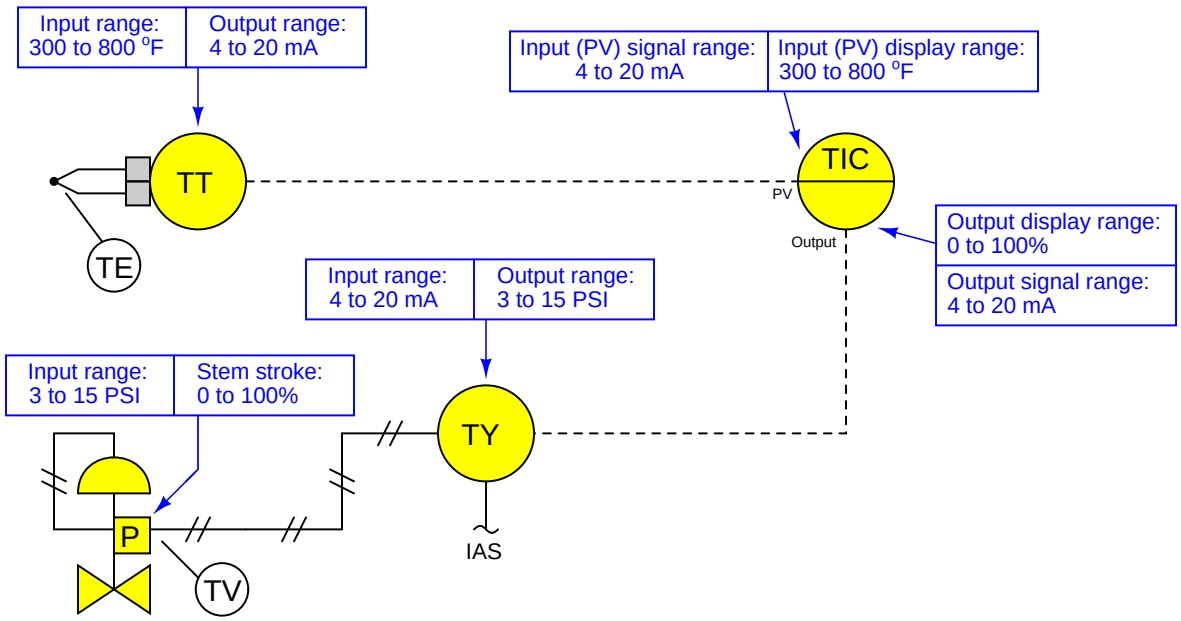
Criterion	(Instructor verifies)
Instructor verifies all signal wires/tubes disconnected	
Instructor verifies controller reset to original configuration	
Instructor verifies DAQ is returned to team tool locker	
Instructor collects your diagrams	

Your mastery score will not be recorded until all steps are complete!

Notes on instrument ranging

An important configuration parameter for any practical measurement or control system is *process variable ranging*. This entails setting both the transmitter and indicator/controller to a specified measurement range, with the controller indicating the process variable in real "engineering units" (e.g. PSI or degrees F rather than just percent). The following tutorial describes how this works and which configuration parameters to modify in a variety of different control systems found in the Instrumentation lab room.

The reason this is an issue at all is because loop controllers operating on 4-20 mA analog signals don't "know" what those signals are supposed to represent unless someone configures the controller with the proper range reflecting real-world conditions. For example, if a student is assigned a temperature transmitter with a range of 300 to 800 degrees Fahrenheit, not only does the transmitter have to output 4 mA when sensing 300 ^{o}F and output 20 mA when sensing 800 ^{o}F, but the controller must display an indication of 300 ^{o}F when it receives a 4 mA signal from the transmitter, and display an indication of 800 ^{o}F when it receives a 20 mA signal from the transmitter. None of this happens on its own – the student must range the transmitter for 300-800 ^{o}F input (and 4-20 mA output) as well as range the controller to display 300-800 ^{o}F over its 4-20 mA input scale. A typical loop is shown here with all instrument ranges displayed:



Analog (non-"smart") transmitters, I/P transducers, and valve positioners are ranged using "zero" and "span" adjustments, typically screws or nuts. The ranging of analog instruments is discussed in the "Instrument Calibration" chapter of the *Lessons In Industrial Instrumentation* textbook.

Digital ("smart") transmitters and valve positioners are ranged by setting LRV and URV parameters using a "communicator" device or a personal computer equipped with the appropriate interface and software. This too is discussed in the "Instrument Calibration" chapter of the *Lessons In Industrial Instrumentation* textbook.

Digital electronic loop controllers contain parameters specifying the process variable (PV) ranges. The following page lists examples of PV range configuration parameters for several different makes and models of loop controllers.

- Siemens/Moore 352 controller: process variable range parameters are located in the "Operator's Display" function block (FB15):
  → LRV = *Process Lo*
  → URV = *Process Hi*

- Siemens/Moore 352P and 353 controller: process variable range parameters are located in the "Analog Input" function block (AIN):
  → LRV = *Minscale*
  → URV = *Maxscale*

- Emerson DeltaV DCS: process variable range parameters are located in the "Analog Input" function block (AI) and "PID" function block (PID):
  → (AI block) = the *OUT_SCALE* parameter contains both high and low range limits, engineering units (e.g. deg F), and decimal point position. The *L_Type* parameter needs to be set to "indirect" to allow scaling to occur ("direct" mode prohibits scaling), and the *XD_Scale* parameter needs to be ranged 0 to 100%. Note that the "direct" and "indirect" options for *L_Type* have absolutely nothing to do with "direct" and "reverse" PID controller action, which is configured elsewhere.
  → (PID block) = the *PV_SCALE* parameter contains both high and low range limits, engineering units (e.g. deg F), and decimal point position. Note: the PID block's *PV_SCALE* range must exactly match the *OUT_SCALE* range of the AI block!

- Honeywell UDC 2500 controller: process variable input #1 range parameters are located in the "Input 1" set-up group of parameters:
  → LRV = *IN1 LO*
  → URV = *IN1 HI*

- Automation Direct "SOLO" controller: process variable range parameters are located in the following registers:
  → LRV = *P3-4 Input Range Low*
  → URV = *P3-3 Input Range High*

- Allen-Bradley PLC5, SLC500, and MicroLogix controllers: process variable scaling parameters are typically located either in a "Scale" instruction (SCL) or a "Scale with Parameters" instruction (SCP). In either case, the instruction takes the raw count value from the input channel's analog-to-digital converter and scales it into the desired process variable display range. A YouTube video on our BTCInstrumentation channel shows how to do this for the networked MicroLogix PLCs in the lab using the SCP instruction. *Note: SCP instruction parameters may be edited online. For this reason, downloading edits is not necessary for the MicroLogix PLCs in our lab. In fact, it is very important that you <u>not</u> save or download the PLC program, because doing so may alter the PLC's network address and lead to communication problems. Just make the changes while the PLC is in "Run" mode and then exit the program*:
  → (SCL instruction) = *Rate* and *Offset* values scale the signal according to the slope-intercept formula $y = mx + b$, where *Rate* is $10000m$ and *Offset* is b
  → (SCP instruction LRV) = *Scaled Min.*
  → (SCP instruction URV) = *Scaled Max.*

- Allen-Bradley Logix5000 controller: process variable scaling parameters are located in the "PID" instruction (PID):
  → LRV = *.MINS*
  → URV = *.MAXS*

- caSCADA "`pid`" control program: process variable scaling parameters are located in one of the source code files which must be modified using a text editor program, then recompiling the `pid` program so the new parameters may take effect. This control program may be initiated from the Linux command line by typing `./pid` and pressing the Enter key, after which a set of instructions will appear on the screen showing the default LRV and URV range values, and which file to find these parameters within. After editing and saving this file, you will need to type `make` at the Linux command line and press Enter to recompile the program. Finally, type `./pid` and press Enter to initiate the recompiled program.
  → LRV = *pid[0].LRV*
  → URV = *pid[0].URV*

file `ranging`

Notes on controller action

An important set of configuration parameters for any control system are *controller action* and *PID tuning*. Proper controller action means that the control system reacts to setpoint changes and process variable disturbances in the correct direction (e.g. a temperature control system that acts to reduce heat input when the process variable is above setpoint). Proper PID tuning means that the control system reacts to setpoint changes and process variable disturbances to an appropriate degree over time (e.g. a temperature control system that applies the right amount of additional heat input when the process variable goes below setpoint). A controller with the wrong action will cause a process to "run away" to one extreme value or the other. A controller with poor PID tuning will fail to achieve setpoint, and/or oscillate needlessly. The following is a list of configuration parameters to modify in a variety of different control systems found in the Instrumentation lab room.

If the controller happens to be programmed using function blocks, these important parameters will be found in the "PID" function block. For other controller models, there will be a menu option with action (direct/reverse) and tuning (P/I/D) parameters. Note that some controllers provide a quick-access feature to edit the PID tuning parameters, but generally not for changing the direction of action. Here are some examples:

- Siemens/Moore 352 controller: control action parameters are located in the "PID" function block (FB13). Note that the P, I, and D tuning parameters may be quickly accessed by pressing the "Tune" button rather than by entering the PID function block edit menu:
  → Direction (Direct/Reverse)= *SA1*
  → Proportional (P) = *SPG1* as a unitless gain value
  → Integral (I) = *STI1* in units of minutes per repeat
  → Derivative (D) = *STD1* in units of minutes

- Siemens/Moore 352P and 353 controller: control action parameters are located in the "PID" function block (PID). Note that the P, I, and D tuning parameters may be quickly accessed by pressing the "Tune" button rather than by entering the PID function block edit menu:
  → Direction (Direct/Reverse)= *DIR ACT*
  → Proportional (P) = *PG* as a unitless gain value
  → Integral (I) = *TI* in units of minutes per repeat
  → Derivative (D) = *TD* in units of minutes

- Emerson DeltaV DCS: control action parameters are located in the "PID" function block (PID) conforming to the FOUNDATION Fieldbus standard:
  → Direction (Direct/Reverse)= Found in the *CONTROL_OPTS* set of parameters as a "check-box" where a checked box sets direct action and an unchecked box sets reverse action.
  → Proportional (P) = *GAIN* as a unitless gain value
  → Integral (I) = *RESET* in units of seconds per repeat
  → Derivative (D) = *RATE* in units of seconds

- Honeywell UDC 2500 controller: control direction is located in the "CONTRL" set-up group of parameters, while the PID tuning coefficients are located in the "TUNING" set-up group of parameters:
  → Direction (Direct/Reverse)= *Action*
  → Proportional (P) = *PB* or *Gain* as a proportional band percentage or as a unitless gain value, respectively
  → Integral (I) = *I Min* or *I RPM* in units of minutes or repeats per minute, respectively
  → Derivative (D) = *Rate T* in units of minutes

Notes on controller action (continued)

- Automation Direct "SOLO" controller: process variable range parameters are located in the following registers:
  → Direction (Direct/Reverse)= *P3-7 Heating/Cooling*
  → Proportional (P) = *P1-4 Proportional band* as a proportional band percentage
  → Integral (I) = *P1-5 Integral time* in units of seconds
  → Derivative (D) = *P1-6 Derivative time* in units of seconds

- Allen-Bradley PLC5, SLC500, and MicroLogix controllers: control action parameters are located in the "PID" instruction. A YouTube video on our BTCInstrumentation channel shows how to do this for the networked MicroLogix PLCs in the lab (reading the PV on the first analog input and sending the output to the first analog output of the I/O card):
  → Direction (Direct/Reverse)= Found in the *Control Mode* field where E=PV−SP represents direct action and E=SP−PV represents reverse action.
  → Proportional (P) = *Controller Gain* K_c as a unitless gain value
  → Integral (I) = *Reset* T_i in units of minutes per repeat
  → Derivative (D) = *Rate* T_d in units of minutes

- Allen-Bradley Logix5000 controller: control action parameters are located in the "PID" instruction (PID):
  → Direction (Direct/Reverse)= E where PV−SP represents direct action and SP−PV represents reverse action.
  → Proportional (P) = K_p or K_c as a unitless gain value
  → Integral (I) = K_i in units of seconds per repeat
  → Derivative (D) = K_d in units of minutes

- caSCADA "`pid`" control program: control action parameters are located on the operator interface screen, above the trend graph. This control program may be initiated from the Linux command line by typing `./pid` and pressing the Enter key. Once the `pid` control program is running (reading the PV on analog input AIN0 and sending the output to analog output DAC0 of the LabJack DAQ), each parameter may be selected by pressing the `S` key as often as needed, and the parameter values changed by pressing the arrow and page up/down keys. Note that the control direction may only be switched while the controller is in manual mode. Tuning parameters may be altered in either manual or automatic modes.
  → Direction (Direct/Reverse)= will either show "`Direct-acting`" or "`Reverse-acting`"
  → Proportional (P) = `K_P` as a unitless gain value
  → Integral (I) = `K_I` in units of repeats per minute
  → Derivative (D) = `K_D` in units of seconds

Notes on controller tuning

For those who have never tuned a controller before but need to set the PID parameters for basic loop stability in automatic mode, here are some tips for setting the P, I, and D parameter values. Every PID controller provides means to alter the tuning coefficients named *proportional* (also called *gain*), *integral* (also called *reset*), and *derivative* (also called *rate or pre-act*). Settings which are virtually assured to yield stable control are as follows:

- **P** – a "gain" value of less than one (i.e. a "proportional band" value of at least 100%).
- **I** – a "reset" value of zero repeats per minute, or the largest value possible for minutes per repeat.
- **D** – a "rate" value of zero.

Mind you, these parameters will not yield *good* control, but merely *stable* control. In other words, these tuning parameter values will make the controller fairly unresponsive, but at least it won't oscillate out of control. Also bear in mind that having an integral (reset) value set for minimum action (i.e. zero repeats per minute, or very high minutes per repeat) will result in a controller that never quite makes the process variable value reach setpoint – instead, there will be a persistent "offset" between PV and SP with integral action essentially turned off.

file `control`

file i00998

Answers

Answer 1

Answer 2

Answer 3

Answer 4

Answer 5

Answer 6

Some of the different OSI layer 1 formats seen here:

- EIA/TIA-232
- EIA/TIA-485
- Bell 202 (HART FSK signals)
- DeviceNet
- Ethernet 10BASE-T (IEEE 802.3)
- IEEE 802.11g (wireless)

Some of the OSI layer 2 addressing schemes seen here:

- HART field device addresses
- MAC addresses for each personal computer

The personal computers are responsible for "wrapping" the disparate data streams into TCP/IP packets, which are then forwarded to the router over Ethernet, then transmitted over ISDN. Once in packetized form, they become portable over any network standard, requiring only a computer with an "understanding" of TCP/IP protocol to reassemble and "unwrap" at the receiving end(s).

Answer 7

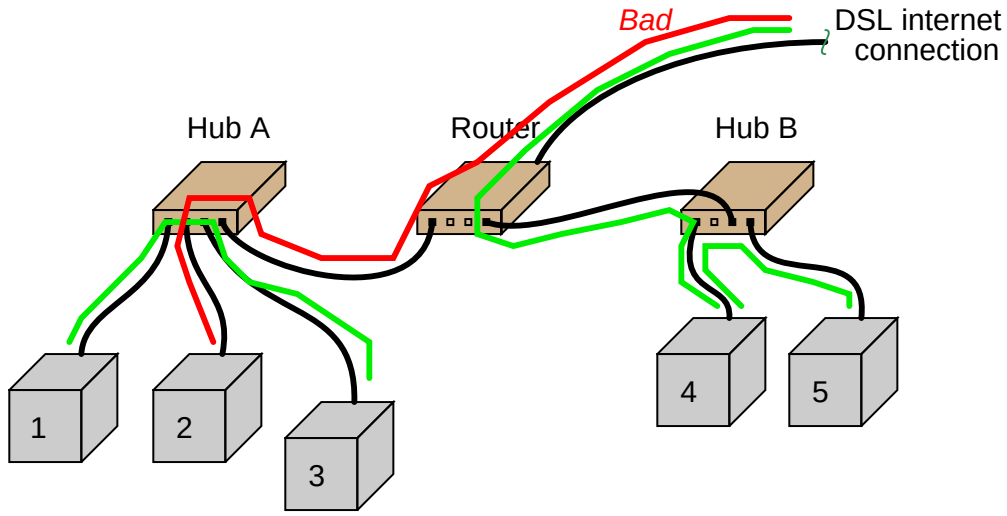
Answer 8

Partial answer:

Fault	**Possible**	**Impossible**
Hub A failed		
Hub B failed		
Router failed		√
Internet service provider failed		√
Cable failed between computer #4 and Hub B		
Cable failed between Hub A and Router		√
Cable failed between Hub B and Router		
Security settings (e.g. firewall) in computer #4		

Answer 9

"Good" paths shown in bright green, "bad" paths shown in bright red:



Suspect components include 2, cable between 2 and hub A, cable between hub A and router.

A good "next ping" test to do is to try pinging 1 or 3 from 2: that would test 2 as well as the cable between 2 and hub A. An alternative test would be to ping 4 or 5 from 1 or 3: that would test the cable between hub A and the router.

Answer 10

Partial answer:

Largest IPv4 address: `255.255.255.255`

Smallest IPv4 address: `0.0.0.0`

IPv4 uses a 32-bit address field. Therefore the total number of IPv4 addresses = 2^{32} = 4,294,967,296

Believe it or not we have already run out of IPv4 addresses (i.e. there are more IP-capable devices in existence than there are IPv4 addresses)!

IPv6 uses a 128 bit address field. Therefore the total number of IPv6 addresses = $2^{128} = 3.4028 \times 10^{38}$

Answer 11

IP stands for *Internet Protocol*, and it specifies how long blocks of data may be divided into smaller chunks called *packets*, how those packets may be re-assembled at the receiving end, and also how devices connected to a large network may be addressed both individually and by group.

TCP stands for *Transmission Control Protocol*, and it specifies (among other things) how to ensure integrity of communication in a network where data has been broken down into individual packets. In essence, TCP guarantees deliver of all data packets even when network connections are less than perfectly reliable, by acknowledging correct receipt of each packet and requesting re-transmission in the event of corrupted or lost packets.

Answer 12

Answer 13

Answer 14

Answer 15

Answer 16

Answer 17

Answer 18

Answer 19

Answer 20

Answer 21

Answer 22

Answer 23

Answer 24

Answer 25

Partial answer:

- Circuit #2: **Yes**
- Circuit #3: **No**
- Circuit #6: **Yes**
- Circuit #9: **No**

Hint: apply the Superposition Theorem to each circuit example, where the HART communicator is the only active signal source in the circuit, and see if the communicator's signal is able to reach the transmitter.

Answer 26

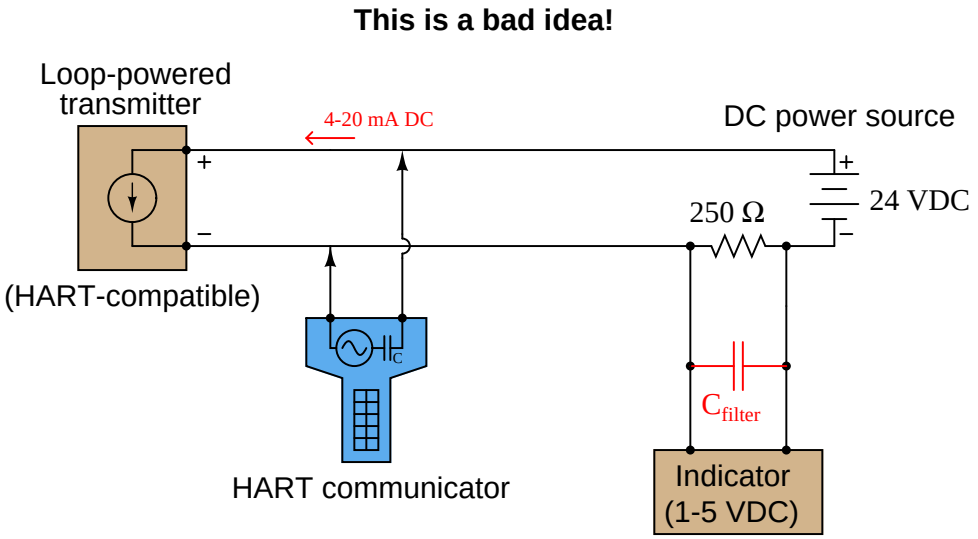
Answer 27

Answer 28

Answer 29

Answer 30

However you plan to filter the HART signals, resist the temptation to do this:



While placing a capacitor across the terminals of the indicator will bypass high-frequency AC HART signals around the indicator, it will also completely short out the HART data so the transmitter and communicator can't talk with one another!

I'll let you figure out a better method of HART signal filtering – one that blocks HART frequencies from getting to the indicator without killing the HART signals throughout the network.

Answer 31

Flow transmitter FT-38 is a Coriolis mass flow transmitter, simultaneously measuring mass flow rate, density, and temperature. Mass flow is the primary variable reported by this transmitter in 4-20 mA form, while the secondary and tertiary variables of density and temperature are extracted by FY-38c (a HART-to-analog converter) and reported to indicating recorders DIR-38 and TIR-38 in 4-20 mA form.

Answer 32

Answer 33

Answer 34

Answer 35

Answer 36

Answer 37

Answer 38

Answer 39

Answer 40

Answer 41

Answer 42

Answer 43

Answer 44

Answer 45

Answer 46

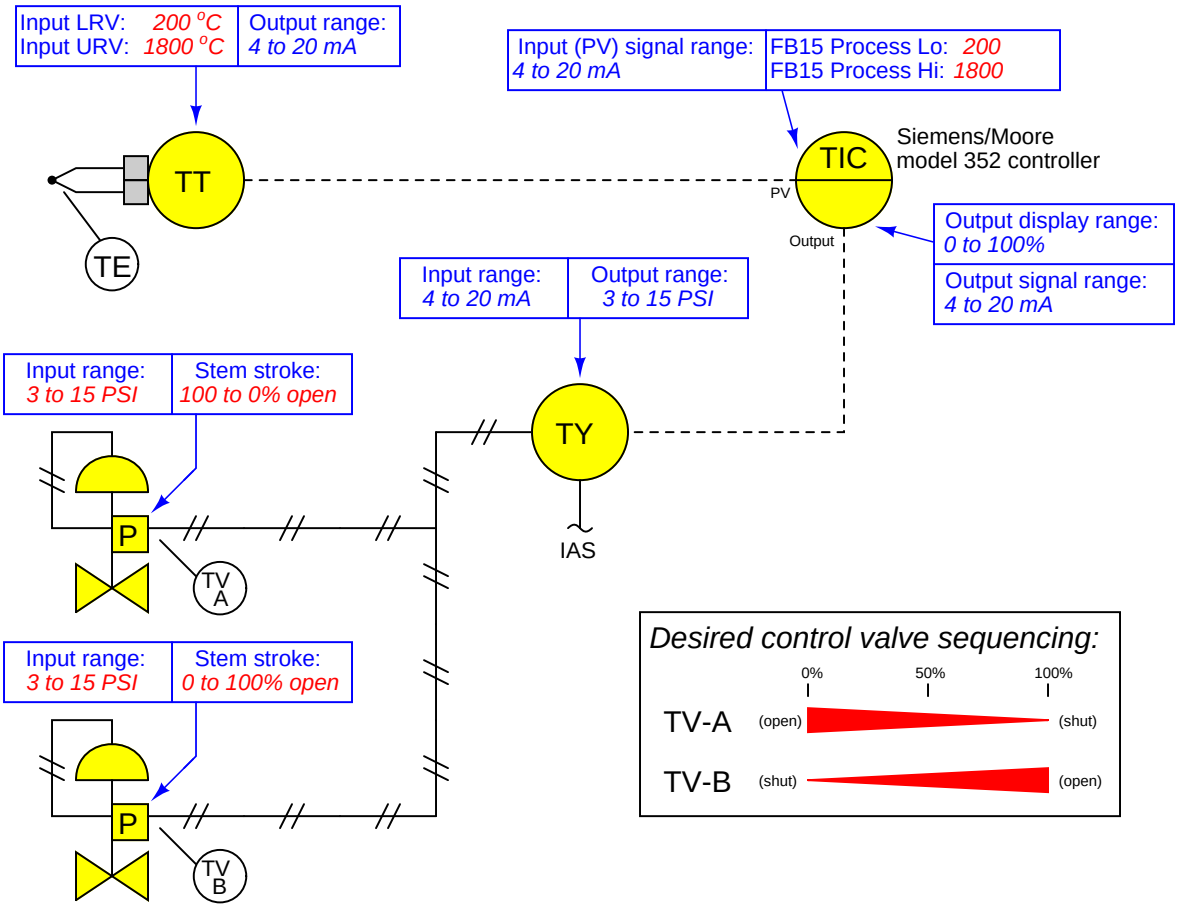
Partial answer:

How secure (i.e. difficult to guess) is your password? When you must change your password, how do you choose and remember a new one? *Here is a sample of one of the author's passwords (not currently being used):* `or2rtaor2ft`. *Kind of difficult to guess, wouldn't you agree? It's very easy to remember, though, because it is based on an easily-memorized phrase. In this particular case, the phrase is from the book "Lord of the Rings" – "One ring to rule them all, one ring to find them . . .", and the password is nothing more than the first letter from every word in this phrase (with the number "2" substituting for the word "to" in order to satisfy certain password systems requiring a mix of alphabetical and numerical characters). You can use song lyrics, poems, movie quotes, scripture verses, or any other easily-remembered phrases to generate very strong passwords in this same manner.*

Answer 47

Partial answer:

An easy way to limit the ability of hackers to disrupt process monitoring and control is to *write-protect* certain features of field devices. For example, HART instruments often come equipped with a small switch that may be set to the "write-protect" position on the physical device itself so as to prevent anyone from altering its configuration via the HART network. Hackers might be able to still read the process data, but at least they won't be able to tamper with the device configurations. The same may be said of the other field devices in this system: the PLC and the protective relays used to control power circuit breakers.


Input LRV: 200 °C
Input URV: 1800 °C
Output range: 4 to 20 mA
Input (PV) signal range: 4 to 20 mA
FB15 Process Lo: 200
FB15 Process Hi: 1800
TT
TE
TIC
PV
Output
Siemens/Moore model 352 controller
Output display range: 0 to 100%
Output signal range: 4 to 20 mA
Input range: 4 to 20 mA
Output range: 3 to 15 PSI
TY
IAS
Input range: 3 to 15 PSI
Stem stroke: 100 to 0% open
P
TV A
Input range: 3 to 15 PSI
Stem stroke: 0 to 100% open
P
TV B
Desired control valve sequencing:
0%
50%
100%
TV-A
(open)
(shut)
TV-B
(shut)
(open)

Answer 49

A *firewall* is a piece of software or hardware intentionally designed to limit connectivity between a private network (LAN) and the outside world (Internet) for the purposes of preventing malicious outsiders from gaining access to important resources on the LAN and/or preventing internal users from accessing certain information on the Internet.

The author recommends the following steps in formulating a security policy:

- Identify all important system functions
- Identify all authorized users of the system
- Carefully map those users to those functions
- Identify how each function shall be kept secure
- Forbid any other use of the system

Filtering firewalls pass or block data packets based on the content of those packets, in a manner similar to how routers direct IP packets on the Internet. These firewalls make no attempt to authenticate the user.

Proxy servers are separate machines that make connections between the LAN and the Internet. Application proxies act as intermediary agents in all data transactions related to certain applications (e.g. web browsing, FTP file transfer, telnet remote access). SOCKS proxies connect different TCP ports together to form complete communication channels between the LAN and the Internet.

Answer 50

An *active* attack involves writing information to the network or system, while a *passive* attack only involves reading information.

A *man-in-the-middle* attack is where the attacking entity intercepts data communicated between two end-points and alters the data's authentication signature(s) so as to pose as the legitimate sender, when in fact the attacker is the real (last) sender to each receiving party. For example, a hacker broadcasting radio data to a WirelessHART network in order to send false messages to the control system that appear to be sent from a legitimate transmitter (and also sending false messages to the transmitter disguised to look as though they came from the legitimate wireless Gateway).

Password sniffing is when an attacker monitors an unencrypted channel of communication to record any passwords sent along that channel. Some password-locked systems do not encrypt the passwords, but rather allow those passwords to be communicated "in the clear" where anybody recording the transaction would be able to monitor those passwords. A *dictionary attack* is the use of a database containing commonly-used words to guess a password by trial and error. Such an attack assumes that the user's password will take the form of normal words, which suggests a way to thwart such an attack is to not use common words when formulating passwords!

Answer 51

Firewalls are systems intended to limit the flow of data between different interconnected systems with the purpose of improving security. Three basic types of firewall criteria exist: **packet filtering**, **stateful inspection**, and **stateful protocol analysis** (otherwise known as deep packet inspection).

Packet filtering consists of screening certain data packets from passing through the firewall based on compliance with pre-programmed rules (i.e. the Access Control List). Filtering criteria include source IP address, destination IP address, network protocol, TCP port, and direction of flow.

Stateful inspection refers to additional filtering functionality where the firewall monitors the expected and actual states of the encountered packet(s). Since TCP employs "handshaking" as part of the procedure for establishing a connection between machines, every TCP packet should exist in one of three different states: established, usage, and termination.

Stateless protocols such as UDP do not benefit from this sort of firewall filtering, because their packets don't come with defined states.

Stateful protocol analysis (a.k.a. "deep packet inspection") goes a step further by having the firewall analyze the contents of the packet itself to see if it makes sense for the application using that data. In order for this to work, the firewall must be "aware" of the intended application and what constitutes valid data for that application. This kind of firewalling may screen packets based on parameters such as argument size, out-of-sequence commands, combinations of packets (e.g. email text with email attachment), etc.

Answer 52

Answer 53

Answer 54

Answer 55

Answer 56

Answer 57

Answer 58

Answer 59

Answer 60

Answer 61

Answer 62

Note: a common synonym for a set of firewall *rules* is an *ACL* (Access Control List).

Answer 63

Answer 64

Hint: *LSM*

Answer 65

Several vulnerabilities exist in this system, and there is *definitely* more than could be done to enhance security than merely configuring a DMZ!

Answer 66

Partial answer:

The results, of course, will vary with your particular computer and operating system. On Microsoft Windows operating systems, you may access the firewall settings through Control Panel. On Linux operating systems, the command `iptables` is used to display and modify firewall rules.

Answer 67

Hint: the red-brick graphic objects shown in several illustrations are supposed to represent *firewall* devices installed in the network.

LAN = Local Area Network, which refers to networks within the span of one network medium (e.g. within the reach of a single Ethernet network) typically restricted to the physical perimeter of the site. *WAN* = Wide Area Network, which refers to networks reaching outside the physical site perimeter, typically spanning multiple media.

BTC's Instrumentation lab hosts multiple LANs: one general-purpose "shop" network connecting PLCs, panel-mounted controllers and HMIs, and other process control devices together; two dedicated redundant Ethernet networks connecting all Emerson DeltaV DCS components together; and finally, the campus wireless network for student access to the internet is another example of a LAN. That last LAN, however, connects to the WAN hosted by the Washington State Community and Technical College system (CTC) which spans the state and provides connectivity to the internet at large.

Three security measures:

- Create Demilitarized Zones (DMZs) for IP-based networks. *This involves the use of multiple firewalls to create an intermediate network through which no direct connections are allowed.*
- Install cryptographic security modules on insecure networks. *The used of VPN devices and comparable encryption/decryption end-points on a network help guard against hacking by making all communications along that network segment more difficult to interpret or spoof.*
- Monitor all activity on vulnerable networks. *This is the least hardware-intensive, consisting of systems monitoring all communications through critical "choke points" in the network, which will alert information security personnel in the event of suspicious activity.*

A *DMZ* (DeMilitarized Zone) is a segment of a digital network isolated from other segments by two firewall devices. The rules programmed into the two firewalls are exclusive of each other, which means no direct communication from outside one firewall to outside the other firewall is possible (i.e. no data is allowed to simply pass through the DMZ). Data-server computers located within the DMZ relay all data passing between the two outside networks, according to processes allowing only legitimate communication. This dual-firewall strategy makes hacking "through" the DMZ much more difficult than if just a single firewall were used.

Stateful firewalls, by tracking the state of all communications, limits the potential for unsolicited network traffic. This makes hacking more difficult, because the only harmful data allowed through the firewall must be in response to a valid request for data from within the protected zone. Stateless firewalls, by contrast, simply allow the passage of data based on data type, not the context of the "conversation" happening between devices.

Answer to Socratic Question about hacking a DMZ: In order for data to go through a DMZ, it must successfully pass through the first firewall to reach a server (or some other computer) within the DMZ, which processes that data and forwards it in an acceptable format to be able to pass through the second firewall. If this server machine becomes compromised in the right way, any communication may be subsequently permitted through the DMZ.

Answer 68

Answer 69

Answer 70

Answer 71

Answer 72

Answer 73

Answer 74

Answer 75

Answer 76

Answer 77

Answer 78

Answer 79

Answer 80

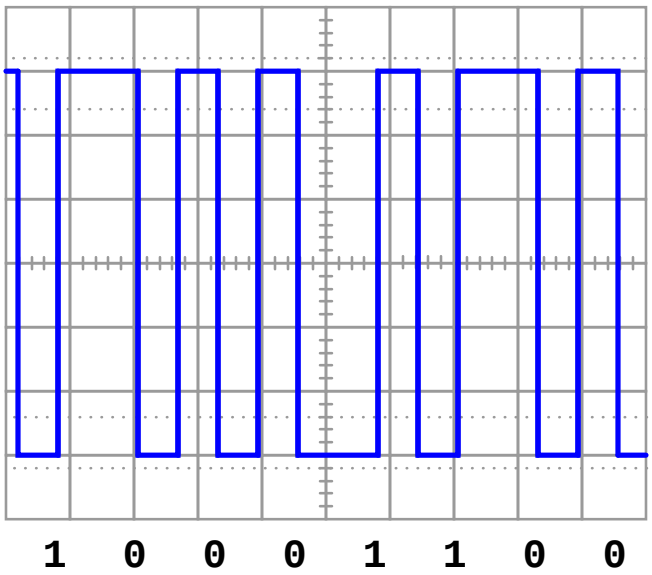
Answer 81

Answer 82

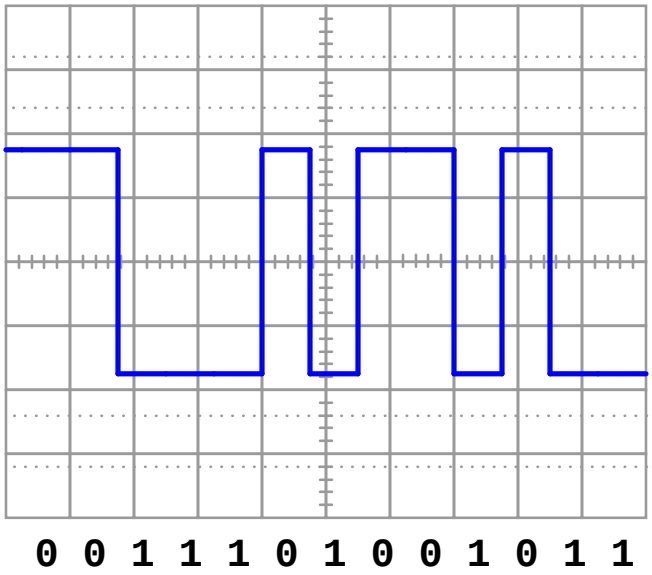
Note: *spear phishing* is a term used to describe an email message sent with malicious intent, disguised as coming from a friendly source. Unlike a regular "phishing" email which simply invites the recipient to visit a hyperlink or download an infected attachment, a "spear phishing" email is disguised to look as though it originated from a trusted sender in order to lure more recipients.

Answer 83

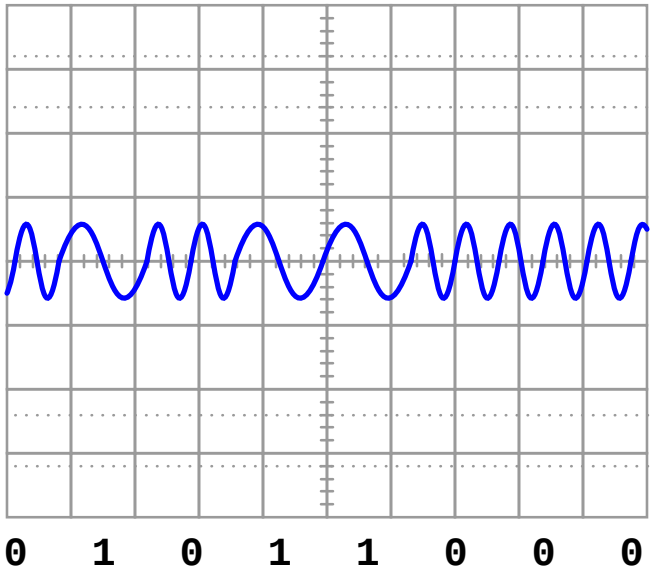
(Manchester encoding)



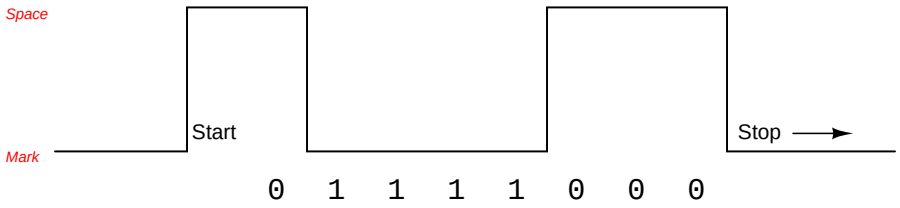
(NRZ encoding)



(FSK encoding)



Answer 85



Answer 86

The bias voltage provided by these resistor values will meet the EIA/TIA-485 standard for voltage at a receiver device (−200 mV), but not for voltage at a transmitter device (−1.5 V). Thus, the noise margin is compromised, and the system may not perform to the standard in a noisy environment.

Answer 87

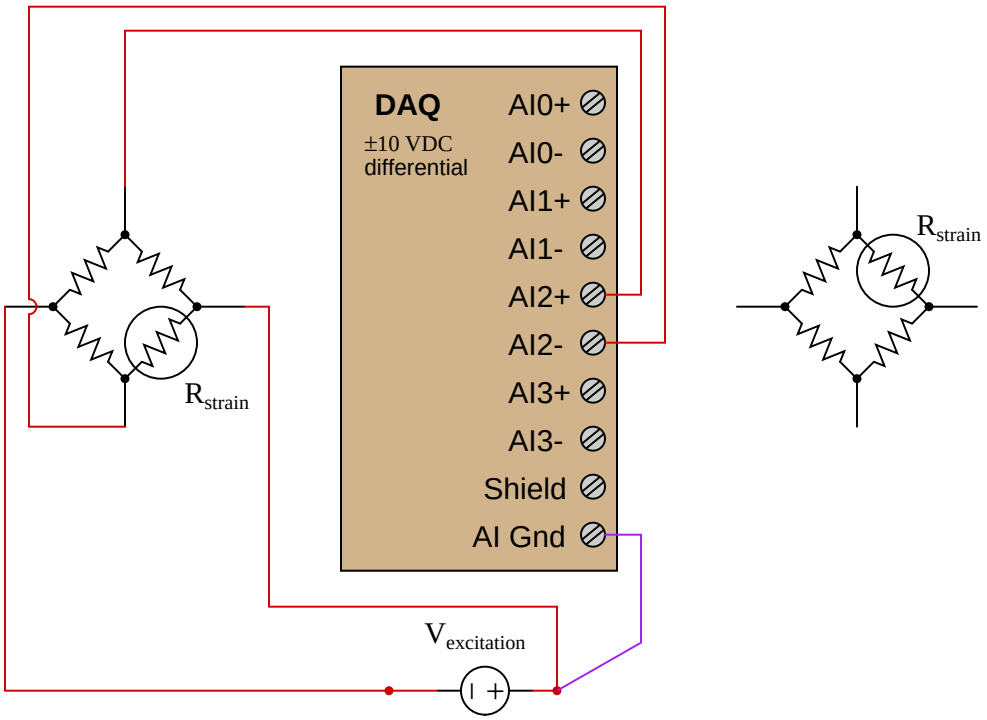
Partial answer:

Input voltage (volts)	Percent of span (%)	Counts (decimal)	Counts (hexadecimal)
1.6	32	1310 or 1311	
	73.8	3022	
	40		666
3.18			A2F

Answer 88

Partial answer:

Note that this is not the only valid solution:



The connection to the AI Gnd terminal is necessary to satisfy the bias current requirements of the instrumentation amplifiers inside the DAQ module.

Answer 89

Answer 90

You may locate the `grades_template` on the `Y:` network drive at BTC, provided you log in to the computer system using your individual student ID and password (not a generic login such as "btc"). It is also available for download at the *Socratic Instrumentation* website.

Answer 91

There are only eight valid ciphers in the octal system (0, 1, 2, 3, 4, 5, 6, and 7), with each successive place carrying eight times the "weight" of the place before it.

- 35_8 into decimal: 29_{10}
- 16_{10} into octal: 20_8
- 110010_2 into octal: 62_8
- 51_8 into binary: 101001_2

Answer 92

There are sixteen valid ciphers in the hexadecimal system (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F), with each successive place carrying sixteen times the "weight" of the place before it.

- 35_{16} into decimal: 53_{10}
- 34_{10} into hexadecimal: 22_{16}
- 11100010_2 into hexadecimal: $E2_{16}$
- 93_{16} into binary: 10010011_2

Follow-up question: why is hexadecimal considered a "shorthand" notation for binary numbers?

Answer 93

`1011 1000 0100` or `1011 1000 0101`

Answer 94

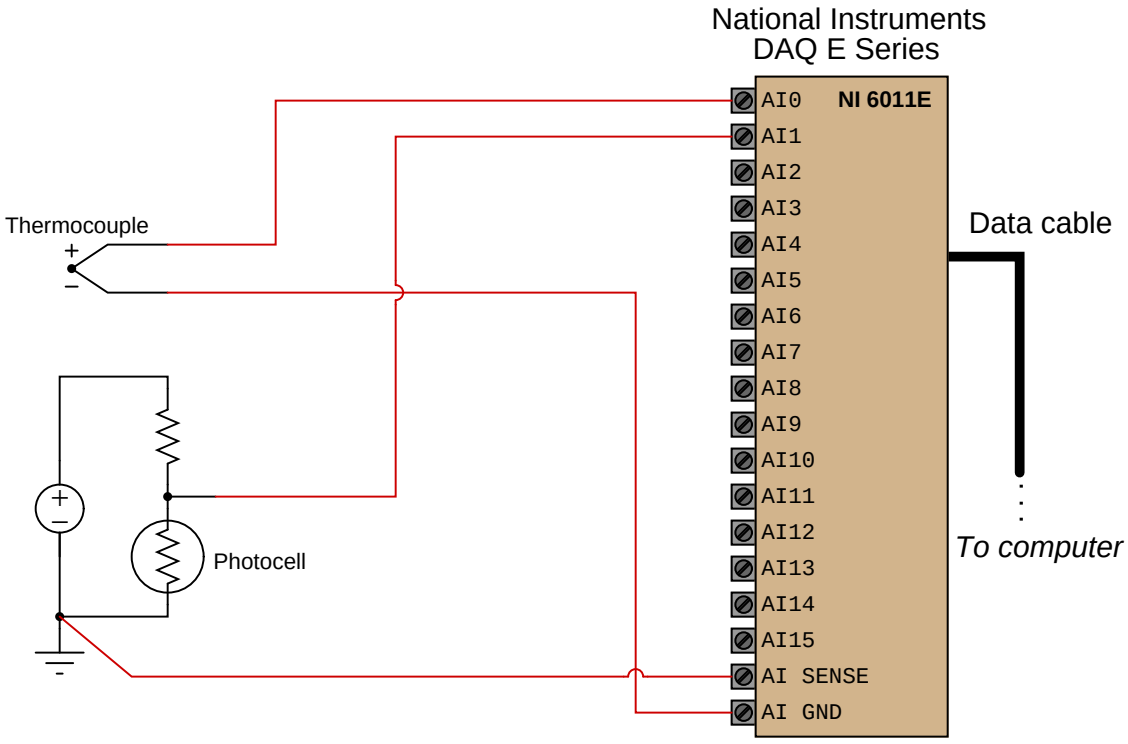
`0110 1011 0111` or `0110 1011 1000`

Answer 95

`0100 0111 1010` or `0100 0111 1011`

Answer 96

This is one possible solution:



Channel	Mode	First terminal	Second terminal
0	RSE	AI0	AI Gnd
1	NRSE	AI1	AI Sense

Answer 97

The reason why we must abandon 4-20 mA signaling in a multidrop HART network should be obvious if you understand the characteristics of parallel DC circuits: the total current is the *sum* of all branch currents.

Unique HART addresses are necessary to ensure the ability to communicate to and from specific transmitters, one at a time.

In burst mode, the field instrument does not wait to be polled by a master device; instead, it continually broadcasts data to the HART network.

You may connect a HART modem or communicator in the following locations in a multidrop network:

- In parallel with the two wires, anywhere along the cable length
- In parallel with the connection terminals of instrument #1
- In parallel with the connection terminals of instrument #2
- In parallel with the connection terminals of instrument #3
- In parallel with the resistor

Unique addressing is required because this "bus" network is *broadcast* by nature.

Answer 98

The HART isolator filters out HART signals to or from one positioner from getting to the other positioner.

We *might* communicate with control valve TV-1b, depending on the high-frequency AC characteristics of the controller output. Certainly, the isolator prevents us from communicating with TV-1a, so we know we can't talk to it. However, the only way we can talk to the other valve from these connection points is if the HART signals are able to "pass through" the controller output. If the controller output acts as an ideal current source, it should block the HART signals completely, and our communicator will talk to no valve at all.

Control valve TV-1a carries the cooling fluid while control valve TV-1b carries the heating fluid. As process temperature rises, the reverse-acting controller decreases its output signal. This will drive TV-1a further open and TV-1b further shut.

Answer 99

Figure 1:
$R_{AB} = 500\ \Omega$

Figure 2:
$R_{AB} = 750\ \Omega$

Figure 3:
$R_{AB} = 1.511\ \text{k}\Omega$

Figure 4:
$R_{AB} = 940\ \Omega$

Figure 5:
$R_{AB} = 880\ \Omega$

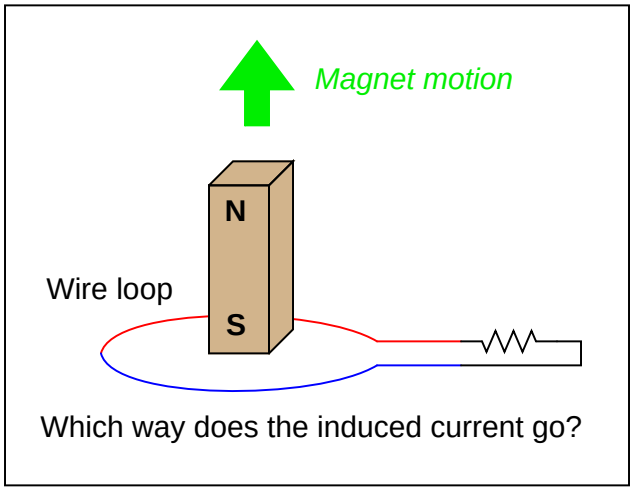
Figure 6:
$R_{AB} = 80.54\ \Omega$

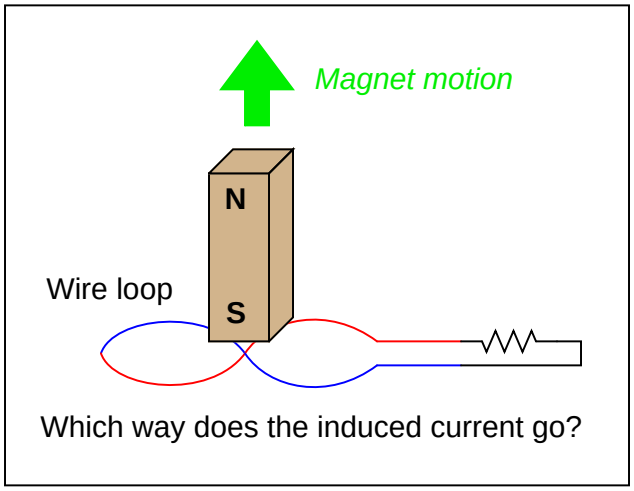
Note that the circuit in figure 4 is a "trick:" two of the resistors contribute absolutely nothing to R_{AB}!

Answer 100

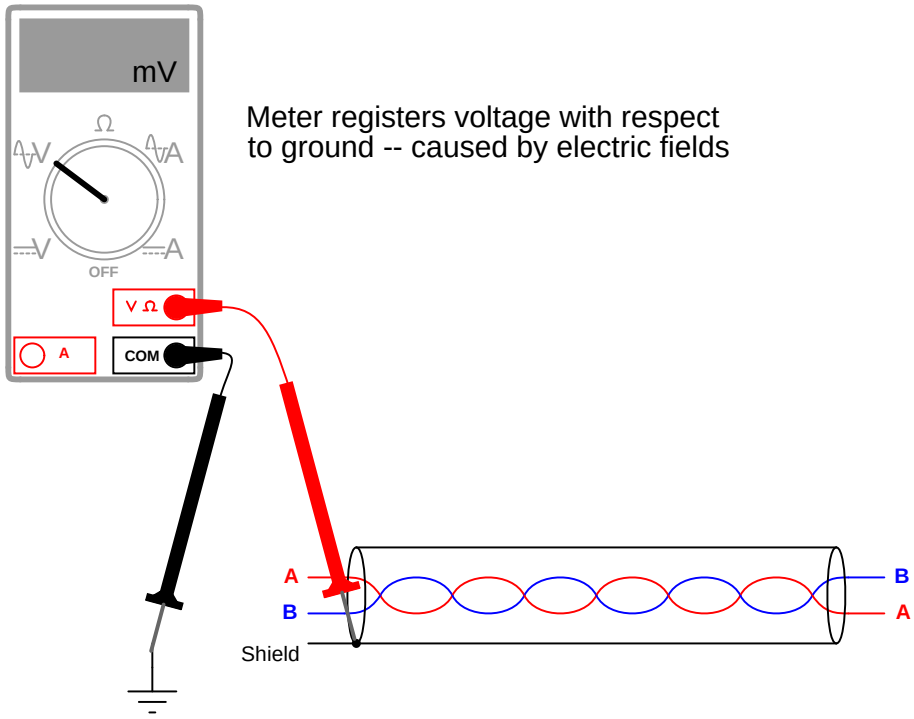
Shielding guards against electric fields by creating a zero-potential surface around the wires to act as a terminal point for any external electric fields. Thus, the space inside the cable is free from external electric fields by virtue of the shield.

Twisting the wires ensures that a current loop will never be formed to allow electromagnetic induction from external (changing) magnetic fields. The following "thought experiment" comparing two scenarios proves this conclusively:





Demonstration of how to measure electric field noise voltage:



Answer 101

This is a graded question – no answers or hints given!

Answer 102

This is a graded question – no answers or hints given!

Answer 103

This is a graded question – no answers or hints given!

Answer 104

This is a graded question – no answers or hints given!

Answer 105

This is a graded question – no answers or hints given!

Answer 106

This is a graded question – no answers or hints given!

Answer 107

This is a graded question – no answers or hints given!

Answer 108

This is a graded question – no answers or hints given!

Answer 109

This is a graded question – no answers or hints given!

Answer 110

This is a graded question – no answers or hints given!

Answer 111

There exist some inexpensive data acquisition modules on the market for personal computers, including some with USB interfaces (and most with RS-232 serial interfaces). If all you have is a serial-interface module and a USB-only computer (as most laptop computers are!), you may use a USB-to-serial adapter to connect the serial DAQ device to the personal computer. Within Microsoft Windows, you may force the operating system to recognize the USB adapter as an old-style COM 1 or COM 2 RS-232 serial device, at which time the DAQ software should "talk" through the adapter to the DAQ module seamlessly.

In order to meet the project standard of data communication via Ethernet with a non-Ethernet DAQ module, you will have to use an intermediary personal computer to poll the DAQ over its serial cable connection, and then use "Remote Desktop" software on another personal computer to view the display of that intermediary personal computer (the remote access taking place over an Ethernet network). `RealVNC` is an example of a very powerful third-party remote access application which may be used for this purpose.

Answer 112

The only "answer" to this question is a properly documented and functioning instrument loop!