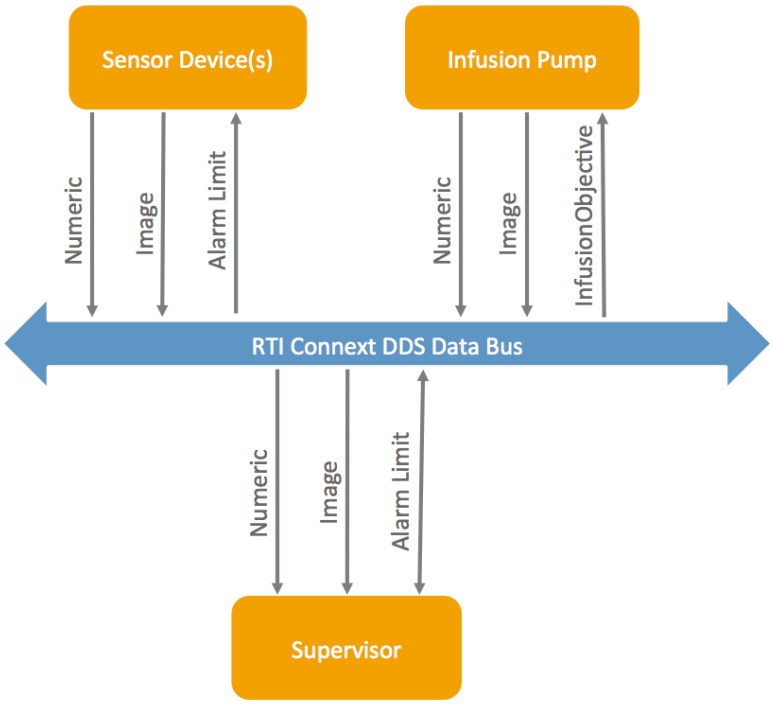
Integrated Clinical Environment (ICE) Overview:

The ICE system contains simulated devices that monitor patient data, a simulated infusion pump that monitors a drug to a patient, and a supervisor app that displays patient vitals, alarms, and is used to control the valid ranges for the system. For example, the supervisor app can decide what a valid pulse rate is for a patient. The supervisor app and the device apps can both show alarms in certain circumstances.



What's in the system?

Simulated devices:

- Simulated devices send their device ID, an image representing the device, and numeric data such as patient vital signs. Simulated devices receive alarm limits that tell them the ranges of vital sign values that should produce an alarm (in the case where the device can display an alarm).

Devices send and receive much more than this, but for simplicity we will describe only some of the important values.

Infusion pump:

- The infusion pump produces and consumes a lot of the same data as the other devices, but it also needs to be able to receive a command telling it to stop infusing immediately.

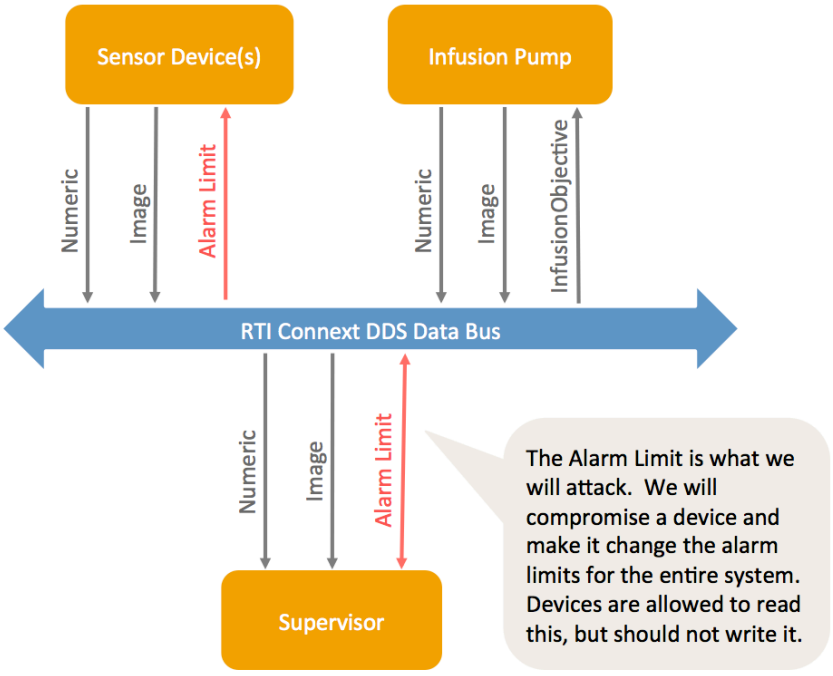
Supervisor:

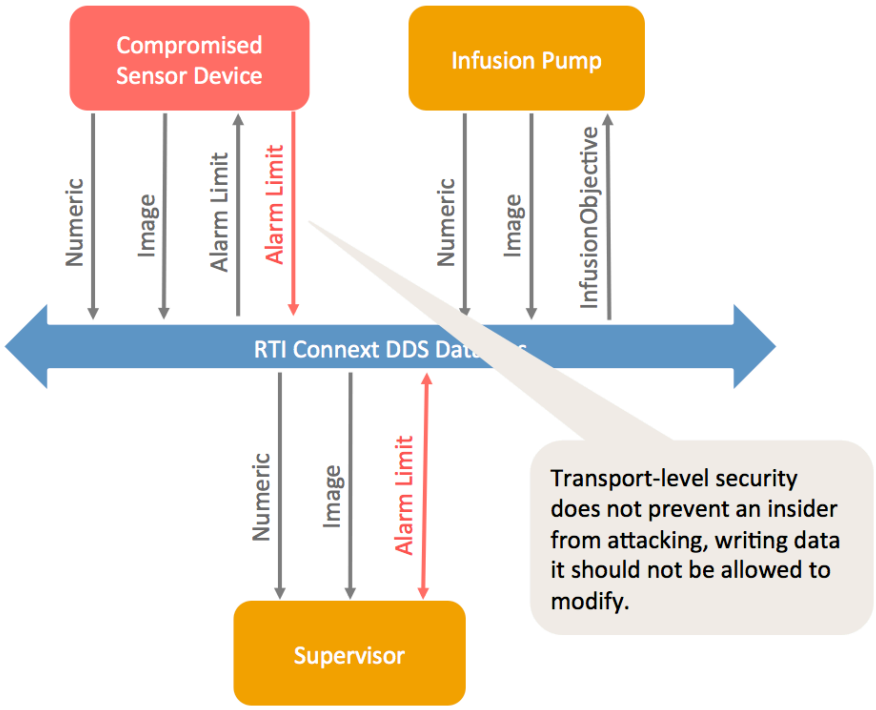
- The supervisor receives the device IDs, images, and vital signs from the devices. It receives the status of the infusion pump.
- The supervisor sends and receives alarm limits, which are used to define what the valid ranges are for each vital sign. Both the supervisor and some devices use these values to decide whether to display an alarm. Or not. This is what we will compromise.

Exercise 2:

Overview:

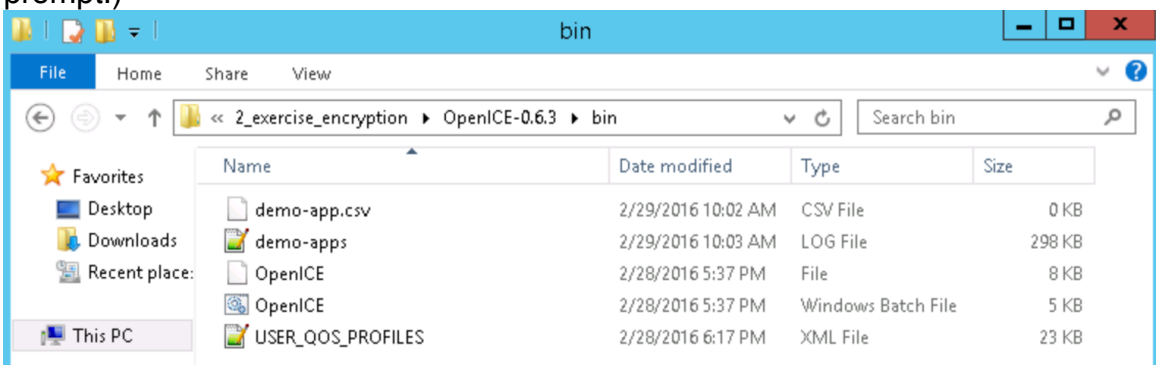
This exercise is taking a look at the ICE demo, with security enabled that is equivalent to transport-level security such as TLS/DTLS. In this exercise, we will show that an insider – in this case, a compromised device– can damage the system.





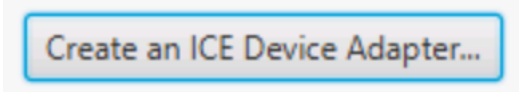
Steps:

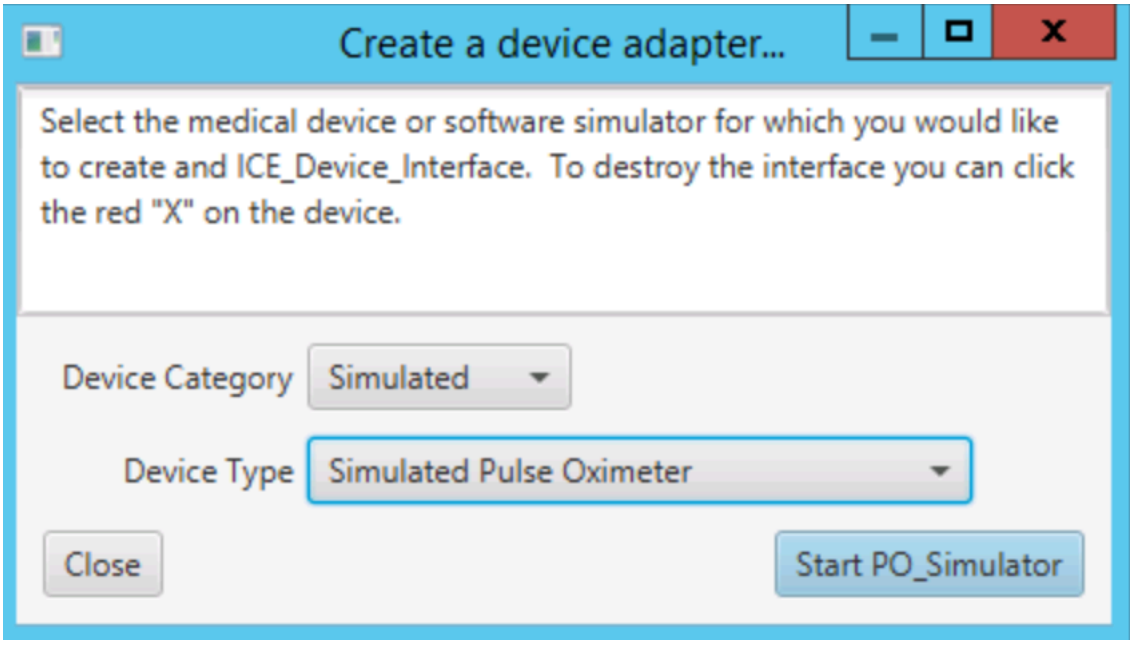
1. Go to the exercise 2 OpenICE-0.6.3\bin folder. Run the OpenICE.bat file. (**Note:** for the purposes of these exercises, you must always run the open ICE project from within the <exercise>\OpenICE-0.6.3\bin directory, either by double-clicking it from the windows GUI or changing into that directory at the command-prompt.)



2. Keep the application in domain 0 (the default)
3. Click on "Start ICE_Supervisor"

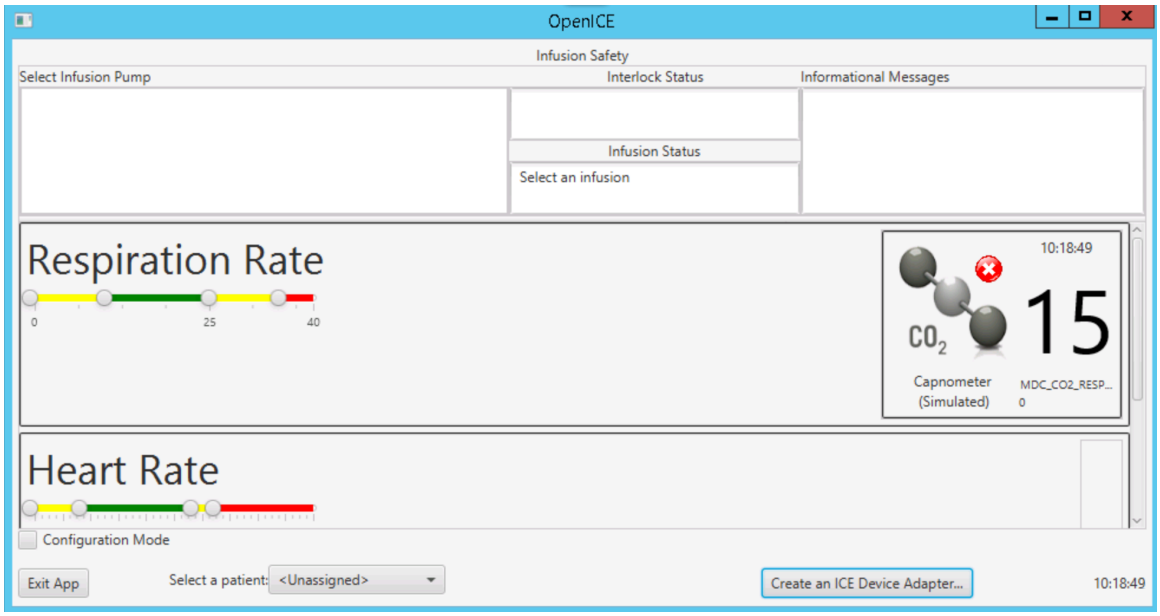
1. Click on "Create an ICE Device Adapter" in the lower-right-hand and create a Simulated Pulse Oximeter. (This is our compromised application). It shows up with a funny icon, but it's really just a pulse oximeter application that's been modified to send data it should not send.



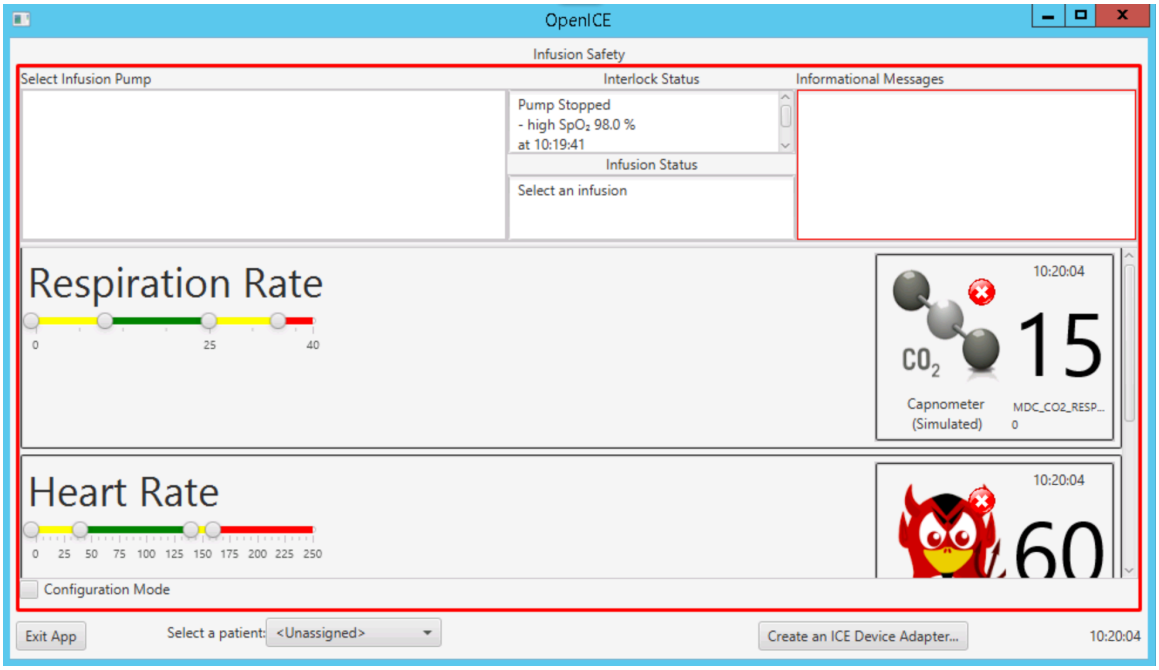


2. To make the system more realistic and interesting, use the same steps to "Create an ICE adapter" to create an Infusion Pump and a Simulated Capnometer.
3. Open up the Infusion Safety application. This application allows you to visualize patient vital signs as a patient is receiving an infusion of painkillers.

4. You should see an alarm appear, because our compromised Pulse Oximeter app is changing system-wide values it should not be allowed to modify. Making an alarm appear when there is none is *one* way to hurt a system, but much more damaging in the real world would be to make an alarm not appear when it should.



Application in Normal State, Showing Capnometer Data



Application in Alarm State with Compromised Device: Note that the infusion pump has been stopped due to the (false) patient alarm. So a patient with normal vital signs is being denied a painkiller due to the compromised app.

Advanced Steps:

5. Optionally, you can open rtiddsspy and Wireshark following the steps in Exercise 1 to confirm that the data is indeed encrypted – you can't find the values that you saw in exercise 1.
6. View the governance.xml file to see how encryption was enabled. The security configuration has configured encryption with no read or write access control:

```
- <domain_access_rules>
  - <domain_rule>
      <domain_id>0</domain_id>
      <allow_unauthenticated_join>FALSE</allow_unauthenticated_join>
      <enable_join_access_control>TRUE</enable_join_access_control>
      <discovery_protection_kind>ENCRYPT</discovery_protection_kind>
      <liveliness_protection_kind>ENCRYPT</liveliness_protection_kind>
      <rtps_protection_kind>SIGN</rtps_protection_kind>
    - <topic_access_rules>
      - <topic_rule>
          <topic_expression>*</topic_expression>
          <enable_discovery_protection>TRUE</enable_discovery_protection>
          <enable_read_access_control>FALSE</enable_read_access_control>
          <enable_write_access_control>FALSE</enable_write_access_control>
          <metadata_protection_kind>ENCRYPT</metadata_protection_kind>
          <data_protection_kind>ENCRYPT</data_protection_kind>
        </topic_rule>
      </topic_access_rules>
  </domain_rule>
</domain_access_rules>
```