Description of CPS for ECE462 (undergraduate) and ECE599 (graduate) Final Project –

Students must develop a 'threat model" for an Smart City Urban Monitoring System deployed in an urban area (e.g. 25 sq. miles or 40x40 city blocks) and complete a report detailing the security exposures, risks and mitigation strategies. See **ECE462FinalProjectInfrastructureDiagram sp2018.pptx** for details on architecture used to implement the Smart City Urban Monitoring System.

The report for both ECE462 and ECE599 must include the following:

- Assets
- System Layers
- Attack Surfaces & Entry Points
- Trust Levels
- Use Scenarios
- Assumptions and Dependencies
- Data Flow Diagram of "operational system" under evaluation
    - Context/Level 0 Diagram
    - Level 1 Diagram
    - Level 2 Diagrams – expect 13-17 diagrams needed to cover project
- Threats (STRIDE) - STRIDE-per-Element analysis tables (one per Level 2 DFDs)
- Threat Tree(s) – Structured List
- Vulnerabilities (CVSS - Common Vulnerability Scoring System)
- Risk Assessment
- Mitigation Strategy

ECE462 Project Reports should be at least 10 pages (including diagrams, charts, tables, etc.) single-spaced 12pt font. The reports must include all the elements listed above.

ECE599 (graduate) students must also complete the following:

- Create and implement the threat model of the project using Microsoft's Threat Modeling tool
- Project reports should include all the elements listed above, plus include Threat Model Tool diagrams and analysis results. Description of the model attributes, constraints, challenges and other key design decisions needed to support the Threat Modeling Tool should also be included in the project report.
- The ECE599 project reports should be at least 15 pages (including diagrams, charts, tables, etc.) single-spaced 12pt font.
- ECE599 students must provide a copy of their Threat Modeling Tool files for review
- ECE599 students must be prepared to present their model and results to the professor and students during class. (note: This may not be practical. May consider presenting in separate meeting and/or after projects have been turned in.)

Microsoft Threat Modeling Tool Getting Started, User Guide, and Application can be found at - https://www.microsoft.com/en-us/download/details.aspx?id=49168 . The Getting Started and User Guide is also available on the class BlackBoard portal.

Threat Model/Assessment Process:

1. Understand Adversary View

1.1. Entry Points & Exit Points
1.2. Which Assets are of Interest
   - Collect Data
   - Trust Levels
2. Create a Data Flow Diagram
3. Determine, Investigate and Assess the Threats
   3.1. STRIDE – Identify and define the threats
   3.2. Threat Trees to assess vulnerabilities using Structured List
   3.3. CVSS to Characterize Vulnerabilities and Risk
   3.4. Create security threat model to analyze risk (e.g. risk assessment)
4. Mitigate Threats – Mitigation Strategy
5. Validate Mitigation Strategy (out of scope for project)

Smart City Urban Monitoring System

Key Features:

- Smart LED Light Fixture on every light-pole in the city. Light Fixture supports three levels of light output: OFF, On-Low, On-High. Light levels are controlled by intensity of natural light (sunrise and sunset) and activity in the area (car traffic and human traffic). Light levels can also be set from central control office via the mess network. Operational information for each Light Fixture is transmitted to the central office via the mesh network every 15mins. Updates to the Light Fixture controller is done on the first Sunday of each month at 12am.
- Sensor Array on every light-pole in the city. Light-poles exist on the corner of every street and in the middle of each block. Number of total Sensor Arrays/Light Poles = [(2xCBNS)+1] x [(2xCBEW)+1] where CBNS = number of North-South city blocks in the grid & CBEW = number of East-West city blocks in the grid.
- Capabilities of the Array –
    - Ambient temperature
    - Air Quality (CO2, Ozone, Dust, Smoke)
    - Rain Fall
    - Wind Speed and Direction
    - Sound Levels & Sound Event Detection
    - Road Surface Temperature
    - Density of Human Traffic
    - Power provide via Light Pole
- Software Environment of Sensor Array
    - Custom Embedded System Code
    - No operating system
    - Arduino IDE used in code development
- Sounds Events Detectable by Sensor Array
    - Gun Shot
    - Sirens, Alarms
    - Glass Window Breaking
    - High Crowd Noise
    - Screams

    - Dog Barking
    - High Traffic Noise
    - Water Running (High Water Run-off)
    - Gas Leak
- Communications (sensor array) – Mesh Network
    - ZigBee Network/Protocol (http://www.zigbee.org/zigbee-for-developers/network-specifications/zigbeepro/) – also see files referenced below are in BlackBoard class portal
    - Redundant Messaging
    - Periodic Scanning – verify node availability
    - CRC Data Checking
    - Node Time Synchronization
    - Supports two-way communications to Sensor Array and LED Light Fixture.
- Code Updates – scheduled for first Sunday in month at 12am.
- Node Synchronization – every day at 2am
- Central Office Systems – Management and operated by external vendor.
    - All systems use a Windows based operating environment and communicate over a wired/wireless Ethernet network using TCP/IP.
    - Data Collection and Analysis Servers (Database, DAS/SCADA/DCS, Historian)
    - Application Servers (example apps – City Events Calendar, Venue Scheduling, Parking Availability, …) – Wired (Ethernet) access to Internet for public consumption of information.
    - Configuration/Code Update /Node Synchronization Server
    - Alerts/Feeds Servers – Wired (Ethernet) access via WWW for "customers" with authentication & encryption.
    - Smart LED Light Fixture control server
    - HMI Workstations
    - Internal Wireless Network for local PC/Workstation access to servers
- Services Provided by Central Office Server (Contracted Services provided by external vendor)
    - Correlation of City Events and Data Collected, Hazard Alerts
    - Sound Event Analysis and Location Services, Event Alerts
    - Road Service Temperature Analysis, Snow/Ice Alerts
    - Crowd Analysis, Human Congestion Alerts
    - Traffic Analysis, Motor Vehicle Congestion Alerts
    - Micro Climate Analysis, Location Specific Weather Alerts
    - Air Quality Alerts
    - Real-time Feeds of sensor data and/or analytics (customized to customer needs)
- Services and Data provided to ….
    - Police
    - Fire Department
    - Emergency Medical Services, Ambulance Services
    - Hospitals
    - Department of Transportation
    - Road Maintenance
    - City Hall & Major's Office
    - Air Quality Administration
    - HUD and Homeless Services Department
    - Public Web Site
    - Department of Homeland Security

- Example Actions taken from Alerts and Data Feeds
    - Stop Light Control (DOT)
    - Dispatch of Parking Lot/Space Management
    - Dispatch of Police, Fire Department, Ambulances
    - Dispatch of Snow Removal & Sand/Salt Road Services
    - Restriction of Landscape/Construction Equipment by Air Quality Administration
    - Dispatch of Utility Maintenance Crews (water, gas, street lights, sensor array)
    - Automated Alerts to Public Web Site
    - Dispatch by Homeland Security
- Access Model to Services
    - Real-time Feed, data streamed on every update from array
    - Real-time Alerts
    - Query-on-Demand, clients can access active data (last 12 months) and analysis via assigned accounts
    - Query-on-Demand, access and analysis of archived data (beyond past 12 months)
- Maintenance
    - Repair and/or Replacement of Sensor Array takes 1 month (min)
    - Diagnostics executed on each Sensor Array monthly

ZigBee Reference Document Files (available on ECE462 BlackBoard Class Portal:

zigbee-specification.pdf

zigbee-pro-stack-profile-2.pdf

IJRITCC_ZigBeeTechStudy.pdf

ZigbeeProtocolMicrochipStackAN965.pdf

See **ECE462FinalProjectInfrastructureDiagram sp2018.pptx** for details on architecture used to implement the Smart City Urban Monitoring System.

Smart City Urban Monitoring System – Constraints, Rules and Assumptions

Control Center Components:

- The SCADA server is the only system element that can access the mesh network, sensor arrays and LED street lights.
- The SCADA server can request and receive sensor, parameter and status data from the sensor arrays.
- The SCADA server can send and receive data from the Database Server
- The DAS is a temporary data store in the SCADA server, holding 24 hours of the most recent data.
- The SCADA server can notify the Application server each time new sensor data is received.
- The SCADA server can transmit and receive configuration data to/from the sensor arrays and mesh network.

- The SCADA server can perform diagnostics on the mesh network, sensor arrays and LED street lights.
- The SCADA server access Config. Data from the Config. Server

- The Configuration Data is stored on the Config. Server.
- Configurations can be entered into the Config. Server via the Eng. Workstation (Config. Tool) or USB Key.

- For any operation that requires actions from both the SCADA and Config. Servers (e.g. config and test an array), communications between the two systems is supported.

- The Data Analytics Server can only request and send data to/from the Database Server.
- The Data Analytics Server can receive request for compute services from the SCADA Server, Config. Server and the Application Server.

- The Application Server can request and receive data from the Database Server and the Historian.
- The Application Server can send data (e.g. data feeds/alerts) to the Database/Archive Server and the Alerts/Data Feeds Server in the Services Center.
- The Application Server can notify the Application Server in the Services Center that new data/alerts have been transferred.

- The Eng. Workstation only communicates with the Config. Server.
- Any network failures are identified and displayed on the Eng. Workstation.
- All diagnostics, config. updates and code updates to the sensor array, mesh network, and firewall is handled through the Eng. Workstation.

- The HMI only communicates with the SCADA Server.
- All sensor data and sensor array diagnostics is viewed via the HMI.

- The Database Server and Historian are simple data stores.

- The Sensor Arrays send raw (unencrypted) data across the mesh network.
- The only deep processing provided at each sensor array is for sound event detection (e.g. FFTs).

- Only authorized entities can transfer data through the Firewalls (authentication at each Firewall).
- There are no authentication services provided in the Control Center. Each server will only respond to requests from other servers specified in these constraints, rules and assumptions.

Service Center Components:

- The Application Server can send and receive data from the Database/Archive Server, the Alerts/Data Feeds and the Event Calendar.
- The Application Server can send notifications to external government agencies and partners.
- The Application Server can send notifications to people/organizations on the internet.

- The Visualization Workstation can send/receive request/information from the Application Server.

- The Event Calendar, Database/Archive Server and Alerts/Data Feeds Server are simple data stores.

- Authorized Entities on the internet or from government agencies can access data on the Alerts/Data Feeds Server and the Event Calendar. Authentication services provided by an LDAP server running on the Application Server.

Mesh Network:

- Auto-routing and re-routing
- Auto-reconfig based on re-routing history
- Config. Server monitors node messaging performance (run-time and scheduled outage)
- SCADA Server monitors node sensor performance via periodic diagnostics (run-time and scheduled outage).

List of System Operations to be analyzed for Security Threats:

Notes:

1. When developing Data Flow Diagrams note that some servers contain both processes and data stores.
2. Numbers in () represent number of Level 2 Data Flow Diagrams expected.

Control Center –

- LED Street Light Control (1)
- Retrieve, record, analyze sensor data (includes database, data analytics and SCADA servers) (2-3)
- Configure, diagnose, maintenance for sensor array infrastructure (3-4)
    - Includes sensor controller synchronization, periodic scanning for availability/function check, code updates, mesh message routing table updates
- Historian Services (1)
- Mesh message re-routing operation (from sensor array controller to control center and from control center to sensor array controller) (1)
- Applications for City Agencies (Alerts and Data Feeds) (3)
    - Correlation of City Events and Data Collected, Hazard Alerts
    - Sound Event Analysis and Location Services, Event Alerts
    - Road Service Temperature Analysis, Snow/Ice Alerts
    - Crowd Analysis, Human Congestion Alerts
    - Traffic Analysis, Motor Vehicle Congestion Alerts
    - Micro Climate Analysis, Location Specific Weather Alerts
    - Air Quality Alerts
    - Real-time Feeds of sensor data and/or analytics (customized to customer needs)

Services Center –

- Database and Archive Services (publicly available information) (1)
- Application Server Services (creates publicly available information stored in data feeds/alerts server) (1)

    - City Event Calendar
    - Venue Scheduling and Availability
    - Sidewalk/Street Congestion Map
    - Sound Levels Map
    - Air Quality/Temp./Wind Levels Maps
    - Visualization services to workstations in services center
- Alerts and Data Feeds to City Agencies (1-2)
    - Correlation of Control Center Alerts with City Events Calendar, Venue Scheduling and Parking Lot Data (note: parting lot data comes from external entity and/or an independent system)

ECE462/599 Final Project Report Expected Content (Rubric)

The following provides more details on what is expected in the ECE462/599 final project report. The high level report sections defined in the CPS Project Description file remains the same and is copied below. The detailed added in this "report expectations document" defines the minimum required elements expected in the reports and what part of your final report grade each represents. I have reduced the extent of a typical report in an attempt to reduce the documentation required. My goal is to have the report focus on the most important operations in the system and the most critical security threats for each of those operations. We can discuss in class if you have any questions.

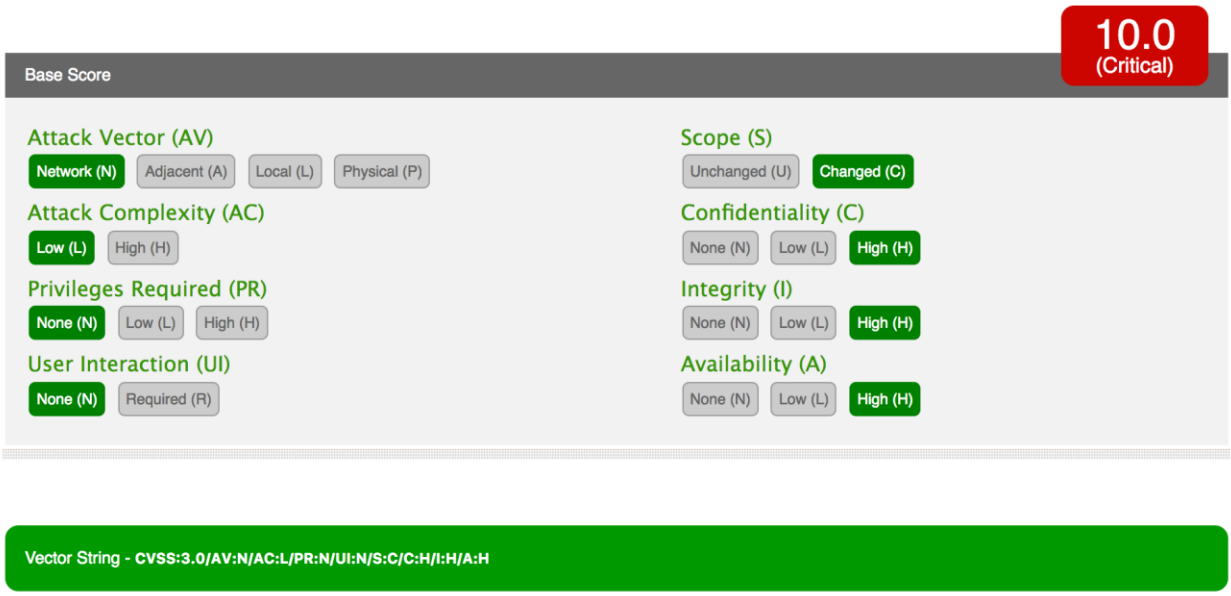
The report for ECE462/ECE599 must include the following -
Notes:
- ECE599 students using the Threat Modeling Tool can leverage the output of the tool to create the STRIDE-per-Element Structured List
- ECE599 students will also be evaluate on the accuracy/completeness of the "stencils/templates" created for the components needed to define the target CPS infrastructure in the Microsoft Threat Modeling Tool. Given these stencils/templates will be key to identifying the critical threats in the system, their completeness and accuracy will be evaluated as part of the "Threats" component of the rubric.
- Numbers in **blue** represent percentage of grade used in the rubric.

- **List of Assets** **(2%)**
- **System Layers** (diagram or list) **(2%)**
- **Attack Surfaces** (Entry/Exit Points) **(12%)**
- **Trust Levels** (List or highlighted on system diagram) **(2%)**
- **Use Scenarios** (**Provided** informally in project description) **(2%)**
- **Assumptions and Dependencies** (drives what threats/vulnerabilities will be in focus) **(20%)**
    - **List unique assumptions made in support of the analysis and assumptions/dependencies provided in project description.**
- **Data Flow Diagram** of "operations" under evaluation **(20%)**
    - Context/Level 0 DFD for entire system
    - Level 1 DFDs for entire system – expect 1
    - Level 2 DFDs per operations of interest (see list in project description) – expect 14-17 diagrams needed to cover all operations of interest.
- **Threats** (STRIDE) – STRIDE-per-Element analysis tables and structure list **(20%)**
    - STRIDE-per-Element analysis tables (one per Level 2 DFD)
    - Threat Tree(s) – STRIDE-per-Element Structured List
    - Provide 1-2 threat descriptions per STRIDE category per Level 2 DFD.

- Focus on the most critical threats for each STRIDE category.
- Expect approximately 180-200 (total) threat descriptions to be provided in the structured lists.
- Note – a STRIDE-per-Interaction approach is also acceptable.

- **Vulnerabilities** (CVSS analysis) **(20%)**
  - Select 3 of the most critical threats per operation analyzed (e.g. per Level 2 DFD)
  - **For CVSS analysis – Provide screenshot of analysis results from CVSS online tool (score + vector).**
  - Note: If assignment requested a DREAD analysis - Create Vulnerability Tables for the critical threat selected would need to be created. These tables would also include Risk Assessment.
  - Include Mitigation Strategy as part of each vulnerability analyzed (**Note** – this is the most important part of this component of the rubric, assuming you have identified the highest impact threats.)

Example Screenshot from CVSS tool:



General Illustrations of Smart Cities Infrastructure:

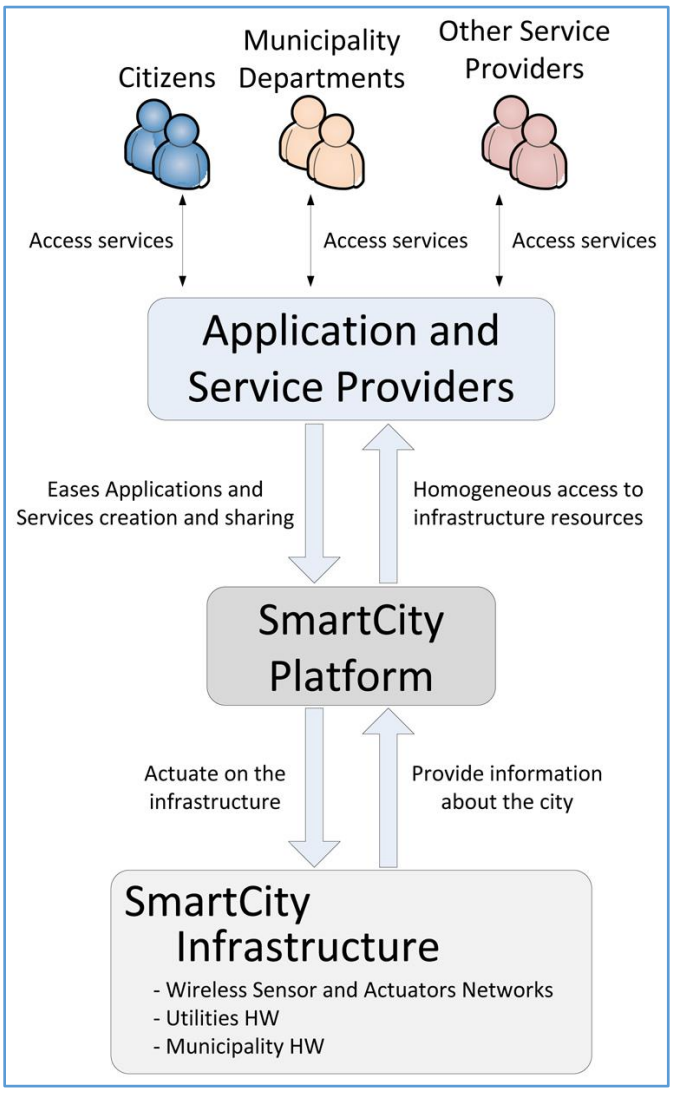


Figure 1. Generic Smart City Actors Interaction

Figure 2. CPS Reference Architecture for Smart City Infrastructure