ECE 462 Spring 2016 Class Calendar:

January 2016

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13 Class Begins	14 1st 462 Class	15	16
17	18 MLK H-Day	19 462 Class	20	21 462 Class	22	23
24	25	26 462 Class	27	28 462 Class	29	30
31						

February 2016

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2 462 Class	3	4 462 Class	5	6
7	8	9 462 Class	10	11 462 Class	12	13
14	15	16 462 Class	17	18 462 Class	19	20
21	22	23 462 Class	24	25 462 Class	26	27
28	29					

March 2016

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1 462 Class	2	3 462 Class	4	5
6	7	8 462 Class	9	10 462 Class	11	12
13	14 SpringBreak	15 SpringBreak	16 SpringBreak	17 SpringBreak	18 SpringBreak	19
20	21	22 462 Class	23	24 462 Class	25 SpringRecess	26
27	28	29 462 Class	30	31 462 Class		

April 2016

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1	2
3	4	5 462 Class	6	7 462 Class	8	9
10	11	12 462 Class	13	14 462 Class	15	16
17	18	19 462 Class	20	21 462 Class	22	23
24	25	26 462 Class	27	28 462 Class	29 Classes End	30

May 2016

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2 Study Day	3 Final Exams	4 Final Exams	5 Final Exams	6 Final Exams	7
8	9 Final Exams	10 Final Exams	11 Commence-ment	12 Commence-ment	13 Commence-ment	14 Commence-ment
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Spring 2016 Semester

Classes Begin .... Wednesday .... January 13
MLK Holiday .... Monday .... January 18
1st Session Ends .... Wednesday .... March 2
2nd Session Begins .... Thursday .... March 3
Spring Break .... Monday-Friday .... March 14-18
Spring Recess .... Friday .... March 25
Classes End .... Friday .... April 29
Study Day .... Monday .... May 2
Exams .... Tuesday-Tuesday .... May 3, 4, 5, 6, 9, 10
Graduate Hooding .... Thursday .... May 12
Commencement.................................... Wednesday-Saturday .... May 11-14
Official Graduation Date .... Saturday .... May 14

Class Description (ECE 462 Cyber-Physical Systems Security)

The phrase "Cyber-Physical Systems" describes systems that include real-time, embedded and/or transactional services systems, with the additional feature of possible communication between system components. This allows cyber and physical processes to collaborate with each other to form a distributed system, increasing the overall complexity of the resulting architecture over traditional real-time, embedded or services systems. These cyber-physical systems include physical or virtual environments where people live, work and play that are instrumented and controlled by some form of computer system.

Cyber-physical systems include (incomplete list)

- industrial automation systems and robots,
- vehicular systems (e.g.: collision avoidance, autonomous driving),
- transportation systems (highways, airports, railways, ports, etc.),
- avionics,
- medical systems (e.g.: integrated diagnostics and medication, remote surgery)
- power systems (e.g.: load balancing between power demand and supply)
- smart homes and buildings (e.g. cooling, lighting, access)

Most of these applications have strict requirements with respect to some or all of the following

- real-time
- reliability and robustness (dealing with uncertainty)
- correctness assurance (verification and validation)
- "human" in the loop interactions

Topics to be covered will include: (This a topical list, not a syllabus. See the syllabus for the specific semester to view the timing of the various topics.)

- What are Cyber-Physical Systems (CPS)
- Example CPS system structures and related applications
- CPS operating environments/modes: real-time, networked, passive, embedded, interactive, …
- Standards used in CPS design and operation, and their effects on security
- Security challenges and techniques at the physical layer
    - Physical infrastructure, human interface, sensor environment, control interface, possible faults and threats
- Security challenges and techniques at the cyber layer
    - Communications/networks (wireless, mesh, sensor), embedded systems environment, development tools, data handling/formats, possible faults and threats
- Security exposures in procedures and protocols
    - Maintenance, recovery, data sharing, data archiving
- Example CPSes and their security challenges and practices
    - transportation systems, air-traffic control, building automation and HVAC, smart grids and power plants, industrial automation, vehicle systems, and SCADA systems.

- Emerging security technologies, protocols and procedures.

Pre-requisite: COSC 160, COSC 302
Registration Restriction(s): Minimum student level – junior.

Required Reading (Class Textbook):

George Loukas, *Cyber-Physical Attacks: A Growing Invisible Threat*, Elsevier 2015

Special Issue of Politico - The Cyber Issue
http://www.politico.com/agenda/issue/the-cyber-issue-december-2015

Recommended Reading:

Matt Bishop, *Introduction to Computer Security*, Addison-Wesley, 2005

Introduction to Computer Security pdf DONE.pdf (on BlackBoard class portal)

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CCYQFjACahUKEwi17u3Tp5XJAhWMkh4KHepNAWw&url=https%3A%2F%2Filocker.bsu.edu%2Fusers%2Fcetaylor%2Fworld_shared%2FIntroduction%2520to%2520Computer%2520Security%2520pdf%2520DONE.pdf&usg=AFQjCNE5UJXLdKuvnL5zMCMd9crUqk4DKw&bvm=bv.107467506,d.dmo

Slides per Chapters, *Introduction to Computer Security*, Addison-Wesley, 2005

http://nob.cs.ucdavis.edu/book/book-intro/slides/index.html

Sajal K. Das, Krishna Kant and Nan Zhang, *Securing Cyber-Physical Critical Infrastructure*, Elselvier, 2012

Adam Shostack, *Threat Modeling – Designing for Security*, Wiley, 2014

Edward A. Lee, Sanjit A. Seshia, *Introduction to Embedded Systems – A Cyber-Physical Systems Approach*, LuLu, 2014

Weekly Schedule & Syllabus (Tentative):

1. Overview of Class, Grading, Topics Covered and Reference Material
2. What are Cyber Physical Systems (CPSs)
    a. Definition
    b. CPS Concept Map
    c. High Level Examples
    d. Challenges
3. CPS
    - Predictable Comp. Architecture
    - Predictable OS Abstractions
    - Timing and Performance Analysis
    - Intro to Models of Computation and Verification.
4. Overview of Computer Security (Chapter 1, Introduction to Computer Security by Matt Bishop)

5. Cyber Physical Security Introduction and History (Chapter 1 & 2, Cyber Physical Attacks by George Loukas)
6. Detailed CPS Attack Examples – Industrial Controls (Chapter 4, Cyber Physical Attacks by George Loukas)
7. Detailed CPS Attack Examples – Power Grid (Chapter 4, Cyber Physical Attacks by George Loukas)
8. Security Policies, Lecture 1 (Chapter 4, Introduction to Computer Security by Matt Bishop
   - Trust
   - Confidentiality
   - Integrity
9. In the Minds of an Attacker (Chapter 5, Cyber Physical Attacks by George Loukas)
10. CPS Threat Modeling – Data Flow Diagrams
11. CPS Threat Modeling – Data Flow Diagram examples
12. CPS Threat Metrics & Identification (STRIDE), Lecture 1 of 2
13. CPS Threat Metrics & Identification (STRIDE), Lecture 2 of 2
14. CPS Threat Modeling – Threat Trees
15. CPS Threat Vulnerability Assessment (DREAD)
16. CPS Threat Vulnerability Assessment, Risk Tables and Mitigation Strategy,
17. CPS Threat Migration Strategy
18. SDL Threat Modeling Tool
19. Protection Mechanisms, Intrusion Detection (Chapter 6, Cyber Physical Attacks by George Loukas)
20. Secure Design Principles (Chapter 6, Cyber Physical Attacks by George Loukas)
21. Cryptography – An Overview (Chapter 8, Introduction to Computer Security by Matt Bishop)
22. Untrusted Computing – Malicious Logic, Lecture 1 (Chapter 19, Introduction to Computer Security by Matt Bishop)
23. Untrusted Computing – Malicious Logic, Lecture 2 (Chapter 19, Introduction to Computer Security by Matt Bishop)
24. Detailed CPS Attack Examples – Automotive Systems (Chapter 3, *Cyber Physical Attacks* by George Loukas)
25. Physical-Cyber Attacks
26. Best Practices in Designing Secure CPSs
27. Open Discussion for Final Project.

Final Project:

- Analyze Security Vulnerability of Urban Area Monitoring, Detection and Deployment System.

Scheduled Meeting Times						
Type	**Time**	**Days**	**Where**	**Date Range**	**Schedule Type**	**Instructors**
Class	9:40 am – 10:55pm	TR	Min Kao Engineering 406	14-Jan-2016 - 28-Apr-2016	Lecture	Mark Edward Dean (P)

Total number of classes – 29 (not including final exam)
Final Exam due May 3.
Check the following website for changes to syllabus: TBD

Note: All class Topics and supporting material are under development.

Mtgs	Date	Topic	Materials/Assignments	Misc.
1	1/14/2016	**Lecture 1 - Overview of Class, Grading, Topics Covered, Reference Material & Final Project**	ECE462_Lecture0_Class_Introduction.pptx ECE462_Lecture1_CPS_Introduction.pptx	
2	1/19/2016	**Lecture 2 - What are Cyber Physical Systems (CPSs)** - Definition revisited - CPS Concept Map - High Level Examples - Challenges	Chapter 1, Cyber Physical Attacks by George Loukas ECE462_Lecture2_What are Cyber Physical Systems.pptx http://cyberphysicalsystems.org/	References - CPS_CourseIntroduction.ppt Homework #1: Exercises from Chapter Chapter 1, *Cyber Physical Attacks* by George Loukas and 5 additional questions on BlackBoard, Due in one week from today.
3	1/21/2016	**Lecture 3 - CPS –** • Predictable Comp. Architecture • Predictable OS Abstractions • Timing and Performance Analysis • Intro to Models of Computation and Verification.	ECE462_Lecture3_CPS_Design_Challenges.pptx	References - CPS_CouseIntroduction.ppt

4	1/26/2016	**Lecture 4 - Overview of Computer Security**	Chapter 1, Introduction to Computer Security by Matt Bishop ECE462_Lecture4_IntroCompSecurity.pptx	Homework #2: Exercises from Chapter 1, Intro to Computer Security, by Matt Bishop, Questions 1-8 Homework #1 Due Today. References –
5	1/28/2016	**Lecture 5 - Cyber Physical Security Introduction and History**	Chapter 2, Cyber Physical Attacks by George Loukas ECE462_Lecture5_Intro_CPS_Security.pptx	Reference - COMP1706-CyberPhysicalSecurity.pptx
6	2/2/2016	**Lecture 6 - Detailed CPS Attack Examples - Industrial Controls Attacks, SCADA Systems**	Chapter 4, *Cyber Physical Attacks* by George Loukas NIST.SP.800-82r2.pdf csd-nist-guidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf https://en.wikipedia.org/wiki/Stuxnet	Homework #2 Due Today. Homework #3: Exercises from Chapter 2, *Cyber Physical Attacks* by George Loukas, Questions 2-9. "Guide to Industrial Control Systems Security" & "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security" by the National Institute of Standards and Technology
7	2/4/2016	**Lecture 7 - Detailed CPS Attack Examples - Power-Grid Attacks & Security**	Chapter 4, *Cyber Physical Attacks* by George Loukas Chapter 25, *Securing Cyber-Physical Critical Infrastructure* by Sajal K. Das, et. al. RISI Attack Examples	Reference – PowerGridSecurity.pdf http://www.risidata.com/Database/event_date/desc

8	2/9/2016	**Lecture 8 – Security Policies Confidentiality Policies Integrity Policies** Three Tenets for Secure Cyber-Physical Systems Design	Chapter 4, *Introduction to Computer Security* by Matt Bishop Chapter 5, *Introduction to Computer Security* by Matt Bishop Chapter 6, *Introduction to Computer Security* by Matt Bishop ThreeTenetsSPIE.pdf	Homework #3 Due Today. Homework #4: Exercises from Chapter 4, *Cyber Physical Attacks* by George Loukas, Questions 1-6 Reference - usc-csci530-f10-part2.pptx
9	2/11/2016	**Lecture 9 - In The Minds of an Attacker – Steps to Cyber-Physical Attacks**	Chapter 5, *Cyber Physical Attacks* by George Loukas Chapter 12, *Securing Cyber-Physical Critical Infrastructure* by Sajal K. Das, et. al.	
10	2/16/2016	**Lecture 10 – CPS Threat Modeling** – **Data Flow Diagrams**	DataFlowDiagram_HowTo .ppt *Threat Modeling* by Frank Swiderski & Window Snyder, Chapter 4 ThreeTenetsSPIE.pdf Reference – http://yourdon.com/strucanalysis/wiki/index.php?title=Chapter_9	Homework #4 Due Today Homework #5: Exercises from Chapter 5, *Cyber Physical Attacks* by George Loukas, Questions 1-6
11	2/18/2016	**Lecture 11 – CPS Threat Modeling** – **Trust Levels, Entry Points, Assets and Data Flow Diagrams Example Exercise**	*Threat Modeling* by Frank Swiderski & Window Snyder, Appendix A	
12	2/23/2016	**CPS Threat Metrics & Identification (STRIDE)**, Lecture 1 of 2	Threat Modeling – Designing for Security by Adam Shostack, Chapter 3	Homework #5 Due Today Homework #6 (optional): Create Level 1 Data Flow Diagram for Final Project (for review only)

13	2/25/2016	**CPS Threat Metrics & Identification (STRIDE)**, Lecture 2 of 2	Threat Modeling – Designing for Security by Adam Shostack, Chapter 3	Reference – CyberThreatMetrics_065.pdf ThreeTenets…Quantitative CPS Metrics (#5 in ThreeTenetSPIE.pdf)
14	3/1/2016	**CPS Threat Modeling** – Threat Tree Diagrams		Homework #6 Due Today Homework #7: Complete STRIDE-per-Element analysis table for Smart Utility System Sensor Data Ingestion operation from Lecture 11.
15	3/3/2016	**CPS Threat Vulnerability Assessment** 1 of 2 (DREAD)		Reference – CyberThreatMetrics_065.pdf ThreeTenets…Quantitative CPS Metrics (#5 in ThreeTenetSPIE.pdf)
16	3/8/2016	**CPS Threat Vulnerability Assessment, Risk Tables and Mitigation Strategy,** 2 of 2,	cvss_basic-2.0_Presentation.pdf	Homework #7 Due Today Exercises TBD cvss-v30-specification-v1.7.pdf cvss-v30-user_guide_v1.4.pdf cvss-v30-examples_v1.1.pdf
17	3/10/2016	**CPS Threat Mitigation**		
Note: Spring Break		**Undergraduate Students have most of the material they need to complete their Final Project.**		
18	3/22/2016	**SDL Threat Modeling Tool from Microsoft**		http://www.microsoft.com/en-us/download/details.aspx?id=49168

				https://www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx https://msdn.microsoft.com/magazine/dd347831.aspx
Note:		**Graduate Students have all the material they need at this point to complete their Final Project.**		
19	3/24/2016	**Protection Mechanisms, Intrusion Detection & Response**	Chapter 6*, Cyber Physical Attacks* by George Loukas p. 182-200	
20	3/29/2016	**Secure Design Principles**	Chapter 6, *Cyber Physical Attacks* by George Loukas p. 211-217	
21	3/31/2016	**Cryptography – An Overview**	Chapter 8, *Introduction to Computer Security* by Matt Bishop	Reference - usc-csci530-f10-part2.pptx
22	4/5/2016	**Untrusted Computing – Malicious Logic**, Lecture 1 of 2	Chapter 19, *Introduction to Computer Security* by Matt Bishop	Reference – IntroComputerSecurity Chapter19.ppt usc-csci530-f10-part2.pptx
23	4/7/2016	**Untrusted Computing – Malicious Logic**, Lecture 2 of 2	Chapter 19, *Introduction to Computer Security* by Matt Bishop	Exercises from Chapter 19, *Introduction to Computer Security* by Matt Bishop Reference – IntroComputerSecurity Chapter19.ppt usc-csci530-f10-part2.pptx
24	4/12/2016	**Lecture 22 - Detailed CPS Attack Examples – Automotive Systems**	Chapter 3, *Cyber Physical Attacks* by George Loukas	
25	4/14/2016	Physical-Cyber Attacks	Chapter 7*, Cyber Physical Attacks* by George Loukas	
26	4/19/2016	Intrusion Detection	Chapter 22, *Introduction to Computer Security* by Matt Bishop	

27	4/21/2016	Open Class to discuss project … Optional Attendance.		
28	4/26/2016	Used in case need to cover missed classes due to snow or other issues.		
29	4/28/2016			
Final Exam	5/5/2016	Final Project Due		

Elements of Final Grade (ECE462)

High Level Elements:

- Final Project = 50% of grade
- Class assignments = 50% of grade
- Attendance = Students must attend 85% of all lectures (24 classes). 0.7 grade points (out of a 4.0 grade scale) will be deducted from the final grade for the 5th class missed. 0.1 grade points (out of a 4.0 grade scale) will be deducted from the final grade for each class missed beyond the 5th class missed.

Course Personnel:

- Faculty member in charge: Dr. Mark E. Dean
  - email: markdean@utk.edu
  - phone: 865-974-5784
  - Office hours: 3:30-5:00pm, Tuesday, Wednesday, & Thursday

    The best way to contact me is via email or during office hours.

- IT Help: https://ithelp@eecs.utk.edu

- Guest Lecturers: TBD

Work Items for Class Material and Preparation:

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.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)
- Vulnerabilities (DREAD and/or CVSS)
- 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
   3.3. DREAD and/or CVSS to Characterize 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.pptx** for details on architecture used to implement the Smart City Urban Monitoring System.

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) (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)

General Illustrations of Smart Cities Infrastructure:

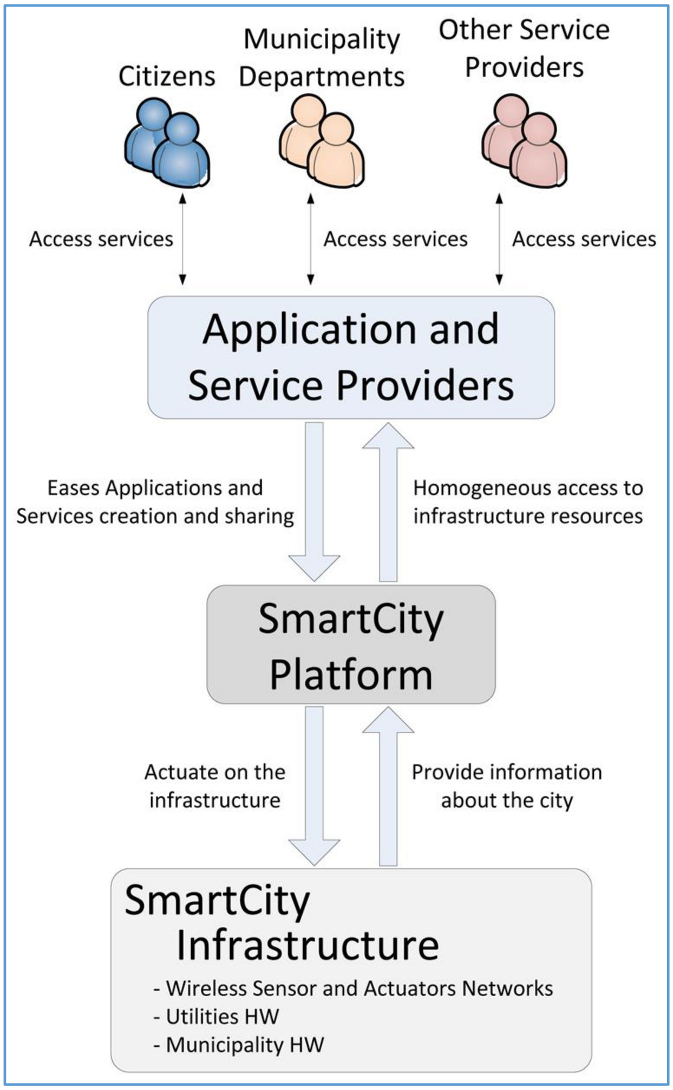

Figure 1. Generic Smart City Actors Interaction

Figure 2. CPS Reference Architecture for Smart City Infrastructure