University of Idaho

A Resilient Real-Time Traffic Control System: Software Behavior Monitoring and Adaptation

Axel Krings
Ahmed Serageldin
Ahmed Abdel-Rahim

This research was supported by grant DTFH61-10-P- 00123 from the Federal Highway Administration - US DoT

University of Idaho

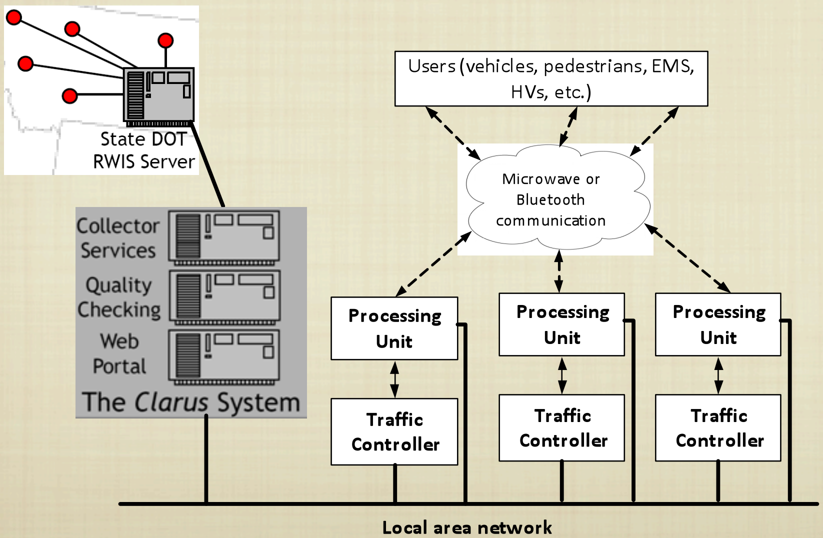
Integrating Clarus data into RT-App.

- Challenges
  - The Engineering Challenge
  - The Security Challenge
  - The Real-time Challenge
  - The Survivability Challenge (includes all "illities")
- Apply the newest technology to a survivability architecture
  - Design Methodology based on *Design for Survivability*

University of Idaho

Project Architecture

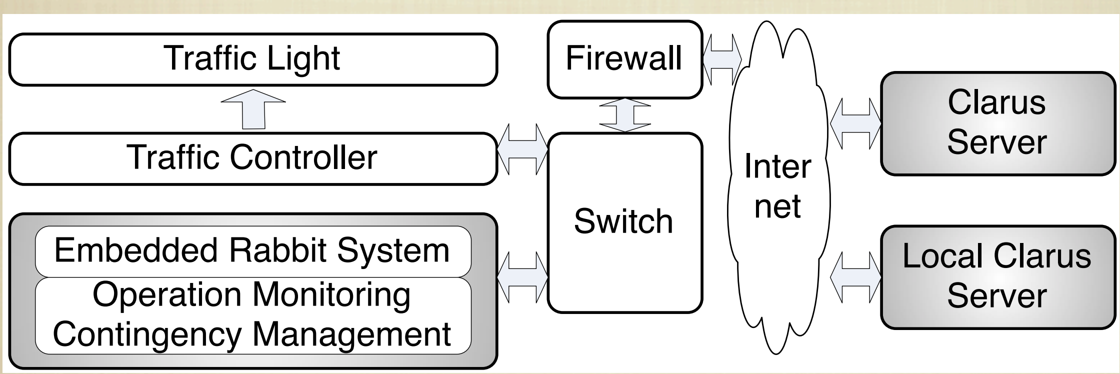
- A system operating in an unbounded environment
- Inheriting all problems from such environment



University of Idaho

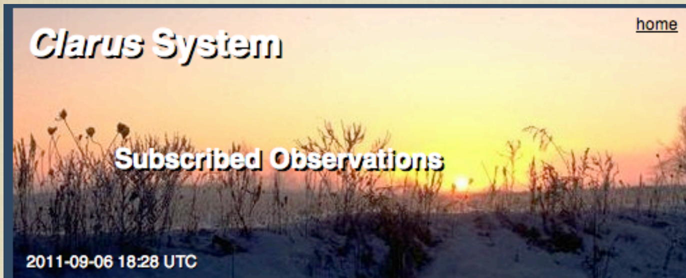
The big picture

- The problem:
  Should we connect the control network to the Internet?



Clarus...

- Utilizing local sensor data to do what?



Observations	Size (bytes)
20110906_1815.csv	420
20110906_1800.csv	5,515
20110906_1745.csv	5,515
20110906_1730.csv	5,515
20110906_1715.csv	5,515
20110906_1700.csv	5,515
20110906_1645.csv	5,515
20110906_1630.csv	5,515
20110906_1615.csv	5,515
20110906_1600.csv	5,515
20110906_1545.csv	5,515

Subscription: 2011082501

Subscription Information:
DateCreated = 2011-08-25
Lat1 = not used
Lon1 = not used
Lat2 = not used
Lon2 = not used
PointRadiusLat = not used
PointRadiusLon = not used
PointRadiusRadius = not used
ObsType = 0 (all)
MinValue = -Infinity
MaxValue = Infinity
RunFlags = not applicable
PassNotPass = not applicable
Contributors = ID_State_TD
StationIds = Shirrod

University of Idaho

Clarus Subscription Data

- Access Clarus data files from the web

http://www.clarus-system.com/SubShowObs.jsp?subId=2011082501&file=20110906_2200.csv

Axel UI Research Finances Misc. Clarus Conferences Music Kitty Hawk MANET TV Find Motorcycle


```
ObsTypeID,ObsTypeName,ClarusSensorID,ClarusSensorIndex,ClarusStationID,ClarusSiteID,Category,ClarusContribID,Contributor,StationCode,Timestamp,Latitude,Longitude,Elevat
ion,Observation,Units,EnglishValue,EnglishUnits,ConfValue,Complete,Manual,Sensor_Range,Climate_Range,Step,Like_Instrument,Persistence,IQR_Spatial,Barnes_Spatial,Dew_Poi
nt,Sea_Level_Pressure,Precip_Accum
554,essAtmosphericPressure,35456,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,922.000,mbar,27.227,inHg,0.913,P,-,P,N,P,/,P,P,-,/,P,/
574,essWetBulbTemp,35422,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,22.000,C,71.600,F,1.000,P,-,P,P,P,/,P,P,-,/,/,/
575,essDewpointTemp,35423,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,16.300,C,61.340,F,1.000,P,-,P,P,P,/,P,P,-,/,/,/
576,essMaxTemp,35424,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,32.400,C,90.320,F,1.000,P,-,P,P,P,/,P,P,-,/,/,/
577,essMinTemp,35425,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,11.700,C,53.060,F,1.000,P,-,P,P,P,/,P,P,-,/,/,/
581,essRelativeHumidity,35426,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,38.000,%,38.000,%,1.000,P,-,P,P,P,/,P,P,-,P,/,/
586,essPrecipYesNo,35462,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,2.000,null,2.000,null,1.000,P,-,P,/,/,/,/,/,/,/,/,/
587,essPrecipRate,35445,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,0.000,cm/h,0.000,in/h,1.000,P,-,P,/,P,/,/,P,-,/,/,/
589,essPrecipSituation,35469,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,3.000,null,3.000,null,0.000,P,-,N,/,/,/,/,/,/,/,/,/
5101,essVisibility,35446,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,1770.300,m,5808.071,ft,1.000,P,-,P,/,P,/,/,-,P,/,/,/
5102,essVisibilitySituation,35463,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,1.000,null,1.000,null,1.000,P,-,P,/,/,/,/,/,/,/,/,/
5733,essAirTemperature,35427,1,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,32.200,C,89.960,F,1.000,P,-,P,P,P,/,P,P,-,/,/,/
5811,essPrecipitationStartTime,35447,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-
116.95223,869,1315342261.000,s,1315342261.000,s,0.000,/,/,/,/,/,/,/,/,/,/,/,/,/,/
5812,essPrecipitationEndTime,35448,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-
116.95223,869,1315342321.000,s,1315342321.000,s,0.000,/,/,/,/,/,/,/,/,/,/,/,/,/,/
5813,essPrecipitationOneHour,35449,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,0.000,cm,0.000,in,1.000,P,-,P,/,P,/,/,/,/,/,/,P
5814,essPrecipitationThreeHours,35450,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,0.000,cm,0.000,in,1.000,P,-,P,/,P,/,/,/,/,/,/,P
5815,essPrecipitationSixHours,35451,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,0.000,cm,0.000,in,1.000,P,-,P,/,P,/,/,/,/,/,/,P
5816,essPrecipitationTwelveHours,35452,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,0.000,cm,0.000,in,1.000,P,-,P,/,P,/,/,/,/,/,/,P
5817,essPrecipitation24Hours,35453,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,0.000,cm,0.000,in,1.000,P,-,P,/,P,/,/,/,/,/,/,P
51137,essSurfaceStatus,35429,2,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,3.000,null,3.000,null,1.000,P,-,P,/,/,/,/,/,/,/,/,/
51137,essSurfaceStatus,35428,1,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,3.000,null,3.000,null,1.000,P,-,P,/,/,/,/,/,/,/,/,/
51138,essSurfaceTemperature,35431,2,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,48.700,C,119.660,F,0.913,P,-,P,N,P,P,P,P,-,/,/,/
51138,essSurfaceTemperature,35430,1,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,49.200,C,120.560,F,0.913,P,-,P,N,P,P,P,P,-,/,/,/
51165,essSubSurfaceTemperature,35432,1,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,24.600,C,76.280,F,1.000,P,-,P,P,P,P,P,P,-,/,/,/
51165,essSubSurfaceTemperature,35434,2,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,24.600,C,76.280,F,1.000,P,-,P,P,P,P,P,P,-,/,/,/
56104,windSensorAvgSpeed,35439,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,2.100,m/s,4.698,mph,1.000,P,-,P,P,P,/,P,P,-,/,/,/
56105,windSensorAvgDirection,35440,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,75.000,deg,75.000,deg,0.816,P,-,P,/,N,/,P,/,/,/,/,/
56106,windSensorSpotSpeed,35457,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,2.000,m/s,4.474,mph,0.866,P,-,P,/,P,/,P,-,N,/,/,/
56107,windSensorSpotDirection,35458,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,63.000,deg,63.000,deg,0.816,P,-,P,/,N,/,P,/,/,/,/,/
56108,windSensorGustSpeed,35441,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,2.800,m/s,6.263,mph,1.000,P,-,P,/,P,/,P,P,-,/,/,/
56109,windSensorGustDirection,35442,0,3283,2809,P,16,ID_State_TD,Shirrod,2011-09-06 21:35:35,46.51329,-116.95223,869,94.000,deg,94.000,deg,0.816,P,-,P,/,N,/,P,/,/,/,/,/
END OF RECORDS -- 2011082501:20110906_2200.csv
```

Highly Critical (Essential) Clarus Data

essPrecipSituation	Describes the weather situation in terms of precipitation, integer values indicate situation
essPrecipYesNo	Indicates whether or not moisture is detected by the sensor: (1) precip; (2) noPrecip; (3) error
essPrecipRate	The rainfall, or water equivalent of snow, rate
essRoadwaySnowpackDepth	The current depth of packed snow on the roadway surface
essAirTemperature	The dry-bulb temperature; instantaneous
essVisibilitySituation	integer value, describes the travel environment in terms of visibility
essVisibility	Surface visibility (distance)
essSurfaceStatus	integer value, a value indicating the pavement surface status

Prototype

What could possibly go wrong?

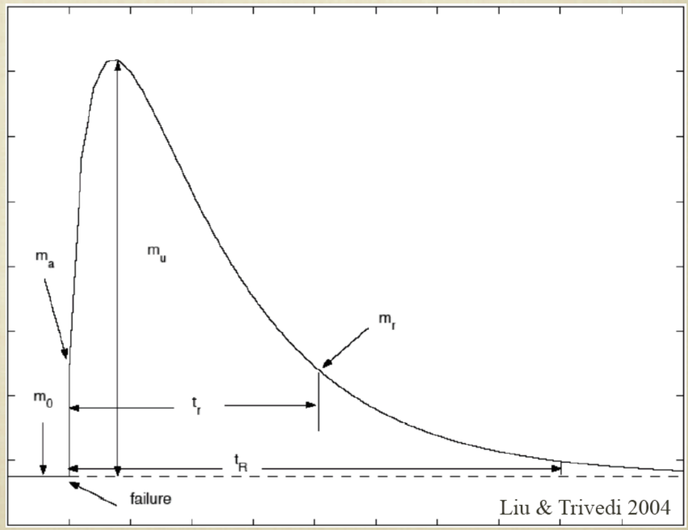
- What assumptions should one place on a system?
  - Anything is possible!
    - and it will happen!
  - Malicious act will occur sooner or later
  - It is hard or impossible to predict the behavior of an attack

Unique Opportunity

- What is unique about this project?
  - The application domain is part of a Critical Infrastructure
  - The project is just small enough to demonstrate a survivability architecture
    - The code is relatively small
    - The execution is relatively deterministic
    - The run-time support is relatively mature

What is Survivability

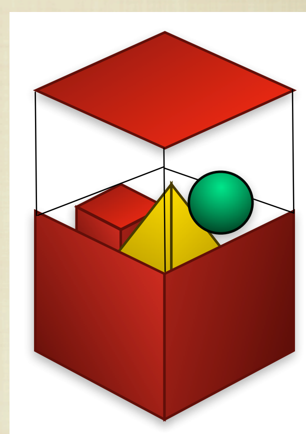
- Closely related Terms
  - Intrusion Tolerance
  - Resilience
- Relationship to
  - Fault-tolerance
  - Security



Liu & Trivedi 2004

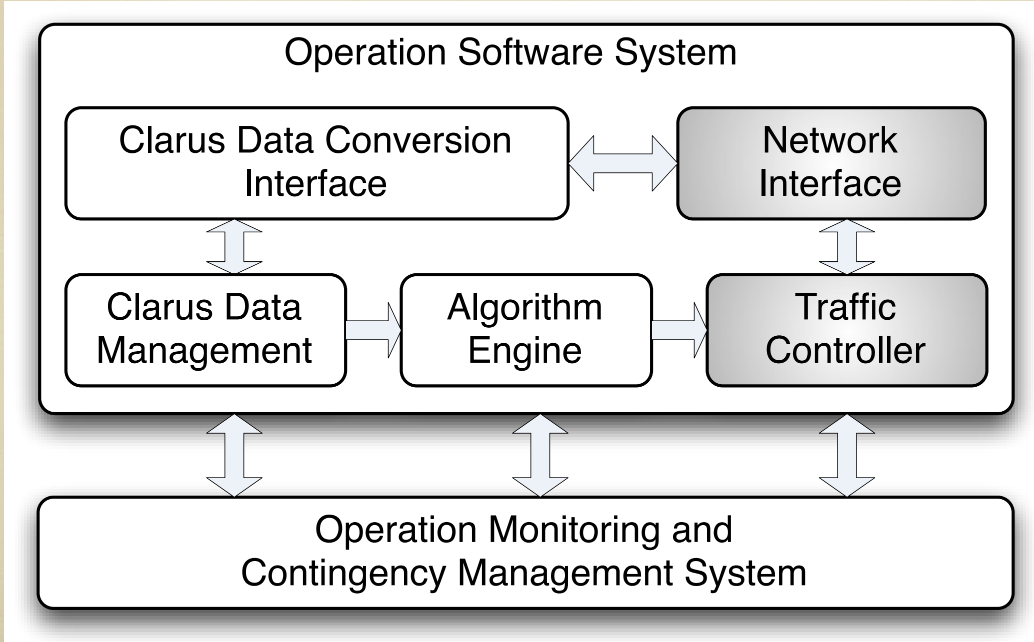
Design for Survivability

- When Systems become too complex
  - Design by Integration of Survivability mechanisms
  - Build-in *not* add-on
  - Design for Survivability has surfaced in different contexts



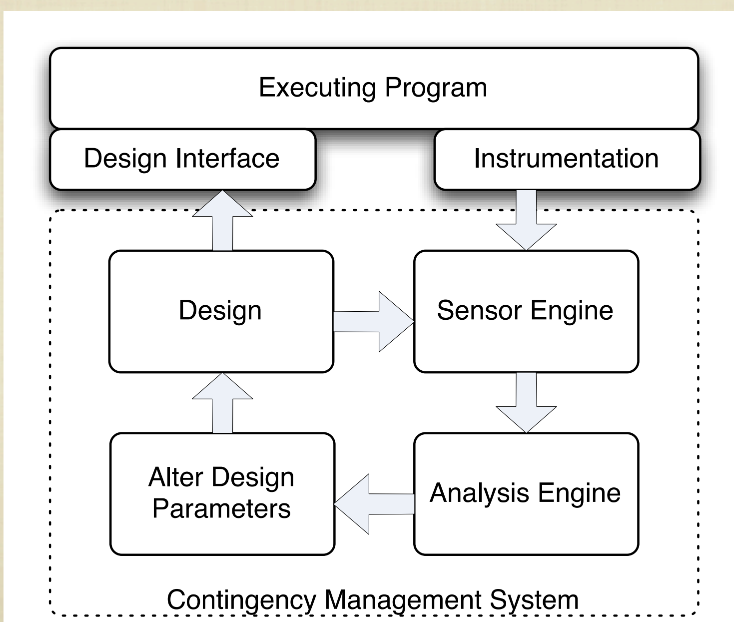
Software Architecture

- Overview



Design Methodology

- Measurement-based design and operation

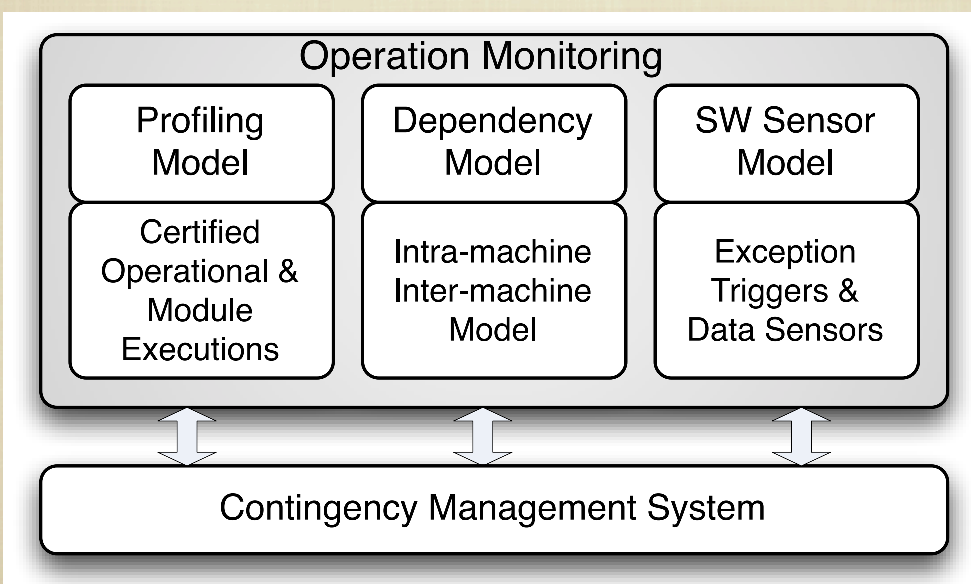


Our view of a System

- Different "machines"
  - Operations
  - Functions
  - Modules
- Epoch
  - defined by transitions

Formal Model of Sys. Arch.

- Measurement-based design and operation



Profiling Model

Profiles

- Frequency Spectrum (...and more)
  - count invocations
  - probability of invocation
  - defined for an epoch
  - defined for operations, functions and modules
  - does not say anything about dependencies!

Profiles

- Module Profile
  - **p** = <p_1, p_2, …,$p_{|M|}$ >

    where p_i is probability that m_i is executing

Profiles

- Observed Profile

$\hat{\mathbf{p}} = (\hat{p}_1, \hat{p}_2, ..., \hat{p}_{|M|})$, where $\hat{p}_i = c_i/n$ is the fraction of system activity due to invocations of module m_i and c_i is the count of invocations of m_i.

$\hat{\mathbf{p}}^k$ denotes the k^{th} observed module profile, observed over n epochs

Profiles and Certification

- System behavior
  - Analyze the observed profiles
  - What is the threshold for "normal" behavior?
  - How do we detect deviation from thresholds for "normal" executions?
  - Set the threshold of "normal" to "certified"
    - Looks like anomaly detection in IDS, or?

University of Idaho

Profiles and Certification

- Interpretation of Certified Behavior
  - If profiles are beyond the certified threshold **we simply have not seen such behavior before**!
  - Could be benign or malicious reasons
- What is our response?
  - We could simply not allow the operation to continue and go to fail-safe state

Profile Vector

- Vector $\hat{\mathbf{p}} = (\hat{p}_1, \hat{p}_2, ..., \hat{p}_{|M|})$
  - notice *log scale*

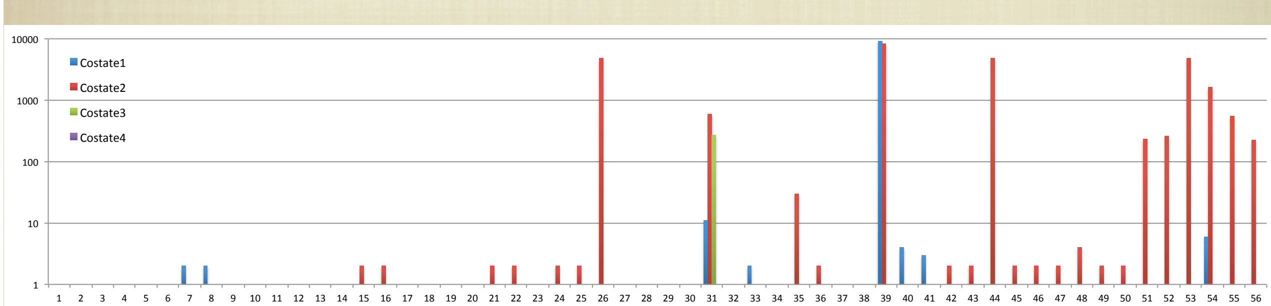


Fig. 5. Typical observed profile of 4 costates (module IDs and frequencies on the axis)

Profile Vector & Scalar

- Observe *h* sequences of *n* epochs
- Define a centroid $\overline{\mathbf{p}} = (\overline{p}_1, \overline{p}_2, ..., \overline{p}_{|M|})$, where

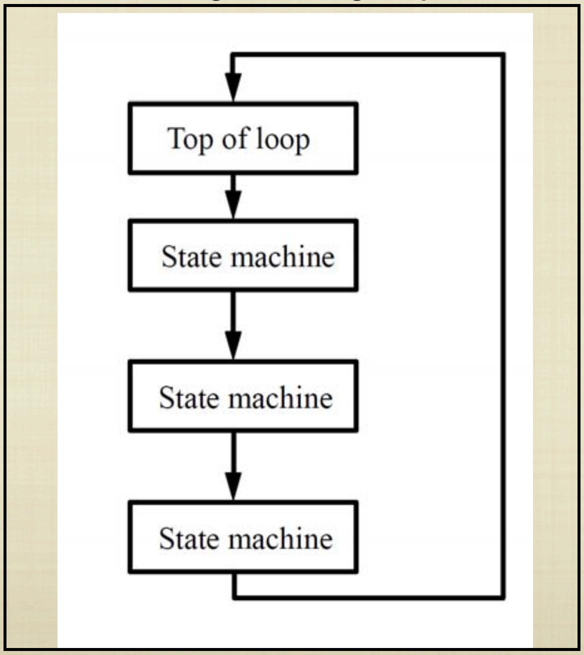
$$\overline{p}_i = \frac{1}{h} \sum_{j=1}^{h} \hat{p}_i^j$$

and the distance of $\hat{\mathbf{p}}^k$ from centroid $\overline{\mathbf{p}}$ is given by

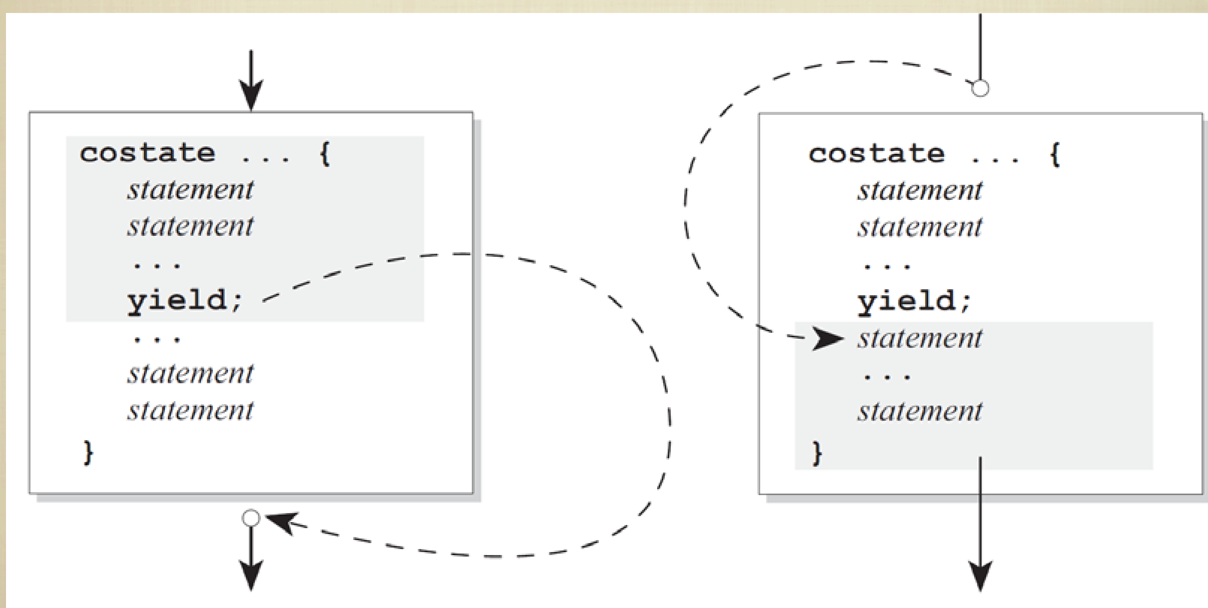
$$d_k = \sum_{i=1}^{n} (\overline{p}_i - \hat{p}_i^k)^2$$

Multitasking Model

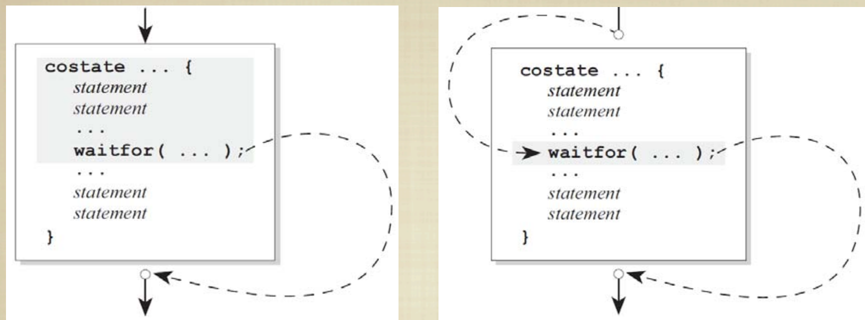
- Rabbit runs Dynamic C which support costatements



- Dynamic C, *costates* and *yield*
  (Figure from Dynamic C Users Manual)

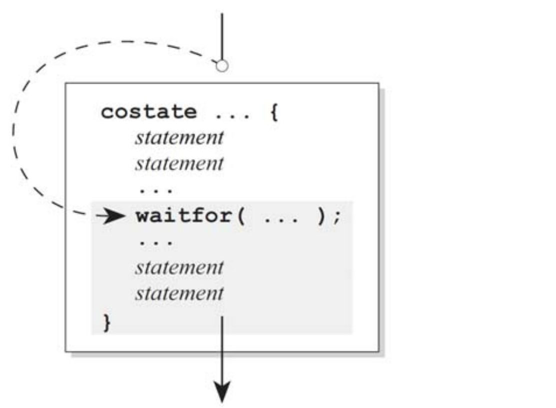


- Dynamic C, *costate* and *waitfor* (Figure from Dynamic C Users Manual)



(a) First Time (b) Subsequent Times

Execution thread when waitfor evaluates to true



Profiles considering costates

- Definitions based on costate α:

$\hat{\mathbf{p}}[\alpha]$, $\hat{\mathbf{p}}^k[\alpha]$, $\overline{\mathbf{p}}[\alpha]$ and $d_k[\alpha]$

Multitasking Model

- One knows which costate is executing
- Profiles of costates are not polluted with activity from other costates
- Result is lower degree of non-determinism of execution

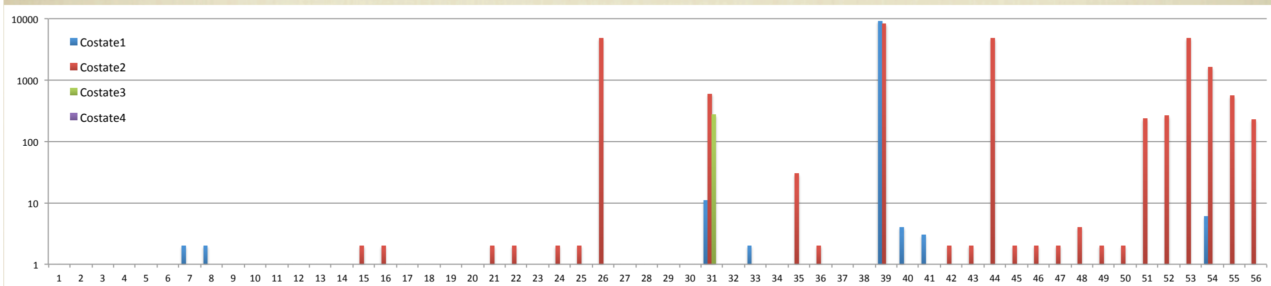


Fig. 5. Typical observed profile of 4 costates (module IDs and frequencies on the axis)

Certified Behavior

- The distance of the observed costate profiles $\hat{\mathbf{p}}^k[\alpha]$ from $\overline{\mathbf{p}}[\alpha]$ can be used so that departure beyond it indicates non-certified behavior of costate α. Two threshold vectors:

$$\epsilon^{max}[\alpha] = (\epsilon_1^{max}[\alpha], ..., \epsilon_{|M|}^{max}[\alpha]) \tag{3}$$

$$\epsilon^{min}[\alpha] = (\epsilon_1^{min}[\alpha], ..., \epsilon_{|M|}^{min}[\alpha]) \tag{4}$$

where $\epsilon_i^{max}[\alpha]$ and $\epsilon_i^{max}[\alpha]$ are the upper and lower threshold values of m_i, representing a dual-bound threshold.

Certified Behavior

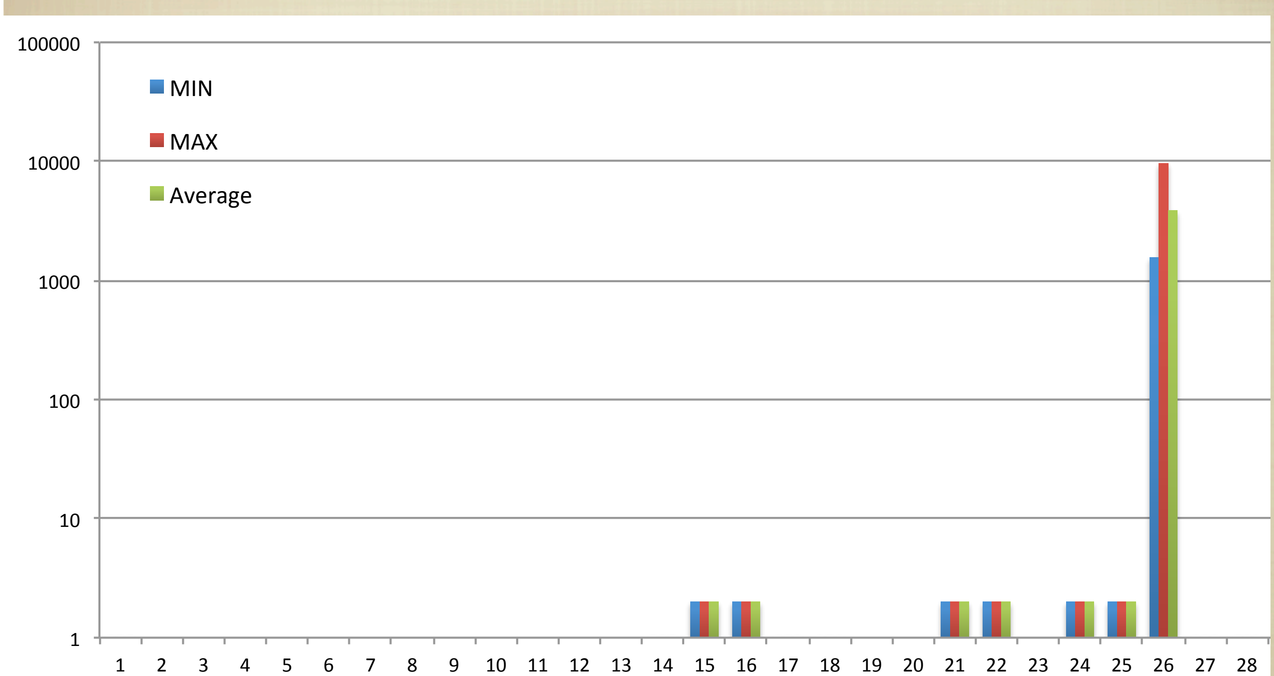
- .

Every observed profile that is in the region between the two vectors is assumed nominal. Thus we certify a profile $\hat{\mathbf{p}}^k[\alpha]$ to be a *nominal profile* if

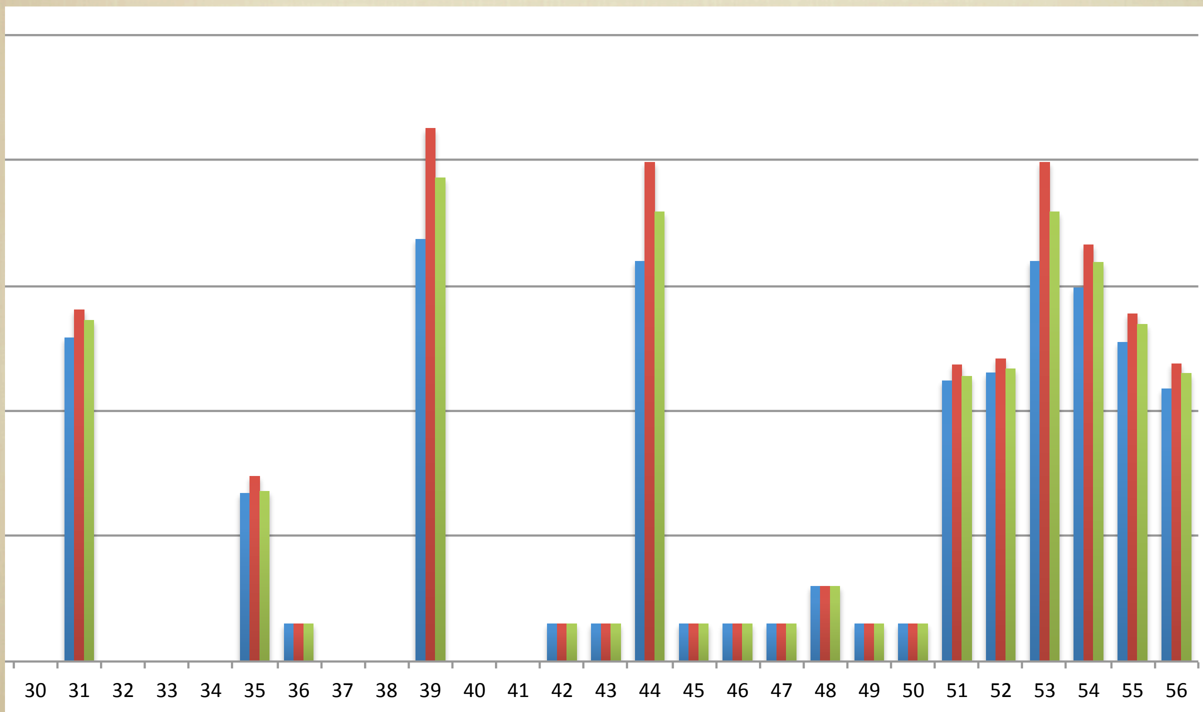
$$\epsilon^{min}[\alpha] \leq \hat{\mathbf{p}}^k[\alpha] \leq \epsilon^{max}[\alpha]$$

i.e., if $\epsilon_i^{min}[\alpha] \leq \hat{p}_i^k[\alpha] \leq \epsilon_i^{max}[\alpha]$ for every $1 \leq i \leq |M|$.

Centroid



Centroid



Synchronized Profiling

- So fare we assumed that there is only one single behavior. However, there could be multiple.

Considering h sequences of n epochs each, we define a centroid of sets $\overline{\mathbf{P}} = (\overline{P}_1, \overline{P}_2, ..., \overline{P}_{|M|})$, where

$$\overline{P}_r = \overline{P}_r \cup p_i, \quad 1 \leq r \leq |M| \quad p_i = \frac{1}{h} \sum_{j=1}^{h} \hat{p}_i^j \qquad (2)$$

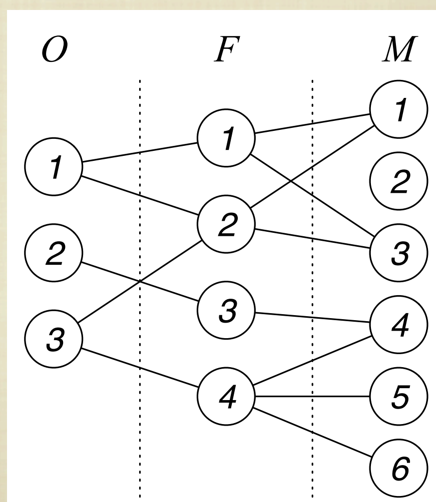
for each behavior i. Thus $\overline{\mathbf{P}}$ is a $|M|$-dimensional structure of sets, and again using the above financial metaphor, each element represents the "h-day moving average" of a specific *set of stocks* (module), where a day is measured as n epochs, and again we want to track the past in order to establish "nominal", i.e., expected, behavior from a *set of behaviors*.

Dependency-based Model

Inter-dependencies

- Relationship between Operations, Functionalities, and Modules

Mappings in $(O \times F \times M)$



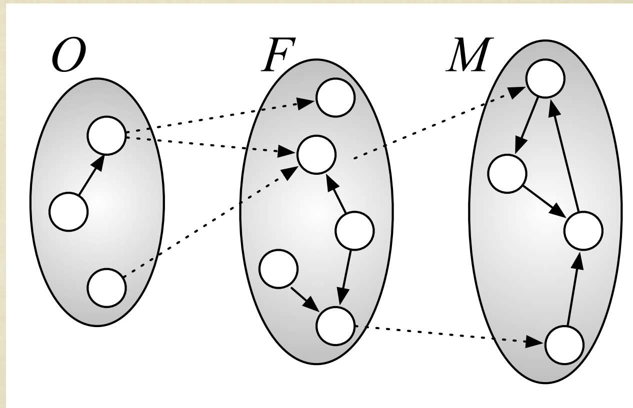
Intra-dependencies

- Relationship **within** Operations, Functionalities, and Modules

$$\mathcal{G}^O = (O, \prec^O)$$

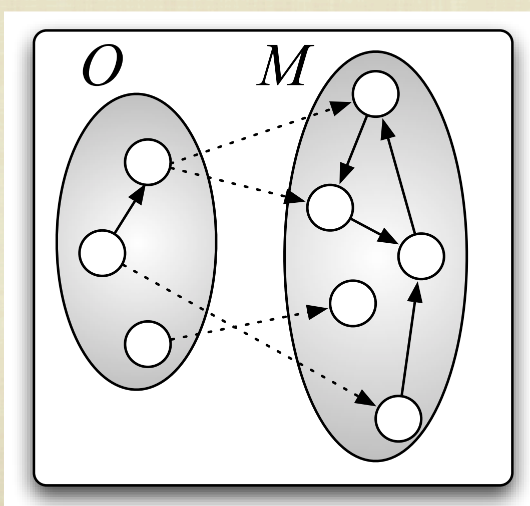
$$\mathcal{G}^F = (F, \prec^F)$$

$$\mathcal{G}^M = (M, \prec^M)$$

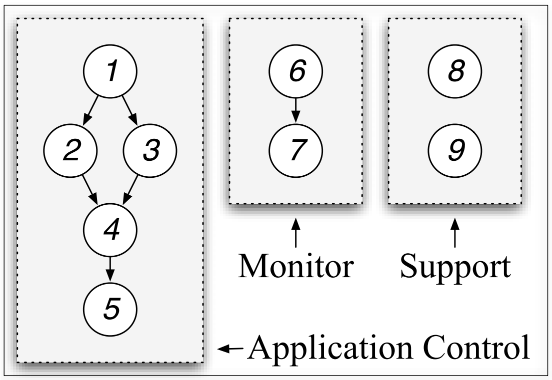


Intra-dependencies

- In our current system we simplify to



Operations & Costates



1 Get Clarus data
2 Receive data from LCS
3 Receive data from Clarus
4 Analyze Clarus data
5 Adjust controller
6 Monitor analysis
7 Monitor adaptive reconfiguration
8 Time synchronization
9 Support routines

Figure 3: Costates and Operations

Sensor-based Model

Sensor-based Model

- Not every behavior can be extracted from profiles or dependencies.
- Specific data sensors are needed to observe specific data values or trigger exceptions.

Exception Triggers

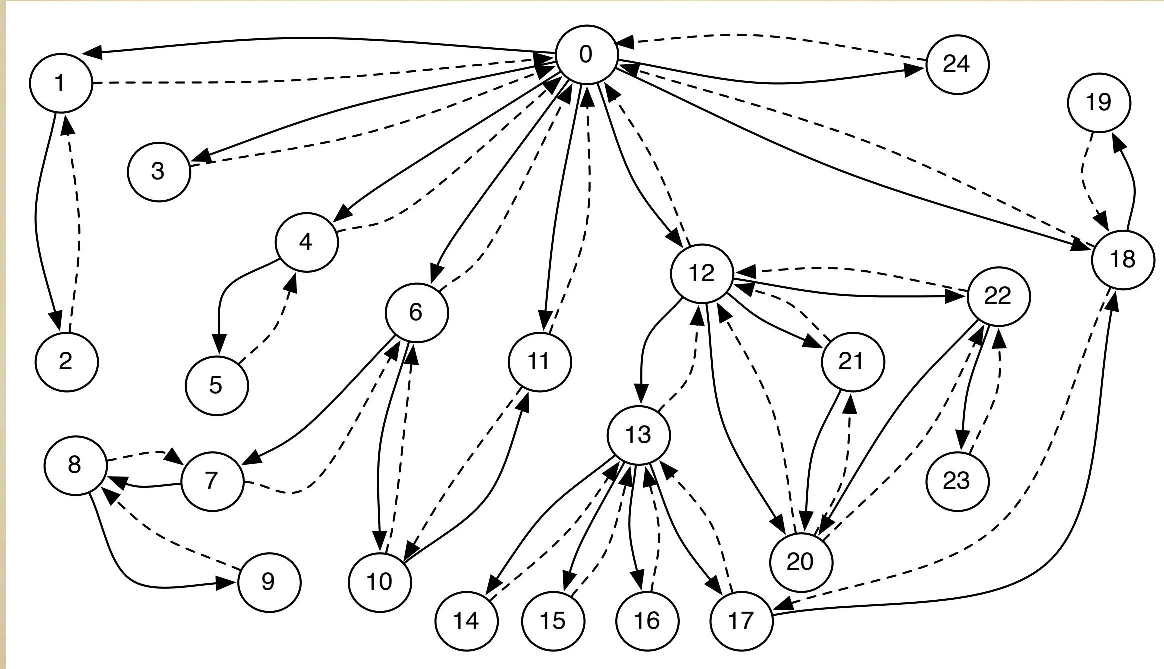
- Exception trigger array
  - identify and profile exceptions, e.g., file does not exist, specific sensor data is not longer available.
  - any error condition can be viewed as an exception trigger

Data Sensors

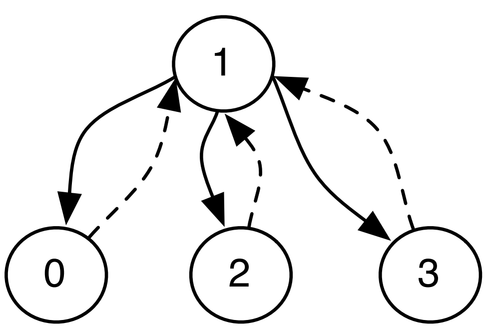
- Observation of specific numeric values for analysis
- Example: the adjustment to the yellow timing
- What happens when someone changes to yellow time to zero? Is that possible?

System Operation & Contingency Management

System Module State Machine



System Operations State Machine

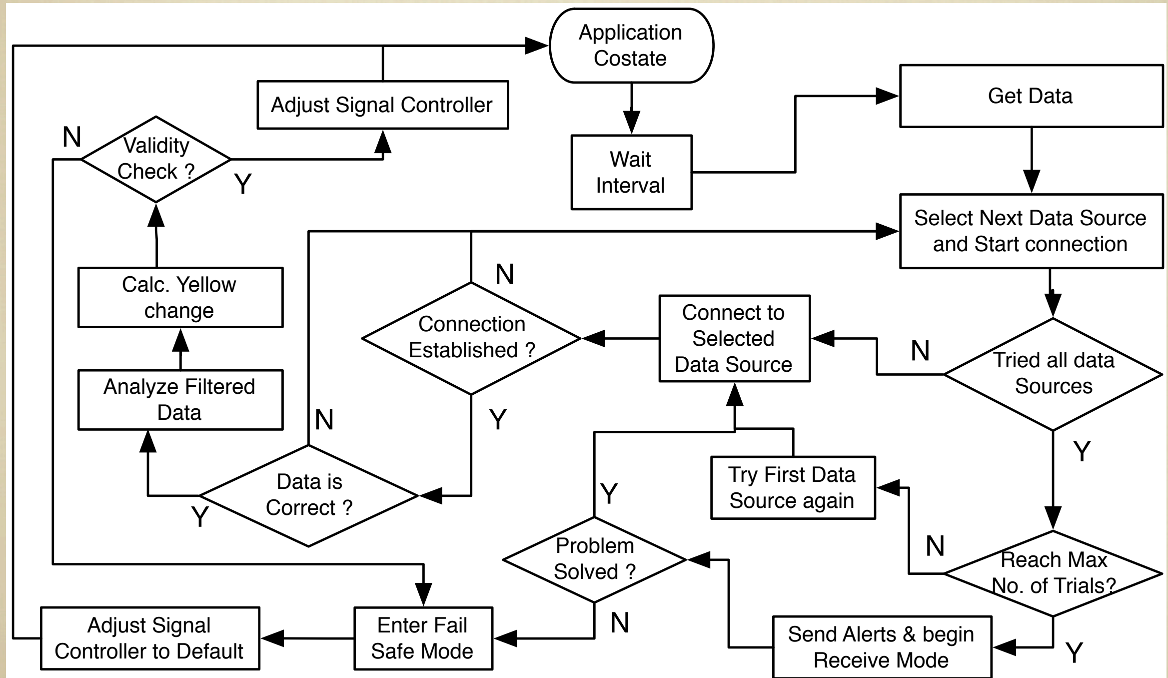


Operations:

0 : Initialize Program
1 : Runtime Timing Module
2 : Get Weather Data
3 : Update Controller

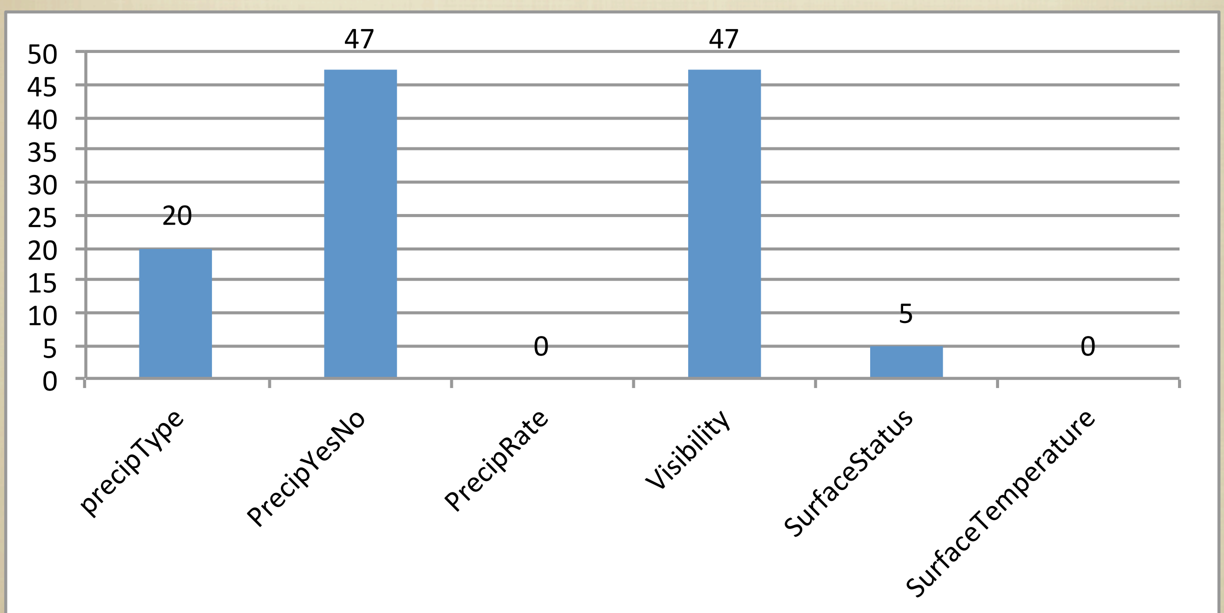
University of Idaho

Application Control Costatement

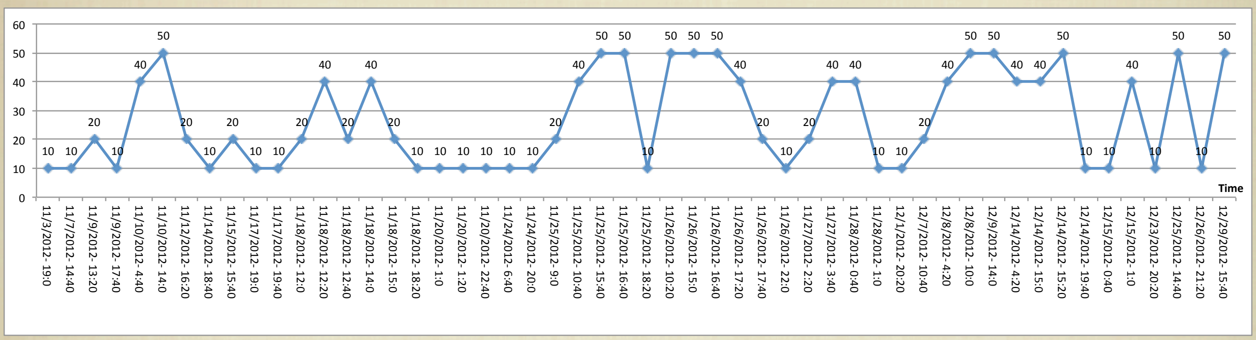


University of Idaho

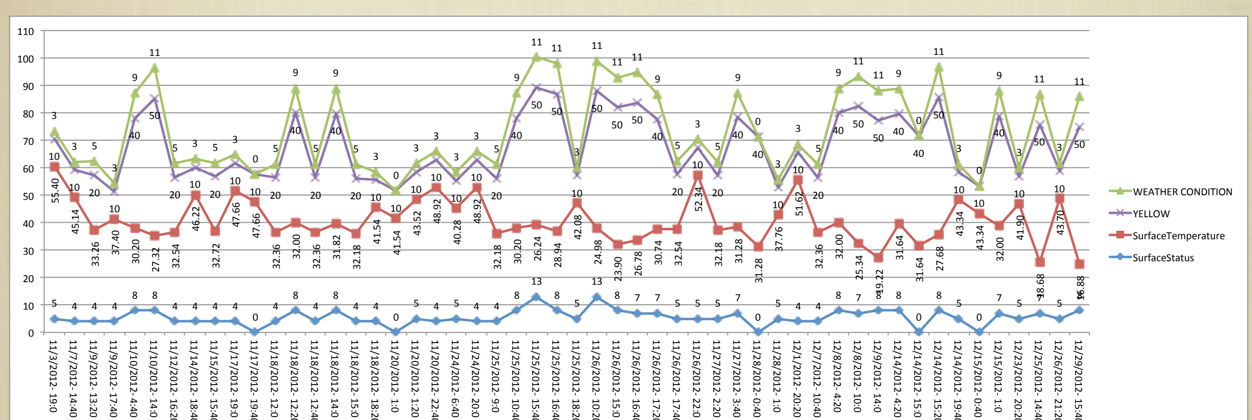
Exception Triggers



Yellow adjustment in % over winter months

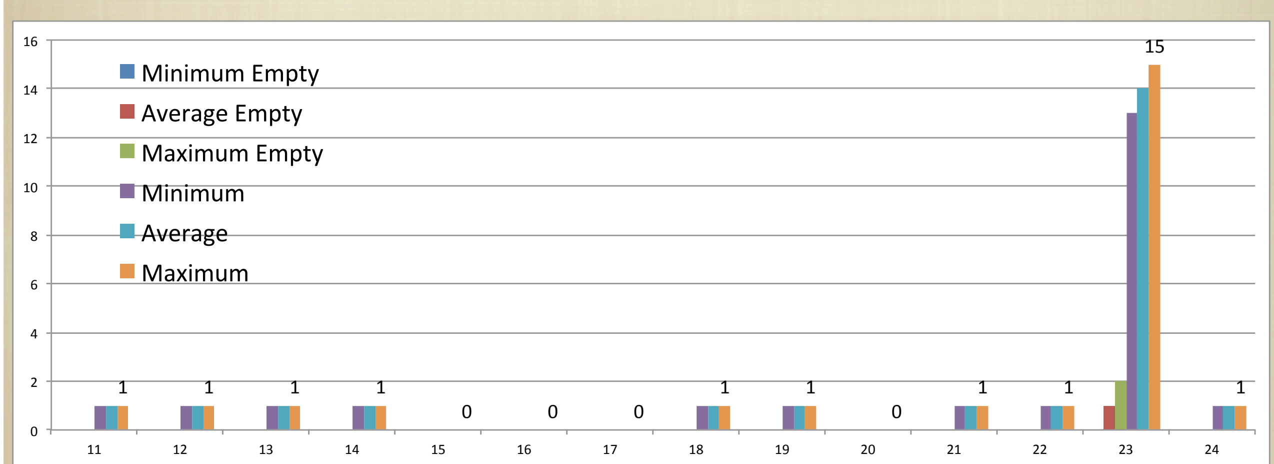


Yellow adjustment in % over winter months



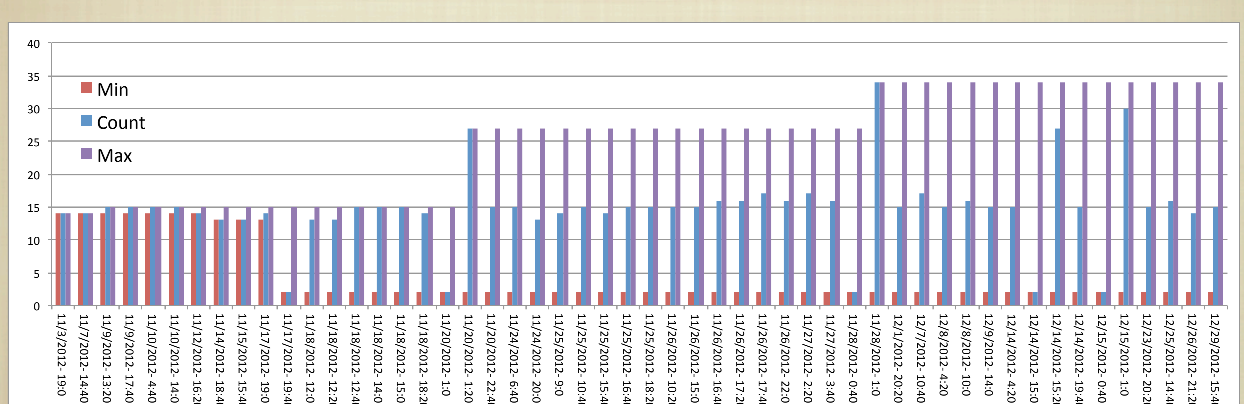
University of Idaho

Profiles of key modules and two nominal behaviors

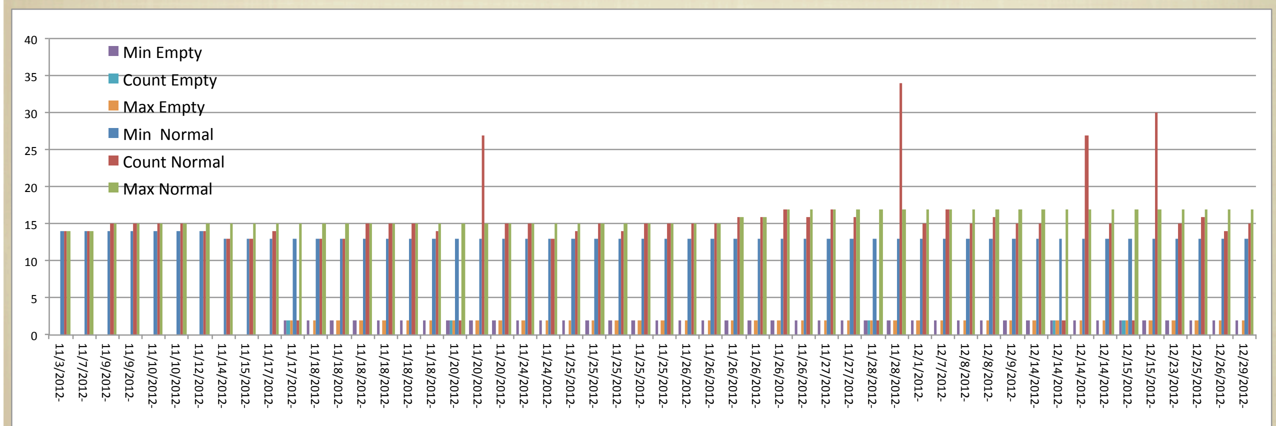


University of Idaho

Profiles of module m23 with behavior set size equal 1



Profiles of module m23 with behavior set size equal 2



University of Idaho

Current Status

- Contingency Management Description:

  A. Serageldin, A. Krings, and A. Abdel-Rahim, "A Survivable Critical Infrastructure Control Application", 8th Annual Cyber Security and Information Intelligence Research Workshop, Oct. 30 Sept. 2 2012, ORNL

  Axel Krings, Ahmed Serageldin and Ahmed Abdel-Rahim, "A Prototype for a Real-Time Weather Responsive System", in Proc. Intelligent Transportation Systems Conference, ITSC2012, Anchorage, Alaska, 16-19 September, pp. 1465 - 1470, 2012.

- Gaining Experience: prototype started running 24/7
  - Mature in setting thresholds.
  - Dealing with realities of Internet access in Intersection

Conclusions

- Prototype has been running over 1 year
  - uses real-time weather data to modify traffic signal timing within safety standard
- Utilization of Design for Survivability
  - Off-nominal executions detected (dual-bound thresholds)
  - Violation of dependencies detected
  - Contingency Management to Recover from anomalies