8.6 Tennessee Eastman Simulation Case Study

8.6.1 Description of the Simulation

The TE model was developed to foster innovation in controller design. The model is non-dynamic and can be considered zero-order; however, the process itself has many variables and can therefore become unpredictable. The model comes with twenty disturbance types defined by Downs and Vogel of which the first twelve were used when applied as one disturbance. To investigate the effect of a generic inline network device such as an industrial firewall on the performance of typical industrial process, a Simulink model was constructed using the TE plant and decentralized controller implemented by Ricker [**7**] and a model of a generic network security device. The architecture for the model is shown in Figure 16.

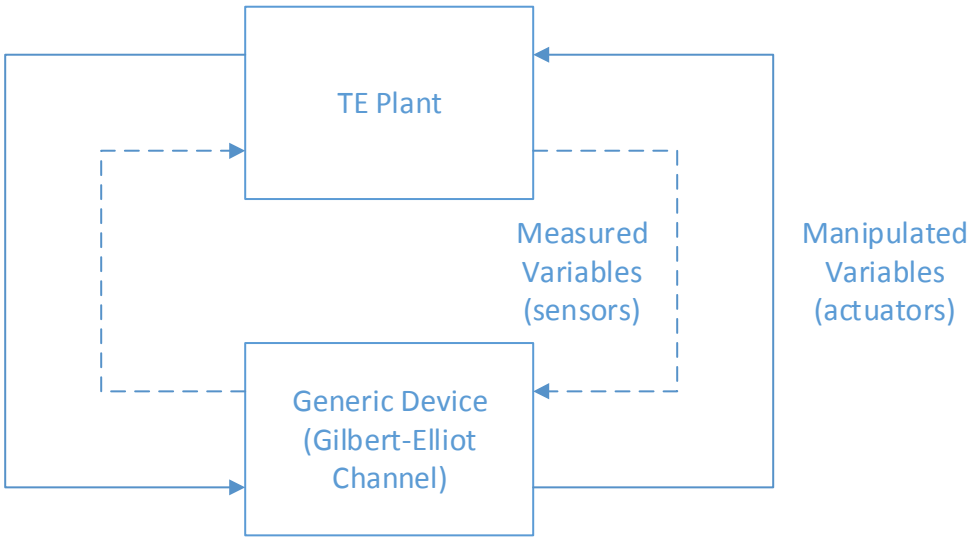

Figure 16. Tennesse Eastman Simulation Architecture using a Gilbert-Elliot Channel Model

A two state Gilbert-Elliot (GE) model [**14**] was chosen to emulate the behavior of a network device in which a scanning device such as a PLC interrogates sensors within a plant process. [**15**] Each scan places a load on the device. The applied load depends on the number of devices scanned, the protocols used, the processing and memory capabilities of the device, and the complexity of the rules being applied. The latency distribution of packets between the plant and controller will determine what sensors are scanned and what actuators are updated successfully. It is assumed that the link states will follow a burst error pattern similar to a two-state Gilbert model that depends on the load applied. The model for a two-state GE channel is shown in Figure 17.[7] Each measured variable is implemented with a Gilbert channel that is independent of the other measured variables; however, each channel is implemented with the same P and R values.

[7] The Gilbert model is one approach to characterizing a generic security device. Using a probabilistic channel model can provide clear guidance to component manufacturers on how to design their devices and to system integrators on how to deploy those devices. Research is required and industry participation will be necessary to select an appropriate channel model for industrial networks. A documented test approach for a generic industrial security device may be necessary to achieve industry acceptance.

The GE model has two states, “good” and “bad.” The good state indicates that the network device is loaded such that traffic is allowed to pass through in time to be captured by the scanning device within its scan interval. The bad state indicates that the network device is overloaded to the point that packets are delayed enough to be missed by the scan or discarded by the device. When the GE channel is in the bad state, the PLC will use the last known measured value.

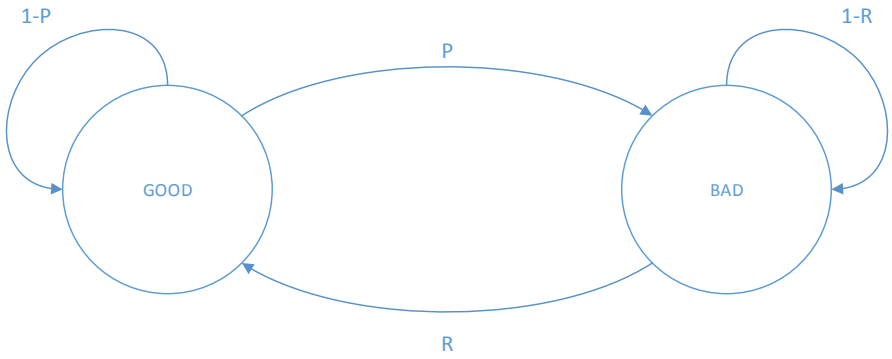

Figure 17. Simple Gilbert Channel Model for a Generic Network Device

8.6.2 Discussion of the Results

A parametric sweep was performed by varying the P and R probabilities for each disturbance type. In addition, four multi-point disturbance vectors were activated at random, and the probabilities were again swept for each. For each disturbance type and probability pair, a time series was recorded for each measured process variable and quality indicator as a function of P and R probability values. The disturbance vector was applied at time t=0, and only the transient response was considered for each. The raw results were stored in a separate folder for each disturbance vector.[8] The time series data was then post-processed to produce selected metrics. Computed metrics types for each measure variable and quality indicator are listed in Table 10.

Table 10. Metrics Types Collected from the TE Simulation

Metric	Description
Shutdown indicator	True if the plant shutdown[9]
Average deviation	The average deviation detected from the baseline condition of all measured variables
Maximum deviation	The maximum deviation detected from the baseline condition of all measured variables
Variance of deviation	The variance of the deviation from the baseline case of all measured variables

[8] The raw output data is stored in the GitHub repository in ZIP format. The TEsim code and data repository can be cloned from the URL https://github.com/NIST-ICS-SEC-TB/TEsim.git.

[9] A shutdown condition will occur in *TEsim* if a measured variable exceeds a predefined threshold. Shutdown thresholds are hard-coded in *temexd.c* and altering the thresholds requires a recompile.

Metric	Description
Correlation to baseline	The correlation of the measured variable to the baseline case of all measured variables
Operating Cost Correlation	The correlation between operating cost and the baseline case
Operating Cost Max. Deviation	The maximum deviation of operating cost to the baseline case
Percent G Correlation	The correlation of operating cost to the baseline case
Percent G Max. Deviation	The maximum deviation between operating cost and the baseline case
Percent G Variance of Deviation	The variance of the molar percentage of G from the baseline case

A full listing of the calculated metrics is given in Table 11.

Table 11. Listing of the METRICS Table in the Results Database

Name	Type
P	Double
R	Double
IDVnum	Double
Shutdown	Integer
AVGDEV from A feed stream 1	Double
AVGDEV from D feed stream 2	Double
AVGDEV from E feed stream 3	Double
AVGDEV from A and C feed stream 4	Double
AVGDEV from Recycle flow Stream 8	Double
AVGDEV from Reactor feed rate stream 6	Double
AVGDEV from Reactor pressure	Double
AVGDEV from Reactor level	Double
AVGDEV from Reactor temperature	Double
AVGDEV from Purge rate stream 9	Double
AVGDEV from Product separator temperature	Double
AVGDEV from Product separator level	Double
AVGDEV from Product separator pressure	Double
AVGDEV from Product separator underflow stream 10	Double
AVGDEV from stripper level	Double
AVGDEV from stripper pressure	Double
AVGDEV from Stripper underflow stream 11	Double
AVGDEV from stripper temperature	Double
AVGDEV from strippx steam dew	Double
AVGDEV from Compressor work	Double
AVGDEV from Reactor cooling water outlet temperature	Double
AVGDEV from separator cooling water outlet temperature	Double
AVGDEV from Reactor feed A	Double
AVGDEV from Reactor feed B	Double
AVGDEV from Reactor feed C	Double
AVGDEV from Reactor feed D	Double
AVGDEV from Reactor feed E	Double

Name	Type
AVGDEV from Reactor feed F	Double
AVGDEV from Purge gas A	Double
AVGDEV from Purge gas B	Double
AVGDEV from Purge gas C	Double
AVGDEV from Purge gas D	Double
AVGDEV from Purge gas E	Double
AVGDEV from Purge gas F	Double
AVGDEV from Purge gas G	Double
AVGDEV from Purge gas H	Double
AVGDEV from Product D	Double
AVGDEV from Product E	Double
AVGDEV from Product F	Double
AVGDEV from Product G	Double
AVGDEV from Product H	Double
MAXDEV from A feed stream 1	Double
MAXDEV from D feed stream 2	Double
MAXDEV from E feed stream 3	Double
MAXDEV from A and C feed stream 4	Double
MAXDEV from Recycle flow Stream 8	Double
MAXDEV from Reactor feed rate stream 6	Double
MAXDEV from Reactor pressure	Double
MAXDEV from Reactor level	Double
MAXDEV from Reactor temperature	Double
MAXDEV from Purge rate stream 9	Double
MAXDEV from Product separator temperature	Double
MAXDEV from Product separator level	Double
MAXDEV from Product separator pressure	Double
MAXDEV from Product separator underflow stream 10	Double
MAXDEV from stripper level	Double
MAXDEV from stripper pressure	Double
MAXDEV from Stripper underflow stream 11	Double
MAXDEV from stripper temperature	Double
MAXDEV from strippx steam dew	Double
MAXDEV from Compressor work	Double
MAXDEV from Reactor cooling water outlet temperature	Double
MAXDEV from separator cooling water outlet temperature	Double
MAXDEV from Reactor feed A	Double
MAXDEV from Reactor feed B	Double
MAXDEV from Reactor feed C	Double
MAXDEV from Reactor feed D	Double
MAXDEV from Reactor feed E	Double
MAXDEV from Reactor feed F	Double
MAXDEV from Purge gas A	Double
MAXDEV from Purge gas B	Double
MAXDEV from Purge gas C	Double
MAXDEV from Purge gas D	Double
MAXDEV from Purge gas E	Double
MAXDEV from Purge gas F	Double
MAXDEV from Purge gas G	Double
MAXDEV from Purge gas H	Double

Name	Type
MAXDEV from Product D	Double
MAXDEV from Product E	Double
MAXDEV from Product F	Double
MAXDEV from Product G	Double
MAXDEV from Product H	Double
VAR from A feed stream 1	Double
VAR from D feed stream 2	Double
VAR from E feed stream 3	Double
VAR from A and C feed stream 4	Double
VAR from Recycle flow Stream 8	Double
VAR from Reactor feed rate stream 6	Double
VAR from Reactor pressure	Double
VAR from Reactor level	Double
VAR from Reactor temperature	Double
VAR from Purge rate stream 9	Double
VAR from Product separator temperature	Double
VAR from Product separator level	Double
VAR from Product separator pressure	Double
VAR from Product separator underflow stream 10	Double
VAR from stripper level	Double
VAR from stripper pressure	Double
VAR from Stripper underflow stream 11	Double
VAR from stripper temperature	Double
VAR from strippx steam dew	Double
VAR from Compressor work	Double
VAR from Reactor cooling water outlet temperature	Double
VAR from separator cooling water outlet temperature	Double
VAR from Reactor feed A	Double
VAR from Reactor feed B	Double
VAR from Reactor feed C	Double
VAR from Reactor feed D	Double
VAR from Reactor feed E	Double
VAR from Reactor feed F	Double
VAR from Purge gas A	Double
VAR from Purge gas B	Double
VAR from Purge gas C	Double
VAR from Purge gas D	Double
VAR from Purge gas E	Double
VAR from Purge gas F	Double
VAR from Purge gas G	Double
VAR from Purge gas H	Double
VAR from Product D	Double
VAR from Product E	Double
VAR from Product F	Double
VAR from Product G	Double
VAR from Product H	Double
CORR of A feed stream 1	Double
CORR of D feed stream 2	Double
CORR of E feed stream 3	Double
CORR of A and C feed stream 4	Double

Name	Type
CORR of Recycle flow Stream 8	Double
CORR of Reactor feed rate stream 6	Double
CORR of Reactor pressure	Double
CORR of Reactor level	Double
CORR of Reactor temperature	Double
CORR of Purge rate stream 9	Double
CORR of Product separator temperature	Double
CORR of Product separator level	Double
CORR of Product separator pressure	Double
CORR of Product separator underflow stream 10	Double
CORR of stripper level	Double
CORR of stripper pressure	Double
CORR of Stripper underflow stream 11	Double
CORR of stripper temperature	Double
CORR of strippx steam dew	Double
CORR of Compressor work	Double
CORR of Reactor cooling water outlet temperature	Double
CORR of separator cooling water outlet temperature	Double
CORR of Reactor feed A	Double
CORR of Reactor feed B	Double
CORR of Reactor feed C	Double
CORR of Reactor feed D	Double
CORR of Reactor feed E	Double
CORR of Reactor feed F	Double
CORR of Purge gas A	Double
CORR of Purge gas B	Double
CORR of Purge gas C	Double
CORR of Purge gas D	Double
CORR of Purge gas E	Double
CORR of Purge gas F	Double
CORR of Purge gas G	Double
CORR of Purge gas H	Double
CORR of Product D	Double
CORR of Product E	Double
CORR of Product F	Double
CORR of Product G	Double
CORR of Product H	Double
Corr_to_OpCost	Double
MaxDev_from_OpCost	Double
Corr_to_PctG	Double
MaxDev_from_PctG	Double
Var_from_PctG	Double

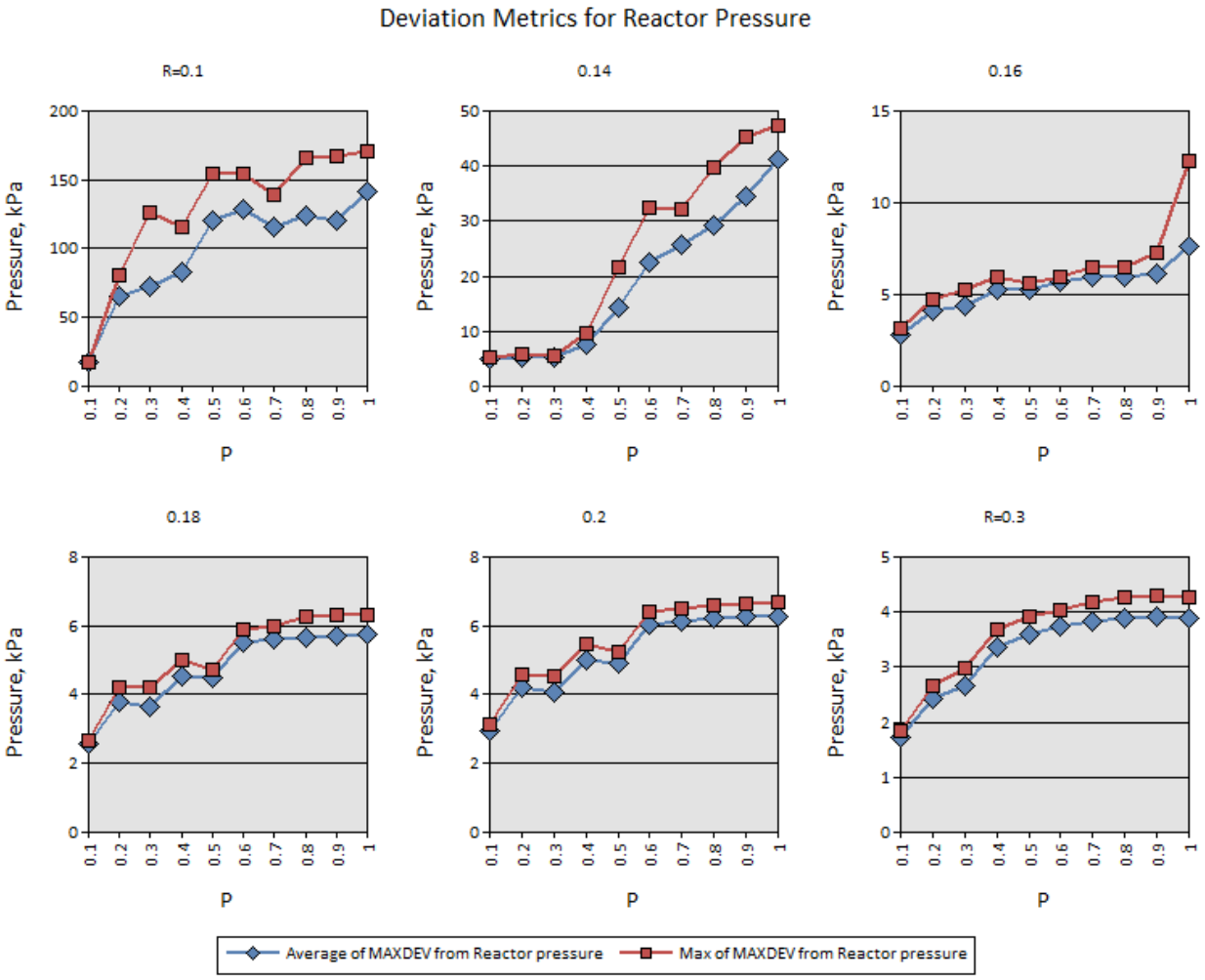

Figure 18. Reactor Pressure Metrics for All Disturbances

Metrics are stored in a Microsoft Access database allowing for easier filtering and analysis of the data.

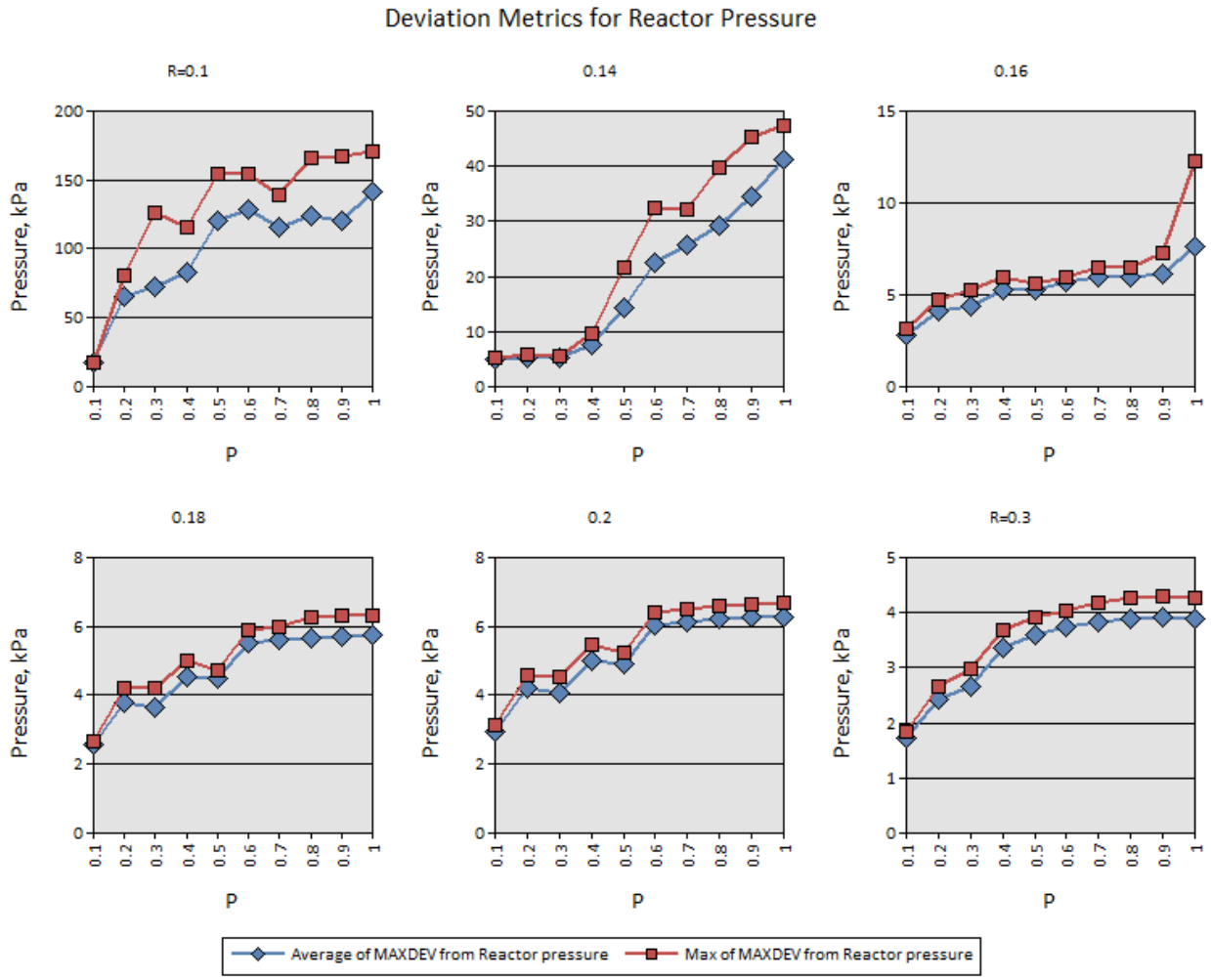

Figure 18 - Figure 22 illustrate some computed metrics for reactor pressure, product quality, and cost. Maximum deviation is computed for each disturbance vector and P-R pair, and each is stored separately in a metrics database.

Investigating the charts in

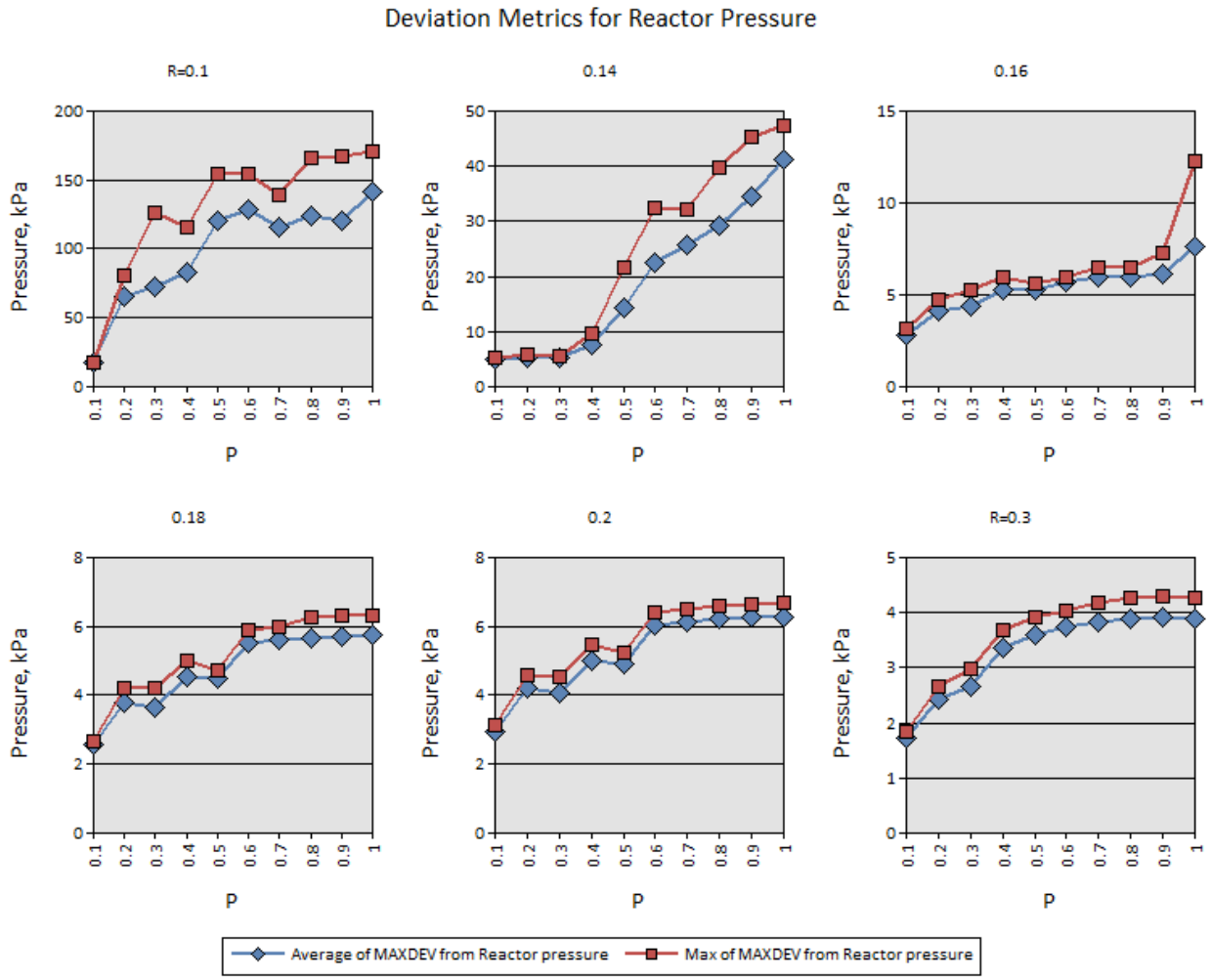

Figure 18, it is clear that the reactor pressure deviates significantly from the baseline case as P exceeds 0.1 and R remains below 0.18. The metrics shown in the charts are for all disturbances vectors combined. Although the metrics shown in the figure are computed for all disturbance scenarios, a benefit of storing the metrics in a database is that the metrics can be refined by targeting a specific disturbance vector or set of vectors by modifying the underlying query.

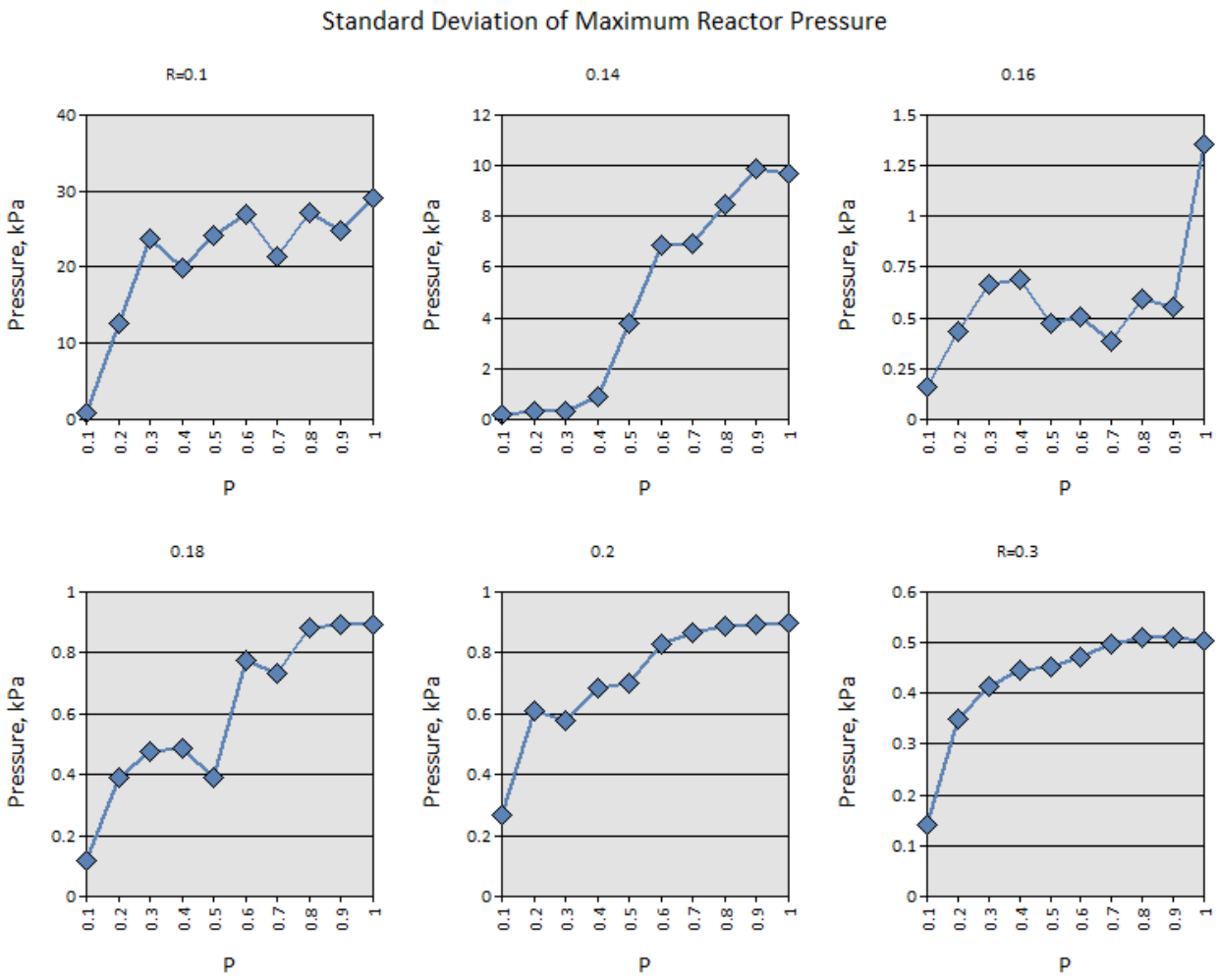

Figure 19. Standard Deviation of the Maximum Reactor Pressure Deviation for All Disturbances

Examination of Figure 19 shows that the 1-σ deviation of the reactor pressure climbs to approximately 25 kPa when all disturbances vectors are considered which may be significant to a plant operator who desires to operate the reactor close to the shutdown pressure threshold of 3,000 kPa. Only the plant operator can determine how significant such a deviation is to plant operations.

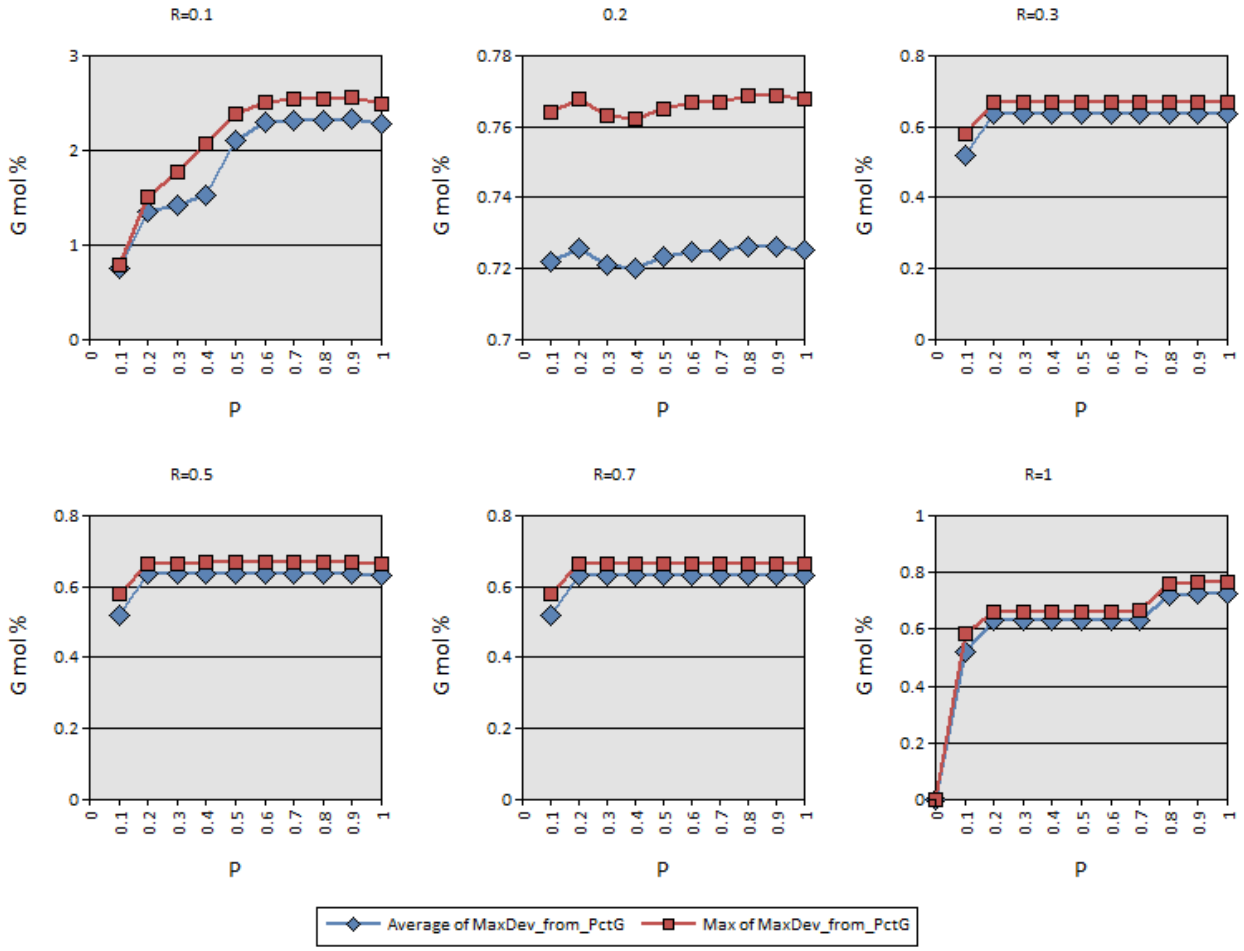

Figure 20. Product Quality Metrics for All Disturbances

Another key performance metric is product quality. Product quality is measured as a molar percentage of the overall production output. The product quality metric is computed here as a deviation to the baseline case. Figure 20 shows the product quality metrics aggregated for all disturbance types. As a sanity check, the baseline case is shown in the bottom right graph for P=0, R=1 to have zero molar percent deviation from the baseline case. All other charts show a deviation in chemical composition of the process output between 0.6% and 0.8%. The significance of these deviations is determined by the requirements of the downstream process which was not described by Downs and Vogel. [**4**]

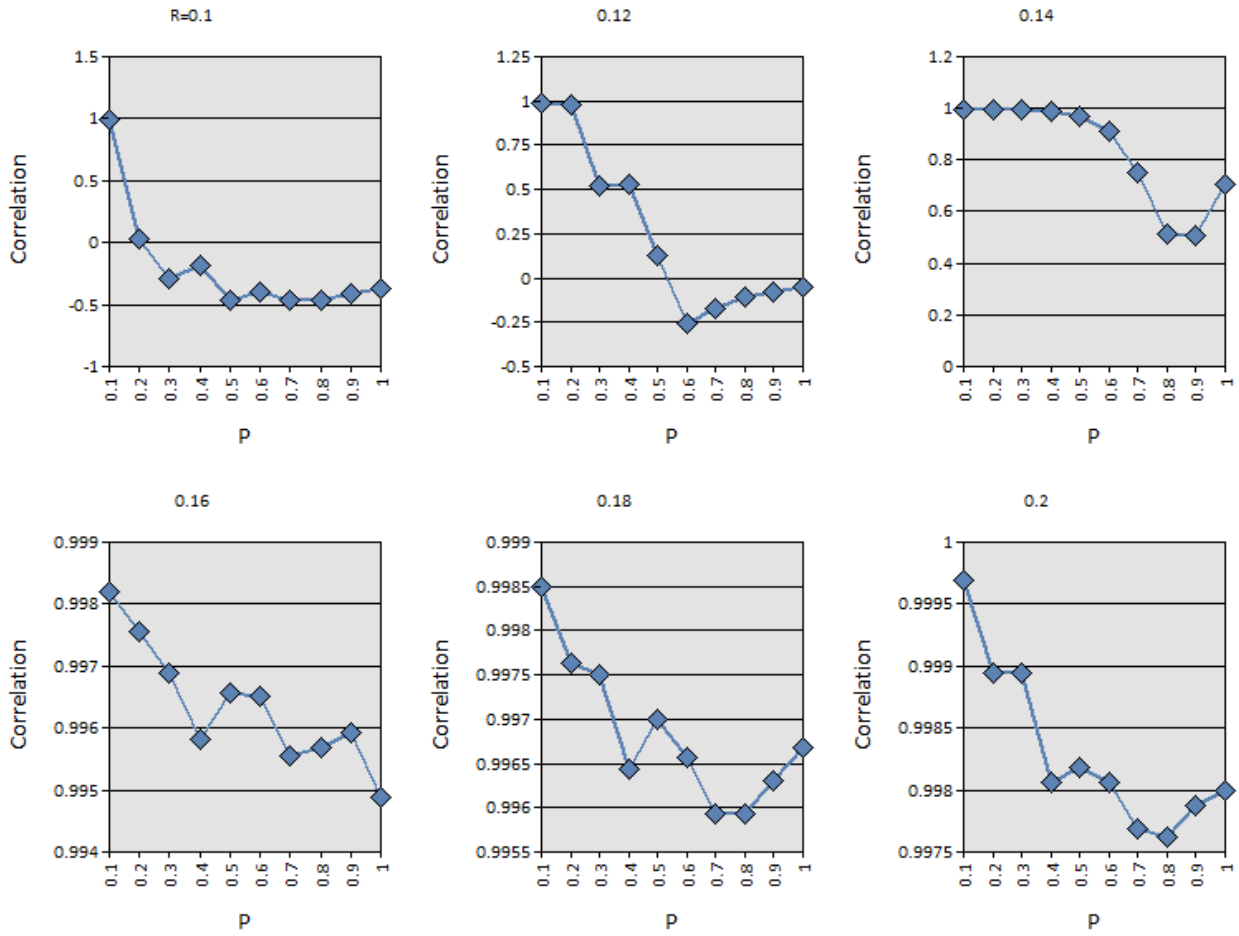

Figure 21. Operating Cost Metric for All Disturbances

Operating cost is a significant metric to process operators and is the final metric presented here. The operating cost metric is presented as a correlation between the baseline case and the test cases. Correlation, calculated as a dot product between two vectors, provides a perspective on how well one signal tracks another assuming that the signals follow a linear regression. A correlation value of 1 indicates the baseline case and the test case track identically. A correlation of zero indicates that the baseline and test cases do not seem to be linked. A negative correlation indicates that the test cases diverge from the baseline case. Shown in Figure 21 are correlations between the baseline operating cost and the operating cost of each test case across all disturbance types for progressively increasing P and R values. For values of R>0.1, the data indicates that the operating cost remains relatively unchanged even for values of P approaching unity. For values of R>0.5, it is clear that the test cases can be considered equivalent to the baseline case. This indicates that a high recovery probability is essential to maintaining expected operating costs.

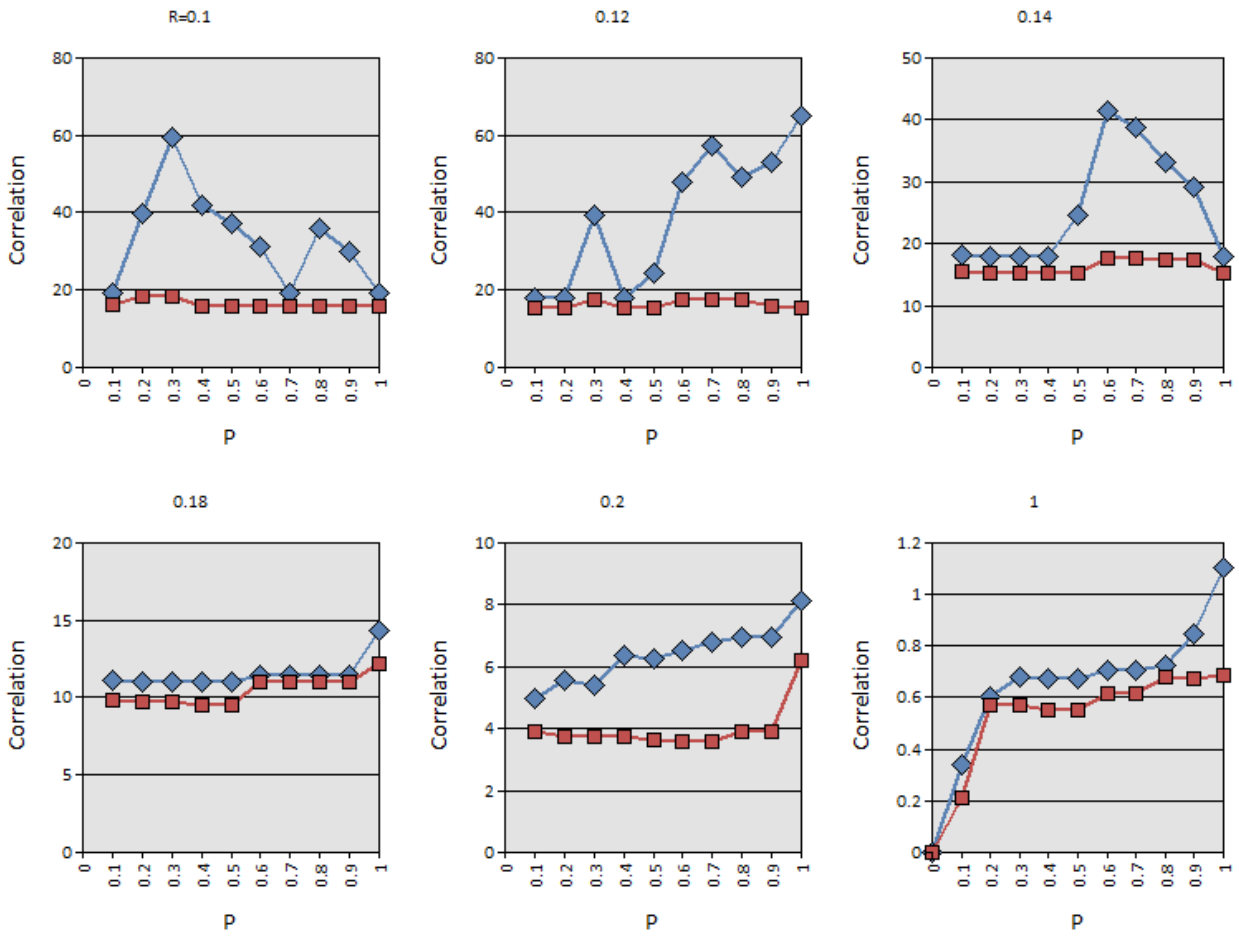

Figure 22. Deviation of Operating Cost from Baseline

While correlation of operating cost between the baseline case and the test cases is an interesting metrics, an operator would still want to understand the cost deviation from baseline. Cost deviation from baseline is shown in Figure 22. Cost Deviation is calculated as the baseline cost minus the test case cost. While one may expect operating costs to rise if the network is impacts, the opposite is actually true for *TEsim*. Operating costs are primarily a function of the rate of consumption of raw materials. Raw materials are lost in the purge gas, the product stream, and by two side reactions. A reduction in cost could indicate an undesirable affect to product quality that may impact downstream processes and ultimately increase costs.

8.6.3 Conclusions and Recommendations

The TE model provides a large number of variables by which to measure performance. By applying various disturbances and channel model probabilities, over 2000 different scenarios were executed. Time series data sets for each of the 41 measured variables and several other indicators for each scenario were generated. The raw output data for each disturbance vector and channel model was stored in a MATLAB formatted data file (i.e., a ".mat" file). Scripts were developed to produce statistical metrics for the data and collect the metrics in both a Microsoft® Excel spreadsheet and a Microsoft® Access database. All code and metrics were stored for public use in the *TEsim* GitHub repository.

The Tennessee Eastman process can be said to exhibit slow dynamics properties, and much of the model as it is implemented can be considered of zero order. However, this does not mean that the "real-world" equivalent would have no dynamic properties. A real world process would exhibit physical oscillations (temperature, pressure, and composition) due to physical and chemical processes. Considering the widespread acceptance of the TE process model by industry and academia, the TE model as it is implemented represents the real-world process accurately enough to measure the effects of a generic network security control on the process.

The *TEsim* results indicate that a simple Gilbert channel between plant and controller does indeed impact process performance when the probability of transition from the good state to the bad state appreciably exceeds zero and the recovery probability, R, remains very low. It is incumbent upon the system integrator to select a network configuration and device capabilities that can accommodate the number of sensors, the number of actuators, and the security policies to be enforced. Enforcement of security may include deep packet inspection, authentication, and encryption all of which will introduce a processing load on the device. It can therefore be recommended that the devices be chosen such that the communications channel between plant and controller is operated in a P-R region appropriate for the application.

Deployment of perimeter security devices to existing industrial applications requires the operator to first ascertain the need for security. This should be performed in accordance with NIST SP 800-82 or an associated standard. If a security posture is required based on the outcome of the risk assessment, the operator must ascertain the impact of security controls on the performance of the industrial process being instrumented assuming that the deployed protocols are compatible with available security devices. Many legacy operations may simply require security controls implemented at the boundary between the ICS and the corporate network or public internet. Other ICSs may require security controls between sensor/actuator space and the controller (i.e., the PLC) as was implemented in *TEsim* model. Once a set of security controls is selected for the ICS, a network architecture must be developed (if the existing architecture can be modified) and security devices must be selected. The security devices should be selected with sufficient processing and memory capabilities to support the intended protocols, traffic, scan rate (if applicable), algorithms, and set of security rules (if applicable). If it is unclear how performance will be affected using the data provided by the device manufacturer, device characterization and simulation is recommended.[10] The GE channel method that was applied to the TE process is one proposed method to measure performance in simulation. Using the *TEsim* method would require the system integrator to characterize each security device with the protocols and rules intended. This approach implies the need for a test method to characterize ICS security devices, yet no NIST-recommended method yet exists for this purpose.

Using *TEsim*, it was demonstrated that for the Tennessee Eastman processes in which sensor and actuators were scanned at a rate of 1 Hz that the channel could tolerate some congestion through the security device if the recovery probability was high enough. As stated, the TE process is slow acting and

[10] A standard test methodology does not yet exist for security device manufacturers and ICS system integrators to measure the performance of a security device as it relates to ICS performance impact assessment.

can tolerate some interruption between plant and controller. Other processes may not be as tolerant to interruption. Examples of such processes may include a robotic assembly process, high speed conveyor operations, and safety applications. Only the plant operator has the knowledge to ascertain the impact of channel congestion on plant performance.

As previously stated, the number of sensors and actuators will impact the load on any aggregating network device including switches, router, and firewalls. Logically grouping networked devices that communicate through a security device may serve as a method to alleviate congestion in a single firewall. While this approach will increase the number of devices to be managed (e.g., rule deployment and key distribution) it could facilitate the enforcement of a stronger security policy on the network or make the network safer to operate.

From a security perspective, it is recommended that the network topology, security devices, and policies be selected appropriate to the estimated security risk in accordance with NIST SP 800-82. It is further recommended that the devices and network topology selected be deployed with sufficient processing headroom should a network-based attack occur. Few industrial network attacks will add significant load to a network channel. Denial-of-service (DoS) attacks are obvious attack types that add significant load to the network as this is the strategy of the DoS attack. Other more stealthy attacks could overload the network channel by putting the security device into a state in which specific rules are executed excessively. Security rules should be designed in such a way that the device cannot be driven into an overload state. Depending on the estimated risk, an accurate software-based simulation that includes the may be used to ascertain the impact of security controls on the performance of the industrial process.