

The Business Case For Automated Robustness Testing: Measuring Return On Investment For Industrial Control System Manufacturers



Introduction

In the never-ending race to offer more features at a faster pace, industrial control systems are getting more complex, open, and inter-connected, making it a significant challenge to ensure robustness and reliability. Accelerated convergence of IP technology along with the increased sophistication and frequency of cyber threats further exacerbates the problem, making system robustness testing ever more important than ever.

Unfortunately, today we are seeing a greater number of unforeseen outages, downtimes, and disruptions which are simply not acceptable in mission-critical operations and that cause significant business risks to not only the end-user but also the vendor. In an attempt to address these risks, large equipment manufacturers of process control systems have been increasing spending on proactive security and robustness testing technology, but the financial benefits of implementing these systems are still poorly understood. Without a strong business case for improved security and robustness testing it is unlikely that the vendor community will move quickly and reliably to widely adopt new technology.

This white paper provides a framework for manufacturers of industrial control systems to estimate the return on investment (ROI) of integrating security & robustness testing technology into their product development lifecycle. We'll first look at the overall costs and benefits of robustness testing and then provide a financial model to estimate the ROI based on input from equipment manufacturers of control systems.

The Business Case For Automated Robustness Testing

Automated security and robustness testing technology is a solution to a growing problem facing manufacturers of industrial control systems: how to produce secure, reliable and safe products with ever-more complex technology under increasing competitive pressure. According to Frost & Sullivan, approximately \$15 billion a year is spent on automated testing for software and network systems in the industrial automation industry and this figure is expected to grow at 10% per year. To understand why this is, and to formulate a strong business case for investment, we need to review the costs and benefits.

How Does Robustness Testing Create Value?

Robustness testing creates value by revealing bugs in a software system before it is released to production or shipped to customers. If bugs aren't found this way, they are said to "escape." Sooner or later (usually sooner) a customer or end user will do something that triggers an escaped bug. On average, it costs 10 to 1,000 times more to fix an escaped bug than fixing before release. Besides the immediate impact of the failure, escaped bugs usually have other negative consequences on a vendor's bottom-line with significant costs such as:

- Increased overhead costs from higher volume of customer support requests
- Unexpected costs associated with patch distribution, service pack updates, or bug-fix releases.
- Loss of customers to competitors due to plant disruption, outages and/or bad overall experience, leading to lost revenue.
- Loss of customers to competitors due to plant disruption, outages and/or bad overall experience, leading to lost revenue.
- Loss of customers to competitors due to negative publicity and/or word-of-mouth about system failures, leading to lost revenue.
- Lawsuits for injury or damage resulting from a system failure in an operational environment.

These costs can quickly add up, which is why many people look at software testing as a kind of insurance. Automated testing goes beyond basic preventative measures to achieve significant competitive advantage and enhanced financial results.

What Are The Direct Benefits Of Automated Robustness Testing?

Increased Productivity & Effectiveness During Product Development

Probably the most obvious payoff comes in the form of reduced resource requirements to conduct the testing process itself throughout the development lifecycle. Human testers average about one completed test per hour, taking into consideration all of the time needed to design, set up, input, run, observe, evaluate, and document one test case. Although manual testing has a role to play, it just isn't fast enough for today's large, complex, multi-platform control systems.

Another factor that must be considered is that the proper testing of industrial control systems can't be conducted by just anybody; it usually requires an engineer that is familiar with the design of the product, the characteristics of likely or known problem areas, the existing cyber threat landscape of known vulnerabilities, the sequence of events required to simulate a particular state, and so on. This expertise is rare and often very expensive to the organization. Reducing these costs are one major advantage of an automated security and robustness testing platform.

Besides just running tests faster, and more effectively, an automated platform has other benefits. For example, suppose a tester finds a bug, which a programmer then corrects. On average, 7% of bug fixes create new bugs, so it's a good idea to run the same test again and repeat previous tests on other parts of the system. But this almost never happens when testing is done manually. In summary, an automated security and robustness testing platform can amplify the basic value of testing in several ways:

- **More testing gets done faster:** This increases the odds of revealing bugs, thereby avoiding the costs and consequences of bugs being found in the field.
- **Tests can be repeated exactly:** Automatic retesting allows existing test scenarios to be run many times, with identical input and timing on each run. The same test cases are used as systems change, providing consistent results.
- **Tests can be reused and rerun at will:** The incremental cost to rerun an automated test is insignificant, so the unchanged parts of a system can be quickly and consistently rechecked. This greatly increases the chance of revealing new bugs that are side-effects of new or changed software.
- **Realistic stress and stability testing becomes feasible:** Many bugs are triggered only when a system is tested with a high input rate or run continuously for many hours. It's usually not possible to achieve these conditions with manual testing.

Reduced Time-To-Market For New Products, Versions or Features

In today's highly competitive market for industrial automation systems, delivering products, or new product features, to market quickly has become an absolute mandate as the financial benefits can be significant. For example:

- Earlier entry with a new product or feature often translates into a greater share of the market.
- Higher market share usually translates to lower unit cost, compared with a competitor's lower volume, higher unit-cost product. Moreover, higher volume usually means greater quantity discounts from suppliers and better operating efficiency. This is especially important if a product requires third-party component integration which is common in industrial automation.
- Having more time to sell your product, or feature before competition typically results in increased total revenue will achieve a higher rate of return on the initial product investment and other investment ratios.
- As revenue is realized sooner, manufacturers can accelerate the investment recovery for the product reaching breakeven and target ROI earlier.

Consequently, every day a product is not available in the market, revenue is reduced by sales being lost to competitors. Of course, this situation is not completely avoidable – there is no such thing as immediate delivery of a new product to market. But minimizing time to market is a goal that just about every equipment manufacturer strives to achieve.

Automated security and robustness testing technology offers the control system manufacturer a way to reduce time to market by compressing the stages of the development lifecycle prior to deployment. For control system manufacturers, the testing phase of the development lifecycle usually comprises a major component of time to market and therefore reducing the time required to test is extremely valuable.

What Are The Indirect Benefits Of Automated Robustness Testing?

The primary purpose of this white paper is to document the tangible financial benefits and cost savings associated with integrating automated security and robustness testing technology into the development lifecycle of industrial control systems, typically measured in three ways: increased test efficiency, increased test effectiveness, and shorter time to market. However, for manufacturers, the benefits go far beyond the return on investment in terms of reduced cost of testing, reduced time to market and improved product quality, and instead provide additional strategic benefits that are essential to an organizations' growth and success.

- **Leverage Security and Robustness As Product Differentiator:** Many security and robustness testing technologies offer an additional certification designation for products that meet proprietary conformance criteria. Manufacturers that embrace security as a strategic priority can differentiate their products from their competitor and generate more revenue.
- **Meet Customer Procurement Requirements:** Many end users are now introducing security and robustness criteria into their formal procurement requirements. Manufacturers that do not meet these criteria will be disqualified from preferred vendor lists and may be unable to bid on new project opportunities
- **Prepare For Emerging Standards:** Another factor to consider as a manufacturer of industrial control systems is that as government regulations increase and international cyber security standards such as ISA SP99 emerge, product robustness will soon be a requirement. By investing early in security and robustness testing technology, manufacturers can plan for, and reduce, the additional expenses associated with product certification and conformance. Although these strategic benefits of test automation are not as readily quantifiable as the tactical or operational benefits discussed in this paper, in the long run, their value to the organization can be many times more important.

What Does The Business Case Look Like In Financial Terms?

Although many studies have been done measuring the direct / indirect benefits for automating software testing in the enterprise software market, there have been no formal studies of test automation for industrial control system manufacturers. Moreover, given the nascent nature of cyber security as a business issue for industrial stakeholders, there is likely a significant asymmetry in the development processes, tools, and manpower investments of the various which makes direct comparisons difficult and model consistency a challenge. However, as outlined above, there are clearly many benefits to be realized by integrating and automating robustness testing into the development lifecycle that can be measured so for the purpose of this paper, we created a light-weight model from which to quantify estimates given a sample of data from a current Achilles Satellite user. The estimates reflect typical test automation costs and benefits as outlined above such as:

- Increased testing productivity
- Increased test effectiveness.
- Reduced time-to-market and the
- Cost to acquire, convert, and use the Achilles Satellite robustness testing platform

Test Investment Parameters

To start, the model needed some baseline assumptions to estimate effects and costs. The following assumptions were made from information provided by an Achilles user:

- The device under test would be their primary Distributed Control System (DCS).
- One control protocol would be tested on one communication module.
- Vendor decided to train both development engineers and quality assurance staff (5 persons in total) on the Achilles Satellite platform.
- Vendor started with 50 individual test scenarios based on the use of Sully, a common manual fuzz test creation platform.
- Testing scenarios could be repeated on four differently configured platforms.
- Manual testing of system would take 8 weeks, or 40 elapsed days.
- Vendor assumed two releases per year.
- Cost of the Achilles Satellite is annualized over 3 years at \$35,000

Number Of Testers	5	Persons	Number Of Developers And Testers To Support
Hourly Cost, Each Tester	\$50.00	Dollars	Average Fully Burdened Hourly Cost Per Tester
Existing Manual Test Procedures	50	Procedures	Number Of Existing Manual Test Procedures
Unique Configurations	4	Platforms	Number Of Different Platforms Tested
Number Of Releases Per Year	2	Releases	Number Of Releases Per Year
Existing Manual Test Duration	45	Days	Average Manual Testing Duration
Scope Growth	10%	Rate	Average Testing Scope Growth
Achilles Hardware / Software Cost	\$ 35,000	Dollars	Annualized Cost Over 3 Years

Test Productivity Parameters

The productivity parameters define the average work hours to create, run, and maintain manual tests and are as follows:

Test Scenario Design Work	11.6	Hours	Average Time To Design A New Test Scenario
Test Procedure Conversation Work	4	Hours	Average Time To Convert A Procedure To A Test Object
Test Object Coding Work	7.9	Hours	Average Work To Code A Test Scenario In A Test Object
Test Object Run Work	0.2	Hours	Average Time To Run A Test Object
Test Procedure Run Work	3.9	Hours	Average Time To Manually Run A Test Scenario
Test Procedure Maintenance Work	2	Hours	Average Work To Change A Manual Test Procedure
Test Object Maintenance Work	4	Hours	Average Work To Change A Test Object

Test Effectiveness Parameters

The effectiveness parameters define assumptions about how many bugs will be found and the average cost of escaped bugs. The following assumptions were provided.

Test Effectiveness Improvement	2	Factor	Expected Improvement In Bug Removal Rate
Baseline Bad Fix Ration	11%	Percent	Observed Percent Of Fixes That Cause New Bug
Baseline Annual Outage Hours	90	Hour	Observed Outage Hours, Annualized
Average Outrage Cost, \$ Per Hour	\$15,000	Dollars/Hour	Average Cost/Loss Of One Hour Of Unscheduled Downtime
Baseline Annual Incident Reports	120	Incidents	Observed Product/Field Incidents, Annualized
Average Incident Cost, \$ Each	\$7,500	Dollars Each	Average Cost/Loss Of One Production Or Field Bug Report

Estimated Total Return On Investment For Achilles

ROI is (Benefits – Costs) / Costs, in percent. Our simple model also computes months to breakeven and net present value. Based on the entered parameters, the model indicates a manufacturer should go ahead with an investment test automation investment.

- Breakeven payback is estimated at seven months after the improvement project starts.
- The estimated test automation ROI is 1,468% over two years.
- The net present value is positive.

Effectiveness Improvement Estimate

The model estimates the effects of improved bug finding, which leads to improved production/field reliability. Using our 2x assumption, significant cost reductions are forecast.

- System downtime would be reduced by 50%.
- The number of reported bugs would be reduced by 50%.
- For each quarter after the next release, hard costs totaling \$303,705 in downtime, incident, and bad fix expense would be avoided.

Productivity Improvement Estimate

With the Achilles Satellite, a vendor can repeat all test scenarios on each platform with little incremental effort. Due to the decreased time to run test scenarios, a vendor can expect a significant reduction in the direct labor expense for testing.

- \$297,000 reduction in the cost to test the target system
- \$408,278 reduction in the cost to test subsequent releases.

Time To Market Reduction Estimate

The ROI model quantified the opportunity cost of delayed entry for management and the estimated benefits for were significant.

- A 69% decrease in the testing cycle time, or 31 days sooner.
- The estimated additional sales opportunity is \$419,178 in the first quarter of the next release.
- The reduction is expected to produce an additional \$295,890 of revenue in each subsequent quarter, compared to later release dates with manual testing.