



Intel[®] Technology Journal

The Spectrum of Risk Management in a Technology Company

Intel Technology Journal (Vol 11, Issue 2) reviews risk assessment and management at Intel Corp for risks in technology treadmill and daily business execution.

Inside you'll find the following articles:

Managing New Technology Risk in the Supply Chain

Risk Management in Restricted Countries

Managing Product Development Risk

Assessment and Control of Environmental, Safety, and Health Risks in Intel's Manufacturing Environment

Managing Goods and Services Acquisition Risks

Assessing and Managing Asset Loss from Hazard Risks

Using Forecasting Markets to Manage Demand Risk

Maturation of Business Continuity Practice in the Intel Supply Chain

More information, including current and past issues of Intel Technology Journal, can be found at:

<http://developer.intel.com/technology/itj/index.htm>



Intel® Technology Journal

The Spectrum of Risk Management in a Technology Company

Articles

Preface	iii
Foreword	v
Technical Reviewers	vii
Managing New Technology Risk in the Supply Chain	95
Managing Product Development Risk	105
Managing Goods and Services Acquisition Risks	115
Using Forecasting Markets to Manage Demand Risk	127
Risk Management in Restricted Countries	137
Assessment and Control of Environmental, Safety, and Health Risks in Intel's Manufacturing Environment	147
Assessing and Managing Asset Loss from Hazard Risks	157
Maturation of Business Continuity Practice in the Intel Supply Chain	165

THIS PAGE INTENTIONALLY LEFT BLANK

Preface

By Lin Chao

Publisher and Editor, *Intel Technology Journal*

Technology innovation and technology leadership are not possible for technology companies without a never-ending attention to risk and its management. Using Moore's Law as a roadmap, we, at Intel, need to translate the roadmap into innovative products for the market place and to manage the risk associated with product innovations. This includes both processor microarchitecture innovation and silicon process innovations; both of which go hand in hand. We have developed a model to minimize the risk associated with the introduction of new silicon processes and microarchitectures by alternating our focus. This cadence between microarchitecture and the silicon cycle is referred to as the "tick-tock" model [1]. The term "tick-tock" comes from the steady recurrent ticking sound made by a clock. Each "tick" represents the silicon process beat rate, which has a corresponding "tock" representing the design of a new microarchitecture delivered in a cycle approximately every two years. This model minimizes the risk associated with the introduction of new silicon processes and microarchitectures by alternating the focus from silicon to microarchitecture.

This Intel Technology Journal (Vol. 11, Issue 2) on "The Spectrum of Risk Management in a Technology Company" takes an intriguing look at a myriad of risk management techniques used at Intel Corp. The first four papers look at the risk associated with the technology treadmill such as those encountered with technological advances; what competitors are doing; and what the marketplace wants. The second group of four papers looks at risk in daily business execution.

The first paper examines risk associated with advanced technology important in the supply chain. It examines a case study on applying strategic bets in the lithographic supply chain. A system was developed to assess technical and business risk for all components of the supply chain. Then a methodology for identifying fellow travelers, including consortia, was used to create programs to establish a foundation of common technologies such as extreme ultra-violet lithography. The second paper looks at managing product development risk through the implementation of a six-step active risk management process and tool. The process provides a consistent language and approach to measuring risk. The tool provides risk visibility despite the many-to-many relationships that exist between Intel ingredients and platforms to avoid potential costly risk events. Monte Carlo simulations are used.

The third paper in this Intel Technology Journal (Vol. 11, Issue 2) looks at acquisition risk for managing goods and services. We describe three specific risk mitigation techniques: Internet negotiations, escrow accounts, and currency risk reduction to reduce exposure to universal business risks. The fourth paper looks at demand forecasting. Demand risk is implicit to manufacturing

businesses, but for high-tech firms it poses a particularly strong threat. As product lifecycles shrink and new generations of technology enter the market more quickly, achieving strong top- and bottom-line results hinges on estimating overall demand and product mix as accurately as possible. We propose using Information Aggregation Mechanisms (IAMs) to address demand risk and other business challenges by improving organizational information flow. Based on results to date, our IAM implementations appear to have had a desirable impact on forecast accuracy and stability.

The next group of four papers looks at risk in daily business execution. The fifth paper reviews doing business appropriately around the globe. Intel has business and manufacturing locations around the world. This paper describes the complexities of maintaining Intel's business activities in restricted countries including maintaining regulatory compliance, adhering to security guidelines, protecting Intel's intellectual property, and employment. Intel must comply with United States and international law without impeding Intel's growth and continued success in these countries. The sixth paper provides an overview of the major environmental, health, and safety risks that apply to semiconductor manufacturing and what specific approaches are used to assess and reduce the risks in each new generation of facility or semiconductor fabrication process. We show how a systems approach that ties all risks together has helped Intel manage these risks despite significant changes in process and facilities design over the last ten years.

The seventh paper looks at managing loss due to hazard risks which include perils such as fire, explosions, floods, windstorms, earthquakes and typhoons. This paper describes Intel's risk management process for the identification, analysis, and control of hazard loss risks. The eight and final paper examines business continuity process in the supply chain. In order to reliably produce quality products, Intel needs to be able to quickly react to a crisis, ensure continuity of our business, and restore the supply chain. Intel's business continuity methodology, infrastructure, and tools used within Intel's Materials organization have improved Intel's ability to quickly recover from a supply chain outage and restore supply to manufacturing and other operations.

We at Intel Corporation have unique risks as a leading computer company. Our manufacturing environments, which are ultra-clean, pristine fabrication facilities with sensitive, specialized high-value equipment, producing high volumes of product at nano-width geometries with uncompromising quality in of itself creates many challenges. Our abilities to assess, manage and react to risk associated with technology treadmill and everyday business is what keeps Intel at the forefront of our business.

Reference:

- [1] Shenoy, Sunil and Daniel, Akhilesh, *Intel® Architecture and Silicon Cadence: The Catalyst for Industry Innovation*, Technology at Intel Magazine, 2006, October, <http://www.intel.com/technology/magazine/computing/cadence-1006.htm>.

Foreword

By Karl Kempf

Fellow and Director of Decision Technologies

Technology and Manufacturing Group, Intel Corporation

Since 1968, Intel has advanced semiconductor technology using Moore's Law as a roadmap. This has resulted in computing-related products with ever increasing capability and performance, fabrication processes with ever smaller feature sizes, and ever more efficient high-volume manufacturing (HVM) facilities. Many of the successes in these and related areas have been reported in the pages of this Journal over the years. However, to evolve to realize over \$35B in revenue in 2006 requires a wide variety of support capabilities as well. While it is necessary for Intel to continue to lead in the semiconductor technology race, it is arguably not sufficient. For example, a previous issue of this Journal entitled "Managing International Supply and Demand at Intel" (Volume 9, Issue 3, August 2005) described such support capabilities as supply chain planning and inventory modeling. This Intel Technology Journal (Vol. 11, Issue 2) on "The Spectrum of Risk Management in a Technology Company," explains Intel's approach to risk as a support capability that includes technical, marketing, and commercial areas.

Risk comes in many guises for Intel. On the one hand, the high technology component of Intel's business faces a number of sequential issues. The concept of a semiconductor technology race is based on the assumption of a never-ending flow of technical advances that can be turned into useful products that a market will pay to acquire. For Intel, this includes at least innovative physics and materials that support Moore's law. Such advances require years (if not decades) of research to realize, as well as financial, technical, and moral support. As the innovation funnel narrows and specific concepts are selected for reduction to engineering practice, whether in product design or process development, projects have to be completed on time and on budget in a coordinated fashion to sustain Intel's technology lead. Production equipment implementing the new physics and using the new materials can be available in modest quantities for these development projects, but once HVM begins, this equipment is required very quickly in very large numbers. And given the nature of Intel's innovative products, the market must be appropriately prepared to accept them.

There is risk in every component of this repetitive sequence and in the coordination of activities. In the early exploratory steps, the innovations may not materialize or may be realized too slowly. Critical development projects may be delayed or fail due to technical difficulties. Equipment and materials may not be available in appropriate quantities or at acceptable prices when HVM needs them. Of course the most catastrophic risk, at the end of this long series of interacting risks, is that the market will not accept the resulting product. Successful management of these sequential interrelated risks is absolutely essential to the success of Intel as a technology company.

On the other hand, there exists a spectrum of risks, many of which are only peripherally related to the high technology nature of Intel's business. Every company faces risks from natural events such as storms, earthquakes, floods, and so on, depending on the physical location of the company and the luck of the draw. Artificial or human-generated events can be just as disruptive as natural disasters and equally beyond the control of the average company. Accidents happen in the form of fires, lost shipments and a plethora of other causes, some of which can be mitigated. Operating internationally brings with it the risk of incompatible regulations and business practices. Every conscientious company works to avoid causing damage to its physical environment or risk to the health and safety of its employees, suppliers, or customers.

Successful management of this range of risks is often measured in terms of business continuity. Did the company continue to function in an effective manner in the face of various combinations of these risks over time? Perhaps an equally important question, as the commercial landscape continues to become ever more complex, concerns the ability of the company to learn from its experience of being exposed to these risks over time. Managing these commercial risks and answering these questions is in many cases equally important to Intel's prosperity as is managing the technical and marketing risks described above.

Moreover, cutting across all of these risks is the sobering fact that risks are dynamic. Old risks subside and new risks rise up to take their place. Risks that were adequately characterized and mitigated with old techniques morph and require renewed attention. New techniques become feasible (sometimes based on Intel technology advances), and old risk management systems can be made to operate more efficiently and effectively. Risks that in the past were independent become coupled with other risks in complex ways as our market broadens. The message is that there is no end to risk management. High-performance companies will always need to be vigilant in detecting holes (and overlaps) in their integrated risk management systems. They will continue to seek a balance between allocating a modest budget to manage an apparently infinite spectrum of risks and proposing a seemingly infinite budget for the impossible goal of mitigating all risks. In this ongoing effort, competitive advantage accrues to the company that can continuously improve its integrated risk management system.

Technical Reviewers

Robert Bristol, Technology and Manufacturing Group
Robert Bruck, Technology and Manufacturing Group
Rajinder K. Chopra, Technology and Manufacturing Group
Keith Core, Finance & Enterprise Services
Kathryn Dornfeld, Technology and Manufacturing Group
Craig A. Drummond, Sales & Marketing Group
Lenny Farello, Technology and Manufacturing Group
Isaac G. Faulk, Intel Information Technology
Dick Hickox, Technology and Manufacturing Group
Carol Kasten, Intel Information Technology
Desmond Kealy, Finance and Enterprise Services
Mary Keegan, Technology and Manufacturing Group
Jim Kellso, Technology and Manufacturing Group
Victoria Gomezy Kelsey, Technology and Manufacturing Group
Karl Kempf, Technology and Manufacturing Group
Tim Higgs, Technology and Manufacturing Group
Diane Labrador, Finance and Enterprise Services
Barry Lieberman, Technology and Manufacturing Group
Laura Phillips, Technology and Manufacturing Group
Jennifer Shane, Digital Enterprise Group
Glenn Shirley, Technology and Manufacturing Group
Peter Silverman, Technology and Manufacturing Group
Dave Stangis, Corporate Affairs Group
Susan Straub, Finance & Enterprise Services
Scott Swanson, Technology and Manufacturing Group
Russ Sype, Technology and Manufacturing Group
Lucy Weflen, Technology and Manufacturing Group
Stephen K. Woo, Digital Enterprise Group
Alfredo Zangara, Digital Enterprise Group

THIS PAGE INTENTIONALLY LEFT BLANK

Managing New Technology Risk in the Supply Chain

Janice Golda, Technology and Manufacturing Engineering, Intel Corporation
Chris Philippi, Technology and Manufacturing Engineering, Intel Corporation

Index words: supply chain, risk management, lithography, R&D investment

ABSTRACT

How do we decide to make strategic bets on multiple, sometimes competing technologies across a portfolio of technology options to maximize our potential for success? Ideally, we can minimize risk by investing in technologies that enable multiple competing technology options; however, not all critical capabilities fall into this category. Investment in orthogonal options must be judicious, as high-risk, high-reward, long lead-time developments will likely also be high cost. In some cases, these larger investments may enable the desired option or a competing option. As long as at least one technology option is available when needed, the investment is ultimately successful. Finally, there may be unique capabilities that may be under-funded, where a nominal investment can enable a technical linchpin.

In this paper, we examine a method to make these strategic bets in the lithography supply chain. We start by looking at a system to assess technical and business risk for all components of the supply chain as they evolve over time. We discuss a methodology for identifying fellow travelers, including consortia, to create programs to establish a foundation of common technologies. We discuss the contractual and competitive aspects of creating investment and joint development programs, with the ultimate goal of improving our probability of success in delivering the right technology at the right time in high volume.

INTRODUCTION

Intel competes in an extremely efficient market. Overinvestment in research and development will compromise product margins, while conversely, underinvestment will likely result in the competitive catastrophe of missing a technology node. Historically, Intel has been successful in making the most strategic, and often most expensive, technology decisions at the last possible moment by ensuring that multiple options were available. Enabling the readiness of multiple options is becoming increasingly difficult in the lithography area

with the demise of “simple” scaling. The complexity of developing an equipment and materials infrastructure to support high-volume manufacturing (HVM) while solving fundamental physics problems can cost billions of dollars. It is imperative that we make strategic bets to create the right technology options at the right time, lest there be an unaffordable spike in R&D costs each time a new lithography generation is introduced.

The nature and scope of the strategic bets in the lithography supply chain differ dramatically between evolutionary and revolutionary technology transitions. For evolutionary technologies, the proposed approach is relatively straightforward, albeit often expensive. Development-level capability is brought in house as soon as possible in order to begin characterizing the issues in integrating the new technology into existing processes and starting the yield learning cycle. This prepares Intel for HVM of the new technology. Evolutionary changes require very few nontraditional strategies beyond buy-sell supplier relationships.

For revolutionary technologies, efforts must begin far in advance, sometimes 10-15 years, of the anticipated high-volume ramp of the new technology. In this case, engagement can start as early as the proof of concept. The scope of engagement must span practically all aspects of the technology, as traditional buy-sell relationships with payment upon delivery of goods often do not meet the needs of the supply chain. Figure 1 illustrates this dramatic difference in scope between evolutionary (193nm) and revolutionary (Extreme UltraViolet-EUV) lithography development, spanning eleven critical aspects of the technology covering the lithography and mask equipment, chemicals, materials, and defect control.

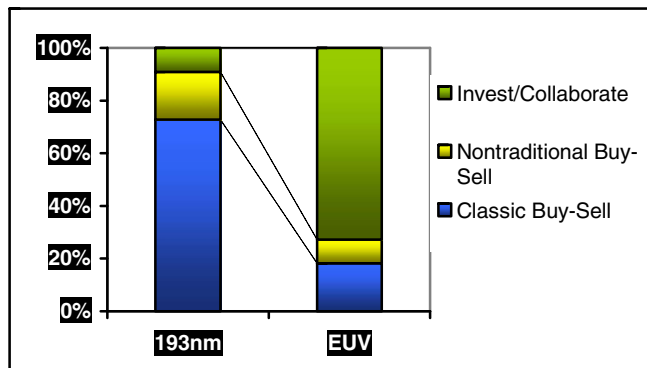


Figure 1: The nature of supply agreements for 11 key lithography component technologies differs dramatically for an evolutionary 193nm transition vs. a revolutionary EUV transition

As part of moving to a revolutionary technology, a thorough risk assessment needs to be completed (and continually updated based on new information). Using the EUV lithography technology as a case study for the strategies discussed, we examine successful business engagements as well as lessons learned from the unsuccessful ones, and we show the importance of effective R&D funding and product strategies to survive the “Valley of Death” encountered prior to high-volume adoption of a new technology. The “Valley of Death” is the process of transitioning from R&D to the commercial market. If a company spends so much money during the R&D phase to develop a technology, it may put itself out of business before it has a chance to commercialize the product [1].

Evolutionary Versus Revolutionary Technology

Intel has always pursued multiple approaches for each lithography generation, with the final decision for each generation being made roughly two years prior to high-volume ramp.

The first approach under consideration is typically evolutionary: enhancing the existing technology. In the case of lithography, evolutionary enhancements have included higher numerical aperture lenses, improved photoresists, optical proximity correction, phase shift masks, and design for manufacturability improvements. Generally, an evolutionary technology has fewer technical risks than a revolutionary technology, so suppliers and customers endeavor to extend existing technologies as long as possible with only incremental research and development costs.

The alternative approaches under consideration are often revolutionary, requiring the commercialization of new inventions in a number of areas. In the case of lithography,

transitioning to a shorter wavelength has been mostly evolutionary to this point. However, future changes will likely be revolutionary, as they can require new hardware architecture, new optical designs and materials, and new resist chemistries. Switching to a revolutionary technology increases the overall technology risk since there are more, and often new, major problems that need to be solved. The uncertainty in the time needed to solve these new problems increases the risk to the technology delivery schedule, which consequently increases the business risk to both the supplier and the customer. This is because most customers are not willing to make solid financial commitments when the delivery time is unknown.

Given these risks, there is a natural desire to extend the existing technology as long as possible, until it reaches a capability wall or the cost/complexity of evolution becomes unaffordable. For lithography, the evolutionary approaches currently under consideration require increasing product layout restrictions and can also require multiple process steps thereby increasing the cost of ownership and the manufacturing cycle time. The revolutionary shift can only occur when the new technology is ready to deliver layout, cost, and/or cycle time advantages. In this paper we explore how to enable the supply chain to deliver the new technology, rather than assessing when the old technology has run its course.

Infrastructure Risk Assessment

Technical Risk Assessment

Multiple methods exist to assess a project’s technical risks, and Intel has often used some combination of the following approaches to manage technical risk:

1. *“Stoplight” chart*: Classifies risk areas into three categories: red (potential showstopper/invention required), yellow (development required), and green (path demonstrated).
2. *Intel risk scorecard*: A 5-point scale, ranging from a score of 1 for invention required to a score of 5 for HVM ready. This is a slightly higher resolution version of the stoplight chart.
3. *Sematech Relative Orders of Magnitude Improvement (ROMI)*: This assesses the order of magnitude of improvement required for key performance components of a new technology. These are summed to calculate an overall risk rating.

Regardless of the tool used, it is critical that the inputs come from a variety of content experts with different perspectives on the technology to minimize blind spots. It is also critical to examine risk reduction over time to determine if the components of the technology are converging to be ready in time. The end result of the technical risk assessment as it pertains to the supply chain

is to identify the critical areas where the supply chain must dramatically improve to deliver a revolutionary technology.

Business Risk Assessment

Evolutionary and revolutionary development differs in the required R&D funding and time to Return on Investment (ROI). Figures 2 and 3 illustrate this point, showing that on a revolutionary technology, the development cycle is significantly longer and the costs of development are larger. This, coupled with fewer firm commitments from customers, puts suppliers in a difficult position regarding ROI. Where a company's initial investment cost is high and its ability to make money is far in the future, there is a risk that the company might reach bankruptcy prior to delivering its product.

In our experience, the fear of the "Valley of Death" has caused larger, more established companies to delay their investment so they can hit the sweet spot of the market where the bulk of their customers will adopt the new technology. Additionally, large, established suppliers need to balance the innovation and timing of new technology with the potential cannibalization of its existing technology. Often, this does not meet Intel's goal of being the leader in introducing new technologies on a two-year cycle. Consequently when switching to a revolutionary technology, it may be necessary to take calculated risks and engage with suppliers who are not currently in the market but are aggressively trying to enter it. Often, these are small startups with limited cash reserves, so it is essential that suppliers have strategies to both raise funding from outside sources and adeptly manage their revenue and expense streams. An additional benefit that may occur by engaging with these smaller or newer suppliers is that it may encourage the incumbent to start its efforts earlier than it would have otherwise, in order to head off a competitive threat.

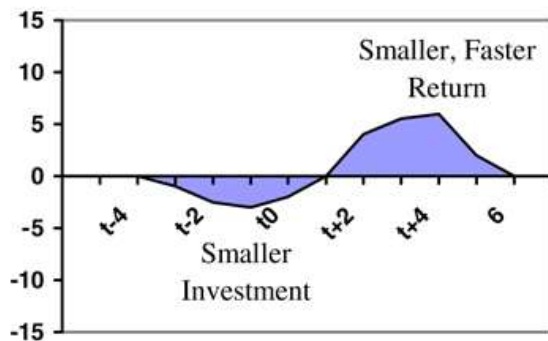


Figure 2: "Valley of Death" for an evolutionary technology. The investment lead-time is shorter, time to return is faster, but longevity of return is limited.

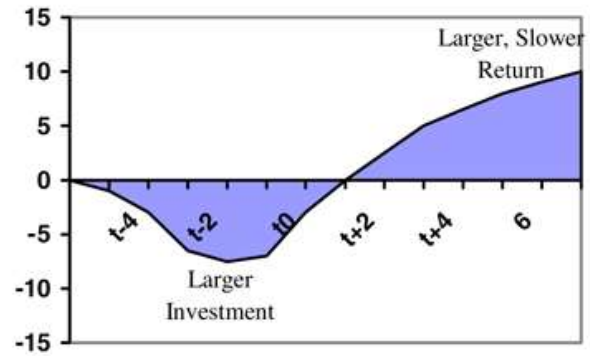


Figure 3: "Valley of Death" for a revolutionary technology. The investment lead-time is long, market adoption takes longer, but ultimate rewards are larger.

A compounding issue when contemplating a revolutionary technology is the "ecosystem risk," i.e., there is additional risk because all links in the supply chain need to be in place for success, or it may be the case that a deficiency in one area increases the burden on another. The chain is only as strong as its weakest link. For example, if a supplier develops a production-worthy lithography exposure tool but product masks are not available due a technology hurdle not yet solved, the lithography tool is, for the most part, useless. In this case, the mask hurdle impacts the mask equipment suppliers, mask making suppliers, and also the lithography tool maker. This highlights the importance of leaving no stone unturned in assessing *all* components of the technology.

The end result of the business risk assessment as it pertains to the supply chain is to identify the critical areas where the supply chain needs financial stimulus to deliver an innovative technology.

Before moving on to funding strategies in the "Strategy" section of the paper, we want to mention two approaches to manage cash flow that are within a small supplier's direct control, and these are areas that Intel evaluates when determining if a small supplier is managing itself wisely:

1. Standards/use of standard components/subsystems.

Suppliers can minimize R&D costs by using existing standards and/or standard components and/or subsystems where appropriate rather than inventing every component or subsystem. Otherwise, the investment required to develop non-differentiating components may mean the difference between surviving or not surviving the "Valley of Death." This may require smaller suppliers to develop industry-savvy and influencing skills to drive standards-setting efforts and to understand their supply chain.

2. Identifying applications with shorter time-to-ROI.

Suppliers engaging in revolutionary technology development can opportunistically find alternative, earlier production uses for the supplier's product. This can be a win for the supplier to be able to generate revenue sooner and collect field data to understand product performance, albeit sometimes in a less taxing environment relative to the ultimate requirements. Alternatively, some components of revolutionary technology development may enable evolution of a current technology, also generating revenue for the supplier. It is important in both cases that the alternative uses do not overly distract from reaching the end goal.

The above approaches help to minimize and smooth the "Valley of Death," but in some critical cases, dramatic actions are necessary.

RISK MITIGATION STRATEGIES

The risk assessment described above identifies technical and financial gaps that must be closed to deliver new technology when needed. If Intel expects to be a leader in adopting new technology, it is necessary to be a leader in driving the strategy to enable technology readiness.

If the technology is in an evolutionary phase, the primary method of help is by making commitments through a traditional buy-sell relationship. Purchasing an early tool, utilizing it in a development pilot line environment, and providing feedback so that the supplier can incorporate improvements into the production version of the tool are the quickest route to production capability. The earlier the influence Intel can provide at this stage, the more likely the tools will meet Intel's needs in HVM. To the extent there are specific areas of concern for the industry regarding the next-generation technology, the industry can work on development plans through avenues such as Sematech.

Intel has found the following strategies important in enabling revolutionary changes across our supply chain:

Risk Mitigation Strategy # 1: Know when to engage others.

History has shown that for major, revolutionary technology changes, supporters are needed, both from a supplier and customer basis. For nearly 30 years, a leading IC company worked on a lithography solution called 1-X X-ray. On top of several technical hurdles, there was really only one company supporting the concept. There was no support from major lithography suppliers and little interest from other IC manufacturers. Developing the technology in isolation failed to develop the needed

infrastructure, and also failed to engage the equipment expertise of lithography suppliers.

At times, an evolutionary technology may need to incorporate one revolutionary component. For this situation, a company may find expertise in universities or national labs to explore the Proof of Concept (POC) on the revolutionary piece of the technology, or if the core expertise lies within the company's walls, the company may be able to develop a significant competitive advantage if the POC is successful for relatively low cost.

Alternatively, if the supply chain requires many revolutionary changes, forming pre-competitive alliances with suppliers and customers to pool expertise to demonstrate POC can help in engaging the entire ecosystem. In this alliance, IC manufacturers, tool makers, sub-component manufacturers, and peripheral technology manufacturers (in the case of lithography, the mask and resist manufacturers) can work together to solve the basic, fundamental problems of the technology. POC is a minimum requirement to get larger industry participation and investment. Once the POC has occurred, the alliance could continue to work together to drive the industry to develop a pre-HVM capability or it could disband.

Table 1 summarizes the considerations for developing a technology internally versus engaging the supply chain.

Table 1: Make vs. buy considerations

Competitive Advantage	High	Engage suppliers (See Table 2)	Make
	Low	Buy	Buy (usually)
		Low	High
		Internal core competency	

Risk Mitigation Strategy #2: Look for extendable solutions.

Developing a revolutionary technology, even after completing a thorough risk assessment, generally takes longer than originally anticipated. Some issues will be relatively minor while others may be showstoppers, or at a minimum, significantly delay development. Technology integration issues often extend the development cycle, often late in the process. For this reason, plus the fact that as the industry resists going to a revolutionary technology

whenever possible, it is important to choose a technology that is extendable to accommodate future requirements.

Risk Mitigation Strategy # 3: Evaluate multiple options to enable commercialization.

Even though POC may have been achieved, experience tells us that going from POC to HVM commercialization, brings significant challenges. It is important to continually assess the risks until HVM happens. As part of the ongoing assessment, Intel has looked for potential competitive or financial opportunities as it evaluates the technology and enables the supply base. If an area of the technology is determined to be especially risky (remember, all of the parts of the technology need be achieved at the same time or else the entire technology will be gated by the missing piece), it is imperative to identify what is needed to close the gaps.

If funding and resources appear to be the solution, it is necessary to evaluate the potential return of engaging with suppliers to drive a solution. If the financial return is low or there is little competitive advantage to be gained; yet, the risk is still high for developing this piece of the technology, engaging industry consortia, such as Sematech, to address the issue, can be a way to reduce the infrastructure risk while sharing the costs across the industry.

For Intel, if the assessment of the possible commercial and financial returns of engaging directly with a supplier(s) working in the risky area turned out to be high, we have used a number of options to help drive a solution while at the same time gaining a competitive advantage.

1. ***Financial Investment.*** Sometimes a cash infusion would benefit a supplier working in the risky area. This could be accomplished through a direct investment in return for equity in the company, through a loan, through warrants, or other venture-capital mechanisms. This cash infusion to the supplier working on the risky area can enable it to hire new people, invest in facilities and equipment, and engage with other experts (universities, national labs, or others) to accelerate learning to deliver the revolutionary technology. This is typically not done for philanthropic reasons, but rather to receive a financial return on its investment if the supplier is successful.
2. ***Collaboration/Joint Development.*** Sometimes direct collaboration between Intel and the supplier can solve the problem. Approaches used to date have included providing data to the supplier on their product performance to increase the learning rate, committing to purchase the product if the program is successful, providing expertise to fill gaps, providing cash to fund engineering programs, licensing Intel

Intellectual Property (IP), or a combination of any of these. Of course, these would be done in exchange for some direct benefit to the customer, such as better commercial terms on the product, early access to the product, or financial return, possibly in the form of royalties.

Table 2 summarizes our model for considering supplier funding options, and has been used in the Intel Technology Manufacturing Engineering (TME) organization over the past several years to determine courses of action. The case studies following show how this model is used to enable EUV lithography technology.

Table 2: Supplier funding options model

Competitive Advantage	High	Collaboration/JDP	Financial investment + Collaboration/JDP
	Low	Consortia	Financial investment
		Low	High
		Financial ROI	

CASE STUDY: EXTREME ULTRAVIOLET LITHOGRAPHY

Over the last 15 years, the lithography wavelength has evolved from i-line (365nm) to DUV (248nm) to 193nm, which is entering its third generation of production with the 45nm node in 2007. Lithography suppliers and sub-suppliers have been working with the same basic refractive optical design all these years: they use transmissive photomasks and have refined the equipment, materials, and patterning techniques over time, with somewhat isolated revolutionary changes, such as chemically amplified resist, along the way. In this model, normal supply and demand market conditions dominate the majority of the interactions. Suppliers and sub-suppliers assume the majority of risk and fund development from the previous generation's sales. Additionally, as the development approaches commercialization, the suppliers receive purchase orders from customers to reduce its business risk. The rest of the infrastructure, such as masks, is evolutionary also. The interdependence risk of the infrastructure is significantly lower in an evolutionary technology.

As Intel lithographers look at Intel's future requirements, it is becoming clear that there will be physics and material

limitations to a purely evolutionary approach at some point. As the lithography wavelength shrinks, more materials absorb the light, few materials can refract or bend the light, and the high photon energy breaks many common chemical bonds, making further evolution difficult.

Development of 157nm lithography demonstrated this complication. The industry spent significant money trying to continue along what was initially assessed to be an evolutionary path. This initial assessment did not account for a revolutionary fact realized too late. The lens materials, in addition to being extremely difficult to produce at acceptable yield, exhibited a phenomenon called intrinsic birefringence. This initially produced confusing optical data on the first lenses measured, and it ultimately delayed programs by roughly one year as the discovery mandated the redesign of the lenses. Additionally, the industry had generally recognized that 157nm would be a one-generation technology, intended to fill the gap between 193nm and EUV, rather than being an extendable approach that would be an option for generations to come. When the material issues arose and delayed the program, there was not time to develop the revolutionary material to satisfy the requirements and meet the market window for the technology. This cost the entire industry hundreds of millions of dollars and distracted resources from working on other multi-generational approaches. Because it was generally thought that 157nm was going to be an evolutionary extension, the strategies discussed above were not implemented or followed. When it was realized that there was a revolutionary component to the technology, it was too late to implement proper risk mitigation strategies to ensure a timely success.

Fortuitously, while working on 157nm lithography, the equipment suppliers also initiated small-scale research programs to assess whether 193nm immersion lithography, using water between the bottom lens element and the wafer, might be a feasible approach to further extend 193nm. This technology currently appears to contain one revolutionary component, the lens fluid, making the development feasible on a shorter time horizon. 193nm immersion appears to fill roadmap gaps in the industry, starting with the 45nm node for many companies. Further extension may be possible using complex mask and multi-step patterning approaches.

As Intel evaluates the 22nm node and beyond, it is unclear that extensions of 193nm immersion coupled with new revolutionary techniques will continue to meet device scaling and affordability requirements (Figure 4). For this reason, Intel is continuing to evaluate a revolutionary technology and evaluate the needs of the overall infrastructure.

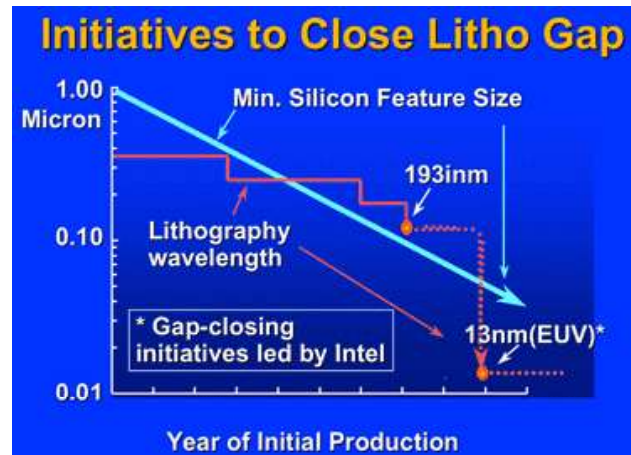


Figure 4: The large leap required from the current evolutionary path (193nm immersion) to the revolutionary path of EUV to maintain Moore's Law

EUV Proof of Concept: The Mid 1990s

In 1996, the US government discontinued funding for the Star Wars weapons program at its National Labs. The scientists working on Star Wars had developed expertise in the EUV region around the 13nm wavelength. At the same time, people within Intel were trying to identify "the cliff" of traditional lithography and its extensions. The National Labs and Intel scientists discussed the potential application of EUV for lithography, and a technical assessment determined that using EUV in lithography could work although there were significant hurdles to overcome. Initially, there were seven potential showstoppers identified with the technology; if just one could not be solved, the entire technology would not be viable. This would be an implied revolutionary change for both the lithography equipment and materials supply chains.

EUV is revolutionary for many reasons. It requires reflective (vs. refractive) optics. It must work in a vacuum environment. High-volume production will require EUV light sources in excess of >180W with power levels inside the source >10 times what they are for a 193nm source today. It will require making reflective optics that can withstand this source power. It will require a reflective mask with tolerances never before seen. New ways of handling the mask will need to be developed due to the lack of a protective pellicle, and a new low expansion material will be required for the mask substrate. It requires a new, novel approach to resist. Lithography has never required so many simultaneous changes, all of which are revolutionary.

After it was determined this was a potentially viable, but revolutionary approach for the future lithography nodes, Intel determined five things:

1. A POC program should be developed at the National Labs where the technical expertise resided, with the learning and IP being transferred to industry.
2. A formal structure needed to be formed to manage the POC development program.
3. The program needed to be set up as a focused risk reduction program to address each module of the technology.
4. The program needed to work with the supply base (litho and litho subcomponents) so the learning would be transferred instantaneously.
5. The program needed to have other IC companies participate to show there was strong support from the customer base.

The above requirements led Intel to conclude that the consortia model would work best in this phase of the technology, and the Extreme UltraViolet Limited Liability Company (EUV LLC), a private consortium, was formed to accomplish these goals. An agreement was secured with the National Laboratories, Intel contributed its risk mitigation methodology and program management expertise, the EUV LLC enlisted two (out of four at the time) lithography suppliers to participate, and the EUV LLC secured five other leading IC manufacturers to participate in and contribute to the ~\$300M program. The goal of the program was to develop and demonstrate EUV as a viable lithography option while enabling the infrastructure with the IP and know-how and at the same time sharing costs and risks across the membership. Figure 5 illustrated the Engineering Test Stand (ETS) built at the EUV LLC to demonstrate POC.

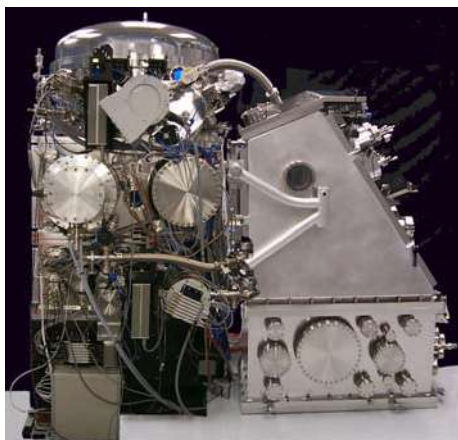


Figure 5: The EUV Engineering Test Stand, which demonstrated full field proof of concept for EUV

On a final note, the initial project timeline planned for this technology assumed that it could be ready for HVM in 2005 to intersect the 65nm node.

Infrastructure Challenges: Fast Forward to 2003

The POC was demonstrated in 2001. This was two years later than originally anticipated due to unforeseen technical issues and lower funding levels due to the general industry downturn. However, based on the success of the POC program, the industry accepted EUV as a leading candidate for “Next Generation Lithography” (NGL). This would not have happened if only a single IC manufacturer was supporting the technology in isolation. The six EUV LLC IC manufacturers then decided it was time to move from the pre-competitive to the competitive phase.

At that time, Intel reassessed the EUV lithography infrastructure and determined the two primary areas that were lagging behind the rest of the EUV infrastructure were the EUV light sources and mask materials/mask equipment. Intel then investigated numerous technical approaches being pursued for the light source and did an overall mask assessment to determine the final mask specs and the allocated error budgets for the mask blank and mask patterning. We then applied the supplier funding options model to determine the appropriate strategy to stimulate development in these areas.

Light Sources: Investment and Collaboration

Looking to both enable high power source capability for HVM and strengthen Intel’s competitive position on this critical technology, Intel had a collection of internal and external experts assess various approaches to the technology problem. Since there were many suppliers with many different approaches, we assessed each approach to determine which approaches might have the highest chance of success. Upon determining the most credible, we applied the supplier funding options model and decided to invest in two EUV source suppliers and fund a joint development agreement with a third supplier. All three of the proposed approaches were significantly different in the engineering risks. It was not anticipated that all three would succeed. However, given the risk level, it was best to work on accelerating all three approaches, pushing for at least one to be successful.

All agreements provide a financial return, a significant competitive advantage, or both, if the supplier is successful. Two of the agreements were with startups trying to enter a new market, while one was with an existing leader in the industry. Sources remain a key technical risk for EUV technology, so time will tell if the choice of funding models was optimal. Additionally, Intel

continues to evaluate not only the suppliers it engaged, but also stays aware of the other potential solutions. If a previously dismissed approach makes substantial progress in the future, Intel can re-engage with the supplier.

Mask: Investment, Collaboration, and Internal Development

At the same time as Intel was assessing light sources, we were assessing the mask materials and equipment markets. We decided to do two things. The first was to develop the world's first full EUV mask pilot line. The plan was twofold: first, we needed to engage with suppliers to develop tools required to make a final EUV mask so that we could demonstrate to the industry it could be done while developing the industry infrastructure. Second, we needed to develop leading-edge capabilities and IP in-house before other companies did so.

Intel engaged with over seven suppliers to develop a pilot line. Assessment of supplier needs and application of the supplier funding model led to the decision to simply purchase tools in most cases, with some early funding being part of the deals. In one case, consortia funding helped to enable a standard tool purchase, while in another case, an equity investment was made in concert with a technical collaboration. Most of the tools have been delivered and excellent progress has been made on EUV mask making.

Out of this early involvement, we encountered both ends of the spectrum with regard to the "Valley of Death." Both suppliers were very small and signed up to deliver revolutionary, first-of-a-kind technology. The first worked in a disciplined fashion to meet schedules and worked closely with Intel engineers who were the expert users of the technology. The tool worked well when delivered, so the engineers on the program thought it might be backward compatible to existing optical mask making with some relatively minor changes. The supplier made the changes. The tool now works for both today's technology and EUV. The supplier has been able to start selling to other customers to quickly exit the "Valley of Death" and moreover was ultimately acquired by a larger company. The supplier funding model worked perfectly to deliver both a competitive technical advantage and a financial return on investment.

The second supplier was constantly late, would not engage with Intel as deeply as the first, started to have cash flow problems, requested an additional prepayment from Intel (with which Intel complied), but ultimately, the supplier went bankrupt. The second supplier was not well managed, practiced poor supply-chain management, and ultimately failed. In this case, the funding model chosen was probably appropriate. Unfortunately, in hindsight, the development complexity was underestimated: the problem

was realized too late due to lack of indicators, and hence the funding was insufficient. This has led us to reconsider additional techniques to monitor the financial health of small, privately held companies, such as more frequent management review meetings (vs. just technical review meetings), more involvement from the Intel finance community to assess the ongoing financial situation of these suppliers, and instituting a "continuous reassessment" of the suppliers that fit this category.

Mask Materials: Investment and Collaboration

The second area Intel felt it necessary to engage in was that of mask material suppliers. Intel finalized two joint development agreements with materials suppliers. In one case, we decided to apply the supplier funding model to provide nominal funding along with technical expertise, as there was an opportunity for both technical and financial advantage. In the case of the other supplier, we provided technical expertise and data from the EUV mask pilot line. Both development projects have made tremendous progress, but still have some technical hurdles to clear to be ready for HVM. Initially, we attempted to engage with the large, incumbent material supplier, who had the majority of the market share. The supplier, for a variety of reasons, did not want to engage with Intel at that time. We engaged with the other, newer supplier and after some solid results were publicly announced, the incumbent increased its development effort. If both the suppliers are successful, these interactions will have enabled a dual supplier strategy for Intel to drive future capability and cost benefits.

DISCUSSION

The case study provides examples of "Risk Mitigation Strategy #1," knowing when to engage others, and illustrates the point that it is necessary to engage people or organizations with different competencies at different times in the research and development cycle. Engaging the National Labs and other IC manufacturers enabled acceptance of the technology as a viable option rather than as a research curiosity. The mask example also illustrates the extreme ramifications of "partially" engaging and not sharing information critical to technical or financial success. The case study does neglect one major incorrect assessment. During 1997, when the assessment was done, it was assumed that the future would be similar to the past. That is, traditionally, microprocessor companies adopted leading-edge lithography first and memory makers followed so the EUV LLC focused its efforts on attracting other microprocessor companies to join the EUV LLC versus memory companies. Today, microprocessor companies and memory companies adopt lithography at roughly the same time, and memory companies may start adopting new lithography even more quickly than

microprocessor makers in the future. For this reason, having a larger group of memory makers in the EUV LLC likely would have been better for the EUV technology as it would have captured more of today's early adopters.

Regarding "Risk Mitigation Strategy #2," pursuing extendable solutions, when the initial program was created as part of the EUV LLC, it was anticipated to be an eight-year program from its inception to the delivery of the first HVM tool. It turned out, like many revolutionary technologies, to present greater challenges than initially anticipated and took longer and cost more than initially anticipated. The extendable nature of the technology has meant that a technology that was originally targeted for a 65nm insertion in 2005 is still a leading candidate for insertion for HVM at 22nm starting in 2011, more than six years later than originally planned. While the delay was not intended, it was not surprising since the industry as a whole will almost always push to solve the evolutionary challenges and extend the current technology for as long as possible, attempting to postpone the shift to a revolutionary change. Because Intel always assesses multiple approaches, even while Intel was investing and driving the EUV infrastructure, it was in parallel pushing for the solving of the issues on the evolutionary technology.

Moving on to "Risk Mitigation Strategy #3" regarding POC being the easy part, the prolonged development of the technology and infrastructure driving toward HVM does show that this is the harder part and requires commitment and judicious program and business management to have a chance at success in the end. In the EUV example above, it took ~four years to achieve the initial POC, but HVM is not planned to start for ~ten years after the initial POC was achieved.

During the time between POC and HVM, Intel has continued its learning of the technology through the continued interactions it has established with the supply base and its continued internal work on masks and process development. This, coupled with the competitive advantages captured in the commercial agreements, should allow Intel to insert and exploit EUV as a technology sooner and easier than other IC companies.

CONCLUSION

Intel has many relationships within the corporate world. Intel purchases equipment from suppliers, sells components to customers, enables new industries that require more processing power, and influences the industry to set standards. As the IC world continues to evolve, Intel will need to continue to be creative in its approaches. Where appropriate, we can be a leader in both shaping the world of silicon while securing a competitive advantage. Recognizing where business as usual may not

achieve success or meet timing goals, we can exert our considerable influence and use our resources to help drive the industry and enable revolutionary approaches. In this paper, we discussed some of the key strategies Intel has applied to help enable a new, revolutionary technology, while at the same time generating industry support.

We looked at just one example, lithography, of a revolutionary approach. Intel, to date, has invested nearly \$500M championing a new, revolutionary lithography option that will allow us and the industry to maintain Moore's Law for several more generations of lithography. In 1997, when we started this endeavor, EUV was not on any supplier's or any IC company's roadmap.

After a careful assessment of both the technology and business, we took a unique approach in forming a consortium of chip makers, tool makers, and infrastructure suppliers and demonstrated this technology could be applicable for manufacturing. Lithography equipment and materials had historically been capabilities that Intel purchased through traditional buy-sell relationships because, while lithography is key to the manufacturing of integrated components, it is not a core competency of Intel's. The investment and industry coordination has helped place this technology on the roadmaps of many equipment suppliers, infrastructure suppliers, and integrated circuit manufacturers. This program required us to take a huge risk, but our methods described in this paper have helped to mitigate both the capability and business risks while also providing capabilities that improve today's processes.

REFERENCES

[1] Evan Mills and Jonathan Livingston, "Traversing the Valley of Death," *Forbes*, November 17, 2005, p1.

AUTHORS' BIOGRAPHIES

Janice Golda is the Director of Lithography Capital Equipment Development (LCED). She manages an organization responsible for creating strategies and working with Intel's lithography suppliers and sub-suppliers to deliver equipment meeting Intel's technology, capacity, and cost roadmap requirements. Janice represents Intel on the Sematech Lithography Program Advisory Group and the US Lithography Technical Working Group. She joined Intel in 1989 and has held positions in lithography process engineering and program management. Janice received a B.S. degree in electrical engineering from Cornell University. Her e-mail is janice.m.golda at intel.com.

Chris Philippi is the EUV Commercialization Manager for Lithography Capital Equipment Development (LCED). Chris has been with Intel for nearly 16 years. He has held

a variety of positions in finance and operations. He has been in LCED for 9 years, first as business manager for the EUV LLC, followed by Intel Mask Operations Commercial Manager and more recently EUV Commercialization Manager, in charge of driving the industry adoption of EUV. Chris graduated from Santa Clara University with a B.S. in finance. His e-mail is chris.s.philippi@intel.com.

BunnyPeople, Celeron, Celeron Inside, Centrino, Centrino logo, Core Inside, FlashFile, i960, InstantIP, Intel, Intel logo, Intel386, Intel486, Intel740, IntelDX2, IntelDX4, IntelSX2, Intel Core, Intel Inside, Intel Inside logo, Intel. Leap ahead., Intel. Leap ahead. logo, Intel NetBurst, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel StrataFlash, Intel Viiv, Intel vPro, Intel XScale, IPLink, Itanium, Itanium Inside, MCS, MMX, Oplus, OverDrive, PDCharm, Pentium, Pentium Inside, skool, Sound Mark, The Journey Inside, VTune, Xeon, and Xeon Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Intel's trademarks may be used publicly with permission only from Intel. Fair use of Intel's trademarks in advertising and promotion of Intel products requires proper acknowledgement.

*Other names and brands may be claimed as the property of others.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Bluetooth is a trademark owned by its proprietor and used by Intel Corporation under license.

Intel Corporation uses the Palm OS® Ready mark under license from Palm, Inc.

Copyright © 2007 Intel Corporation. All rights reserved.

This publication was downloaded from
<http://www.intel.com>.

Additional legal notices at:
<http://www.intel.com/sites/corporate/tradmarx.htm>.

Managing Product Development Risk

Allison Goodman PMP, Corporate Program Management Office, Intel Corporation

Esteri J. Hinman PMP, Corporate Platform Office, Intel Corporation

Doug Russell PMP, Corporate Program Management Office, Intel Corporation

Kerry Sama-Rubio, Corporate Platform Office, Intel Corporation

Index words: Risk Management, Product Development, Risk Methodology, Risk Database, HSD, Monte Carlo, Risk Assessment, Risk Identification, Risk Planning, Risk Tracking and Control, Risk Management Results

ABSTRACT

Product development at Intel has become increasingly complex as the company moves from delivering independent components to delivering usage-centric platform/ingredient systems. To better address the business issues that could prevent the success of the platform strategy, a product development risk process was developed and deployed. This process is based on the standard corporate risk management methodology and uses a database tool to provide consistent deployments across teams. The current process focuses on qualitative assessment of risks across product development. The deployment of this process has improved the quality of product development processes and reduced last-minute fire-fighting responses to issues. Active risk management, using common processes and tools has resulted in increased communication across large platform development teams, accelerated product launches, and quick responses to ecosystem changes. As teams gain experience in active risk management the focus will move towards more quantitative analysis. The future of product development risk management will tie schedule and risk management more closely together with Monte Carlo simulations to improve the predictability of launching a platform with the needed feature set in the time-to-market window.

INTRODUCTION

Intel is an innovative, cutting-edge semiconductor company, one of perhaps only a small handful of such companies. It has historically had significant market share for the worldwide semiconductor market, enjoying large margins.

Today, the business model is changing. Margins are shrinking under pressures from an increasingly

competitive market, which requires new solutions to problems in new areas such as power consumption, form factor, and usage models. To successfully deliver in this market, Intel is changing its business model to deliver usage-centric platforms that require ingredients and ingredient groups to work with each other, and with external companies, to deliver complete integrated solutions—a new paradigm for Intel.

These challenges translate into a product development environment at Intel that is dynamic, intense, and stressful.

Risk management can help alleviate the negative qualities of this environment. Over the past two years, Intel's Corporate Program Management Office (CPMO), a group within the Corporate Platform Office (CPO), has dedicated a team to focus on development and deployment of standard Risk Management Processes and Tools across Intel that meet the needs of the product development environment. We, the members of the CPMO and CPO, have affected significant change in how Intel's product development teams approach risk.

Intel has a world-class risk management methodology. From this methodology we developed a process and a central risk database, High Speed Database-Risk (HSD-Risk), to provide a standard way to identify, assess, prioritize, and plan to prevent and deal with risks. This allows all members of the product development world to think of and talk about risk management in the same way. Before the risk management team began its work, there were many examples of different risk grading and impact systems, as well as different, non-compatible tools for capturing and communicating their risks, even within the same team. In the flexible multi-level team environment required by platforms, this simply wouldn't work.

While we achieved some successes in implementing risk management across Intel, we found that a common

process and database tool wasn't enough to ensure success. Team behavior had to change: instead of performing risk management as a "check the box" activity, teams had to learn to manage risk on a day-in day-out basis. The key to changing team behaviors lay in clearly defining the difference between "passive risk management" and "active risk management."

Actively managing risks has provided several teams with tangible results ranging from pulling in product launches to quickly reacting to the Microsoft Windows Vista* operating system changes. They have gone from proactively investing more capacity in verification systems to keeping the backend development timeline of a product in line with launch. As more teams across Intel adopt this common process and tools, success will become commonplace and have more impact.

Quantitative techniques using Monte Carlo schedule analysis are being piloted within the product development environment with excellent success. As Intel's active risk management capabilities continue to mature, quantitative techniques will play a greater role in decision making.

STANDARD RISK METHODOLOGY

Intel developed a Corporate Risk Management Methodology specification in 2001. The specification is broadly defined encouraging use by many different divisions and groups within the corporation. Adoption within product development was slow but steady with each team or group applying the specification in the way they thought best. With Intel's paradigm shift to a platform company in 2004 the need to develop and deploy a standard risk management process for product development became imperative. The many ingredients that make up a platform are spread across various business units, with each using their own risk management processes, terminology, and tools with different levels of sophistication. The first step was to standardize risk terminology, which was no easy feat, taking six months to complete. Once that was settled we moved on to adopt a standard process that proved to be much faster as we leveraged the professional standards provided by the Project Management Institute and the existing internal Corporate Risk Management Methodology specification. Our process is visualized in a simple 6-step cycle (Figure 1) and is explained as follows:



Figure 1: Risk management 6-step cycle

Step 1: Risk Management Planning

This is the process of deciding how to approach and conduct risk management activities. The key deliverable is the Risk Management Plan developed by leveraging a standard template.

Step 2: Risk Identification

This is the process of identifying, clearly describing, and documenting uncertainties that have the potential to impact project objectives.

When it comes to identifying risks many are found in the areas of the "Triple Constraint," i.e., schedule, cost (resources), and scope (requirements). Intel's competitive business terrain has market windows that reward first entrants to market. Intel sometimes meets those windows through whatever "brute force" means are required (e.g., extra headcount, 24/7 coverage, closely managing vendors). In these cases, schedule is fertile ground for risks (e.g., disconnects, assumptions) with the potential for high Return on Investment (ROI). At the same time, product development physical resources (head count) are expensive, and the right skill sets are hard to find and retain, and they are located all around the world. Scope is seemingly never reduced and new features are always being added to respond to an ever-changing marketplace.

In addition to these common risk categories are some "unique" risk categories. Technology risks are abundant; Intel develops cutting-edge products, as witnessed by its recent disclosure of 45nm technology. This leads to the need for new design tools, process flow tools, and equipment, all of which bring risks. Another unique category for risks is platform integration risk. Historically, Intel has sold microprocessors for desktop and laptop PCs. Now Intel has to learn how to create platforms that integrate CPUs, chipsets, boards, and software into

platforms that their customers want. Finally, Intel now has a more competitive climate. As a result, there is significant increased business risk from the subsequent margin compression pressures.

Drawing out these risks requires application of *identification techniques*. We considered many such techniques and have adopted several as good fits for Intel. The most commonly used techniques include structured brainstorming, expert interviews, and assumptions analysis.

When teaching teams about the importance of risk identification we discuss the concept of *known* versus *unknown* information (Figure 2).



Figure 2: Known/unknown risks

The goal of the team is to drive as much information down into the Known portion (bottom half) as possible. Only the information in the bottom half is actionable. The majority of problems come from the Known-Known quadrant (lower left). Most risks are found in the Known-Unknown quadrant (lower right).

To drive more information down we encourage teams to “dial for data” i.e., call up people on previous projects and talk to them about what happened. Also, project managers are encouraged to study, in depth, post mortems from previous projects. These actions will drive information from the Unknown quadrants into the Known quadrants.

This is a critical concept for teams to understand. If we don’t identify the risk we can’t proactively manage it and our project objectives will suffer if and when the risk occurs.

Once a risk has been identified our standard requires that all risks be written in IF/THEN format with the “IF” stating what we are concerned about and the “THEN” stating why we are concerned. This phrasing helps make risks actionable.

Step 3: Risk Assessment and Prioritization

This is the process of determining the probability, impact, and urgency characteristics of individual risk items. The

results are then used to establish risk response priorities across the collective set.

Without standard assessment criteria it would be impossible to prioritize across projects and divisions consistently. Cross-organizational risk prioritization is crucial to the success of our platforms. The two key assessments we make are regarding *severity* and *priority*. Like most risk processes, we assess severity using *probability* and *impact*. These two combined give us a risk code (Figure 3).

Risk Codes

	100%	R	R	R	R
P r o b a b i l i t y	75-99%	3	2	1	1
	50-74%	3	3	2	1
	25-49%	4	3	3	2
	0-24%	4	4	3	3
		Low	Medium	High	Showstopper
		I m p a c t			

Figure 3: Risk code calculation

Action Messages

	R	Realized	Realized	Realized	Realized
R i s k C o d e	1	Monitor and prepare to act	Take action in the near future	Implement risk response plan immediately	Implement risk response plan immediately
	2	Monitor and prepare to act	Monitor and prepare to act	Take action in the near future	Implement risk response plan immediately
	3	Accept consequences if risk is realized	Monitor and prepare to act	Monitor and prepare to act	Take action in the near future
	4	Accept consequences if risk is realized	Accept consequences if risk is realized	Monitor and prepare to act	Monitor and prepare to act
		Much Later	Later	Soon	Immediate
		Time to Action			

Figure 4: Action message calculation

Intel’s product development risk process varies from most others with the addition of a third element to the assessment: *time*. We use Time-to-Action, which indicates how quickly the team must respond to the risk to reduce

its probability and/or impact. Once we have a risk code assigned for each risk we combine it with the Time-to-Action and calculate what we call the “Action Message” to assist in prioritization (Figure 4). The Action Message tells the team what action to take next based upon their assessment.

Step 4: Risk Quantification

This is the process of using statistical techniques to quantify risk impact. This is an optional step. These techniques are currently being piloted at Intel. More information is available in the “Future of Risk Management” section.

Step 5: Risk Response Planning

This is the process of developing and documenting Risk Response plans.

Table 1: Risk Response strategies

Proactive Risk Response strategies	
Avoidance	Transference
Prevention	Mitigation
Active Acceptance	
Reactive Risk Response strategies	
Contingency	Passive Acceptance

We use many response strategies, both proactive and reactive (Table 1). The most commonly used strategies are Prevention (which attacks probability), Mitigation (which attacks impact), and Contingency (which addresses the situation after the risk has occurred). We also differentiate between active and passive acceptance of risks, though some argument can be made that passive acceptance is a proactive response.

Response plans should clarify ownership, trigger dates and/or events, and the specific actions that will be taken to reduce the probability of the risk occurring and/or the resultant impact if it does occur.

The Action Message tells the team which risks require Risk Response plans. We generate many more risks than we can actually address, so setting priority and developing plans for the top risks are critical when it comes to using our limited resources wisely.

Step 6: Risk Tracking and Control

This is the process of periodically and continuously monitoring risks in order to ensure risk information is kept current and risk response plans are being executed, as required.

We encourage all product development teams to meet weekly to review risks and ensure they have been accurately prioritized based on the latest assessment data, and to ensure that response plans are being developed and executed as needed.

STANDARD RISK MANAGEMENT TOOL

The unprecedented challenges of managing platform risks resulted in the opportunity to develop a single standard solution for use across all product development teams. The Corporate Risk Management team partnered with an internal team that develops validation tools who had a database product called “High Speed Database” or HSD. The idea was to enhance HSD to enable tracking risks across a complex environment consisting of many-to-many relationships. Further, we built the risk methodology and process into the tool that in turn drove and enforced the process.

Up until early 2005, all HSD-Risk instances were set up for ingredients; platforms were not comprehended in the tool. During 2005-2006, the HSD team developed and released a new technology called the virtual data engine that sits on top of HSD. This new technology provides the ability to address the complexity of many-to-many relationships between ingredients and platforms (Figure 5). Coupled with HSD’s existing capabilities, the new technology provides an integrated, reliable, and measurable platform data management system that enables the capability to track and manage the health and quality of a platform and its ingredients as a cohesive unit throughout the entire product life cycle. HSD-Risk allows both ingredients and platforms a measure of customization in how the risk management processes are applied. It is the first tracking system at Intel that supports hierarchical platform/ingredient tracking.

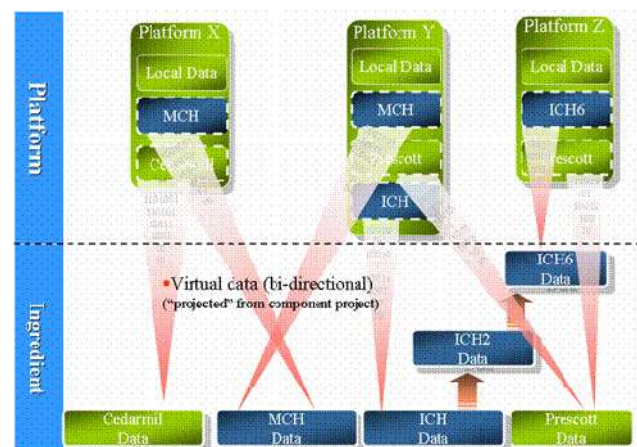


Figure 5: HSD virtual data technology

BEHAVIORAL CHANGES (ACTIVE RISK MANAGEMENT)

While successes were seen in the implementation of the risk management processes with the HSD-Risk tool, behavioral issues still persisted that were preventing good risk management processes from becoming widespread in Intel.

Mostly, we saw product development teams doing what we came to call “passive risk management.” This usually meant that risks were generated one time at the beginning of the project, and then only updated for monthly/quarterly reviews with management in an effort to appear to be managing project risks. In reality, at the working level there was little more than fire fighting occurring. This kind of risk management is only window dressing, and in reality it drives very little improvement.

We advocate a simple approach that we call Active Risk Management to differentiate the desired state from previous passive risk management. This simple approach involves using HSD-Risk and a team commitment to do the following:

1. Carry out intact team training for the project team on the corporate risk management methodology, process, and tool.
2. Create a risk management plan that briefly describes how the project management team has agreed to deal with risk on their project.
3. Assign ownership (data entry, maintenance, accountability) of risks to the appropriate project person.
4. Commit to periodic reviews (weekly recommended) of the project risks by the project.

Since we have started emphasizing the increased communication, teamwork, and accountability behavioral changes necessary to perform active risk management, we have seen more examples of where teams can improve their chances of success. Success is defined as getting the project concluded earlier than it otherwise would have been with the potential of additional features. This comes about because active risk management is really driven by an increased emphasis on team communication and individual accountability.

RESULTS

The CPMO has implemented the active risk management process using the HSD-Risk tool on over 150 platform and ingredient programs throughout Intel with repeatable, measurable success. The first Intel® Centrino® processor technology platform development team to use active risk management was able to pull in their launch date eight

weeks. Additional mobile platform teams were able to adapt to Microsoft's constant Vista launch changes, and were able to take a platform from concept to product in one year (typical platforms take three+ years).

Success with each of these programs was highly dependent on using the risk database, HSD-Risk, as a communication tool. Project managers used risk score cards generated by the tool to monitor potential problem areas in the project and focus their attention on these areas. In turn, the project team used the database to let the managers know what areas were headed for trouble. The program teams used valuable face-to-face meeting time to review the highest severity risks, ensuring the whole team understood the cause and possible impacts. They then created solid prevention, mitigation, and contingency plans for all involved stakeholders. Risk management became an integral part of the daily program management and a way to decrease fire fighting at major milestones.

The risks managed by each platform team varied greatly in scope and area (Table 2). The risk process was used to manage third-party deliverables, customer enabling plans, silicon stepping schedules, late validation boards, unit volume constraints, and marketing resources, to name but a few.

Table 2: Example platform risks taken directly from risk database

If problems with the new manufacturing process lead to the need for an additional quick stepping of the chipset, then the CPU tape-in would have to be delayed day-by-day from current commits to allow a minimum 1-week validation checkout with the chipset, ultimately resulting in day-by-day engineering sample delivery delays to the customers with current fab TPT commits.
If an application engineer is not committed for each platform ingredient by the closure of planning, then OEMs will not productize all ingredients at launch.
If third-party digital TV cards are not available to validation x weeks before qualification samples release, then TV usage models will not be adequately validated resulting in issues being found by customers late in the product development timeline and no healthy TV for launch.

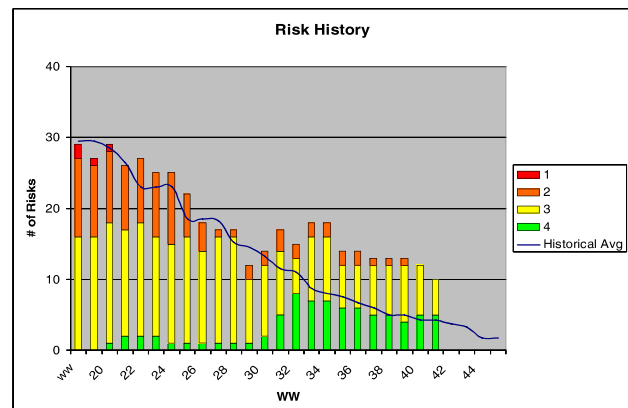
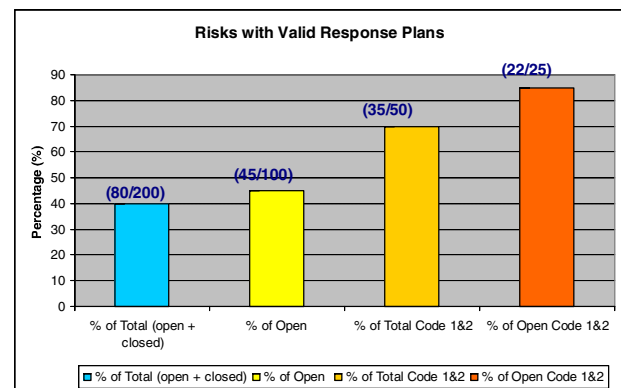
For active risk management to become part of the project/program team's culture, the project/program manager must be a role model for the team. Most of these project teams have five to fifty key members for whom this process required behavior changes. In each successful example, the project managers asked to see the risk score cards on a regular basis. They requested that risks be entered in the database and kept up-to-date through the use of checkpoints. Most importantly, the project managers asked the right questions. They asked about response plans. They asked about true impacts and challenged risk data presented as well as the response plans to ensure robustness. The standard qualitative database fields for impact, probability, and time to action gave the project managers a method for more accurately weighing the severity of one risk against another. Managers were able to focus on the right risks, the ones with high impacts and high chances of occurring, without being influenced by risk adverse team members who spoke the loudest. Focus on the right problems leads to the biggest improvements, as 80% of the problems a project faces usually comes from only 20% of the risks.

This kind of role modeling led to mitigation and removal of a high severity risk on a core development project in Austin, TX. The engineering design manager closely monitored the top ten risk list and was instrumental in getting quick upper management approval for a large capital investment needed to prevent a coming bottleneck in verification testing. Following the active risk management processes, several individuals, layers of teams, and senior management worked together to raise and mitigate this risk until it was no longer a concern; this

occurred several months before the risk would have negatively impacted the program.

The CPMO supplies project risk administrators to aid in the adoption of active risk management throughout the project teams. Risk administrators are responsible for setting up the databases, providing training to team members, and monitoring entered risks for quality. The risk administrator generates the score cards and other basic indicators on a regular basis.

Regular use of indicators from the risk tool provides a way for project managers to monitor risk management effectiveness and drive the right behaviors. Project managers look at the database's current status to see that all higher severity risks have response plans (Figure 7) and that all risks have update checkpoints indicating when more information will be available. Indicators showing risks over time are used to monitor overall trends, such as the severity of the risk over time (Figure 6), risks being closed out on a regular basis, and unexpected new risk spikes that occur because of decisions or events in the project ecosystem.

**Figure 6: Sample indicator: trend of open risks by severity over time****Figure 7: Sample indicator: risks with response plans broken out by all risks and high severity risks**

One of the key indicators for the project manager is seeing risks closed as “avoided,” instead of “resolved” or “realized” (Figure 8). Avoiding risks means the team is actively making decisions to take less risky paths that increase their confidence in hitting their commits, rather than just tracking a risk to resolution. Each risk that becomes realized is carefully scrutinized in post-mortems to understand how the team might have avoided it. These realized risks, as well as resolved and avoided risks, are extracted from the database and given to new projects starting with similar features and timelines to give project managers a head start on potential risks they may face.

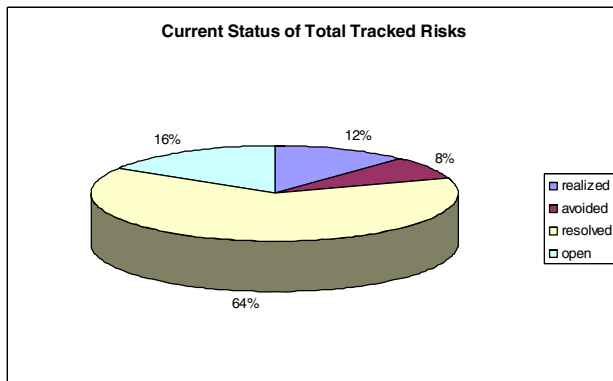


Figure 8: Sample indicator: current disposition of risks to measure risk management effectiveness

Within Intel’s product development groups risk management is quickly becoming an integral part of platform program management. Team members expect to have risk databases in place for them to communicate risks, and project managers expect to have risk score cards and indicators available to help ensure high quality, on-time launches of high-risk, high-complexity products.

FUTURE OF RISK MANAGEMENT IN PRODUCT DEVELOPMENT

Risk practitioners will notice that we have described only qualitative techniques for risk management. When we first implemented risk management into product development we made the decision to avoid quantitative techniques to begin with because of the following reasons:

Quantitative techniques tend to imply a level of accuracy and precision in risk management that simply does not exist. Engineers love their decimal points and will use them whenever possible. We felt it was important to first increase the development community’s comfort level with the imprecision of risk management before giving them quantitative tools. We, therefore, developed an imprecise process that was good enough to get the job done.

Many managers still struggle to see the bottom line value that risk management can bring to their project. Keeping the process quick, easy, and intuitive is a critical success factor in active risk management adoption in these project teams. Quantitative approaches tend not to have those qualities.

There is a future for quantitative risk management techniques at Intel. In 2006 we entered into our first test of managing schedule risk through a Monte Carlo simulation. The team uses HSD-Risk for their risk register and qualitative analysis. Risks are actively managed on a weekly basis and the project manager regularly reviews not only the status but the quality of the risks in the database. This environment was supplemented with the use of a schedule Monte Carlo simulation. The team collected 50% and 90% confidence level duration estimates. The estimates were entered into an add-on tool for Microsoft Project[®] using Beta distribution curves (Figure 9). Monte Carlo analyses were performed daily during the beginning of the project, then weekly, and now monthly, providing an ever narrowing range of completion dates (Figure 10). The data from the Monte Carlo simulations have supported decisions that allowed this team to pull in their schedules by 15 weeks from the original baseline of 92 weeks (about a 15% change). Their ability to quickly respond to changes in their environment through their thorough understanding of their schedule and risks is a key contributor to this achievement.

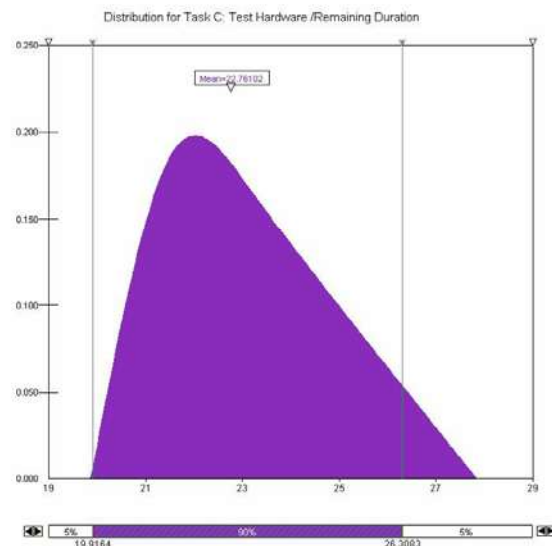


Figure 9: Monte Carlo task input distribution

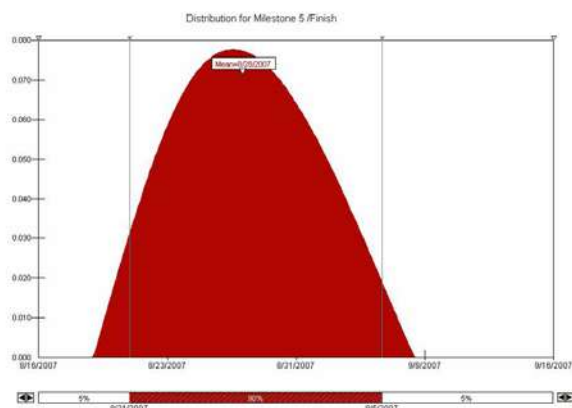


Figure 10: Monte Carlo Milestone Finish output curve

A second application of schedule Monte Carlo techniques led to an equally successful, although different, result. This project was for a product with very specific timeframes and features. Early on, the question wasn't "Is there a market?," but "Can we get it done on time?" The team assessed over 25 different what if combinations involving schedule, resources, delivery dates, and use of third-party vendors. Using the schedule Monte Carlo techniques they were able to comprehend the level of schedule buffer needed to absorb the amount of risk on the project. The project was too risky for the constraints given. It was cancelled in the planning stages, and the resources were applied to another development project with a greater potential for success.

Interest in quantitative techniques is growing with the success of these first two efforts. The future of quantitative risk analysis at Intel is bright.

CONCLUSION

Technology companies have a pervasive engineering mindset, which assumes that purely technical questions and issues are paramount. There is no question that solving technical problems was, is, and always will be one major key to Intel's success. The days when most managers believed that technical innovation is all that matters in their business success are coming to an end.

Intel has improved the predictability of its product development efforts through the implementation of a 6-Step Active Risk Management process and tool. The process provides a consistent language and approach to measuring risk. The tool provides risk visibility despite the many-to-many relationships that exist between Intel ingredients and platforms. Together, they promote inter-team communication with a bias towards proactively avoiding potentially costly risk events.

With the addition of quantitative techniques to Intel's repertoire of risk management techniques, we look

forward to the day when schedule pull-ins are the norm and schedule slips the exception.

Active risk management is a goal well worth attaining. The costs are tremendous in product development projects with their sometimes several hundred person headcounts, empty factories ready to run the wafers based on a now late design, and marketing campaigns all primed to sell high-margin products. Finally, there is the future impact to other projects which were planning to use the roll-off resources. Clearly, the ability to finish a project sooner or with additional features is a great motivator.

ACKNOWLEDGMENTS

Mei W. Sun (HSD)

Mark Van Saun (Corporate Program Management Office)

Alfredo Zangara (Corporate Platform Office)

AUTHORS' BIOGRAPHIES

Allison Goodman PMP is a senior platform analyst in the Corporate Program Management Office supporting mobile platforms. She has a B.S. degree in electrical and computer engineering from Cornell University. Allison worked in packaging path finding, post-silicon validation, and the digital home group at Intel prior to joining CPMO two and half years ago. Her e-mail is allison.goodman@intel.com.

Esteri J. Hinman PMP is the Capability Line Manager for Risk Management and Requirements Engineering. She is part of the Corporate Platform Office. Esteri earned an MBA in Project Management from Wright State University in 1995. She has twenty years experience in Project/Program Management in the Information Technology, Communications, Financial, Defense, and Manufacturing industries. Her e-mail is esteri.j.hinman@intel.com.

Doug Russell PMP is the Corporate Program Management Office Manager for the Ultra Mobile Group CPU team. He has a B.S. degree in Electrical Engineering from Clemson University and an MBA from Duke University. Doug has 18 years of experience in project/program management in defense and commercial communications and C3I projects, as well as 7 years on core development projects in the semiconductor industry. His e-mail is doug.russell@intel.com.

Kerry Sama-Rubio works in Intel's Corporate Platform Office as the Global Risk Manager. Her team has been responsible for the development and deployment of Intel's Standard Risk methodology and Tool for the Product Development groups at Intel. Kerry was a speaker at the 2006 PMI Risk Symposium and has a passion for Risk Management. She holds a B.A. degree in Marketing and

Spanish from the University of Portland, Oregon. Her e-mail is kerry.sama.rubio@intel.com

BunnyPeople, Celeron, Celeron Inside, Centrino, Centrino logo, Core Inside, FlashFile, i960, InstantIP, Intel, Intel logo, Intel386, Intel486, Intel740, IntelDX2, IntelDX4, IntelSX2, Intel Core, Intel Inside, Intel Inside logo, Intel. Leap ahead., Intel. Leap ahead. logo, Intel NetBurst, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel StrataFlash, Intel Viiv, Intel vPro, Intel XScale, IPLink, Itanium, Itanium Inside, MCS, MMX, Oplus, OverDrive, PDCharm, Pentium, Pentium Inside, skool, Sound Mark, The Journey Inside, VTune, Xeon, and Xeon Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Intel's trademarks may be used publicly with permission only from Intel. Fair use of Intel's trademarks in advertising and promotion of Intel products requires proper acknowledgement.

*Other names and brands may be claimed as the property of others.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Bluetooth is a trademark owned by its proprietor and used by Intel Corporation under license.

Intel Corporation uses the Palm OS® Ready mark under license from Palm, Inc.

Copyright © 2007 Intel Corporation. All rights reserved.

This publication was downloaded from
<http://www.intel.com>.

Additional legal notices at:
<http://www.intel.com/sites/corporate/tradmarx.htm>.

THIS PAGE INTENTIONALLY LEFT BLANK

Managing Goods and Services Acquisition Risks

Ken Fisher, Components Automation Systems Group, Intel Corporation

Shawn Holland, Finance, Intel Corporation

Kenneth Loop, LCED, Intel Corporation

Dave Metcalf, Components Automation Systems Group, Intel Corporation

Nancy (Sam) Nichols, Customer Fulfillment, Planning and Logistics Group, Intel Corporation

Ike Ortiz, Materials, Intel Corporation

Index words: supply chain, escrow, Internet negotiations, currency risk, logistics

ABSTRACT

In this paper we look at risk from the total supply chain perspective with the realization that there are inherent risks at every stage of the supply chain. Although we cannot control all the risks, we may put methods and tools in place to help mitigate risks, especially in the areas that require the most focus. We outline effective tools used at Intel to reduce risks in the supplier sourcing process, prevent the risk of business interruption, and moderate risks related to currency fluctuations in the capital equipment purchasing process. We conclude by demonstrating how risk management may be applied across a diverse organization, in this case Logistics, resulting in not only risk mitigation, but also in a continual cycle of process improvements, increased efficiency, and cost savings.

INTRODUCTION

For the Intel manufacturing and supply chain to execute and deliver product to our customers, we require goods and services from a diverse and wide range of suppliers around the globe. These goods and services encompass a) manufacturing equipment that includes Fab/Sort (F/S) and Assembly/Test (A/T) tools including associated spares and in some cases services for installing and maintaining these tools; b) materials that include F/S and A/T production materials as well as materials for supply chain packaging and shipping; c) capacity subcontracting; d) warehousing subcontractors; e) freight forwarders and integrators; and f) miscellaneous, an array of other relatively minor goods and services that are vital to our functionality—for example, the laundering of clean room or “bunny” suits.

Our environment within the total supply chain is both complex and dynamic with old risks morphing and new risks appearing over time generating an infinite number of

things that can go wrong at any given moment. We cannot control risks such as natural disasters, but we can minimize their impact by having proactive plans in place. Other risks we can control, but we first must identify them in order to put proactive mitigation measures in place, such as capacity options to reduce equipment lead-time [1]. The challenge, given finite resources, becomes what to focus on at any given time. This requires constant vigilance and discipline to implement and monitor the effectiveness of controls across the supply chain so we may effectively manage significant risk areas. If we don't do this well, the consequences could be serious and costly resulting in an interruption of goods and services flow within the supply chain.

Once risk areas are identified and prioritized, dealing with them is a matter of using world-class tools and methods for creative supplier and logistics management. Figure 1 highlights various tools and methods that Intel employs to help mitigate risks in both the pre- and post-buy phases of the procurement cycle.

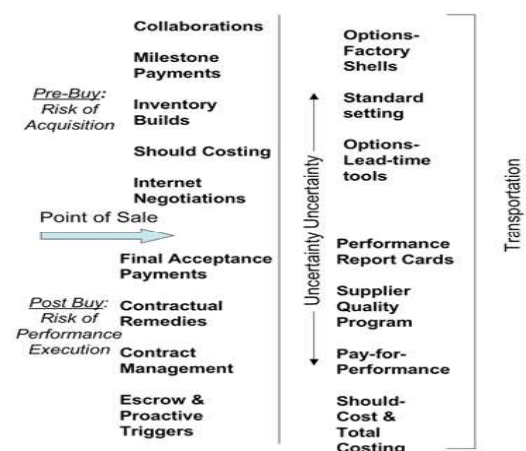


Figure 1: Risk mitigation tools and methods

In this paper, we highlight several high-risk areas that Intel currently mitigates and showcase the tools and methods used to address those risks. We first look at the specific tools used to deal with procurement risks and the support continuance risks posed by high-risk suppliers. Then, methods used to address currency fluctuation risks when buying equipment are explained. For the remainder of the paper we focus on how risk management may be effectively applied across the supply chain to minimize logistics risks.

Reducing Procurement Risk Through Internet Negotiations

More than five years ago, Intel Corporation decided to introduce Internet negotiation tools and processes. Intel's intent was to determine what benefits such tools would bring into our strategic sourcing efforts, especially in the area of cost savings, and how we could use these new tools and processes to complement traditional negotiation methods at Intel. In addition to cost savings, Intel improved process efficiencies [2] through reducing risks inherent to the sourcing process.

Internet negotiations at Intel comprise two capabilities: eRFX and On-line Negotiation Events or ONEs. Other companies sometimes refer to ONEs as eAuctions. eRFX is the on-line execution of RFX; i.e., Request for Proposals (RFP), Quotes (RFQ), or Information (RFI). ONEs have been used at Intel since 2002. eRFXs, on the other hand, were introduced at Intel in 2006, and are really just establishing a foothold in the Corporation.

Before providing ONE and eRFX details, it is important to discuss the program infrastructure that has made Internet negotiation tools successful at Intel. Experts (White Belts) exist at the Internet Negotiations Program Office and within each of the Materials organizations. Formalized continued training and regular forums to discuss key lessons of recently completed events are fundamental components of the program. White Belts generally work directly in the Materials organizations they support. A strong White Belt community is critical in ensuring a successful Internet Negotiations program as it is the true caretaker of the program. Black Belts possess the highest level of expertise and are less common within the organizations because of the extra requirements, such as the ability to support ONEs or eRFXs across different commodities in various Materials organizations. Both sets of experts assist in reviewing market conditions and respective specific supplier bases. They act as resources for event setup and as strategic sourcing consultants. Successful ONEs are optimized by the strategies employed for each event as guided by these experts (see the section on On-line Negotiation Events later in this section).

As stated, eRFX is the on-line execution of RFX. eRFX introduces many efficiencies into the traditional RFX process. Among these efficiencies are standardized or customized templates, the ability to copy (and modify) past events, automated scoring, more accurate supplier responses, a data repository, audit trails, and the ability to easily evaluate multiple responses.

The use of standardized templates, customized templates, and even the use of past eRFX events (changing and improving specific items as necessary) to create a new eRFX eliminates or reduces time spent developing a standard RFP, as traditionally completed by a commodity manager or buyer. When developing an eRFX, the scoring of potential supplier responses can be automatically executed with the proper upfront planning amongst the commodity team. In fact, the process enforces this discipline in upfront planning. This eliminates after-the-fact discussions over scoring rules and allows for quick and efficient eRFX scoring. Additionally, suppliers are not able to provide incomplete eRFX responses. This ensures all suppliers provide complete responses, which eliminates the need to compare incomplete RFXs against fully completed RFXs, as is sometimes common with traditional RFXs.

Further efficiencies are introduced with the use of a common data repository. An Intel engineer needing to submit a diagram as part of the eRFX is able to log into the document and place it there directly. Suppliers deposit their responses and any required attachments into the eRFX document as well. Additionally, potential suppliers may submit questions within the eRFX document for the entire commodity team to see and answer. With all these items being inserted, moved, and changed, a complete audit trail is not a bonus but a necessity. Commodity teams can view who logged on, when they logged on, and what they did. All actions by all parties are completely visible. Taken together, these capabilities enable the commodity team to send, receive, and evaluate more suppliers than they could evaluate using traditional RFX methods. Figure 2 shows a high-level depiction of this process.

Before delving into a more detailed ONE discussion, it is important to point out that Intel's ONEs are performed with only qualified suppliers. We do not allow just any provider of materials or services to participate in them. Equally important is that these ONEs are carried out with total cost factored on-line, or executed as price-only events with other total cost factors pulled in after the event. The total cost consideration is foremost in these events just as it is in traditional negotiations conducted at Intel.

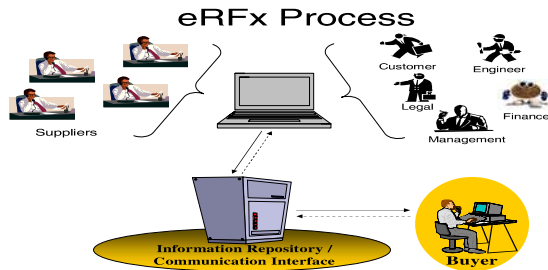


Figure 2: eRFX—enables communication with multiple suppliers and multiple internal partners in a controlled auditable environment

One of the main differences between ONEs and traditional negotiations is that a ONE is a single negotiation executed simultaneously with multiple suppliers (see Figure 3). Just as with eRFX, sourcing professionals are able to use templates or copy and modify past ONEs. This reduces some non-value added work and allows the commodity manager or specialist to concentrate on sourcing strategies. Actual negotiation time is reduced from days or sometime weeks (in traditional negotiations) to 20-30 minutes (for almost all ONEs at Intel) because of early-in-the-process work completed by both the commodity team and the suppliers. The actual event itself eliminates emotions from the negotiations by its very nature. Additionally, ONEs allow Intel's private market to dictate what price it can actually bear.

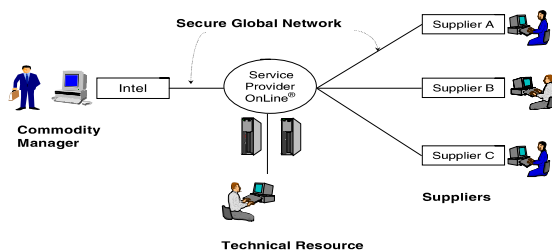


Figure 3: ONE—enables procurement professional to negotiate with multiple suppliers simultaneously thus shortening the negotiation timeframe

Our benchmark studies have shown that we are usually able to achieve cost savings of between 7% and 24% per ONE executed over traditional negotiation methods. A word of caution here is necessary. ONEs are most successful in a supply unconstrained market with multiple potential sources of supply. The larger the number of bid participants, the better the opportunity to see true market dynamics. We saw this in the case of a recent furniture supply ONE where our supply base for the event included more than half a dozen qualified suppliers. In this case we were able to achieve cost savings of 50%. We are even able to achieve cost savings, albeit smaller ones, in a

supply-constrained market. This is where our White and Black Belt experts come in: they help with specific event strategies based on commodity-specific market conditions in order to ensure success. In some cases, review by the program experts results in recommendations of executing traditional negotiations. As mentioned earlier, Intel's intent is not to use ONEs to replace traditional negotiations but to complement them. Although Intel achieves cost savings using Internet negotiations ONE tools and processes, it is essential to point out that the process efficiency benefits are equally important.

These tools and processes are not without some issues. A complaint among new users is that the tool itself is not completely user-friendly. There is some training required and some ramp-up time is necessary. However, after a couple of events (eRFX or ONE), the end user is able to start pulling together their own eRFX or ONE. Reliance on a White Belt diminishes dramatically after consistent use. We have seen this occur in many commodities. Another initial-user issue the Internet Negotiations Program Office encountered is initial resistance to its use, particularly in the case of eRFXs. This is because eRFX demands discipline in executing up-front work sometimes relegated to the latter portions of a traditional RFX. This issue is overcome after the user completes several eRFXs and realizes that the up-front work pays off in better, more efficiently executed eRFXs.

What experienced users find with Intel's Internet negotiation processes and tools is just the opposite of what one might expect when it comes to supplier relationships. Specifically, supplier management and supplier relationships must be stronger especially when it comes to executing ONEs with established and qualified Intel suppliers. The up-front work required of the commodity team translates to smoother execution of eRFX events or ONEs. This early work requires good communication with our qualified suppliers. In fact, a twenty-minute ONE event requires solid before-bid-day communication with these suppliers. We have to ensure suppliers know exactly what is being offered for bid, any portioned allocations (by month, quarter, or year), lots (by time or geography), and total cost factors. Suppliers need to be comfortable with everything, from how they will log into the system and post bids to how the commodity will be allotted (for winning bids, second-place bidders, etc.) to various clarifications regarding the bid process itself. In short, the ONE process requires discipline in up-front planning and solid communication with suppliers in order to be able to execute a 20- or 30-minute ONE. Internet negotiations at Intel do not guarantee large cost savings as we have seen in some supply-constrained, price-pressured market conditions where margins may already be compressed; however, they do guarantee discipline and therefore

provide consistency and less variation in the sourcing process.

PROTECTING AGAINST RISK OF SUPPLIER SUPPORT CONTINUANCE

Another Universal Business Risk that Intel strives to mitigate is business interruptions. Escrow accounts are utilized to minimize potential risks to factory production that are due to a supplier becoming financially unstable or failing to provide adequate support for his or her manufacturing equipment and software. These accounts contain critical supplier intellectual property to sustain the customer's manufacturing environment. Account contents should include all necessary documents and/or software source code to allow complete self-sustaining support. In this section we explore some of the issues with effectively utilizing escrow accounts as a risk mitigation strategy, and offer some new innovative solutions. No disruption to production is our ultimate goal, and our hope is to never require access to the escrow account contents. Suppliers can benefit by establishing these accounts to ensure uninterrupted supply, which can lead to securing initial or future business.

Having third-party escrow accounts in place has created a false sense of security. Escrow account contents cannot be obtained when required, which impacts the ability to mitigate potential risks to production.

Intel has encountered instances where escrow accounts could not be accessed after a supplier filed for bankruptcy. Most courts protect creditors in bankruptcy situations and do not allow any account contents to be used if obtained within 90 days prior to the filing for bankruptcy.

When a supply disruption occurs, many issues need to be resolved. Manufacturing equipment spare parts inventory must be micromanaged to ensure adequate supply to each factory. Alternative sources for supply of the spare parts must be identified and qualified. The inability to access contents of an escrow account during a supply disruption makes sourcing of manufacturing equipment spare parts difficult (especially when patents are involved or the parts are manufactured internally by the supplier). Service expertise must also be available to resolve any issues with manufacturing equipment.

In response to situations where escrow account contents could not be obtained when needed, a team was formed to develop new ideas on how to deal with these issues. As a result of this effort new methodologies were developed for managing at-risk suppliers. The team developed proactive financial and performance triggers to access account contents prior to a supply chain issue.

High-risk proactive financial ratios were defined to allow the release of account contents in advance of bankruptcy. The ratios are net operating cash flow divided by current liabilities less than 10%, return on equity (net equity divided by total equity) less than 0%, earnings before interest, taxes, depreciation and amortization (EBITDA) divided by interest expense less than 1, and retained earnings divided by total assets 0%. Accounts are structured so that contents are released if any of these high-risk ratios are met.

Release of account contents based upon the proactive financial triggers allows time to address supply-chain issues and avoid any disruption to production. Based upon previous experiences where account contents could not be accessed, having these triggers in place would have allowed release of the account contents at least a year in advance of the supplier filing for bankruptcy. Having this time to source and qualify parts would have been a big advantage in minimizing or eliminating the potential risk.

In order to effectively use the proactive financial ratios, financial statements must be provided by the supplier on a timely basis to determine if ratios have been breached. If financial statements are not provided as agreed upon, account contents must be released to the customer.

It is also critical that favorable release conditions are negotiated with both the supplier and the third-party escrow account agent. The third-party escrow company must be able to ship the account contents as soon as the customer provides documentation that a release condition has been met. Any issues that arise from releasing the account contents must be worked independently by the customer and supplier (after the release has been made). Any delay in releasing the account contents takes time away from pursuing solutions to mitigate risk.

If performance release conditions are used they should be customized to the unique supplier and situation. Release conditions must be based upon the potential high-risk issues that would require immediate access to the account contents. An example might be a performance trigger of not meeting on-time delivery. Release conditions can also be defined with a specific amount of time for the supplier to resolve the breach before account contents are released.

Obtaining a license for the account contents is vital. It needs to be clearly stated in the escrow agreement that the license cannot be used unless a release condition is met. A license granted up front establishes the right to use the account content (even in bankruptcy situations). The license must also allow the right to make, or have manufactured, any spare parts necessary to service the equipment (even if the spare parts were not included in the escrow account). If a third-party is used to develop and/or

manufacture the parts required, the supplier must help and/or establish a third party as a viable source.

In bankruptcy an automatic stay is granted, which would prevent the release of the account contents. Under the new release conditions, relief from the automatic stay must be granted. This helps to ensure account contents can be released after a filing for bankruptcy.

Proactive release of the account contents is very important with regards to bankruptcy. Anything that is obtained less than 90 days before the supplier files for bankruptcy is set aside, potentially rendering the released account contents within this window useless.

Account contents should include detailed instructions to navigate any account files, which is a step-by-step process to locate purchased parts, manufactured parts, and assemblies. The account should also include spare parts lists, a bill of materials, and specific manufacturing documents (electrical, mechanical, jigs, and special tools), detailed assembly instructions, software/firmware, and manuals for maintenance and training.

Risk versus required resources must be considered when determining what potential account content should be audited (see Figure 4). Both current and future risk should be taken into consideration. A supplier might be financially stable now, but what happens if a substantial amount of revenue is lost due to another supplier being selected for future process requirements? The installed base of tools must continue to be supported with spare parts and service.

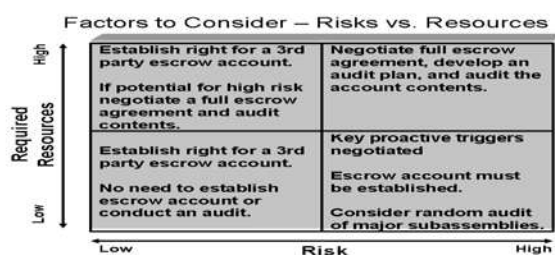


Figure 4: Risks versus resources

To enable an effective and efficient audit, the supplier needs to understand what the account will contain and the required format. Without proper planning for the audit, it will take a lot of extra time and resources to achieve the desired results.

Holding the account contents internally is being utilized with several suppliers. In one situation, proactive financial ratios were already outside of predefined limits when discussion began to put this type of account in place. Since the proactive financial ratios would not work in this situation, a creative solution needed to be found. The financially unstable supplier ended up providing Intel

shrink-wrapped source code for their software. If there is any disruption to the manufacturing environment as described in the contract, Intel has the right to access and use the source code. Holding the shrink-wrapped software source code is a creative solution to minimize risk with this particular supplier.

Another option to consider is for the customer to hold the account contents internally with the same release conditions as a third-party escrow account. If the contents are held internally by the customer, the account contents must be protected (i.e., lockbox in a bank vault). Account contents cannot be released unless a release condition has been met and the proper authorization has been obtained as defined by the account agreement. This eliminates the cost of a third-party escrow agent.

The above-mentioned innovative concepts have been successfully implemented with Intel suppliers. Accounts have been established with proactive triggers and a mechanism for quick release of account contents, if a breach occurs. Specific terms and conditions have been negotiated with suppliers to limit potential release issues due to bankruptcy. A process has been defined and utilized to ensure effective and efficient account audits are conducted. Implementation of these changes made the escrow account process a viable option to minimize potential supply chain disruptions.

After bankruptcy is filed there is no way to ensure, with 100% confidence, that account contents can be obtained. This is why it is so important for release of the account contents to occur prior to any bankruptcy filing.

The tools outlined in this paper provide the framework for this kind of scenario, but creative solutions need to be identified based upon each situation and supplier. In potential high-risk situations, proactive strategies must be developed to allow enough time to establish alternate sources of supply and minimize risk.

CURRENCY RISK REDUCTION

The inherent fluctuation in the exchange rate when purchasing a product from a foreign supplier creates a volatile cost structure for the buyer. When buying capital equipment, this volatility could have a significant impact on the expected or planned costs. Capital equipment pricing is set either when the contract becomes effective or when a purchase order (PO) is placed, depending upon the type of pricing. Since lead times and fabrication facility (FAB) ramp cycles extend over a one- to two-year period, the average price of a piece of equipment is subject to the volatility of the foreign exchange rate over that period. Based on the historical data shown in Figure 5 this has resulted in an up to 30% swing in pricing. Similarly, the supplier is subjected to the same risk. The

volatility for suppliers affects their revenue stream and income statement, whereas it affects buyers' capital expenses, which are depreciated over time. Both supplier and buyer try to stabilize this volatility and curb the risk to their subsequent revenue and expense items. There are several options to consider to mitigate this risk. Understanding the portfolio of options and applying a disciplined process to select the best methodology results in the most consistent mitigation of this risk.

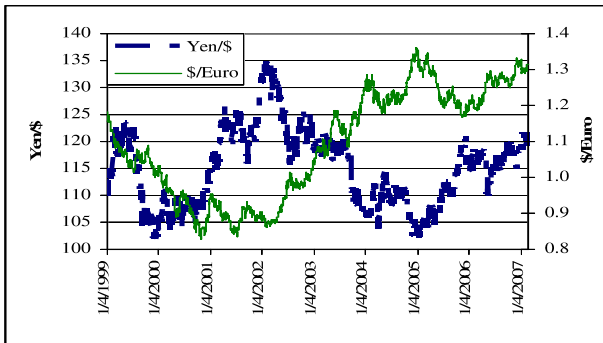


Figure 5: Exchange rate volatility from 1999 to 2007

Supplier's Currency Pricing

One of the most effective methods of achieving a "win/win" in managing exchange rate risk between suppliers and buyers is the practice of denominating the equipment price in the supplier's local currency. Pricing equipment in the supplier's local currency transfers the risk of currency fluctuations to the buyer. The transfer of risk to the buyer should translate into an equipment price discount greater than or equal to the supplier's hedge cost or value of risk mitigation. The buyer has the ability to eliminate or significantly reduce this risk by hedging. Hedging is the taking of a position; either acquiring a cash flow or purchasing a financial contract, that will change in value and offset a change in value of an existing position. Corporate treasury departments have numerous financial instruments at their disposal ranging from forward contracts and currency options to currency swaps, to perform hedging activities. The procedures used to determine the appropriate financial hedging instrument are company specific and are not discussed here. It is important that whichever financial instrument is used that it be treated as a hedge under accounting rules and not a speculation on foreign currency movements. If the buyer is a US dollar-based corporation, there are specific accounting rules the buyer will need to meet to align the gains and losses from hedge contracts to the fluctuations in equipment prices. There are many benefits to both the buyer and the supplier when pricing is in the supplier's currency. First, buyers can better forecast the equipment purchases required to meet their forecasted production output, and therefore they are better able to meet FAS133 requirements than suppliers. Second, when pricing in the

supplier's currency, currency fluctuations impact the buyer's income statement at the same rate as the underlying asset, which could be between 4 to 30 years—a less immediate volatility than impacting the supplier's revenue, which could have an immediate impact on stock. Also, the buyer could choose to accept a higher level of risk by leaving purchases exposed, if the cost to hedge is prohibitive; suppliers, on the other hand, will be better served by eliminating risk to revenue. Buyers can also choose to hedge after the PO is placed for purchases that are deemed "risky" as the confidence level of the purchase increases; suppliers are required to implement hedges at the time they receive a PO. Additionally, if the credit rating of the buyer is higher than that of the supplier, it results in a lower hedging cost overall. The opposite is true if the supplier's credit rating is greater than that of the buyer. When pricing is in the suppliers' currency, it creates a "natural hedge" for suppliers, since the pricing should match their revenue with a majority of their expenses.

Buyer's Currency Pricing

Even with numerous advantages in pricing in the supplier's currency, a majority of buyers prefer to have equipment priced in their own currency. By pricing in the buyer's currency, the risk from exchange rate fluctuations is transferred completely to the supplier. This risk can have an immediate impact on the supplier's revenue; therefore, most suppliers would hedge the full amount of the exposure. Unfortunately, hedging revenues do not completely eliminate the risk, because there is no certainty in the sales revenue. In cases where hedged sales revenue doesn't come to fruition due to a cancellation of a purchase by the buyer, the supplier would be required to unwind the hedge and have the effects of the hedge impact their other comprehensive income (OCI) on the balance sheet. Additionally, the lead time of the tools and the credit rating of the supplier would have a significant impact on the cost of those hedge activities, costs that supposedly would be passed onto the buyer in higher equipment prices. There are advantages to contracting equipment prices in the buyer's currency. If suppliers purchase their materials to construct the equipment in the buyer's currency, then suppliers can experience a "natural hedge" between their sales and expenses. Additionally, some buyers prefer to have prices set in their own currency because the systems their corporation uses may not have the ability to support the use of the supplier's currency. Buyers' systems would require a frequent, manual conversion to the buyer's currency if priced in a supplier's currency. Additionally, the procurement organizations of the buyers' corporations may not be as familiar with the suppliers' currency and therefore may not be comfortable negotiating in the suppliers' currency.

Also, if the credit rating of the supplier is stronger than that of the buyer, the supplier can enter into hedging activities at a lower cost than the buyer.

Combination Currency Pricing (Bands)

Lastly, buyers and suppliers can enter into contract terms whereby equipment is financed in the buyer's currency, but regularly affected by the supplier's currency. Usually the buyer and the supplier agree to a fixed price in the buyer's currency, if the exchange rate is between two predetermined points. If the exchange rate at the time of the PO placement is outside the predetermined points, the price the buyer pays is adjusted, depending upon whether the buyer's currency is strong or weak. This type of pricing is referred to as a currency band (see Figure 6).

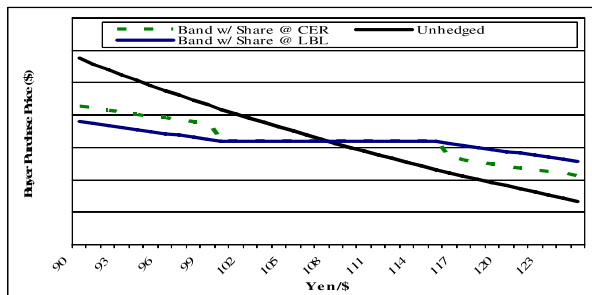


Figure 6: Combination currency pricing example

In the case of a currency band, the supplier is impacted by all fluctuations of the exchange rate while the buyer is not impacted, as long as those fluctuations stay between the band limits. If the spot rate moves outside of the band limits, the impact of the exchange rate is felt by both the supplier and the buyer. The challenge in creating the currency band at the time of the contract negotiation is determining where to place the band limits. Often times, the band limits are set 5-10% away from the spot rate at the time of the negotiations. For example, if the spot rate, or contract rate, is set at 100 Yen/\$ using 10% the band limits would be 90 Yen/\$ and 110 Yen/\$, respectively. As long as the spot exchange rate at the time of the PO placement is between 90 and 110 Yen/\$, the buyer pays a fixed cost, but the supplier experiences a gain or loss depending on whether the spot rate is above or below 100 Yen/\$. If the spot rate is above 110 Yen/\$, buyers pay a lower amount due to the strength of their currency. That amount would be determined by the rate of risk sharing agreed upon by the buyer and the supplier. Since the effect of the currency exchange movement is shared outside of the band limits, neither the supplier nor the buyer is completely impacted by the volatility of foreign currency. In the extreme circumstances where a currency is catastrophically weakened, the risk is borne by both corporations. Additionally, since the price is determined at the time of the PO placement, buyers can lock their price and eliminate their exposure by placing the POs as soon as

they are highly confident of the purchase. This effectively fixes those POs in the buyers' currency, effectively shifting the risk to the supplier until such time as the payment is made. These "early POs" can help the supplier determine future needs to meet the demands of the buyer, and could even help suppliers negotiate their own volume discounts with their sub-suppliers.

Currency Risk Mitigation Results

There are several variables to consider when choosing a currency risk mitigation plan. Three options are discussed in this paper. Each has been used at Intel when the optimal conditions existed between supplier, buyer, and the macro economy to best reduce the inherent variability in the currency markets. Most recently the supplier currency methodology has delivered the best results for the supply chain. This methodology diverts the risk to the buyer where more flexibility to manage the risk lies, thereby reducing the overall cost to the supply chain. It is important for the supply chain members to understand the portfolio of options to mitigate this significant cost risk and to apply a disciplined process to determine the best solution for the situation.

ORGANIZATION-BASED RISK MANAGEMENT

As demonstrated previously in this paper, risk management can convey a competitive advantage when applied to specific functions to mitigate risks to business execution. Internet negotiations reduce risks by driving discipline and consistency to the sourcing function, thereby reducing variation in the process. Reducing volatility of currency exchange rates is beneficial both to buyers and sellers. Escrow accounts may be used to minimize the potential risk to the buyer, including risks associated with the disruption to the supply chain.

All these individual functions touch and impact the logistics organization that moves equipment from the manufacturer to Intel, raw materials from suppliers to Intel, semi-finished goods from Intel to Intel, and finished goods from Intel distribution centers to customers.

In the remainder of this paper, we demonstrate how risk management may be taken to the next level and applied across the diverse organization of logistics to mitigate risks to business execution, to drive process improvements that enhance critical success indicators, and to achieve cost savings through efficient and effective controls.

The Customer Fulfillment, Planning and Logistics Group (CPLG) Risk and Controls department was chartered in 1998 to manage risks inherent in a global supply chain. CPLG is a worldwide organization that utilizes internally owned and operated distribution centers as well as third-

party forward staging hubs in Asia, the Americas, Europe, the Middle East, and Africa. The global transportation organization that sources contracts for transportation providers via Internet negotiations and manages these suppliers worldwide resides under the Logistics umbrella. Planners, supply chain strategists, industrial and packaging engineers, information systems experts, hazardous materials specialists, quality analysts, program managers, freight security personnel, and safety engineers augment the business unit.

Without one group overseeing risk management and driving consistent compliance to processes, distribution center and transportation personnel were interpreting specs and guidelines differently. This approach impacted cost savings and efficiency and fostered the development of conflicting business procedures that created issues across the supply chain.

The CPLG Risk and Controls department was authorized to drive consistent application of processes worldwide and to ensure as much as possible that risks related to the management of financial reporting and potential loss of assets and revenue were addressed. The team uses a three-pronged risk management approach to alleviate issues: 1) facilitating audits for compliance and risk identification; 2) conducting annual risk mapping sessions with business units to proactively identify risks and drive mitigation; and 3) serving as controls consultants for project managers.

Risk Mitigation Plan

The risk mitigation plan contains an audit roadmap and strategies to address high risks identified through risk mapping. The site audit roadmap is determined by calculating risk factors based on the site shipping volumes and inventory on hand, recent or expected major changes at distribution centers and third-party hubs, past audit history, risk mapping results, and quality and security excursions. The mitigation plan is approved by a Controls Management Review Committee (MRC) consisting of CPLG senior leaders. Mitigation strategies for high risks focus on attributes such as meeting requirements for new environmental laws, complying with Sarbanes-Oxley (SOX) legislation, reducing threats to freight lanes, improving segregation of duties controls to reduce the risk of product loss, and mitigating the impact of business interruptions caused by system failures or weather. The MRC members review audit results and propose audit strategy changes monthly, supporting new controls and challenging existing controls to reduce bureaucracy and keep the focus on critical areas.

Audit Facilitation and Management

The audit team developed a series of audit probes based on standard business risks and published guidelines and

specs for internal facilities, and on contractual terms and conditions for third-party run operations. Because there are countless risks in a global supply chain, the group focuses resources on high risks and maintains a dynamic database to mitigate continually shifting risks and to support changing business models such as outsourcing and consignment.

The team worked with software developers to create an audit management tool (AMT) to house audit probes and detailed business process flows, audit findings, and required corrective action plans. The tool was designed to enable multiple auditors across the world to utilize standalone versions on their laptops simultaneously while conducting field work. After their data entry is complete, the auditors synchronize with a master tool housed on a central server. The audit process, including a detailed audit checklist and management review of findings; plus the tool, enable reasonable and sufficient audit results whether the audit is conducted by a new or seasoned auditor. The tool configuration enables scalability of audits as probes may be associated with a type of audit, for example, finished goods distribution center, freight payment, or third-party cross-docking operation. The AMT reporting capability is used to provide data to site and business unit stakeholders and to set the focus of future audits. Among the available reports is a listing of all audit findings that may be sorted by site, audit category, and closure detail. Audit data automatically downloads from the tool into a spreadsheet available to site controls leaders via the Intranet. This enables sites to learn from one another and proactively manage similar risks. Furthermore, the tool allows the flexibility to rapidly edit, add, or delete audit probes while conducting field work. The AMT houses over 1700 active audit probes, all mapped to International Organization for Standards (ISO) elements. It serves as a repository for historic records, and it references audit working papers stored on the team's shared drive.

Developing to Internalizing

The logistics organization recognizes the value of the audit program and actively consults with the Risk and Controls Team when developing processes to meet new business needs and when improving existing processes. The team is routinely engaged in the development of the statement of work, from which contracts for third-party logistics forward staging hubs are written. Team members worked with a joint operations team for third-party hub management to create a cookbook for rapid start-up of hubs. Finance engaged the team in developing improvements to the cycle counting (unit accountability) process. By using a statistical method rather than a set percentage to be counted each month, 30,000 annual hours of cycle counting have been reduced by

approximately 60%. As the value and time savings of proactive risk mitigation was acknowledged, consulting grew and now comprises 40% of the Risk and Controls Team's work.

Staff members facilitate over 20 risk-mapping sessions each year in areas such as supply planning, freight security, information engineering, order management, returned materials, finished goods operations, and supply-chain business continuity. They guide business groups in developing plans to mitigate high-level risks as well as evaluate the effectiveness of the new or improved controls. Closure of risk mapping issues has a five-year history of success in terms of process improvements, time, and cost savings. For example, new processes to manage inventory to be scrapped provide unit traceability in the system of record. The addition of a business continuity program to the Risk and Controls scope supported a reduction in the impact of business interruption to shipments by 18% in 2006 over 2005. The controls continuum (Figure 7) demonstrates the evolution of the Intel logistics controls program over a nine-year period.

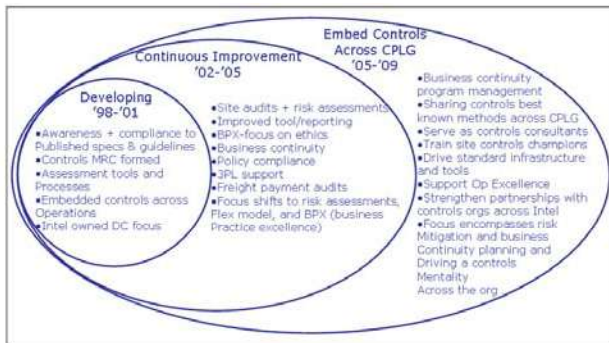


Figure 7: CPLG controls continuum

Challenges

The top challenges to maintaining a central risk management function for a worldwide organization with multiple responsibilities and a broad scope of business processes and risks include maintaining and increasing skill sets to meet the business needs and comprehend the risks; developing and maintaining strong cross-functional partnerships; and influencing business groups over which the risk management team has no direct authority.

The team must have current knowledge of external requirements including customs requirements, SOX legislation, and ISO requirements. To meet these needs, team members obtain American Production and Inventory Control Society (APICS) and International Organization for Standards (ISO) lead auditor certifications. They complete internal training on corporate policies, review new and revised CPLG specs, and attend conferences such

as the MIT Center for Transportation and Logistics Business Continuity Planning Workshop. SOX (Section 240) requires that companies use a "suitable recognized control framework" for evaluating the effectiveness of internal controls over financial reporting. Intel uses the Committee of Sponsoring Organizations (COSO) of the Treadway Commission model of establishment of a controlled environment, risk assessments, control activities, and monitoring. The CPLG Risk and Controls Team leverages the COSO model and publications and the experience of other risk management personnel across Intel.

The team must also be cognizant of internal controls drivers including cost savings, minimizing the risk of loss and/or destruction of products, and productivity improvements. Strong cross-functional partnerships are necessary for maintaining trust in the audit process and results, and for engaging content experts in consulting projects. The ability to influence is imperative to bringing people with diverse agendas together to solve common problems.

The risk mitigation model facilitated by CPLG Risk and Controls resulted in a continual cycle of process improvements, improved efficiencies, and cost savings. After three years of mitigating risks across the business units through audits, risk assessments, and consulting, Corporate Internal Audit findings in the logistics group dropped by 90%. After eight years, internal indicators improved, loss of assets is well below industry standards, logistics ISO certification scores remain high, the organization is compliant to SOX provisions, and time expended in SOX controls testing has been reduced by over 60% as the team challenged external testing and worked to ensure time is spent on relevant areas. The team is viewed as a resource for driving controls compliance and efficiencies, enabling successful project deployment to meet business requirements, and meeting the challenges of emerging risks.

CONCLUSION

In this paper, we demonstrated how Intel Corporation uses three specific risk mitigation techniques: Internet negotiations, escrow accounts, and currency risk reduction to reduce exposure to universal business risks [3]. Additionally, we discussed how risk management can be applied not only to specific issues, but across a diverse organization to reduce business risks, create a continual cycle of process improvements, improve efficiencies, and reduce costs.

Internet negotiations provide cost savings through process efficiencies and decrease risk by reducing variations in the bidding process. Standard and custom templates, automated scoring, and specific required supplier

responses leading to more accuracy are key components of the success of Internet negotiations. Formal post mortems of these negotiations lead to continual improvement in the process.

Supplier escrow accounts minimize risk to production and provide the ability for a wide range of suppliers to secure initial and future business with Intel. The challenge is in the ability to access the account to avoid the pitfalls of micromanaging a disruption to the supply chain. Proactive financial and performance triggers that allow access to account contents prior to bankruptcy or a supply chain issue are key, as well as negotiating release conditions that are customized to the unique supplier situation.

Fluctuation in currency exchange rates when purchasing from a non-US-based supplier creates a volatile cost structure that can fluctuate up to ~30%. There are many options to consider to manage this risk. Careful selection of the method through a rigorous process will deliver less exposure to this volatile variable.

The supply chain has interactive elements and multiple risks that must be managed for success. Examples of this are illustrated by the supply chain risk mitigation pictorial (Figure 8)

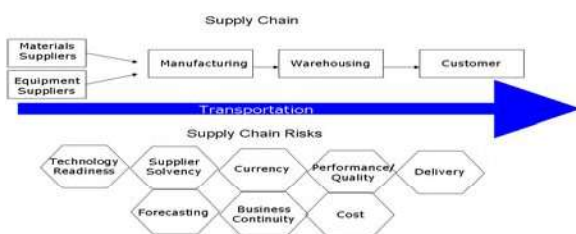


Figure 8: Supply chain risk mitigation factors

Risk management is used to mitigate specific risks and must be applied at the organizational level as well. The Intel Logistics organization empowered a central risk management team to audit for compliance, facilitate risk assessments to identify current and emerging risks, and provide internal consulting to reasonably ensure universal business risks are addressed.

Risk management is essential to successful organizations. Today's environment is dynamic, and past solutions will not continue to serve indefinitely. Organizations must strive for continual improvement and employ new and innovative methods to manage supply chain risks.

ACKNOWLEDGMENTS

The authors acknowledge many valuable discussions with and feedback from Karl Kempf, Bob Bruck, Yuval Engel,

Issac Faulk, Tim Hart, Mary Keegan, Laren Olson, Jackie Sturm, Maureen Vittoria and Lucy Weflen,

REFERENCES

- [1] Vaidyanathan, V., Metcalf, D. and Martin, D., "Using Capacity Options to Better Enable Our Factory Ramps," *Intel Technology Journal*, August 3, 2005.
- [2] Ghiya, K. and Powers M., "e-Procurement—Strengthening the Indirect Supply Chain Through Technology Globalization," *Intel Technology Journal*, August 3, 2005.
- [3] "Ten Universal Business Risks, Internal Auditor," *Journal of Institute of Internal Audit*, December 1996, pp. 38–39.

AUTHORS' BIOGRAPHIES

Ken Fisher has been with Intel since 1987 and is currently the Platform Supplier Business Manager within the Components Automation Systems group. Ken graduated from Michigan State University with a B.A. degree in Materials Logistics Management and received his MBA degree from the University of Phoenix. His e-mail is ken.l.fisher at intel.com.

Shawn E. Holland has been with Intel Finance since 1999 and has been the Procurement Foreign Currency and Controls Manager for the past two years. He graduated from Texas Tech University in 1994 with a B.S. degree in Mechanical Engineering. He received his MBA degree from the University of Arizona in 1999. His e-mail is shawn.e.holland at intel.com.

Ken Loop has been with Intel since 2002 and has been a Capital Supply Manager for several capital equipment suppliers during this time. He graduated from the University of California at Los Angeles in 1995 with a B.S. degree in Chemical Engineering. He received his MBA degree from the University of Southern California in 2002. His e-mail is kenneth.b.loop at intel.com.

Dave Metcalf has been with Intel since 1987 and is currently the Supplier and Business Manager within the Components Automation Systems group at Intel. Dave graduated from BYU in 1986 with a B.S. degree in Accounting. He received his MBA degree from Arizona State University in 1987. His e-mail is david.r.metcalf at intel.com.

Nancy (Sam) Nichols has been with Intel since 1991 serving in the Customer Fulfillment, Planning and Logistics Group Risk and Controls for most of that time. She is a founding member of the Risk and Controls team and has worked to improve risk management within logistics for nine years. She is currently the technical lead of the team. She is a graduate of Portland State University

with a B.A. in English. Her e-mail is sam.l.nichols at intel.com.

Ike Ortiz has been with Intel since 1996. Ike is Intel's Internet Negotiations Program Manager. He received a B.A. degree in Economics from the University of California, San Diego in 1985. In 1996, he received his M.B.A. with a concentration in Supply Chain Management from Arizona State University. His e-mail is ike.d.ortiz at intel.com.

Bunny People, Celeron, Celeron Inside, Centrino, Centrino logo, Core Inside, FlashFile, i960, InstantIP, Intel, Intel logo, Intel386, Intel486, Intel740, IntelDX2, IntelDX4, IntelSX2, Intel Core, Intel Inside, Intel Inside logo, Intel. Leap ahead., Intel. Leap ahead. logo, Intel NetBurst, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel StrataFlash, Intel Viiv, Intel vPro, Intel XScale, IPLink, Itanium, Itanium Inside, MCS, MMX, Oplus, OverDrive, PDCharm, Pentium, Pentium Inside, skool, Sound Mark, The Journey Inside, VTune, Xeon, and Xeon Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Intel's trademarks may be used publicly with permission only from Intel. Fair use of Intel's trademarks in advertising and promotion of Intel products requires proper acknowledgement.

*Other names and brands may be claimed as the property of others.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Bluetooth is a trademark owned by its proprietor and used by Intel Corporation under license.

Intel Corporation uses the Palm OS[®] Ready mark under license from Palm, Inc.

Copyright © 2007 Intel Corporation. All rights reserved.

This publication was downloaded from
<http://www.intel.com>.

Additional legal notices at:
<http://www.intel.com/sites/corporate/tradmarx.htm>.

THIS PAGE INTENTIONALLY LEFT BLANK

Using Forecasting Markets to Manage Demand Risk

Jay W. Hopman, Information Technology Innovation & Research, Intel Corporation

Index words: prediction markets, forecasting, planning, performance incentives

ABSTRACT

Intel completed a study of several generations of products to learn how product forecasts and plans are managed, how demand risks manifest themselves, and how business processes contend with, and sometimes contribute to, demand risk. The study identified one critical area prone to breakdown: the aggregation of market insight from customers. Information collected from customers and then rolled up through sales, marketing, and business planning teams is often biased, and it can lead to inaccurate forecasts, as evidenced by historical results.

A research effort launched in 2005 sought to introduce new methodologies that might help crack the bias in demand signals. We worked with our academic partners to develop a new application, a form of prediction market, integrated with Intel's regular short-term forecasting processes. The process enables product and market experts to dynamically negotiate product forecasts in an environment offering anonymity and performance-based incentives. To the extent these conditions curb bias and motivate improved performance, the system should alleviate demand miscalls that have resulted in inventory surpluses or shortages in the past. Results of early experiments suggest that market-developed forecasts are meeting or beating traditional forecasts in terms of increased accuracy and decreased volatility, while responding well to demand shifts. In addition, the new process is training Intel's experts to improve their use and interpretation of information.

INTRODUCTION

Demand risk is implicit to manufacturing businesses, but for high-tech firms it poses a particularly strong threat. As product lifecycles shrink and new generations of technology enter the market more quickly, achieving strong top- and bottom-line results hinges on estimating overall demand and product mix as accurately as possible. Products with manufacturing lead times of months or even quarters are all the more critical to forecast correctly because last-minute inventory adjustments are limited or sometimes just not feasible. Our study of multiple

generations of product transitions discovered that producing high-quality demand forecasts is difficult to achieve consistently and that mistakes can be quite costly [1].

Managing demand risk is critical to Intel's success, but it is only one of many business challenges the company faces. Across the organization, teams grapple with questions such as how many units of products x, y, and z customers will demand at certain prices, how much factory capacity should be funded, which products should be brought to market, which features and technologies should be included in new products, and when new products will be ready for production and distribution. Interviews with employees trying to answer these questions reveal a common issue: belief that they do not have the best available information and insight to guide business decisions.

Tackling demand risk and other challenges requires moving information around decentralized organizations in new ways. If employees across Intel's many functional groups have information and insights that can help inform our planning and forecasting decisions, we need a way to aggregate that information and turn it into intelligence. Prediction markets are a potential solution to this problem and have been written about extensively for the past five to ten years. Our research discovered that, despite the buzz around prediction markets, the integration of prediction markets and similar Information Aggregation Mechanisms (IAMs) into organizational forecasting processes is still in its infancy. Popular stories on prediction markets still frame the potential as being greater than the demonstrated value, and reports of usage at companies such as Hewlett Packard, Microsoft, Google, Eli Lilly, and others suggest that application is often viewed as experimental and that markets are largely separate from other organizational forecasting processes [2, 3].

While our research of prediction markets is growing to explore more business problems over time, the area we first tackled at Intel is demand forecasting. We have developed and piloted an IAM that is integrated into our

regular forecasting processes and, through this development, have considered many questions and ideas about designing markets real companies can use to address real problems. It will take extensive research and experimentation to answer these design questions, but we are encouraged that even trial solutions based on the experience of other researchers, feedback from our business partners, and our own intuition are producing good results.

CHALLENGES TO ANTICIPATING MARKET DEMAND

Since 2001, we have been studying the release of current and historical products. We have tracked the evolution of forecasts, factory production, and inventory for many major product releases and studied how the signals flow through teams across Intel's organization. Our methods have included both quantitative analysis of our data sets and interviews with personnel in groups that work with these data sets to understand policies, strategies, and perspectives on the product transitions.

We learned that calling demand correctly for new products—and the products the new products replace—is a formidable task. Four fundamental sources of noise cause difficulty in determining true market demand: *current data*, such as orders and inventory; *market assessment*, such as intelligence and consensus on how appealing products and promotions (and competing products) might be to the market; *market objectives*, the goals Intel has for its products, such as unit sales, average price, market segment share, and technology leadership; and, *strategic plans*, such as the decisions about which products and stock keeping units (SKUs) to sell, how to price them, and how to take advantage of technological and manufacturing capabilities. Nearly all the pitfalls we have discovered in forecasting demand can be linked—with the benefit of hindsight—to one or to a combination of these factors. The question, of course, is how to account for these factors in advance to systematically and repeatedly do the best possible job of forecasting and planning.

The fundamental problem in managing forecasts is twofold. First, the hard data being created, judged, and passed from group to group lack credibility based on past performance, so each group feels the need to adjust the information based on any number of experiences and heuristics. Groups preparing to publish data are aware of how other groups will likely judge the data and are therefore prone to gaming the system, i.e., adjusting numbers in anticipation of future judgment.

Second, data sets themselves do not really convey any specific meaning. Meaning can be inferred from how the data compare to expectations or previously published

data, but numbers in enterprise applications or spreadsheets cannot explain the strategies Intel and its customers are employing or the uncertainties they are facing. Decentralized organizations must find a means of transmitting business context; in other words, instead of transmitting mere data sets, they must transmit information and intelligence from employees who have it to employees who need it to make decisions and plans. We learned that Intel has many informal networks that attempt to move that knowledge across the organization, but these networks have many failure modes: turnover of employees in key positions, limited bandwidth of each individual and team, and difficulty systematically discovering the important information to be learned (stated differently, whom to include in the network).

Our research has led to three methods that are being used at Intel today. One focuses on market assessment and uses data from across the organization to score factors affecting ramp rates (Product Transition Index). The second ties market objectives, strategic plans, and market assessment, identifying risks and developing contingency strategies to improve coordination and cooperation (Transition Playbook) [4]. And, the third (IAM) paradoxically uses the most structured of the three methods to promote transmission of the most unstructured information, i.e., any and all information participants feel is relevant to developing a forecast.

The source of demand uncertainty for Intel begins with biased signals from the interaction with our customers. Customers typically signal strong demand for popular upcoming products. In fact, if Intel fulfilled all bookings (advance orders) for all customers, the result would most often be substantial oversupply. Customers want to assure supply and be certain that a competitor does not procure an unfair share, so the condition of “phantom demand” develops. Orders are inflated to keep the playing field level across customers and so that each can lock in as much supply as possible in the event of a shortage. Conversely, orders for new products are sometimes deflated, signaling that customers do not want to go to the new product too quickly. Perhaps they prefer the prior product for any number of reasons, or they believe low demand might lead to price reduction, or in some cases, new technologies and supporting components are relatively scarce and will increase in supply (decrease in price) over time. Whatever the exact cause, a study of orders and forecasts developed by Intel's geographical sales organizations shows that the volatility of these signals is large, and it is not unusual for the forecasts to be over 20% high or low.

Once geographical (“geo”) forecasts are published, a central business planning group is responsible for publishing official demand forecasts that guide the supply

network. The geo forecasts are one input considered by this team, but many other factors including models of worldwide sales growth, Intel's share of the market segment, product mix by any number of attributes, sales versus price point, historical product ramp rates, and various inventory data (for instance, work in process, finished goods, customer stocks) are used to produce official forecasts. While historical results show that the central business planning team does reduce the volatility of the geo data and often achieves improved accuracy, their track record shows that overcalling or undercalling sales, especially during product ramps, is not as rare as we might hope. These missed calls can lead to significant surpluses or shortages that take money right off the bottom line. Intel's factories, keen not to get caught in these situations, do not always build to the official forecasts. They also use models to help maintain proper inventories, smooth production, and achieve high operating efficiency, but our research has found no evidence to date that this final judgment improves demand fulfillment systematically or repeatedly.

The challenge of demand forecasting is real and costly. Demand risk is among the greatest threats facing Intel and other manufacturing firms day to day. To demonstrate how formidable demand risk can be, the following are actual situations we have discovered:

Various groups across Intel estimated sales of a new product over an initial period after launch to be anywhere from one million to four million units.

Two similar products (common architecture) were released within a quarter of one another in different (essentially non-competing) market segments. One resulted in a shortage, the other in a surplus.

Geo forecasts for one new product were as low as 13.5 million units for a fixed period, while official forecasts were guiding the factories to build 26.5 million and sales targets were 27 to 28 million.

Two products were projected to sell over 10 million and below 7.5 million units during a future period. In three months the forecasts flipped to under 5 million and over 11 million, respectively.

Sustained growth in the mobile PC segment beginning in 2004 caught the whole industry by surprise. Four quarters of year-over-year growth, roughly double what was expected, made for a tough supply picture.

Certainly not all misses are this extreme. Intel's forecasting teams routinely perform quite well given the challenge of their task, often achieving forecasts with less than +/- 5% error. However, sustained high performance does not make up for each isolated miss that costs the

company millions to, conceivably, hundreds of millions of dollars. Everyone involved in forecasting at Intel continually strives to achieve better performance across the board, and we are always exploring new approaches that might bring improvement.

MARKET MECHANISMS AS FORECASTING TOOLS

In essence, all markets are prediction markets. The value of assets traded in a market depends on information that is not fully revealed and will not be known for some time, if ever. Market valuations are explicitly or implicitly predictions of that unknown information, perhaps the future value of a commodity, the expected cash flows generated by a firm, or the outcome of a potential corporate merger.

While commodities futures are often used as financial instruments to hedge long or short positions, the markets also reward traders with better information while punishing those with worse information. Giving traders incentives to reveal good information is the core function of prediction markets, even where no underlying assets, in the traditional sense, are available to be traded. Prediction markets trade future events or outcomes, and the settling process amounts to using a documented and published formula to determine winners and losers and to pay out incentives. Many experiments and real-world tests show that market mechanisms can be implemented simply to create predictions and that these systems work rather well.

Perhaps the best known of all prediction markets are the Iowa Electronic Markets, which enable traders to forecast the outcomes of future elections. The power of these markets to generate forecasts accurate and stable enough to inform decision makers has been demonstrated for nearly two decades [5]. Another set of experiments at Hewlett Packard demonstrated the ability of prediction markets to call future sales more effectively than traditional forecasting processes [6].

In our research at Intel we are extending the idea of prediction markets to create "forecasting markets," which are essentially prediction markets or similar IAMs integrated into the company's standard, ongoing forecasting processes. Participants reveal not just an expected outcome but a series of expected outcomes for the same variable over time. So, the forecasting market captures individual and collective assessments about trends such as increasing or decreasing demand just as weather forecasts anticipate warming and cooling trends.

We believe that three factors enable markets to outperform other types of forecasting systems and more effectively move information from source to decision maker. First, the features of anonymity and incentives

work together to draw out good information. The experiments of Kay-Yut Chen and Charles Plott at Hewlett Packard suggest that people provide the best information when rewarded to do so and when protected from potential ramifications of expressing their honest opinions. Incentives encourage participants to search for the best information they can find and reward trading behavior that is unbiased. Anonymity helps prevent biases created by the presence of formal or informal power, the social norms of group interaction, and expectations of management. We found many individuals at Intel who told us that their opinions sometimes differ from stated targets or unstated expectations. Looking back at forecasts that were off substantially, we have been told that teams sometimes did not believe the forecast they published but were pressured, perhaps overtly, to adjust forecasts upward or downward. To the extent anonymity and incentives curb bias and motivate the hunt for good information, they should improve the signal created by market mechanisms.

Second, the simple mechanism of aggregating data through a survey or market has two remarkable properties. It smoothes results over time, which is great for guiding supply, and it tends to produce a group forecast more accurate than the forecast of at least a majority of individual participants. A study by Scott Page demonstrated that even among a fairly homogeneous group this effect holds true. In the context of forecasting selection order in professional sports drafts, he found that averaging the individual forecasts of experts soundly outperformed the forecasts of any individual [7].

Finally, in many forecasting examples it has been found that increasing the diversity of a pool of participants increases the accuracy of the collective forecast. As long as each additional participant brings some information, adding more, diverse opinions improves the collective judgment. This condition holds true in many cases because good information tends to be positively correlated and sums, while errors are often negatively correlated and cancel [8].

DESIGN CONSIDERATIONS AND ELECTIONS

The first steps toward implementing a new IAM are finding business problems to address and teams interested in gathering better intelligence to solve those problems. In the context of demand forecasting, we started by partnering with two teams responsible for developing forecasts for product families. We determined that quarterly unit sales—with rules to define exactly which sales are included or excluded—would be useful to forecast with an IAM. With agreement on the result to be forecasted, the design process begins.

We have found through the development of current and upcoming IAM implementations that design considerations can be organized into five categories: interface, information, incentives, integration, and inclusion. The Appendix “Five categories of considerations for designing Information Aggregation Mechanisms” lists examples of design questions that should be evaluated within each category. Since we have found that design choices in one category often depend on choices in other categories, the five categories are developed more or less in parallel. Many companies implementing markets may start by designing the interface or simply assume that the only available IAM mirrors the stock market with regular, continuous trading periods and double auction trading. In fact, many interfaces exist, and choosing the best one should be guided by many other considerations. To demonstrate the application of the five categories of design considerations, the remainder of this section covers the design process for our original pilot market.

We began our design process by considering *inclusion*. As a first experiment we wanted to enable the central business planning team that creates the official forecasts to generate a collective forecast using an IAM. We would compare their collective forecasts created through the IAM to their current and historical collective forecasts created through Intel’s standard processes. We invited this team, and other participants who had a global perspective on the business and function more as analysts rather than sales or marketing staff. It was a relatively homogeneous pool of experts (but not without differences of opinion) and about as unbiased a group as we could put together, and we felt it would be a good baseline for future experiments that would tend toward greater diversity and bias. The total pool invited numbered from 20 to 25.

We carefully weighed how the IAM process would *integrate* with the workflow and processes of our participant pool. Knowing that the official forecasts are published monthly and that the potential participants are quite busy with that process for nearly two weeks out of the month, we decided against a continuous market; instead, we elected to time a snapshot IAM at the midpoint between official forecast publication dates. This scheme would maximize participation while effectively doubling the beat rate of new forecasts. The official and IAM forecasts would leapfrog each other, each outcome feeding the other process roughly two weeks later. (Since having the official forecasts and IAM forecasts influencing each other was unavoidable, we decided at least to make their interaction systematic.)

Structuring the *information* in the market was simple, as we decided to mirror the structure of the regular forecast. Each market would create separate forecasts for unit sales

of a product family in the current quarter, the next quarter, and the quarter after that. A packet to be sent to all potential participants before each market was developed. It included the definition of the results to be forecast, how incentives would be awarded, instructions for using the forecasting application, the current official forecast, and a small set of (already available) information such as historical sales and current orders. The market interface itself would provide some information during and after each snapshot. Once actual results were determined, prizes would be announced to individual winners, and a list of prizes awarded, showing amounts but not recipient names, would be published to the whole participant group. At no point would lists of participants be published, giving all participants the option of anonymity.

The *interface* design was based on the experience of our academic partners and the design choices in the above sections. We knew which information we wanted to collect and that we wanted to use a monthly snapshot to collect it, so the team opted for a synchronous Web-based application that seemed a good fit. It is essentially a survey mechanism that enables each participant to create a probability distribution of unit sales while watching others enter their distributions. Participants can learn from the aggregate forecast of the group while continuing to invest their own individual budgets into the offered investments, each corresponding to a range of potential unit sales. This method had demonstrated solid results in laboratory experiments outside Intel and can develop a complete forecast in as little as 15 to 20 minutes.

The behavior of participants in the IAM is based on the way *incentives* are awarded. Once the actual result is known, investments made in the range containing the result are placed in a drawing for cash prizes. Each participant's chances of winning prizes are proportional to his or her share of all investments in the winning range. We wanted to avoid extremes of all incentives going to a single winner or dividing incentives among all winning tickets, because we did not want to encourage participants to concentrate their investments too narrowly or spread them too broadly. Incentives were a hot topic in the design phase—how large should they be? In the end we settled on an amount significant enough to attract and retain interest (we hoped) but not large enough that employees might shirk other job responsibilities.

Our overall design structures each investment as a decision based on both the individual's expectations for the outcome and the aggregate group prediction. Participants weigh owning lower percentages of more likely outcomes against higher percentages of less likely outcomes. In the end, we believe the system works well because having each participant weigh the conditional probabilities of various outcomes creates a robust

collective forecast. And, the final outcome of the market—the amount of investment in each potential range of unit sales—forms a probability distribution based on the intelligence of the entire group.

We analyze not only the collective forecast but also the transaction records of individual traders. Assessing trading behaviors and inferring strategies from the behaviors helps us understand how the systems work, under what conditions they might work well, and why certain types of participants or investment strategies may contribute more or less toward a good (or bad) outcome. Over time we also expect to use the observed data to determine whether the formal outcome is the best possible forecast the market had to offer. Perhaps other information based on the demonstrated knowledge and track records of participants, individually or grouped by function, geography, or experience, will lead us to be able to handicap traders by the knowledge they impart to the system over time.

RESULTS

We are using three primary measures to assess the performance of our markets: accuracy, stability, and timely response to genuine demand shifts. Having run pilot markets for approximately 18 months, we are starting to get a sense for how the markets are performing. Although the market forecasts and official company forecasts are not independent, it is nonetheless interesting to compare the signals and then assess how effectively they are working together. In terms of accuracy, the markets are producing forecasts at least the equal of the official figures and as much as 20% better (20% less error), an impressive result given that the official forecasts have set a rather high standard during this time period with errors of only a few percent. In the longest sample to date, six of eight market forecasts fell within 2.7% of actual sales. The accuracy of the official and market forecasts has been remarkably good, well within the stated goal of $\pm 5\%$ error for all but a few individual monthly forecasts. Until more results are generated over time we will not be able to determine the extent to which this strong performance stems from the introduction of the market forecasting process. It is also possible that sales were unusually easy to forecast. Regardless, specific results from the pilots have shown the value of the market forecasts and are leading us to believe the markets are having a positive impact.

On one occasion we saw the first market for an upcoming quarter's sales vote "no confidence" on the prior official forecast. Ranges of potential sales in the IAM are structured so that the prior official forecast is roughly centered in the set of ranges. A "no confidence" vote occurs when all investments from participants come in

either above or below that official forecast, meaning that the group believes there is a 100% chance of falling on one side of the official forecast. The only time this has occurred the market forecast was correct. The official forecast published prior to the market forecast was off by over 10%, and the market led it in the right direction.

Much like public stock markets, we have seen our IAMs react quickly and decisively to strong news and then take time to assess and properly discount it. One IAM dropped by 4.7% and then bounced back to almost exactly where it was before the drop. This was not accidental. A rash of cancelled orders and bad news that appeared to signal softening demand turned out to be an aberration, and the market needed time and additional information to make that call. These sorts of sudden shifts are unusual. In fact, the IAM forecasts are quite stable, with as much as 20% less fluctuation from month to month than the official forecasts during the same period. The business planning team responsible for the official forecast observed that the market signals were more stable and implemented a new process step to try to filter noise from each new official forecast.

Surprisingly, the market forecasts are not necessarily improving as the forecasting horizon shrinks. Although we will need a longer history of data to draw a firm conclusion, we have some evidence that the forecast is as likely to get worse in the final month before the actual result is known as it is to get better. The reason, as we understand it today, is that as the amount of signal goes up rapidly toward the end of the period, the amount of noise goes up rapidly as well. As the amount of information explodes and the time to assess it shrinks, it would not be a surprise to see humans unable to tell the forest from the trees. Fortunately, forecasts out in the 3-8 month horizon, which provide the factories ample opportunity to plan product starts, are performing quite well.

Another key set of results is feedback from owners of the official forecasts, as well as market participants. Discussion with the owners has centered around learning to produce better official forecasts from the market results. The value or credibility of the results has never been questioned; in fact, the one month we were late publishing the market results brought reminder e-mails from the owners. Not long into the pilots the owners began discussing new markets for other key forecasts. Clearly, they are seeing the value of this new data source. Participants have been quite positive as well. Quotes such as "I enjoy participating in the trials" are common. Another trader cited the IAM process as a welcome break from the often mundane job of forecasting: "I think it's great we're doing this simply because it makes work more fun and incentivizes us to do our homework and make the right call, which should lead to better results." We are also

amused that although we never publish the list of participants and winners, everyone knows who participated and who won.

Based on the results and word-of-mouth advertising, interest in expanding the research into new parts of the business is growing. We expect the number of forecasting markets to quadruple in the next three months. More implementations producing more data will accelerate our pace of learning.

CHALLENGES

The main challenge in implementing IAMs in a corporation, as with many innovations, is securing buy-in that the time invested is worth the potential benefits. It helps that certain teams are forward thinking and some of these same teams have been burned by poor forecasting performance in recent years. We generally look for those customers first. In fact, we have had little trouble finding volunteers—teams—that want to try something new. At present we have as many teams wanting to run experiments as we can accommodate.

As we propose market mechanisms to aid with forecasting, potential participants and managers have most often expressed three concerns: incentives, anonymity, and groupthink. Regarding incentives, why does it make sense to pay for performance when employees are already paid to do their jobs? This is an interesting question because most businesses think nothing of offering commissions for sales. Do businesses not already pay the sales force, and should they not be selling anyway? We learned that the first time an Intel factory achieved all of its performance targets across a suite of metrics was when a program offered direct incentives, i.e., cash to each individual employee, for that precise outcome. We do not feel it is out of line to offer forecasters incentives for performance or general market participants incentives for good information. The potential value of the improved forecast is orders of magnitude greater than the cost of the incentives.

The feature of anonymity is somewhat incongruous with Intel's culture of direct, constructive confrontation. If employees disagree they engage and resolve their differences. Allowing employees to participate in systems without identification (to others, not to the research staff running the system) is foreign and may be difficult for some employees to swallow. However, Intel is also a company that values results, and there is room in the culture for improvement.

Can IAMs enable or even cause groupthink? A classic approach toward defeating groupthink is assigning private roles to individuals. For instance, everyone on a team gets a card, and everyone knows that some cards say "devil's

advocate.” With some individuals assigned the role but no one knowing who those individuals are, everyone is able to dissent with less fear of reprisal. A market system where all participants are anonymous and incentivized for performance takes this approach to the limit, freeing individuals to express themselves. Interestingly, although some IAMs that enable participants to observe the group forecast develop could potentially lead to artificial consensus, in all market-like mechanisms the primary opportunity to win and win big comes from being right when everyone else is wrong. This feature certainly helps prevent too great a consensus.

A few more specific challenges have also been faced. Running synchronous IAMs across a global corporation is a problem, given that it is always 2 a.m. somewhere. Teams are reluctant to schedule anything out of normal hours, and it is challenging to find a good time for any large group of people to do something together. This issue is forcing us to consider asynchronous approaches as well.

Another issue has been dealing with a world made up of local geographies. If global sales are the sum of several geographies’ sales, how does one tap local knowledge to forecast the global outcome? We have found our experts within a geography reluctant to try to forecast global results because they feel they do not have enough information to perform the task. That leaves three choices: limiting the markets to global forecasts and participants with a global view, running multiple markets specific to local geographies, or swaying the local experts to participate in a global forecasting market. In the latter case, participation is a critical consideration. If sales are 50% geo A, 30% geo B, and 20% geo C, do we need participation roughly proportional to sales from each geo? Or, is a result weighted by recent sales preferable to the formal market result, which is weighted by participation?

Two remaining challenges we have identified are scalability and long horizons. Forecasting total sales for a product family is valuable, but it does not address the mix of products or SKUs within those products. The market solution probably cannot scale to forecasting all SKUs, and it may not even be suited for that task. Perhaps the right balance is forecasting total product family sales and key products—new or of strategic importance—that will have the greatest impact on financial performance. Regarding horizons, markets are better suited to the short term. Incentives lose power if the payoff is too remote, and feedback is important for driving participation and performance. Forecasting a result within a few quarters seems to work, but over a year begins to feel like a stretch. We are experimenting with alternative market structures that might help forecast the distant future while paying incentives more quickly.

SUMMARY AND CONCLUSIONS

Demand risk is a serious threat to bottom-line performance at Intel and other manufacturing firms. Our studies identified numerous cases where poor information flow led to poor forecasts, which in turn led to decreased business performance.

Markets, and more generally IAMs, promise to help companies address demand risk and other business challenges by improving organizational information flow. Based on results to date, our IAM implementations appear to have had a desirable impact on forecast accuracy and stability. The key drivers that we believe have led to strong performance are 1) anonymity and incentives, which encourage honest, unbiased information, 2) the averaging of multiple opinions, which produces smooth, accurate signals, and 3) feedback, which enables participants to evaluate past performance and learn how to weigh information and produce better forecasts.

Although greater diversity in our participant pool may improve the collective forecast, many ways to increase diversity also increase the potential for bias in our real-world scenarios. Crowds have demonstrated the ability to solve problems such as estimating the weight of a steer [8] or choosing the winner of an upcoming election. But, the prediction may not turn out so well if the new diverse opinions come from those who will profit from selling a heavier steer or from members of the election campaign team for one of the candidates. We hope to explore this issue in upcoming phases of our research.

Our framework for designing IAMs is enabling us to systematically develop new solutions for a number of business problems, and experience, be it in the form of successes or failures, will make us more effective designers. Of particular interest are forecasts that tend to break the simplest IAM designs, predictions with long horizons or predictions whose outcomes may never be known. For instance, was product A better to bring to market than product B? We are defining solutions to these problems today and will soon be testing them in our organization.

Many business processes in use today are neither perfectly effective nor efficient; yet, they are the lifeblood of the organizations that use them. IAMs are a new approach toward business management, promising, and at the same time frightening to potential adopters. As with many such innovations, starting small and running in parallel to existing processes are keys to success. As our trials are demonstrating excellent results at remarkably low cost, expanding their use at Intel is a natural and expected outcome.

APPENDIX

Five Categories of Considerations for Designing Information Aggregation Mechanisms

Information: What is the result to be forecast, how is it defined, when is it known, and to what precision is it known? What range could the result cover, and what granularity of forecast is material to the business? What level of granularity might participants be able to forecast? What information is provided to participants in advance of the market, during the market, and after the market? Where is the line between providing a baseline to improve inputs and providing an anchor that might undermine accurate information? What types of analyses will the information produced by the market enable, and which business decisions will be informed by that analysis?

Integration: Which business processes are related to the market? What is the timing of key decisions or events that will inform the market or be informed by the market? Which other processes attempt to forecast the same result, and should the market function independently or coordinate with the other processes? Based on business cycles or other processes and workflow, when are participants available or busy?

Inclusion: Who should participate in the market? How many participants are needed to achieve good results? Should participants have local and specific views or more aggregate views? Should groups that demonstrate bias in other forecasts participate, and would they bring the same biases to the market? Can people across wide ranges of time zones participate together, and will participation skew results? Might anyone outside the firm participate?

Interface: How will individuals interact with the market? Will the market be continuous or provide snapshots? Is participation synchronous or asynchronous? What level of anonymity is provided? How do traders convert their knowledge and preferences into data and, ultimately, collective forecasts?

Incentives: What will motivate participants to enter the market, and what will motivate strong performance? How do incentives compare to salaries, awards, or other incentives within the corporation? To what extent are strong performance and bragging rights incentives? Will management support the incentives? Are systems available to pay the incentives out without undue cost? Will those processes scale to large numbers of participants?

ACKNOWLEDGMENTS

Thanks to our academic partners whose creativity and insight has yielded new approaches toward solving tough problems: Feryal Erhun, Paulo Goncalves, Jim Hines, Blake Johnson, Thomas Malone, Charles Plott, and Jim Rice.

Thanks to partners in Intel who have driven, supported, and challenged this research: Nicholas Day, Jim Kelloso, Karl Kempf, Adam King, Rich Krigger, Jeff Loose, David McCloskey, Mary Murphy-Hoye, Chris Parry, Jason Seay, and Paul Thomas.

REFERENCES

- [1] Erhun, F., Gonçalves, P. and Hopman, J., "Managing New Product Transitions," *Sloan Management Review*, vol. 48 num. 3, Spring 2007, pp. 73-80.
- [2] Kiviat, B., "The End of Management?," *Time*, July 6 2004 at <http://www.time.com/time/magazine/article/0,9171,660965,00.html>*
- [3] King, Rachael, "Workers, Place Your Bets," *Business Week*, August 3, 2006 at http://www.businessweek.com/technology/content/aug2006/tc20060803_012437.htm*
- [4] Hopman, J., "Managing Uncertainty in Planning and Forecasting," *Intel Technology Journal*, vol. 9, Issue 3, 2005, pp. 175-183.
- [5] Berg, J. E. and Rietz, T. A., "Prediction Markets as Decision Support Systems," *Information Systems Frontiers*, 5(1), 2003, pp. 79-93.
- [6] Chen, K.-Y. and Plott, C. R., "Prediction Markets and Information Aggregation Mechanisms: Experiments and Application," *California Institute of Technology*, 1998.
- [7] Page, Scott E., *The Difference: How the Power of Diversity Creates Better Groups, Firms, Schools, and Societies*, Princeton University Press, Princeton, NJ, 2007, pp. 210-212.
- [8] Surowiecki, James, *The Wisdom of Crowds*, Doubleday Press, 2004, New York, New York.

AUTHOR'S BIOGRAPHY

Jay Hopman is a researcher and strategic analyst in the IT Research Business Agility cluster. His research interests include product management, decision making, forecasting, planning, and organizational coordination. Jay received a B.S. degree in Computer & Electrical Engineering from Purdue University and received an

MBA degree from the University of California, Davis. His e-mail is jay.hopman@intel.com.

BunnyPeople, Celeron, Celeron Inside, Centrino, Centrino logo, Core Inside, FlashFile, i960, InstantIP, Intel, Intel logo, Intel386, Intel486, Intel740, IntelDX2, IntelDX4, IntelSX2, Intel Core, Intel Inside, Intel Inside logo, Intel. Leap ahead., Intel. Leap ahead. logo, Intel NetBurst, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel StrataFlash, Intel Viiv, Intel vPro, Intel XScale, IPLink, Itanium, Itanium Inside, MCS, MMX, Oplus, OverDrive, PDCharm, Pentium, Pentium Inside, skool, Sound Mark, The Journey Inside, VTune, Xeon, and Xeon Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Intel's trademarks may be used publicly with permission only from Intel. Fair use of Intel's trademarks in advertising and promotion of Intel products requires proper acknowledgement.

*Other names and brands may be claimed as the property of others.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Bluetooth is a trademark owned by its proprietor and used by Intel Corporation under license.

Intel Corporation uses the Palm OS[®] Ready mark under license from Palm, Inc.

Copyright © 2007 Intel Corporation. All rights reserved.

This publication was downloaded from
<http://www.intel.com>.

Additional legal notices at:
<http://www.intel.com/sites/corporate/tradmarx.htm>.

THIS PAGE INTENTIONALLY LEFT BLANK

Risk Management in Restricted Countries

Martin D. Martinez, Information Technology, Intel Corporation

Index words: restricted countries, risk management, security in restricted countries

ABSTRACT

Assessing Intel's risks, mitigating those risks, and protecting Intel's Intellectual Property (IP) are three key items that facilitate or impact Intel's continued success when working with or in *restricted* countries. Failure to comply with US government restrictions when working with or in these countries can result in heavy fines, loss of an export license, or imprisonment. Understanding the rules of engagement is critical in today's global economy. Which countries are restricted, what are the technology restrictions, and the consequences for non-compliance with the laws that govern working with or in those countries are discussed.

Intel faces numerous challenges when working in or with *restricted* countries because of cultural differences, different business practices and ethics, and weak IP laws and their enforcement. All of these challenges need to be considered to establish a solid and effective program that keeps Intel compliant with the US and international law, and yet does not impede Intel's growth and continued success in these countries.

In the last five or more years, Intel has seen an increase in the number of foreign nationals hired at Intel who have access to or contribute to Intel's IP. Foreign nationals continue to contribute to Intel's intellectual pool across many disciplines including research and development, sales and marketing, manufacturing, engineering, and software development. Maintaining regulatory compliance across Intel and driving an effective security program while growing the business is a continuous challenge.

Over the last 10-15 years, Intel has grown overseas and established a multi-faceted program that protects its IP at home and abroad. Intel has risk mitigating strategies in several areas including export and import of Intel technologies, data and network protection, data center operations, and physical security (domestic and international).

Intel constantly stress-tests its processes, procedures, and security tools while continuing to adapt to the changing

business environment in an effort to stay ahead of internal business and process changes. The results of our effort have allowed Intel to develop an adequate infrastructure that secures our IP on many different levels to keep us compliant with regulatory requirements while growing our business overseas.

INTRODUCTION

In 1985, Intel became one of the first American semiconductor companies to establish a presence in the People's Republic of China, with the opening of an office in Beijing. In 1991, Intel began its operation in Moscow, Russia and in February 2006, Intel announced a \$300 million investment to build a semiconductor assembly and test facility in Ho Chi Minh City, Vietnam.

Every decision involving Intel's expansion overseas has a multitude of legal and security requirements that have to be met. Failure to comply can result in loss of export licenses or loss of Intel's IP. For years Intel has been so successful in complying with legal and security requirements that on March 26, 2007 Intel announced plans to build a 300-millimeter (mm) wafer fabrication facility (Fab) in the coastal Northeast China city of Dalian in Liaoning Province. The \$2.5 billion investment for the factory will become Intel's first wafer Fab in Asia and yet another major milestone for Intel.

The challenges for Intel have not only been to understand the technology restrictions imposed by the US government, but also to push the envelope by introducing advanced technologies in several foreign countries. Then Intel has the additional challenge of implementing the best possible comprehensive program for protecting our IP.

Prior to introducing a new facility in a foreign country Intel uses a pre-production model (Figure 1) to address potential technology restrictions and potential risks.

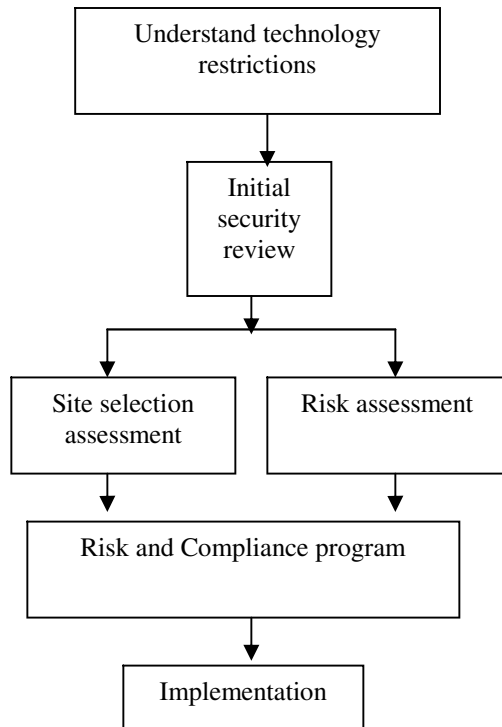


Figure 1: Pre-production model

A sustaining model (Figure 2) is used once Intel has established a facility in a foreign country and this model addresses any expansion or new businesses at that facility.

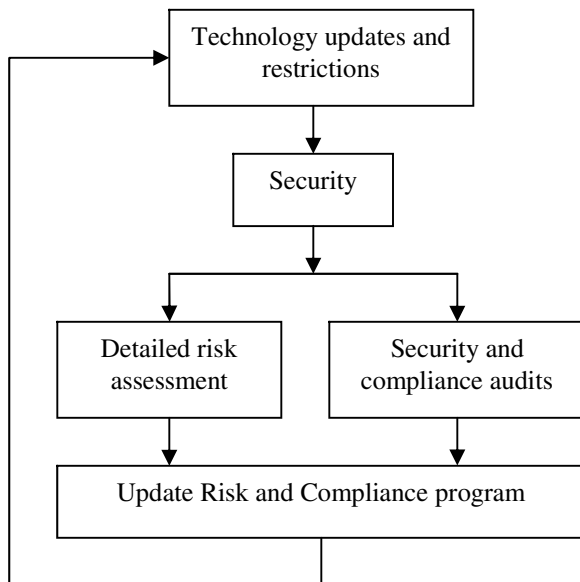


Figure 2: Sustaining model

The two models feed directly and independently into Intel's security requirements that drive Intel's overall risk and compliance program involving multiple efforts and organizations.

The consistency between these two models has contributed to the evolution of Intel's risk management and compliance program and both have played a significant part in expanding our growth in foreign countries. Intel has successfully introduced and expanded sales marketing, research and design, software development, assembly and test facilities, and Fabs in various countries around the world.

The technology restrictions and security requirements continue to be complicated, but Intel's risk management efforts continue to support business growth as Intel expands overseas.

RESTRICTED COUNTRY CLASSIFICATIONS

Foreign countries are considered "restricted" by the U.S. [Bureau of Industry and Security](#) (BIS) [4] for a variety of reasons; e.g., national security, foreign policy, terrorism, proliferation activities, etc. Intel further divides restricted countries into three categories (Table 1): High Performance Computing (HPC) Countries, Controlled Countries (CC), and Embargoed Countries.

Table 1: Intel's own categorized list of restricted countries

High Performance Computing (HPC)	Controlled Countries(CC)	Embargoed and Sanctioned Countries
Brazil	Albania	Burma (Myanmar)
Costa Rica	Armenia	Cuba
Hong Kong (region)	Azerbaijan	Iran
India	Belarus	North Korea
Israel	Cambodia	Sudan
Korea	China	Syria
Malaysia	Georgia	
Philippines	Iraq	
Singapore	Kazakhstan	
Taiwan etc.	Kyrgyzstan	
	Laos	
	Libya	
	Macau	
	Moldova	
	Mongolia	
	Russia	
	Tajikistan	
	Turkmenistan	
	Ukraine	
	Uzbekistan	
	Vietnam	

Note that even though Hong Kong is part of mainland China, export regulations identify Hong Kong as an HPC country. Therefore, the China technology constraints are not applicable to Hong Kong business activities.

The additional classification in Table 1 allows Intel security groups the flexibility to manage risk and compliance more effectively.

TECHNOLOGY RESTRICTIONS

Export regulations are imposed on restricted countries, and these regulations are monitored for compliance by the BIS. These regulations outline legal requirements for

exporting or re-exporting various products and technologies. When dealing with a restricted country, being aware of the regulations is very important. Failure to comply with export regulations can result in fines, loss of export licenses, or even imprisonment, all of which can vary depending on the nature of the incident and the restricted country involved.

Based on the three categories in Table 1 Intel adheres to the following technology restrictions (not all-inclusive):

High Performance Computing (HPC) countries: Currently Intel identifies and maintains a list of ~140+ countries as HPC. An export license is required to export or re-export HPC technology, generally involving design collateral for advanced chipsets. The BIS has a specific formula for calculating computer performance measured in Weighted TeraFLOPS (Trillion Floating point Operations per Second) that also sets boundary conditions for specific technologies that are applied across all restricted countries.

Controlled Countries (CC): Of the 21 countries on the list, Intel has facilities in nine of the CCs. Export licenses are required to export or re-export CPU design or manufacturing information, encryption products and technology, and HPC technology. Intel also has several export licenses that enable limited R&D and coordination throughout the company on new product development.

Embargoed Countries: US companies and individuals are prohibited from doing business with countries embargoed by the BIS. There are no license exemptions for these countries, and there is a presumption of denial for all exports and re-exports of products and technologies.

Intel has to abide by US regulations when exporting US technology from the US directly to a restricted country. However, when Intel is re-exporting US technology from within a restricted country to another restricted country we have to abide by both US regulations and any export or import regulations imposed by the countries involved.

For example, if we have an export license to export high-end chipsets with embedded encryption from the US to Russia and then that same product or technology is re-exported from Russia to Vietnam, we have to have an export license for Vietnam to comply with US export regulations. Russia may have additional export laws that Intel has to comply with, and Vietnam may have import regulations as well.

BIS also maintains a definitive list of *Non-Controlled Countries (Non-CC)* that are not considered restricted and generally there are no export restrictions when dealing with Non-CCs (e.g., Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Ireland,

Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, United Kingdom, and United States). Export restrictions are however applicable any time a Non-CC is dealing with any of the other three categories of restricted countries. Note that other regulatory agencies (i.e., Department of State, Office of Foreign Asset Control, or Department of Treasury) might impose regulatory restrictions on these countries that are not covered by BIS restrictions.

The Global Trade group within Intel is responsible for tracking the frequent export regulation changes, assessing the impact to Intel's business activities, and implementing control processes as required. Intel has an excellent relationship with BIS officials and routinely meets with licensing officers to resolve questions and obtain export license approvals. Intel's proactive efforts continue to be one of our key successes in working with or in restricted countries, something that is demonstrated by the various export licenses that we currently have in place among HPC countries and CCs.

Bilateral and multilateral requirements are in place in every aspect of Intel's business (e.g., sales and marketing, research and development, assembly and test, manufacturing, etc.) that are governed by specific export requirements, and determining these requirements ahead of time is crucial.

METHODOLOGY FOR DETERMINING RISKS AND THREATS

Intel's next challenge is comprehending the risks and threats. The methodology used (Figure 3) outlines the basic components of Intel's security and risk model.

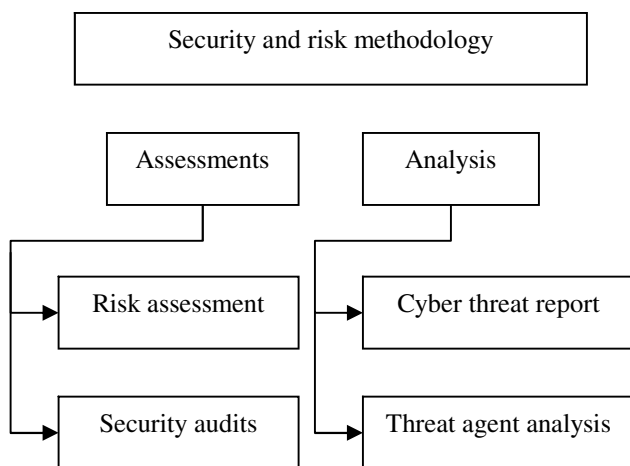


Figure 3: Security and risk model

In the assessment component of Figure 3, risk assessments are conducted as part of Intel's site selection process when considering opening a new facility. The site selection process evaluates political stability, terrorism, IP vulnerability, corruption, crime, and site security services. Each category is rated across five levels ranging from unacceptable to exceeds expectations.

Additional risk assessments are conducted diving deeper into the business to determine risks and threats. Security professionals work closely with internal customers to understand the business environment, and to identify major or minor gaps that could potentially compromise Intel's IP. Security audits are conducted to determine overall compliance with security standards and to find any new security risks. In addition, all risk and security assessment teams use an in-house developed tool as a standard base for all risk assessments. Domestically and internationally, the assessments and audits are conducted annually and randomly.

In the risk assessments component in Figure 3, we evaluate regulatory compliance, ethical and business practices, business issues, espionage, safety, personnel, information technology (IT), IP protection, and physical security. A common risk and threat equation used within Intel evaluates total risk as:

$$\text{Threats} \times \text{Vulnerability} \times \text{Asset value} = \text{Total Risk}$$

During this assessment Intel security understands the basic risks and threat without any additional mitigation controls in place. This provides a general overview of the issues Intel will need to address and tells us where to focus our resources.

Adding the mitigation controls provides a clear picture of the residual risks, and Intel can determine if risks and threats have been reduced to an acceptable level.

$$(\text{Threat} \times \text{Vulnerability} \times \text{Asset value}) \times \text{Mitigation controls} = \text{Residual risk}$$

The combination of the two equations yields the likelihood of a risk, potential impact, and a final ranking of each risk (e.g., business, regulatory, ethical, and security).

In the analysis component of Figure 3 an ongoing process that incorporates a team of security professionals across multiple security groups is conducted.

Quarterly cyber threat reports evaluate current and future cyber threats to allow security groups to understand implications to the business environment and the possible mitigation strategies available.

The Threat Agent Group (TAG) provides analysis across an extensive list of "characteristics" that represent the human factor within Intel's threat model. A standardized

approach is used that facilitates security professionals to speak in a common language regarding the various threat agents and provides the means to measure the threats in a relative manner.

The threat agent matrix considers non-hostile threats (e.g., employee recklessness or untrained employees) and hostile threats (e.g., terrorist, vandalism, data miners, internal spy, disgruntled employees, corrupt suppliers or government officials, etc.). The process attempts to determine desired outcome, skill level, and resources available to the threat agent, among other criteria.

Additional assessments are also considered: for example, the office of the [US Trade Representative](#) [2] maintains an IP report on how well a country is managing IP protection that helps companies like Intel in driving policy changes within restricted countries. [Transparency International](#) [3] is another organization viewed by Intel security professionals that identifies various indicators on overall corruption in a given country.

The benefit of having the right data (e.g., corruption indicators, IP protection issues, etc.) allows Intel's security groups to conduct the best analysis possible; which provides a more accurate assessment of the risk and threats.

Business and security groups within Intel need to know who is after Intel's IP and what resources are being brought to bear to counteract this threat. Resources and finances are limited, so having the correct data in a timely fashion allows Intel to focus its resources in the countries that pose the greatest risks to Intel. This allows us to establish the best and widest possible parameters to protect our assets.

WHAT ARE THE RISKS AND THREATS

Kidnappings, street crime, organized crime, road traffic accidents, resistance to foreign-ownership by state-owned enterprises, medical problems (i.e., Avian flu) are but a few intangible considerations revealed by past site selection assessments.

Current Intel cyber and threat assessment reports a continued rise in cyber security risks. The ease of technical surveillance is also increasing, which causes IP and regulatory concerns to remain high.

Immediate benefits have been realized from the cyber and threat agent analysis. For example, this analysis can help us determine if risks or threats are driven by the private sector, or are sponsored by governments or the military. The private sector can be driven by a desire to be more competitive with multinational companies to avoid having their own small to midsize companies less competitive due to US influence or the influence of other multinational

companies. Governments can be driven by a desire to be more competitive on a global scale to help their own economies improve. The military of course can be driven by a desire to utilize US technology to not only upgrade their own weapons, but also to sell their own military technology to other countries at a much reduced rate, or to sell arms to countries that the US might not sell to.

Government- or military-sponsored activities tend to be better financed than those of the private sector. To complicate matters further, once the wrongdoer is identified, the judicial system may not always be in Intel's favor. IP protection is obviously a big concern and Intel aggressively pursues this with the legal establishment in restricted countries, especially in ones that are known to have weak IP protection laws.

Past assessments and analysis have indicated that the values and culture of a country can be a challenge and must be understood. Intel's business ethics may sometimes be diametrically opposed by certain individuals, groups, or suppliers. Failure to understand other cultures can be costly, bribes being a prime example. Bribes are viewed differently in Asian, Latin, or Eastern European cultures. They can be seen as a necessity in not only getting things done, but also in building the necessary relationships with the right people. If mishandled this can result in "losing face" on one end and impacting business on the other. Consequences of not giving bribes can be felt from construction to food services to obtaining permits, and therefore can easily double the time required to complete the simplest of tasks. However, one of Intel's key corporate principles is to *not* offer or accept bribes or kickbacks under any circumstances.

Misplaced or stolen laptops can sometimes be an issue also. In some countries it is a common practice for employees to sell their laptops to supplement their own income.

What is called plagiarism or copyright infringement in the US is viewed as borrowing from the best or copying with pride in some countries. Attempts to educate a local culture with Intel's business culture can be difficult but it has to be done. Patience is required: change seldom happens overnight. Cooperation between security and business groups moving to restricted countries helps Intel to be proactive in managing risks and threats.

Disciplinary actions can also vary given that in some regions (e.g., Asia) there are laws in place that can make termination of employees difficult. Each case can vary depending on the circumstances, but Intel works with all parties involved to come to an amicable solution.

DEEMED FOREIGN NATIONALS

Another area that needs to be addressed, and that is equally important to understand, is the use of deemed foreign nationals (DFNs) that have access to restricted technology within Intel. DFN is the classification used to identify foreign nationals hired in the US. Generally DFNs are hired from US universities, but sometimes they are also hired from other US-based companies.

Intel has a significant population of DFNs from many restricted countries. When Intel hires a DFN, business groups have to take into account if that DFN is from an HPC country, a CC, or an Embargoed country. If a DFN is from a CC or an Embargoed country, an export license will need to be obtained when that person is hired. Since Intel generally hires DFNs for technical positions, an export license is automatically a requirement. In the event a DFN moves onto another job that may require access to restricted technology Intel avoids any delays by having an export license in place in the early stages of employment.

DFNs from an HPC country generally do not require the same level of scrutiny, due to the fact that the threshold of technology is much higher for an HPC country. In those rare cases where a DFN from an HPC country requires access to restricted technology beyond what an HPC country is allowed, then Intel has to obtain an export license.

Also note that when a DFN obtains permanent residency or becomes a US citizen, then an export license is no longer required. Obtaining permanent residency or US citizenship can take between three to seven years.

Obtaining credible background data on employees equivalent to what Intel can obtain in the US is also a challenge. In Asia, for example, a person can potentially pay to have damaging information removed from their records or to even add false information. Hiring foreign nationals in the US comes with additional challenges. Intel is still limited to the information provided by the country the foreign nationals come from. Competitive intelligence (a.k.a., espionage) and the insider threat have taken on a whole new meaning in the 21st century.

The better-educated Intel employees are about the risks and mitigating strategies, the culture, how best to do business in restricted countries, the better Intel can deal with problems they may face when doing business in or with restricted countries.

HOW INTEL MANAGES RISKS AND THREATS

Intel defines overall requirements for managing risks and threats based on regulatory, and security and risk managements efforts.

The regulatory component is driven by the Global Trade group and drives compliance with US and international export regulations. Some key aspects of the regulatory component include the following:

The Global Trade group interprets export regulations, classifies restricted technology, and determines export restrictions to international destinations.

The Global Trade group and Information Security conduct technology reviews with business groups in advance of moving operations (part or all) to overseas destinations. Such reviews assess the scope of the project, associated technologies, and determine license and security requirements that allow Intel to have consistent controls across the corporation.

The Global Trade group defines and manages the global hiring processes and foreign national license reviews. Here, Global Trade evaluates the job requirements of Intel's foreign national employees, classifies the type of technology the employee will be able to access, and obtains the appropriate export license for each foreign national.

The security and risk management component (Figure 4) drives Intel's IP and regulatory protection efforts consistently across the various security groups at Intel.



Figure 4: Security management model

Having clear security policies that outline roles and responsibilities, expectations, and requirements is the cornerstone of Intel's security program. Flexibility is maintained within security policies by working with the business groups to understand the demands of the business. For example, data segmentation or additional security monitoring may be required when sensitive IP is involved in certain high-risk countries.

Security groups work closely with Global Trade and take additional precautions to adhere to any conditions that are spelled out in any export license that Intel obtains.

To stay current with competitive intelligences, cyber threats, and availability of the latest security tools, education of Intel's security professionals is actively pursued. Through participation in security conferences and seminars and working with external security organizations (e.g., [Information Risk executive council](#) [1]) Intel is able to stay abreast of the latest information in the security field.

Additionally, most security professionals at Intel have or are pursuing some type of security credentials. Among the most common are Certified Information System Security Professional (CISSP), Professional Certified Investigator (PCI), Physical Security Professional (PSP), and Global Information Assurance Certification (GIAC). The wide variety of certifications maximizes the capabilities of Intel's security professionals and maintains a high standard across multiple security groups.

Training Intel employees is just as important as educating Intel's security workforce and is paramount in keeping Intel compliant. Intel's training and awareness programs cover both security and global export education. Courses provide basic understanding on expectations, regulatory and security requirements, and case studies to educate Intel employees. The native language of a country is also used where possible to facilitate learning.

The combination of regulatory and security efforts allows Intel to conduct compliance assessments across the company. Assessments are conducted annually while differentiating between export and Intel security compliance. Business groups require a clear understanding between US government vs. Intel requirements to better manage their own resources to address gaps and continually improve.

CONSEQUENCES OF NON-COMPLIANCE

Intel makes a tremendous effort to understand regulatory requirements, comprehend risks and threats, and implement the right amount of security based on those risks. Failure in any area can result in loss of IP or legal action from the BIS.

There are legal ramifications for compromising Intel's IP as such actions adversely impact Intel's strategic competitiveness or result in financial loss. Recovery from IP loss can take several years and within Intel's competitive environment significant or critical IP loss is not an acceptable risk.

The complexity of the regulatory environment mandates that questions be asked to determine if an export license is needed; e.g., what type of technology will be used, which restricted countries are involved, are DFNs a factor, will technology or products be re-exported, etc. Each one of the above may come with conditions or restrictions that have to be clearly understood and implemented.

Honest mistakes can and will be made, but the ones that are not reported can do the most damage. Export regulations are complex and often have "gray" areas that might be open to interpretation. By working very closely with the BIS and other government agencies Intel has avoided potential road blocks.

The consequences of a bad interpretation of an export regulation or for not adhering to conditions that are part of an export license, for example, can result in penalties to Intel and its employees.

The BIS breaks down Export Administration Regulations (EAR) violations into two categories: criminal and civil:

Criminal

For *willful violations* that involve a company and/or employees who deliberately are involved in covering up an EAR violation and do not report it, the consequences can be severe:

A corporation could be fined up to \$1,000,000 or five times the value of the exports for each violation, depending on which is the greater.

An individual could be fined up to \$250,000 or be imprisoned for up to ten years, or both, for each violation.

For *knowing violations* that involve a company and/or employees who are involved in an EAR violation but report the violation upon discovery, the consequences can also be severe:

A corporation could be fined up to \$50,000 or five times the value of the exports for each violation, depending on which is the greater.

An individual could be fined up to \$50,000 or five times the value of the exports, or can be imprisoned for up to five years, or both, for each violation.

Civil

For each violation of EARs companies and individuals can be penalized as follows:

They can be *denied export privileges*. This means all of the export privileges of a company or individual will be removed to prevent an imminent export control violation. These orders cut off not only the right to export from the US, but also the right to receive or participate in exports from the US.

They can be *excluded from trade* and/or a fine of up to \$11,000 for each violation can be imposed.

Violations involving national security can result in fines of up to \$120,000 for each violation.

To better illustrate the consequences, here are two examples of recent cases.

In September 2004, the BIS assessed a \$560,000 administrative penalty against Lattice Semiconductor Corporation for sending extended range programmable logic devices and technical data to China and sharing restricted technology with Chinese foreign nationals in the US. The items and technology are controlled for national security reasons.

In April 2006, Boeing Corporation settled a long-running case with the State Department's Directorate of Defense Trade Controls for a sum of \$15 million in penalties for violation of export laws involving gyro chips to China.

Export laws change from year to year and specific country-based restrictions can change numerous times during any given year: staying abreast of these changes is a necessity.

Intel is very assertive in maintaining the proper security to restrict and avoid inadvertent access to unauthorized

technology by restricted country employees. Both Global Trade and Corporate Security take an active role to protect Intel's IP. Intel's expectation is that every employee shares in the responsibility of keeping Intel compliant with export regulations, internal security, and IP requirements at all times.

SUMMARY

Managing Intel's business activities in restricted countries, maintaining regulatory compliance, and adhering to security guidelines is complex and challenging, as is maintaining compliance with license requirements for DFNs.

Intel's ability to build a Fab in China, and the great strides Intel has made in other countries such as Russia and Vietnam have been possible due in large part to Intel's due diligence in understanding regulatory requirements and mapping a successful security and risk management strategy.

Intel's security and risk management efforts have been discussed in varied detail and are summarized in Figure 5. This figure illustrates the high-level components of Intel's effort to remain compliant, protect our IP, and still be flexible enough to stay on track with our dynamic business environment.



Figure 5: Security and risk management model

Intel understands the job requirements, business goals, and the diversity of cultures in these countries and realistically maps the risks and threats by country.

As Intel continues to grow and expand into restricted countries, new market segments and new technology areas, Intel's export and security compliance program continues to evolve in support of corporate objectives. We have established one of the most assertive security programs for our industry. Dealing with export requirements and numerous cyber security threats, along with internal and external security issues requires due diligence on the part of all employees. Educating everyone in the company on the risks, threats, consequences, and expectations protects Intel's IP and employees, our most valuable corporate assets.

ACKNOWLEDGMENTS

We acknowledge Keith Core, Information Risk and Security, Data Protection Compliance manager, Carol Kasten, Information Risk and Security, Data Protection Department manager, Victoria Gomez Kelsey, Technology and Manufacturing Group–Risk and Controls, Glen Shirley, Principle Engineer, Technology and Manufacturing Group, and Susan A. Straub, Director of Global Trade, for their contributions to this paper.

REFERENCES

- [1] Information Risk executive council at <https://www.irec.executiveboard.com/Public/Default.aspx>*
- [2] Office of the US Trade Representative at <http://www.ustr.gov/>*
- [3] Transparency International at <http://www.transparency.org/>*
- [4] US Bureau of Industry and Security–US Department of Commerce at <http://www.bis.doc.gov/>*

AUTHOR'S BIOGRAPHY

Martin D. Martinez is the Control Country Business Manager for Intel since 1999. Martin worked in China for two-and-a-half years and travels overseas on an annual basis. He has a B.S. degree in Computer Science from the University of Texas in San Antonio. His current interest revolves around competitive intelligence. His e-mail address is martin.d.martinez@intel.com.

BunnyPeople, Celeron, Celeron Inside, Centrino, Centrino logo, Core Inside, FlashFile, i960, InstantIP, Intel, Intel logo, Intel386, Intel486, Intel740, IntelDX2, IntelDX4,

IntelSX2, Intel Core, Intel Inside, Intel Inside logo, Intel. Leap ahead., Intel. Leap ahead. logo, Intel NetBurst, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel StrataFlash, Intel Viiv, Intel vPro, Intel XScale, IPLink, Itanium, Itanium Inside, MCS, MMX, Oplus, OverDrive, PDCharm, Pentium, Pentium Inside, skool, Sound Mark, The Journey Inside, VTune, Xeon, and Xeon Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Intel's trademarks may be used publicly with permission only from Intel. Fair use of Intel's trademarks in advertising and promotion of Intel products requires proper acknowledgement.

*Other names and brands may be claimed as the property of others.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Bluetooth is a trademark owned by its proprietor and used by Intel Corporation under license.

Intel Corporation uses the Palm OS® Ready mark under license from Palm, Inc.

Copyright © 2007 Intel Corporation. All rights reserved.

This publication was downloaded from <http://www.intel.com>.

Additional legal notices at:
<http://www.intel.com/sites/corporate/tradmarx.htm>.

THIS PAGE INTENTIONALLY LEFT BLANK

Assessment and Control of Environmental, Safety, and Health Risks in Intel's Manufacturing Environment

Steve W. Brown, Environmental Health & Safety, Intel Corporation
Todd Brady, Environmental Health & Safety, Intel Corporation
Milt Coleman, Environmental Health & Safety, Intel Corporation
Tom Cooper, Environmental Health & Safety, Intel Corporation
John Currier, Environmental Health & Safety, Intel Corporation
John Harland, Environmental Health & Safety, Intel Corporation
Ted Reichelt, Environmental Health & Safety, Intel Corporation
Scott Swanson, Environmental Health & Safety, Intel Corporation

Index words: risk, environmental, manufacturing, safety, hazard, goals

ABSTRACT

This paper provides an overview of the major environmental, health, and safety risks that apply to semiconductor manufacturing and what specific approaches are used to assess and reduce the risks in each new generation of facility or process. We describe how this approach fits the classic "risk reduction hierarchy" of eliminating inherent risks *FIRST*. We describe how a systems approach that ties all risks together has helped Intel manage these risks despite significant changes in process and facilities design over the last ten years.

INTRODUCTION

Successfully controlling risks in semiconductor manufacturing requires a comprehensive and repeatable approach to evaluating chemicals/materials, facility and system design, effective integration of real-time monitoring, pre-start-up review, and complementary administrative (e.g., procedural) controls. This kind of "systems approach" has proven to be the key in developing a thorough understanding of process manufacturing hazards and associated environmental impacts. With thorough assessment and exchange of information between multiple disciplines, comprehensive risk reduction and control can be implemented early, as part of process development, and shared formally as part of the process transfer. The overall intent is to avoid negative business impacts due to product bans (e.g., "lead-free"), business interruptions (e.g., facility or asset loss), or a catastrophic event affecting employees and surrounding communities that can have negative impacts for many years.

Semiconductor manufacturing requires the use of many restricted and highly regulated materials. These regulations require due diligence to evaluate risk and implement appropriate control measures to eliminate or significantly reduce immediate and long-term risks to employees, the public, and to the environment. These regulations apply to almost all aspects of Intel's manufacturing: wafer manufacturing, which is classified as a "high-hazard" occupancy and one of the most highly regulated types of facilities; equipment, which is covered by a host of consensus safety standards as well as regulations (electrical codes, plumbing codes, etc.); chemicals/materials, which are covered by an extensive and broad list of regulations throughout the world addressing such things as workplace exposures, environmental discharge limits, fire protection, and product content, to name a few.

Intel's Environmental Health and Safety (EHS) organization is responsible for the identification, assessment, and control of hazards to employees, surrounding communities, and the environment. In the mid 1990s EHS recognized that a comprehensive approach was needed to minimize risk to Intel's business and ensure it was well positioned to meet the following goals:

Have the safest workplace possible for our employees.

Do no harm to surrounding communities.

Reduce our environmental footprint to enable fast factory ramps and flexibility.

Address EHS concerns early in the development of new manufacturing processes and products.

Meet customer needs for environmentally responsible and low energy products.

We discuss the approach that is taken to effectively identify and reduce risks associated with Intel's operations worldwide.

Early Warning System

Predicting the future is impossible, but identifying emerging issues and trends early allows for better planning and resolution of EHS issues, before they cause employee, community, or business risk. EHS has established a business process that identifies emerging issues through an internal scan (sonar) of our technology roadmaps and an external scan (radar) of the regulatory and external stakeholder landscape. Identified issues are sorted, prioritized, and incorporated in the annual business planning process.

Internal scans of process technology roadmaps, product roadmaps, and other business plans are conducted by several internal groups. Process technology is covered by the Chemicals and Natural Resources SCS and the Assembly Chemicals and Natural Resources Steering Committee. Product trends and roadmaps are handled by the Product Ecology Steering Committee.

External scans and planning are done through a strategic partnership between EHS, Public Affairs (PA), Government Affairs (GA), Corporate Product Regulations and Standards (CPRS), and Legal. Teams composed of representatives from these organizations are assembled for each region: the Americas, Asia, and Europe, Middle East, and Africa (EMEA). The regional teams develop external engagement plans customized to their geography. A global senior management committee oversees the regional teams and the plans developed by these teams. There is close coordination with the internal teams.

From benchmarking with other leading companies, this process appears unique in producing consistent globally co-coordinated results with minimum resources. Also note that this process is also valuable in identifying areas of possible business opportunity or advantage.

ENVIRONMENTAL

In the 1990s, as Intel's operations expanded and diversified, an increased risk of not meeting current or future environmental requirements was recognized. Waiting for regulatory agencies to issue more stringent environmental permits resulting in time-consuming and costly delays due to public review was not an option. Limiting expansion and flexibility on the grounds of environmental constraints, real or perceived, was clearly a risk Intel could not take.

Many companies rely solely on end-of-pipe expansion tactics like adding expensive abatement equipment or moving their manufacturing operations to less regulated countries. Intel developed a unique and strategic plan to avoid these risks: research and development teams were given process-specific environmental goals or targets prior to beginning product development. By using this strategy and achieving the goals, each new process generation would be at minimum environmental risk as it transferred to high-volume manufacturing (HVM) sites. In this section we define Intel's environmental goal-setting process, its global applicability, and how it minimizes risk throughout each technology lifecycle.

Environmental Risk Assessment

Setting Intel's process environmental goals is complex and demands a complete review of both current and future environmental risks. Tying this program into Intel's long-term expansion planning is a key piece of the goal-setting process. For this reason, environmental engineers are integral to Intel's site selection and long-range planning teams. Environmental concerns vary due to differences in geography, population density, other industrial infrastructure, local regulations, and global initiatives. Despite these differences, Intel proliferates environmentally consistent technology worldwide, designed to protect the most sensitive site from adverse environmental impacts throughout the expansion roadmap. This proactive strategy enables flexibility and reduces the risk of environmental restrictions. After years of developing this process, Intel is currently setting process goals in four main categories: air, wastewater, chemical waste, and ultra-pure water use. Each area demands a unique approach to risk management. See Table 1 for details.

Table 1: Intel environmental process goals and drivers

Parameter		Driver
Air Pollutants	Volatile organic Compounds (VOC)	Remain federal minor source
	Hazardous Air pollutants (HAP)	Remain federal minor source
	Perfluorinated compounds (PFC) Global Warming	Corporate goal (10% <1995 by 2010)
Wastewater Pollutants (<70% any permit)		Avoid POTW interference and pass-through
Ultra-pure Water (UPW/URW)		External community commitments
Chemical Waste		Community concern about toxic waste

Air

The United States Environmental Protection Agency defines facilities as major emission sources of air pollutants if they exceed certain thresholds of volatile organic compounds (VOCs), which can cause smog or hazardous air pollutants (HAPs). Sites that are major sources are generally subject to more restrictive requirements that can limit flexibility to make process changes or introduce new equipment. Intel's business model requires that new manufacturing processes be introduced rapidly and that there is the flexibility to continuously improve existing manufacturing processes. Intel has a policy to remain a US Federal minor source of air pollutants making it a win-win for Intel: the communities have less air pollutants, and Intel reduces risk by having the flexibility to rapidly make process improvements. Air emission goals are established to enable manufacturing sites to remain as minor air emission sources.

Increased concern about global warming raises the risk that high global warming chemicals may be severely restricted. Perfluorinated gases (PFCs) such as SF₆, C₂F₆, and NF₃ are critical chemicals in semiconductor manufacturing as etchants and for in-situ chamber cleans. Chemicals in this class also tend to cause global warming because of their stability in the atmosphere. Intel has worked with the World Semiconductor Council to establish the first worldwide industry voluntary reduction target for global-warming emissions. This target is to reduce absolute global warming emissions from the

worldwide semiconductor industry by 10% below 1995 levels by 2010. Because of the high compound annual growth rate of the industry this is equivalent to about a 90% reduction in emissions per production unit or per chip. The world-wide agreement ensures all companies start on a level playing field and no one company reduces its competitiveness by investing to address this important environmental issue.

Wastewater

While clear directives regarding air emissions are given by both international and national governing bodies, defining risks from discharges associated with wastewater pollutants is site specific. At each of Intel's fabs, the wastewater is discharged to a Publicly Owned Treatment Works (POTW). These POTWs treat both industrial and residential wastewater and discharge their treated wastewater to varied end uses including rivers, irrigation ponds, and even directly into groundwater aquifers. To minimize the risks of impacting local infrastructure and the environment Intel has established close relationships with the ten POTWs serving the worldwide manufacturing facilities and has also partnered with key consultants specializing in wastewater modeling, control, and treatment.

In order to establish the appropriate goals, Intel's wastewater engineers engage the technology development researchers and their process roadmaps to scan for materials that may be considered risks to these POTWs and ultimately to the environment. Intel uses the USEPA's Office of Wastewater Management Local Limits Development Guidance as the basis for each wastewater goal and to help understand early in development what pollution prevention or infrastructure changes will be needed. The process takes into consideration domestic and industrial growth projections in each region along with other factors such as POTW operational limitations, POTW infrastructures, worldwide wastewater permits, and water quality. For those chemicals where little or no data exists, structured scientific analyses are conducted to understand the control requirements. By using the same process to set goals as the local municipalities use to set permit limits, Intel's goal-setting process is consistent and defensible, thereby minimizing the risks that changes in local requirements will impact the technology lifecycle.

The wastewater goal-setting program and its successes have been shared with a number of POTWs, governmental officials, and industry groups. In each case Intel has received accolades for being innovative, environmentally friendly, and proactive.

Chemical Waste

Several process generations ago, Intel recognized the risk associated with shipping off site increasing volumes of

chemical waste. In addition to cost, the risks of exposing the public to Intel's chemical waste, and the image this portrayed, was a driver for establishing a chemical waste goal. To reduce chemical waste, Intel applies the pollution prevention hierarchy: replace, reduce, reuse, recycle, abate. A successful application of the hierarchy (Figure 1) is the optimization in volume and the reclamation of copper from a plating waste that was once shipped offsite. Intel developed and installed a system to reclaim elemental copper for recycling, while returning clean water to the watershed. In this way, Intel has reduced the liability (and cost) of shipping large quantities of waste off site, while taking the responsibility to minimize the environmental impact of its operations.

Water

Although water use is generally not regulated by permits, excessive use can have considerable environmental impacts. The risks of operating sites in arid and desert regions are evident as water rights, water recycling, and water conservation have become community priorities. Maintaining public support of site manufacturing and expansion is very important. The greatest opportunity to reduce water consumption is during the selection of new manufacturing equipment. In 2006, Intel established a goal to reduce its 2010 normalized water use to below 2005 levels.

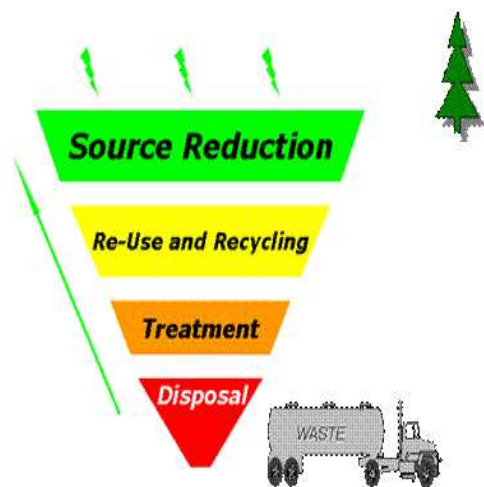


Figure 1: Intel's design for environment strategy

Validation

When new manufacturing processes are ramping at the HVM sites, engineers measure the performance to the environmental process goals in each of the areas outlined above. Although goal setting takes place up to three years prior to HVM, validating the performance of each technology provides the feedback to determine the

effectiveness of the goals and the gaps that exist with respect to the current performance. In identifying these gaps, site engineers can more accurately understand the risks associated with future expansion plans.

Product Ecology

EHS and the Corporate Product Regulations and Standards (CPRS) organizations work closely with product development groups to avoid conflicts between designs and requirements for energy use, materials content, and recyclability. External engagement to ensure workable product standards and globally harmonized requirements is of increasing importance as regulations are increasingly put in place in emerging geographies. The Product Ecology Steering Committee and the higher-level senior management review group coordinated product ecology priorities and strategies.

Chemical Use, Industrial Hygiene and Toxicology Concerns

In order to continue to meet Moore's Law the design and development of Intel's semiconductor products requires the use of new and novel materials. In fact over 9,000 materials were evaluated at Intel's technology development centers in support of new logic, memory, and packaging products. The drive for increasing performance is resulting in not only the use of new materials in the semiconductor fabrication process but is also driving the need to custom create new compounds and formulations that have never been used in commerce before. The introduction of new chemicals and manufacturing processes without adequate controls has resulted in the past in personnel exposure to toxic materials, adverse chemical reactions (fire/explosions), and facility problems such as blockage of critical waste streams of on-line HVM factories.

As part of Intel's Chemical Use Policy, all materials purchased for use undergo an EHS review prior to their use. The EHS review includes a determination of the product's hazards and a review of the applicable legal requirements governing its use. The regulatory review includes not only the requirements specific to the Technology Development facility but also includes the restrictions applicable to the potential HVM site as well. Early identification of site-specific, chemical-specific legal requirements is critical to understand their potential for use in HVM. External engagement also identifies regulatory restrictions for the use of critical materials. Teams are actively working on the development of the Registration, Evaluation, Authorization for Chemicals (REACH) in the European Union and reserving the ability to use critical chemicals until workable alternatives are proven (e.g., PFOS, lead for certain product applications). Based on the hazard review and legal requirements

determination the proper use requirements are provided to the researchers in order to ensure the safe and regulatory compliant use of the material. Examples of the types of use requirements provided to the researchers include toxic gas monitoring requirements, use of personal protective equipment, designation of waste disposal methods, storage requirements.

Since many of the materials are either new to the semiconductor industry or are a new material entering commerce there is frequently little to no published health hazard information available on the specific compounds of interest. Intel EHS utilizes a board certified toxicologist to perform toxicity assessments to determine if the materials are carcinogenic, cause reproductive problems, are extremely toxic, or otherwise hazardous to human health. Intel's toxicologist employs sophisticated EPA models for toxicity determinations when no published toxicity information exists.

Based on the hazards identified, a site-specific team of experts evaluates the proposed use of the material to

determine the use requirements. Included in the team are chemists, environmental engineers, industrial hygienists, toxicologists, facilities engineers, and materials purchasing representatives. This multi-discipline approach has proven invaluable in identifying potential safety issues in new chemicals with respect to their impact on facility waste systems. Of particular importance is the identification of adverse chemical reactions during the use of the material or subsequent facility waste treatment processing.

Materials that are identified as posing a high risk to personnel, processing equipment, or facilities undergo an additional Process Hazard Analysis (PHA) to ensure all safety issues have been identified and resolved. An example of the use of PHA would be the introduction of a highly toxic reactive gas into a diffusion furnace. The PHA would be performed with Intel engineers and representatives from the diffusion furnace manufacturer to fully identify the new hazards and to ensure that the necessary engineering controls are in place to safely use the material on a specific furnace (Figure 2).

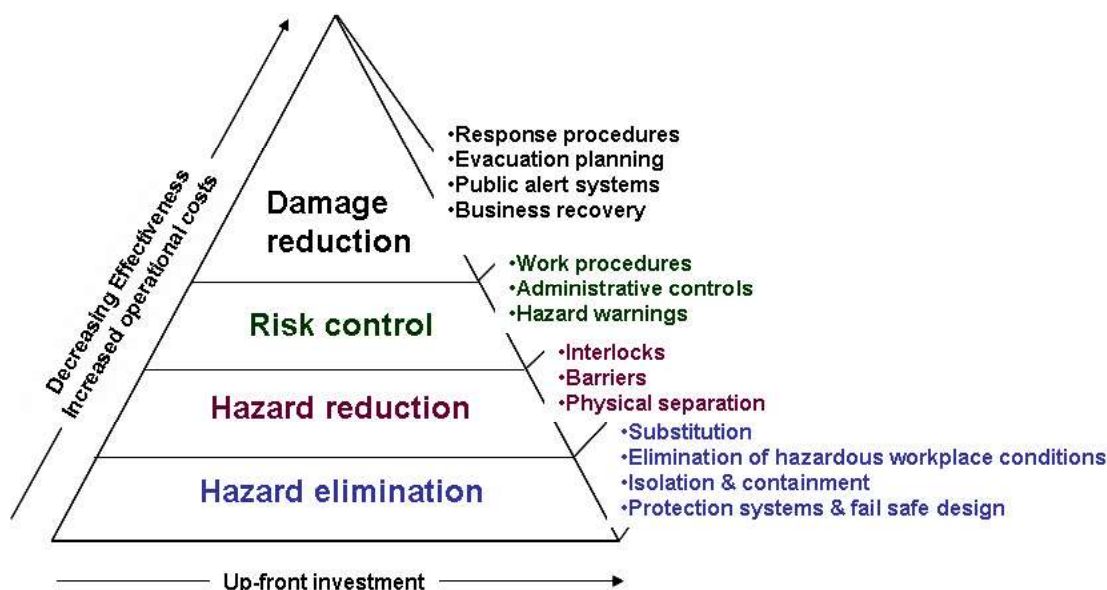


Figure 2: Model for early engagement with technology development: broader impact and effectiveness with fewer operational resources

Safety in Design

The Hazard Profile

Today's semiconductor facilities utilize toxic, corrosive, pyrophoric, and flammable materials. These materials are inherently hazardous, sometimes in small quantities, and therefore safety engineering is required to contain the hazard, reducing the risk to meet acceptable risk levels. Elimination of any single point of failure causing a release is one basic premise utilized. Figure 3 shows the critical

points of risk that must be addressed, and the activities to address these risks are discussed in the following sections. The risk management and control of these risks starts by integrating EHS systems into the procurement and installation of process equipment, facilities design, the safe commissioning and pre-startup safety process of these new facilities, and finally into influencing external codes and standards.

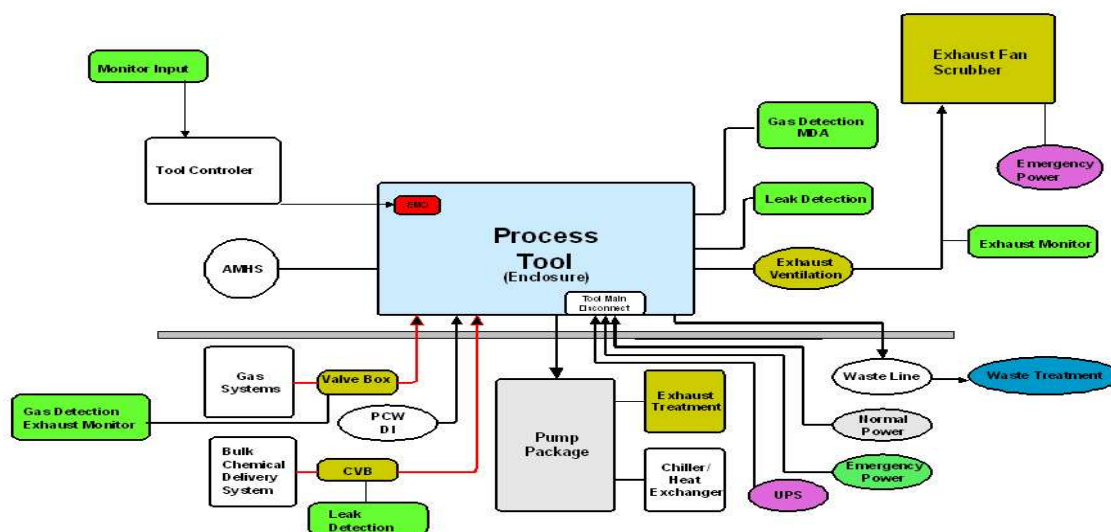


Figure 3: Critical points of failure and control in typical process tool installation

Safety in Equipment Design

Intel's EHS requirements for the procurement of process equipment are primarily driven to the front of the supplier chain through the Semiconductor Equipment Manufacturers Institute (SEMI) guideline process, an organization that develops standards for its members. Intel has long participated in SEMI, serving and chairing several committees over the years, and it was the first company to include EHS-related SEMI standards in its purchase agreements in the mid 1980s. EHS requirements such as SEMI S2 (safety), SEMI S8 (ergonomics), and S10 (hazard classification) are just part of the "S" series of SEMI guidelines intended to define these industry standards for process equipment. In addition, Intel-specific requirements are included to address other risks. These include combustible material restrictions to reduce fire risk and insurance costs, and environmental characterization and emissions requirements to control and manage our site environmental permitting requirements for air, waste, and water emissions (see Environmental section, earlier in the article).

After the procurement of process equipment, it must be installed and integrated into facility systems. To accomplish this, EHS has integrated its requirements into the process equipment installation standards. This includes ergonomic clearances for safe maintenance and operation, ventilation, spill control, gas detection, and all EHS aspects related to how the process equipment is

installed. After these requirements have been established for equipment installations at the TD site, they are transferred via the Master Design Package, which documents how all process equipment is installed at HVM sites.

Facilities and Chemical Distribution Systems

Semiconductor process equipment is supported by larger facilities systems that perform gas distribution, bulk chemical delivery, and waste treatment. EHS requirements are integrated into the design of this equipment through the Facilities Equipment Procurement Process, which is an Intel master specification for all newly procured and designed facilities systems. As with process equipment, driving these requirements up the supply chain is the philosophy employed. This starts with outlining expectations early in the Request for Proposal (RFP) and Request For Quote (RFQ) from each supplier, and ends in the final design of the equipment. In addition, all new facilities systems have a formal Process Hazard Analysis (PHA) conducted to assess the upset conditions the equipment may present, the controls in place, and the adequacies of these controls to prevent events with high or catastrophic potential. As with process equipment, these facilities systems are procured at the TD site, and these EHS aspects are copied and transferred to the HVM sites through the Facilities Transfer Process.

Safe Building Design

Process equipment and facilities equipment must all reside within the walls of the actual fabrication facilities. EHS has integrated its requirements through the EHS Master Design Standard (MDS). The EHS MDS defines the requirements and expectations for the fabrication facilities; a second MDS exists for AT facilities and office buildings. This standard is used to support the many codes, standards, and regulations that drive the design of our facilities.

Pre-Startup Safety Review

After the integration of EHS requirements into the procurement, design, and engineering aspects is complete, it is critical to ensure that these new facilities are constructed to the design, and that all safety systems are in place and functional prior to startup. This is especially important for high hazards chemical and gas systems. For this reason, EHS requirements are a key part of the pre-startup and commissioning process. EHS has developed these checklists for process equipment, facilities systems, and factory commissioning.

External Influence

Semiconductor facilities are highly regulated by fire and building codes and other standards. Intel participates in various committees, such as NFPA 318 (Fire Protection and Life Safety in cleanrooms) and SIA FABS (Fire and Building Codes) to influence the International Fire and Building Code, and the Center for Chemical Process Safety to influence publications and research related to process safety. By doing this Intel strives to maintain a high degree of occupant safety and to also ensure increased flexibility and reduced cost where opportunities exist.

RESULTS AND DISCUSSION

Over the past decade, Intel has nearly doubled its revenues, added significant manufacturing capacity, introduced new complex technologies, and added many new employees in diverse geographies to support this growth. During this same time period, Intel's proactive programs to reduce EHS risks have paid off. For example, over the past ten years, employee injury rates were reduced by 75% to world-class levels. In the past five years alone, air emission rates and water usage rates have dropped 50% and 30%, respectively. Such results not only reduce the EHS risks of the company, but directly benefit our employees and the communities in which we operate. In addition, cost savings are achieved through fewer injuries, fewer waste treatment facilities, and fewer utility purchases.

These achievements have not gone unnoticed. In the past five years alone, Intel has received over 50 EHS awards

around the globe for its programs and practices. In 2006, Intel was named the Technology Sector Leader in the Dow Jones Sustainability Index for the sixth year in a row.

Likewise, early engagement in public processes and regulatory initiatives has paid dividends. Intel was the first company to become part of the EPA Project XL program¹, a voluntary program for environmental improvement activities coupled with transparency to the community. The results have been remarkable: fewer emissions, less use of natural resources, more dialogue with the community, and flexible operations for Intel. Similarly, by working with other industry leaders within the semiconductor industry, Intel was instrumental in developing the first worldwide agreement to voluntarily reduce gas emissions.

Another measurement of success for Intel's EHS risk management program is the lack of EHS incidents associated with a new technology ramp. New technologies to support the march forward of Moore's Law is critical to the company's success. For the past four technology generations, Intel's teams have been successful in setting and achieving environmental goals to minimize the EHS impact of its factory operations. Techniques have included process modifications, alternative chemistry development, manufacturing process modifications, and abatement equipment development. Recent examples include reduced ammonia use, replacement of hazardous solvents, changes from PFC chemistries with high global warming potential to chemistries with much lower global warming potential, implementation of wastewater treatment systems to reclaim metals, and the removal of organic pollutants.

Intel's technology ramp has also demanded the construction of many multi-billion dollar semiconductor fabrication plants. Although construction schedules were compressed and fabs were built in record time, safety at the construction sites remained paramount. World-class injury rates were achieved. It was not uncommon for construction jobs to log millions of man hours without a single injury.

CONCLUSION

Intel's EHS risk management system consists of six core elements:

1. Protecting our people.
2. Protecting our communities.
3. Reducing our environmental footprint.

¹ Overview of Intel's Project XL program at <http://www.intel.com/intel/other/ehs/projectxl/>

4. Identifying potential EHS issues early and designing them out.
5. Aligning products and manufacturing processes to external trends.
6. Continuous improvement.

Such an approach has proven successful for more than a decade. As the company has experienced significant growth, injury rates have fallen, our communities have been improved, our environmental footprint has been reduced, and EHS risks have been minimized in our products and manufacturing processes. Four very important assets have been protected: Intel employees, communities in which Intel operates, Intel's reputation as a good corporate citizen, and Intel's fixed assets. We believe that equals success.

ACKNOWLEDGMENTS

David Harman—Fab TD EHS Environmental Engineer

Steven Kinsler, PhD—Americas Region Toxicologist

Melissa Greahsam—Fab TD EHS Environmental Engineer

Cherry Moyer—Global Environmental Engineer

Jim Charley—Global Environmental Engineer

Richard Parker—Ergonomist, Americas Region EHS

AUTHORS' BIOGRAPHIES

Scott Swanson is a Senior Safety Engineer in the Fab Technology Development EHS organization. In his 17 years in the field, he has worked as an industrial hygienist, safety engineer, and EHS Supervisor within the aerospace, petrochemical, and semiconductor industries. He has been employed with Intel for 10 years. He is board certified as a Safety Professional and Industrial Hygienist and holds a B.S. degree in Public Health and an M.S. degree in Industrial Hygiene from the University of Minnesota-Duluth. His e-mail is scott.swanson@intel.com

Todd Brady is the Corporate Environmental Manager for Intel Corporation. In this role, he leads Intel's corporate-wide environmental programs. Todd holds a B.S. degree in chemical engineering from Brigham Young University and an M.S. degree in environmental engineering from the University of Illinois at Urbana-Champaign. His e-mail is todd.a.brady@intel.com

Tom Cooper is the Worldwide Water Program Manager for Intel Corporation and his responsibilities include wastewater policy and program development, groundwater and site remediation, and water conservation initiatives. He has been with Intel for 10 years and has a B.S. degree

in Environmental and Systematic Biology from Cal Poly (SLO) and an M.S. degree in Environmental Engineering from the University of San Francisco. His e-mail is tom.cooper@intel.com

Ted Reichelt is a Principal Environmental Engineer in the Global Environmental Group at Intel. He is involved with the development of international environmental regulations, product ecology issues, green buildings, and technical leadership. His e-mail is ted.reichelt@intel.com

Milt Coleman has management responsibility for EHS programs in the Americas Region West and Fab Technology Development EHS programs. From 2003 to 2006 he was a member of the International SEMATECH Process Advisory group for Environmental Safety and Health. He is also a member of the Semiconductor Equipment Manufacturers Institutes (SEMI) International regulatory committee. Milt holds a M.S. degree from the University of So. California. His e-mail is milton.coleman@intel.com

John Currier is a Senior Environmental Engineer in the Technology Development EHS Group. His primary responsibility is to set environmental goals that allow expansion of Intel's manufacturing operations while minimizing adverse environmental impacts. During John's seven years at Intel, he spent his first three as a facilities process engineer, owning waste treatment systems at Intel's Rio Rancho, NM facility. Prior to joining Intel, John spent 12 years in the power industry with the Tennessee Valley Authority as a chemical engineer, optimizing ultrapure water systems for use in steam cycle applications. John's holds a B.S. degree in Chemical Engineering from North Carolina State University and an M.S. degree in Engineering Management from the University of Tennessee. His e-mail is john.r.currier@intel.com

John Harland is a Principle Environmental Engineer and co-chairs the group chartered with setting Intel's environmental roadmap. During his 23 years at Intel, John has had responsibility for environmental compliance, waste system design, and design for environment in new process development. John holds an M.S. degree from the California Institute of Technology. His e-mail is john.harland@intel.com

Steve Brown is a Certified Industrial Hygienist employed by Intel Corporation and is responsible for the safe introduction of new process chemistries and manufacturing technologies into Intel's global manufacturing facilities. Mr. Brown is the Convener of the International Standards Organization (ISO) Technical Committee 229 on Nanotechnologies which is charged with developing ISO Health, Safety and Environmental standards for the safe introduction of nanomaterials into

worldwide commerce. Mr. Brown has 21 years experience in semiconductor and aerospace industries. His e-mail is steven.w.brown@intel.com

BunnyPeople, Celeron, Celeron Inside, Centrino, Centrino logo, Core Inside, FlashFile, i960, InstantIP, Intel, Intel logo, Intel386, Intel486, Intel740, IntelDX2, IntelDX4, IntelSX2, Intel Core, Intel Inside, Intel Inside logo, Intel. Leap ahead., Intel. Leap ahead. logo, Intel NetBurst, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel StrataFlash, Intel Viiv, Intel vPro, Intel XScale, IPLink, Itanium, Itanium Inside, MCS, MMX, Oplus, OverDrive, PDCharm, Pentium, Pentium Inside, skool, Sound Mark, The Journey Inside, VTune, Xeon, and Xeon Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Intel's trademarks may be used publicly with permission only from Intel. Fair use of Intel's trademarks in advertising and promotion of Intel products requires proper acknowledgement.

*Other names and brands may be claimed as the property of others.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Bluetooth is a trademark owned by its proprietor and used by Intel Corporation under license.

Intel Corporation uses the Palm OS® Ready mark under license from Palm, Inc.

Copyright © 2007 Intel Corporation. All rights reserved.

This publication was downloaded from
<http://www.intel.com>.

Additional legal notices at:
<http://www.intel.com/sites/corporate/tradmarx.htm>.

THIS PAGE INTENTIONALLY LEFT BLANK

Assessing and Managing Asset Loss from Hazard Risks

David Namyst, Finance Enterprise Services, Intel Corporation

Index words: identification, control

ABSTRACT

Risks to physical assets from hazard events are omnipresent. Hazard risks include perils such as fire, explosions, floods, windstorms, earthquakes, typhoons, etc.

Intel has unique risks related to clean room environments: it runs an ultra-clean, pristine work environment with sensitive, specialized high-value equipment, producing high volumes of product at nano geometries with uncompromising quality.

The Risk Management Process for hazard risk evaluation is a disciplined approach that consists of identification, control, transfer, and mitigation. In this paper we describe how this process is applied with exceptional results in establishing specific studied controls to address the hazards of fire, flood, and windstorm. The result is the mitigation of the consequences of these risks within semiconductor manufacturing facilities. Combined with the Business Continuity and Emergency Response programs addressed elsewhere in this issue of the *Intel Technology Journal*, this hazard identification and mitigation process reflects one of the crucial pieces of an integrated approach to managing operational risks. Challenges and solutions are discussed.

While we define the role of risk transfer and mitigation in the overall Risk Management Process, the focus of this paper is on the identification, analysis, and control of hazard loss risks.

INTRODUCTION

Risk of loss can come from many sources. Clean room environments used in semiconductor manufacturing offer specific challenges to create best-in-class fire protection and property loss control. Intel has taken a leadership role in developing and applying the appropriate balance of passive and active control measures to reduce loss from catastrophic hazard risks in its facilities and clean rooms. Processes are established to identify, quantify, and

implement appropriate levels of property loss control or damage-limiting controls for buildings.

The hazard risk of fire within semiconductor industry clean rooms was the leading cause of large and often catastrophic loss events prior to 1999. Facilities affected by fire and smoke were often unusable for years due to the latent issues related to particulates generated as by-products of combustion that compromised the clean room environment. Intel Risk Management understood the importance of taking the lead in finding solutions to identify fire scenarios, quantify the impacts, and develop and implement control mitigation as an integral part of the corporate property insurance program cost management and overall business continuity.

Loss investigations of catastrophic fires determined the root cause and identified the various elements that lead to uncontrolled events. In nearly all of the large fires that were investigated, the combustible materials used in process tools were identified as the main contributor to small fires that developed into catastrophic fires. A process of risk identification and control was used to develop a detailed understanding of failure mechanisms, assess both passive and active control solutions, and to determine a long-term strategy for implementing non-fire propagating materials solutions within process tools.

Windstorm and flood hazards are present in many geographic locations where Intel conducts manufacturing. The data to determine flood and wind speed exposures to buildings and structures may not be available in many geographic areas. Even when flood and wind speed maps exist, they may not provide the specific details needed for site location exposure analysis. Risk Management reviews insurance industry data of windstorm losses to roofing systems and evaluates what roof and wall systems perform well from a property loss control perspective in severe hurricanes and typhoons. A process has been established to implement appropriate property loss control by performing site-specific evaluations of Intel locations, determining the appropriate controls required for new buildings, and looking at when to implement potential

improvements to existing buildings through existing Intel processes.

RISK MANAGEMENT PROCESS

The Risk Management Process has four elements: identification, control, transfer, and mitigation. Risk identification is a means of categorizing risks and perils in order to baseline the measurement of impact relative to a loss event or scenario. Control measures are engineering applications of passive and/or active means to avoid or mitigate a loss exposure. Risk transfer can be achieved through contract terms management where applicable, or through insurance contracts. Mitigation includes a diligent claims management process to minimize the cost/impact of a loss. In this paper we discuss two of the four elements: the identification and control process.

Identification

Risk of property loss can be categorized into common perils: hazards or activities that cause a loss. Losses from these perils are quantified by measuring the severity of their financial impact. Loss data can cluster the frequency of events. The data should include both events within the company and also reported losses from within the industry via public information sources. Various loss modeling tools can be utilized such as Risk Maps, Risk Impact and Likelihood Matrices, FMEA studies, etc.

One tool Intel Risk Management uses is a detailed quantification study method called an Intel Loss Scenario, or ILS, that develops very specific hypothetical event parameters and consequences in the facility. The event selected is often a fire and is based on results of fire science research and/or external loss histories. The extent of the loss within a facility is then modeled to quantify the resulting financial impact for both physical damage and business interruption. Included in the analysis is the mitigation resources identified from credible business continuity plans. The goal of this table-top exercise is to quantify and measure a specific loss caused by a perilous event and to determine a baseline for what a relative level of risk might be for other loss scenarios.

Acceptable Level of Loss

Determining an acceptable level of loss is often the most difficult task, as each stakeholder can have a different value amount or metric for loss. A threshold needs to be established to determine what if any risk control should be applied to identify events from both a frequency and severity perspective. Analysis is required to then evaluate the implementation capability and cost for control mitigation options, focused on prioritizing resources needed to achieve the desired result.

Risk Control

Based on risk identification and quantification results, control measures can be evaluated to determine the appropriate implementation to mitigate the loss exposure. Normally the initial focus is on high-severity and moderate-to-high-frequency events; however, identification may highlight simple and inexpensive control measures that do not require appreciable resources to implement. There are two protection methods for controlling risk: passive and active. Passive protection does not require a system activation (mechanical or electrical) to achieve the desired result. An example of a passive system is a firewall within a building that is designed and built to a specific requirement based on the building occupancy. A properly designed and installed firewall limits fire spread within a building without the need for a system to activate. The cost of passive systems is often incurred upfront during initial construction. Maintenance costs thereafter are usually limited to periodic evaluation of the physical condition of the system.

Active protection requires a system to be activated (normally mechanical or electrical) to achieve the desired result. These systems are therefore not as inherently reliable as passive systems as most are not inherently fail-safe. In the example of the firewall, any unprotected doors or other openings needed for building functionality require rated doors or fire shutters to operate or close properly to ensure the integrity of the containment design. A door that does not close due to an obstruction would defeat the purpose of the entire control system.

Active controls are often times included in emergency preparedness planning and business continuity plans. These programs are critical to reducing losses from all events, not just hazardous ones. They are actively initiated, managed, and require periodic review to ensure they address current business operations.

The costs of active systems are incurred in development or in initial system installation and continue over time. These on-going costs are generally higher than those for sustaining passive controls, and they include hardware, controls, monitoring, acceptance testing, and periodic testing and maintenance of the systems.

Risk Transfer

Once a hazard risk is identified, assessed, and quantified, a decision should be made on how to manage that exposure from a financial aspect: is this a risk exposure that the corporation should transfer to a third party via insurance or another financial tool (e.g., a catastrophe bond); is this an exposure that can be transferred via contract to a third party, (i.e., getting a vendor to accept

Risk of Loss or damage to Intel goods in transit); or ultimately, is this an exposure that the corporation should insure against or fund, such as earthquakes? Earthquake insurance is expensive to purchase and is limited in coverage with a percentage of loss deductible that makes the coverage unattractive.

The reality is that there are insurance market limitations and complexities that must be addressed: not every insurance carrier is interested in underwriting technology clean room environments, for instance. Intel must develop a strategy around what hazard risks should be insured. It would then need to determine what the appropriate deductibles should be, what the optimum levels of overall insurance limits should be, and what form of insurance should be purchased.

If insurance is to be purchased, the corporation's risk profile has to be marketed to the right insurance partners, and the best premiums negotiated. Another limitation is that Intel's size is such that there is no single insurer that is capable of absorbing a significant loss in our factory network: Intel must syndicate its insurance program among many different insurers. Our Property Insurance Program, for instance, comprises 20 different insurers from different countries including: Britain, Germany, Bermuda, America, and Japan.

Mitigation

An often overlooked portion of the Risk Management continuum is Risk Mitigation via aggressive Claims Management. Just as post-loss planning through a thorough Business Continuity (BC) plan is essential to getting the business operations back up and running as quickly as possible, having a well-planned strategy and process for making a recovery from a loss caused by vendor or supplier liability within the supply chain is just as critical. In most cases, you will need to recover losses from another party's insurance carrier, but in some cases, there will be no insurance money available. This strategy involves many internal players, facilities groups, business divisions, and legal, financial, and risk management groups.

The claims mitigation process is tedious and disciplined: a claim must be investigated, analyzed, documented, and negotiated to support any recovery, whether it is from an insurer or a contractual partner. The time line from the date of loss to closure often spans several quarters and could last over several years. Depending on the complexity of the claim, legal and forensic accounting specialists may be required.

Results

Semiconductor industry loss history shows fires within clean rooms cause the largest losses. Despite industry

clean-room fire losses that have affected numerous companies, Intel has not had a significant loss in over three decades. Risk Management championed hazard identification, modeling, and control processes for the fire hazard risk perils that led to the development and implementation of a best-in-class process called the Combustible Material Management Program (CMMP). Risk Management maintains results through efficient partnering with existing stakeholder processes. This program is embedded in the technology development material selection process within the clean room envelope that includes tools and support infrastructure. These successes are effectively proliferated to high-volume manufacturing (HVM) sites through "copy exactly" controls to manage these location exposures.

Intel has sites in geographic location where buildings have been exposed to significant natural hazard events such as windstorms and flooding. These include Hurricane George in 1998 that affected the facility in Las Piedras, Puerto Rico; and most recently, Typhoon Xangsane (also known as Milenyo) in September 2006 that affected Cavite in the Philippines. Implementing effective wind resistive roof and wall fastening controls based on previous loss analysis studies, and having well-developed emergency response plans for typhoon and flooding mitigated serious damage to Intel operations at these sites.

The diligent Risk Management Process approach has resulted in recoveries for various losses over the last five years of over \$11M. When benchmarked against a national indicator of various industries for Cost of Risk (COR) (premiums + expenses + losses) as compiled by the Risk and Insurance Management Society, Intel maintains one of the lowest COR levels.

FIRE EXPOSURE WITHIN CLEAN ROOMS

Fire Science Basics

When evaluating fire hazards, the elementary fire triangle principal is used to evaluate this risk. In order for fire to occur, three elements need to be present: fuel, a source of ignition, and sufficient levels of oxygen. Not quite rocket science! In common environments, removing any one of these three elements will prevent a fire. When applying the fire triangle principal to identify hazards within process tools, each element offers unique challenges.

The fabrication process often requires the use of flammable or combustible chemicals. In addition to process chemistries, the tools themselves require non-corrosive or non-reactive construction materials to allow for the high-yield fabrication of wafers. Using noncombustible chemicals or tool construction materials

can eliminate the fire risk from the fuel leg of the fire triangle.

Ignition sources from electrical sources are controlled in normal operations. Static electricity sparks are controlled through normal grounding. However, investigation of loss events and subsequent research testing indicate electrical component failures are the most prevalent ignition sources. Electrical devices used to heat acid chemicals in the process tools fail over time, as they are in areas of the tool that are subject to corrosive environments and are in concealed spaces. Removing electrical ignition sources in areas where combustible materials exist in oxygen atmospheres can eliminate fire risk from the ignition leg of the triangle.

The clean-room environment requires high airflow and filtration over process tools to ensure clean environments for processing wafers, and to exhaust chemical vapors resulting from the processing. Common gaseous fire suppression systems that reduce oxygen concentrations below levels to support combustion include carbon dioxide, nitrogen, or other inert gas mixtures. Although these systems could be effective in eliminating the fire risk, reducing oxygen levels may be impractical in airflow environments or in clean rooms that are occupied by people. Therefore, removing this leg of the fire triangle may not be a viable option.

Passive and Active Controls

Control solutions for the fire risk involving process tools were developed by further analysis of each fundamental fire triangle element. A process to examine potential passive and active controls for each of these elements (fuel, ignition source, and oxygen) was used to meet the objective of reducing the loss exposure of fire to an acceptable level.

From the risk identification process, fuel sources were determined to include chemicals used in wafer fabrication processing, tool materials of construction, and peripheral materials within the facility systems supporting fabrication processing. Where flammable or combustible chemicals are used, tools are constructed with noncombustible materials to provide passive protection. Active controls of the chemical delivery systems incorporate fail-safe shut-off controls to prevent continued fuel or chemical dispensing.

Process tool construction materials were selected for compatibility for wafer processing within acid environments. Research was conducted in conjunction with the plastics and insurance industries to determine if acid resistive materials could be developed that would meet process compatible requirements and also meet non-fire-propagating material requirements.

The prevalent ignition sources identified from the risk identification process were from electrical component failure within the tool, including the heating elements and controls. Passive control solutions for electrical failure are limited. Active controls would remove the energy source upon incipient detection of fire. Other solutions included removing the heating elements from the tool itself by heating the liquid acids solutions remotely and circulating heated liquids to the tool.

Implementing Solutions

For the fire event within the clean room, the acceptable level of loss was defined to be a fire within a process tool that remains contained to the tool and does not propagate to an adjacent tool or equipment. The resulting physical damage and factory business impact cost are compared to a predetermined acceptable level of loss amount.

Intel Risk Management led industry efforts in developing insurance industry and fire protection equipment vendors' partnerships to conduct fire research and testing of failure modes and fire growth within process tools. Fire detection and suppression system solutions were developed and tested to work within the corrosive environments within these tools. Validation, testing, and approval of local application fire suppression system add-ons required coordination with many Intel groups within technology development and manufacturing. An implementation plan was developed to install fire detection and suppression solutions on existing tool bases without affecting wafer processing production and yields. New process tool orders had to have pre-installed fire detection and suppression systems prior to delivery when needed.

Material science engineers from the plastics industry, tool equipment manufacturers, and the insurance industry partnered with semiconductor fabrication companies to test and develop potential non-fire-propagating materials. The criteria, also known as the 4910 Protocol defines a set of testing requirements that include a Fire Protection Index (FPI), Smoke Damage Index (SDI), and Corrosion Damage Index (CDI). The materials meeting the fire propagation and micro-contamination requirements were tested for process compatibility of the acceptable materials by technology development groups. Technology development process controls determined the successful materials were acceptable for use. Intel Risk Management drove the implementation phase beginning with the intercept of 300mm process equipment generations through partnerships with Intel stakeholders. Today SEMI S14 (Fire Risk Protection) has been developed and is the accepted standard to assess tool fire risk and controls. Intel's EHS group manages this one element of the overall effort to address occupant safety, health, and environmental risks addressed elsewhere in this issue of

the *Intel Technology Journal*. A limitation metric of 1 pound per square foot of tool footprint was integrated in tool purchasing specifications. The process technology transfer process for manufacturing proliferate the successful result of limited catastrophic fire exposure within the Intel FAB network.

As part of the review process, a program was implemented to eliminate several fire suppression systems originally required on new tools as part of the program, based on updated risk assessments. The program was extended to remove some of the legacy local fire suppression systems on the existing process equipment tool base to capture cost savings.

NATURAL HAZARDS

Building Design for Windstorms

Tropical windstorms create severe challenges to Intel buildings that are within geographic areas prone to this natural hazard. These regional events cause devastation in a widespread area, and Intel sites must rely on resources available to reduce catastrophic loss. A large property insurance carrier, FM Global, reports that over the past 25 years, wind-related damage accounted for over 11% of their property losses, and 70% of those losses were from severe tropical storms such as hurricanes and typhoons [1]. The loss history indicates that in most cases the main structure of the building does not sustain damage; however, damage occurs when the building components such as roofs, walls, and windows fail and the interior is subjected to the elements. Property damage losses can be vastly mitigated in severe storms if the integrity of building components and interior occupancy do not become compromised by low-frequency but high-severity wind and wind-driven rain.

Windstorm Basics

The Risk Identification process for wind exposure begins with understanding what potential site-specific conditions may occur within the expected useable lifetime of the building. Historical wind maps are based on statistical analysis to determine the probability of maximum wind speeds to occur in a given year. The wind speeds are measured and averaged to determine various time durations of sustained winds and peak gusts. An average wind speed peak in a given year and the peak wind within a multi-year frequency period could be an event. These intensity factors establish the basis of building system design requirements for wind.

Wind and wind forces become dynamic as they meet obstructions in their paths. This often occurs around buildings in urban areas. As wind changes direction and moves around buildings, significant suction and uplift

forces are created, particularly on the corners and perimeters of a building, which stresses the building roof systems.

Controls for Wind Exposure

Passive control measures would include avoidance of these exposures by simply not building in high-exposure wind areas. Although Risk Management is involved in the site selection activities of Intel and provides natural hazard exposure analysis as part of this activity, obviously other economic business factors drive the business decision to build in a given location. Intel has moved manufacturing operations from high hurricane wind exposure locations in its history: it sold its Puerto Rico Test and Board facility in the 1990s and its Barbados Assembly facility in the 1980s. Wind loss exposures are still present at the Cavite site in the Philippines and in Pudong and Shanghai, China Semiconductor Manufacturing facilities.

The options for active controls are rather limited for windstorms. However, the site Emergency Preparedness Programs that address site exposures and conditions are a critical component of loss control and mitigation during a severe windstorm. Plans need to be specific but realistic: the resources, such as manpower, need to be available in the case of an emergency. Installing storm shutters on windows, doors, and other exterior openings when windstorms are predicted is an example of a scenario-based plan element. Other controls embedded in emergency preparedness include Business Continuity planning for operations of the site and the supply chain before and after the event to reduce the business interruption consequence of windstorms.

Implementing Solutions

Property loss control solutions for wind exposures to existing building and roof systems are specific to the building and the immediate general site area. Factors also include the age and life expectancy of the building, the number of people in the buildings, the ability to make improvements to the existing building components and structure, and the cost of making any improvements.

Risk Management defines the appropriate passive wind controls to be used for roofing and wall systems of buildings through the existing Master Design Specification (MDS) system process. The process to implement passive controls for new construction of buildings is embedded in Intel's established design review process through all phases of a project. Various stages of review allow for the appropriate timing to incorporate wind mitigation design features. Minimizing the number of windows in manufacturing buildings early in a project is an obvious example. More challenging is understanding

the building system design and capabilities to incorporate property loss control.

Mechanical fastening of the roof coverings and membranes to the structural elements along the roof perimeter and corners is the preferred method to mitigate wind uplift forces. As part of the overall property loss control audit process, existing sites are periodically evaluated, and feedback is coordinated with local project teams on potential roof upgrades or replacement. Risk Management is embedded in the review and approval process of these projects to ensure cost-effective property loss control of the building.

Flood

Flood exposures can create challenges to Intel buildings that are prone to this natural hazard. Floods can cause devastation locally and in the surrounding areas. The property insurer, FM Global, reports its loss history indicates 20% of property flood losses are in buildings outside of designated flood maps [2]. Property damage losses can be vastly mitigated in severe storms if the integrity of building components and interior occupancy do not become compromised by wind and rain. Intel buildings will need to have their own resources available to mitigate catastrophic damage.

Flood Maps and Data

The Risk Identification process for flood exposures begins with understanding what potential site-specific damage may occur. Historical flood maps are based on statistical analysis to determine the maximum water level over a specified interval of time and averaged for a given year. As with windstorm exposures, many geographic areas do not have good reliable data available for analysis. Risk Management conducts site-specific analysis to determine site requirements for finished floor elevations and also the locations of utilities and facility equipment that are vital to the continuance of manufacturing operations at the site.

Controls for Flood Exposures

As with locations subject to windstorms, avoidance of sites subject to flooding is not always possible; i.e., passive controls. Active controls, although limited, are best implemented through site emergency preparedness programs that address the various exposures and conditions for a severe flood. Plans need to be specific in proactively addressing mitigation of the potential damage, as well as realistic in the availability of resources such as manpower in a regional emergency. Using sandbags, temporarily relocating equipment susceptible to water damage, and the use of pumping systems to displace water using reliable self-sufficient electrical power generators are examples of a scenario-based plan. Other controls

embedded in emergency preparedness plans include BC planning for operations at the site and the supply chain before and after the event.

Implementing Solutions

Risk Management defines the appropriate finished floor elevations for new construction through the existing MDS system process. The process to implement passive controls for new construction of buildings is embedded in Intel's established design review process through all phases of a project similar to the windstorm exposure. Various stages of review allow for the appropriate timing to incorporate wind mitigation design features. Site-specific reviews are conducted to determine specific requirements.

MEASURING SUCCESS

Intel's 300mm fabrication clean room environments have no loss history of fire losses. The measurement of loss expectancies within new process tools and semiconductor manufacturing facilities continues to validate loss expectancies that remain below predetermined acceptable levels.

Detailed studies for windstorm exposures were conducted in 2002 on Intel buildings in Cavite and Pudong. Deficiencies noted in the roof systems were evaluated for severity, potential impact to business operations in each building, and the cost and ability to remediate deficiencies. A prioritized remediation plan was developed in partnership with local site services to correct deficiencies. Typhoon Xangsane traveled near Cavite in the Philippines in September 2006 and in buildings where wind-resistive roof-fastening controls were in place, the roof systems performed well, and Intel did not incur significant property damage. These physical building system improvements as well as the well-developed emergency response plans for typhoons and flooding mitigated serious damage to manufacturing operations.

Risk transfer programs are a beneficiary of the successful results made in property loss control engineering. Reducing the catastrophic risk of loss through engineering control measures and Intel's excellent property loss history from hazard events allows Intel to take out insurance against hazards with optimal coverage and premiums.

CHALLENGES

Codes are the minimum requirements established to safeguard the lives of building occupants: they generally do not address property conservation. If companies, such as Intel, want to design above the minimum criteria to help mitigate property losses, they have to consider

whether the costs are worth the additional investment. Companies need to understand the total cost delta of implementing improvements above minimum code relative to the level of loss they are prepared to accept.

The programs in place for managing the fire risk in clean rooms require continuous monitoring. Process technology development and the evolution of chemical processes used in manufacturing create challenges for our current acceptable materials of construction. Issues such as Electro Static Discharge (ESD) and off-gassing of materials expose wafer processing and can limit available materials for manufacturing as the transistor geometries continue to shrink. Implementing non-fire propagating material requirements within other manufacturing technology risk issues requires continued diligence. Potential processes for fabricating 450mm wafers will require all tools and construction materials to change. Embedding construction material management controls within existing processes will maintain passive control solutions of this fire hazard risk.

Determining and agreeing on the applicable wind speed design criteria relative to the design of building structures with design teams is not always a simple task. As previously mentioned, detailed wind speed data may not be available in various geographies. In these cases, engineering judgment based on available data collected at the site is required to determine the specific performance levels to meet the objective of adequate passive protection.

CONCLUSION

As the Intel approach to doing business continues to change, the effect of risk of loss from hazard events changes as well. The Risk Management Process for identifying and quantifying hazard events is ongoing and remains an integral part of influencing the appropriate loss control measures to reduce the consequences of loss. The effectiveness of these programs can be measured in the efficient and cost-effective program management embedded in existing processes for defining and implementing risk mitigation controls within Intel's manufacturing environment.

ACKNOWLEDGMENTS

The author thanks Diane Labrador, Mark Slight, and Ken Kwidzinski of Intel Risk Management, Scott Swanson of Intel Environmental Health and Safety, and Dave Brown of FM Global for their support and contributions to this paper.

REFERENCES

- [1] FM Global, "Understanding the Hazard, Wind From Tropical Storms," *P0046*, February 2001.
- [2] FM Global, "Understanding the Hazard, Potential for Flooding," *P0303*, February 2003.

AUTHOR'S BIOGRAPHY

David Namyst has been in the Intel Corporate Risk Management department at Intel since 1990 and has been involved with fire protection engineering and property loss control since 1980. He is responsible for placing and maintaining Intel's property insurance program, managing risk management property conservation engineering programs, and overseeing corporate fire protection engineering activities. Dave is a code committee member of NFPA 55 (Industrial and Medical Compressed Gases). He is also involved in various insurance industry groups, semiconductor industry and related research and development activities, and professional development groups. He has a B.S. degree in Chemical Engineering from Arizona State University. His e-mail is david.d.namyst at intel.com.

BunnyPeople, Celeron, Celeron Inside, Centrino, Centrino logo, Core Inside, FlashFile, i960, InstantIP, Intel, Intel logo, Intel386, Intel486, Intel740, IntelDX2, IntelDX4, IntelSX2, Intel Core, Intel Inside, Intel Inside logo, Intel. Leap ahead., Intel. Leap ahead. logo, Intel NetBurst, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel StrataFlash, Intel Viiv, Intel vPro, Intel XScale, IPLink, Itanium, Itanium Inside, MCS, MMX, Oplus, OverDrive, PDCharm, Pentium, Pentium Inside, skool, Sound Mark, The Journey Inside, VTune, Xeon, and Xeon Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Intel's trademarks may be used publicly with permission only from Intel. Fair use of Intel's trademarks in advertising and promotion of Intel products requires proper acknowledgement.

*Other names and brands may be claimed as the property of others.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Bluetooth is a trademark owned by its proprietor and used by Intel Corporation under license.

Intel Corporation uses the Palm OS® Ready mark under license from Palm, Inc.

Copyright © 2007 Intel Corporation. All rights reserved.

This publication was downloaded from
<http://www.intel.com>.

Additional legal notices at:
<http://www.intel.com/sites/corporate/tradmarx.htm>.

Maturation of Business Continuity Practice in the Intel Supply Chain

Ann Hepenstal, Technology Manufacturing Group, Intel Corporation
Boon Campbell, Technology Manufacturing Group, Intel Corporation

Index words: BC, supply chain, risk management, crisis management, hurricane, disaster, fire

ABSTRACT

Natural disasters and other catastrophic events could interrupt Intel's global and interconnected supply chain at any time, any where. In order to reliably produce quality products, Intel needs to be able to quickly react to a crisis, ensure continuity of our business, and restore the supply chain. Business Continuity (BC) planning in Intel's worldwide Materials organization has matured over time, moving from crisis management and response, to a more mature BC approach. The BC methodology, infrastructure, and tools used within the Materials organization have improved Intel's ability to quickly recover from a supply chain outage and restore supply to manufacturing and other operations. The BC approach enables the Materials organization to determine the appropriate level of effort/investment to make in BC and focus on the business needs, risks, and available resources. Real-life events have demonstrated Intel's BC and crisis response capability and its improvement over time.

INTRODUCTION

Business Continuity (BC) planning can be an overwhelming task. It can be an endless challenge because of the wide range of events that can cause business interruptions such as natural disasters, transportation interruptions, equipment malfunctions, pandemic disease, and acts of terrorism.

Intel has always planned for BC and crisis response in order to manage its business. As manufacturing and supply chain systems became more streamlined, with tighter and tighter timelines, BC became more critical to successful manufacturing, and to Intel's bottom line.

In this paper, we discuss how Intel's approach to BC planning in the supply chain has matured within the Materials organization. Intel needs to be ready to quickly restore the supply line and resume normal operations; yet, preparing a plan for every potential scenario is not

possible. We must be *prepared enough*: we must invest enough resources so that the organization can quickly respond to a supply chain outage, avoid over-investing in the planning efforts, and appropriately focus our resources based on the risks.

We describe the phases of supply chain BC planning and the evolution and maturation of our BC practice over time. We describe how the continuously improving BC practice in the Materials organization enabled Intel to quickly react to recent supply chain outages and improve our response.

PROBLEM

Intel's manufacturing sites are located in many countries around the globe. These sites rely heavily on a dependable supply line of raw materials and parts and services that make up Intel's supply chain. In order for Intel to provide quality products to all its customers, this supply chain must be robust, flexible, and resistant to interruptions.

Intel's worldwide supply chain is complex and multi-tiered with dependencies for material and services across all levels of manufacturing processes and other operations. This supply chain encompasses hundreds of suppliers, located at multiple locations throughout the globe, supplying thousands of parts that support a variety of Intel CPU, server, and chipset product variations. In addition, Intel's products are constantly evolving and changing as the number of transistors on a chip doubles every two years (Moore's Law). These facts drive the need for a multitude of supply chain materials that includes both commonly sold materials and unique materials that contain intellectual property or have trade secret restrictions that limit the available supply. The Materials organization sources and buys the goods and services needed for Intel's manufacturing and operations.

Significant interruptions to the supply line can have a direct impact on Intel's revenue and end customers. As a result, Intel needs to understand and mitigate the key supply chain risks. These risks include, but are not limited to, natural disasters (earthquakes, cyclones, etc.), labor

outages, transportation interruptions, terrorism, governmental restrictions/interruptions, fire, and global raw material shortages. The severity and frequency of these risks vary from one world geography to the next, further complicating the overall picture of supply chain risk. Therefore, the core problem for Intel is to develop and implement the right BC approach to mitigate these risks in order to meet the business needs.

MATURATION OF BC PRACTICE

Intel's approach to managing the risk of business interruption to the supply chain has matured over time

(see Figure 1). Intel's Materials organization has always applied knowledge of the supply line, the raw materials, the business, etc., to restore supply as quickly as possible. However, now that our global manufacturing and supply chain are more streamlined and interconnected, robust BC planning has become an imperative for successful manufacturing.

As the BC practice has matured over time, we have put in place tools and methodologies that help Intel to more effectively use resources to prepare for and respond to crises.

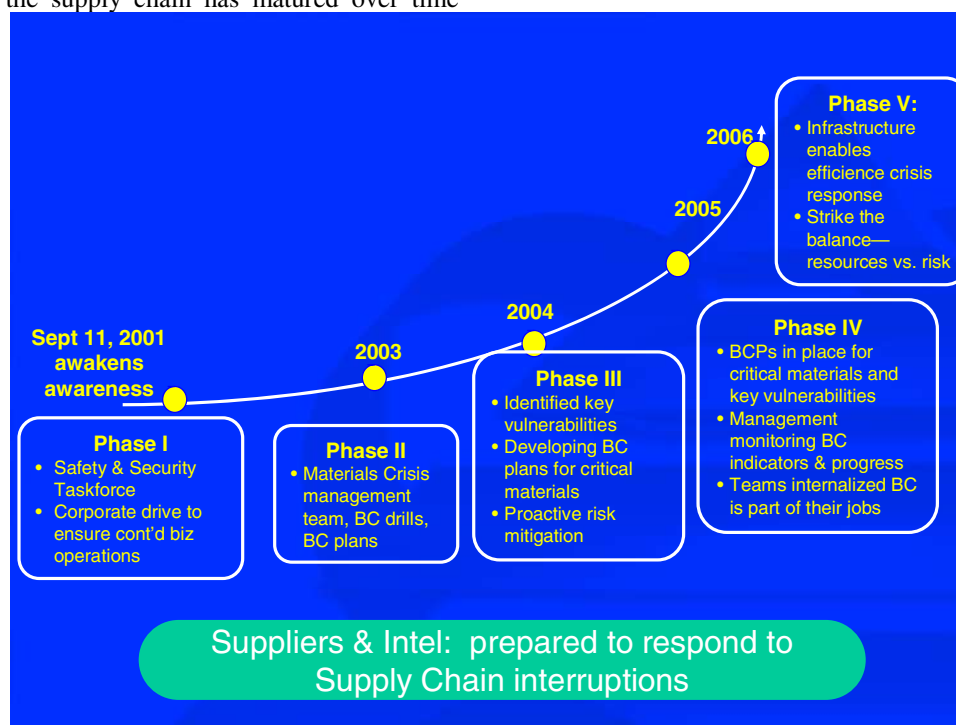


Figure 1: Materials Business Continuity program

Phase I: “Corporate Said”

The events of September 11th awakened Intel's awareness of BC and the need for proactive planning to prepare for crises. Intel CEOs took the lessons of that day to heart. As Craig Barrett and Paul Otellini noted in a message to the Intel Board of Directors in April 2002:

“The events of 9/11 were a wake-up call to expect the unexpected. Employees, customers, stockholders, and the investment community are all raising the bar on what is expected of corporations. Every Intel organization must make BC a core business practice.”

Intel launched a corporate Safety and Security taskforce, taking a multidisciplinary approach to identifying threats and Intel's exposures, and to preparing our employees and corporation to respond. The taskforce established a BC program management function, coordinating BC planning across the corporation. The corporate BC program provided basic tools and methodological guidance to help ramp up the business units on their crisis management and BC plans (see Figure 2). With these tools, and under the direction of the corporate BC program, Materials and other business units across the corporation formalized BC programs and put organizational plans in place under this corporate umbrella.

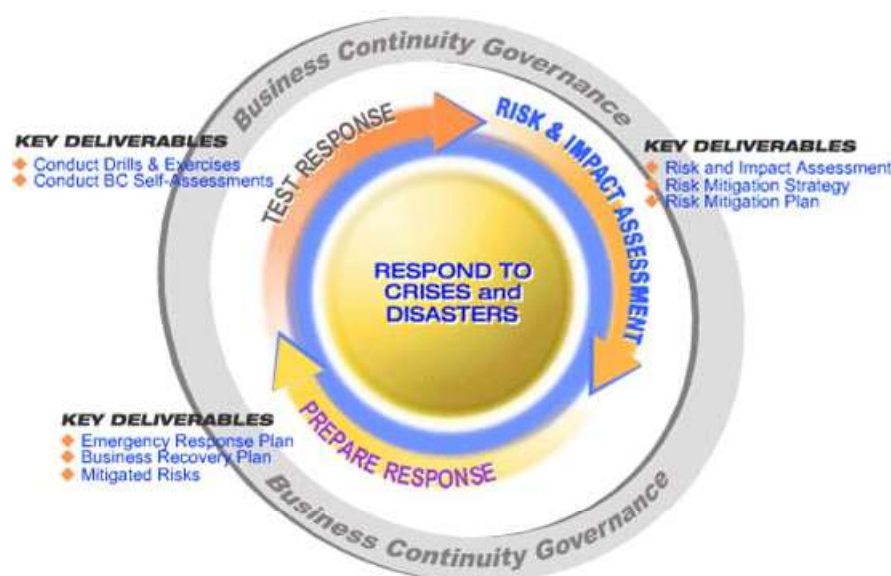


Figure 2: Business continuity cycle

Phase II: “Materials Internalizes”

The Intel Materials organization named a BC manager to drive the organizational BC planning and engage with the corporate BC program. Materials established the BC infrastructure within the organization and gained management support for the importance of BC planning to the success of Intel’s business.

Materials crisis management team: This team formalized how the organization would manage crises. We named representatives from the various departments within Materials as well as from key support organizations (e.g., Finance, Legal, and HR). We set up emergency contact procedures to assemble the team in the event of a crisis, in order for the organization to quickly respond to the situation and recover the business. We established a crisis escalation flow, providing guidance on when this team needed to be activated, and the steps to follow in assessing the state of the crisis.

Scenario-based BC plans: Each organization identified the three to five key functions that it performs. Then for each key function, the organization assessed the risk to that function under several scenarios, such as loss of a building, loss of access to data/systems/Internet, etc.

Plan testing: Materials began running BC drills to test the ability to activate the crisis management team, and to test BC plans. We drove improvements to the plans based on gaps identified, or additional needs uncovered.

BC embedding: Materials incorporated BC considerations into several of the core business processes such as supplier selection, strategic sourcing, our annual supplier performance award process, etc. This helps to ensure that BC is built into Intel’s engagement with a supplier from the very beginning.

Phase III: “Move to Proactive”

In the next phase of development, the Materials organization moved beyond crisis management and response planning, and into proactive risk mitigation. Intel’s worldwide supply chain is highly complex. It includes both highly specialized/unique parts as well as commonly sold parts, and relies not only on our suppliers, but also on their suppliers. As a result, we face a long list of business interruption risks. The task of planning responses or mitigating these risks could easily overwhelm the organization if we let it.

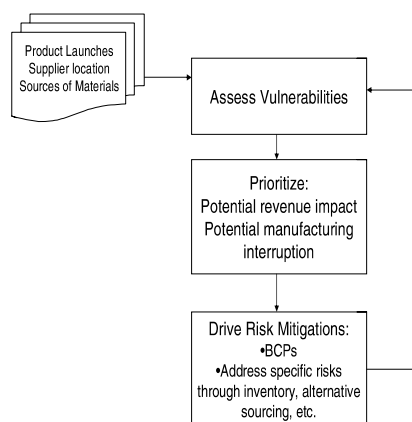


Figure 3: Proactive risk mitigation

The Materials organization assessed the BC risks and identified the key vulnerabilities (see Figure 3). We discussed the potential impacts of these vulnerabilities, and we decided to prioritize our BC planning work based on the potential impact on revenue posed by vulnerabilities. Once we gained management ratification on the key vulnerabilities, the prioritization criteria, and the approach, we began the proactive risk mitigation work.

Determining risk mitigation targets. The procurement teams assessed the materials they manage, reviewed each against the key vulnerability list and the prioritization criteria, and determined which materials would require risk mitigation.

Setting the infrastructure. The Materials BC manager installed a management review and progress tracking infrastructure. This included indicators tracking completion rate of the Business Continuity Plans (BCPs) and some basic formats/coaching on writing BC plans, so the teams didn't have to start from nothing.

Once the procurement teams identified these most critical materials for which they needed BC plans, they engaged the supplier in BC discussions. They expected the supplier to put BC plans in place to enable the firm to quickly recover supply to Intel. They expected suppliers to have a crisis communication plan, enabling them to reach key employees in a crisis and to notify their Intel contact. With their understanding of the business need, the risks, and the material, the procurement team then set about risk

mitigation. They identified ways to mitigate the risk of losing a supply of a critical material, e.g., by stockpiling inventory, and switching to alternative sources of supply and alternative locations.

Phase IV: "Middle Management 'Gets It'"

Through indicators, we monitored completion of the prioritized BCPs and the risk mitigation activities. Management supported the BC activities, but the organization as a whole viewed BC as a burden that got in the way of their "real work."

Then we experienced a crisis: a fire broke out at a major supplier impacting several Intel product lines by creating immediate supply constraints. A crisis management taskforce was quickly formed to determine the damage and mitigate any risk to Intel's customers. The taskforce members comprised management, manufacturing, planning, commercial, engineering, operations, and development department representatives. Sub teams were also formed with core focus areas of supply chain, technical, supplier management, and development. The taskforce gathered data, assessed technical risks, and quickly defined an offload strategy. The taskforce's plan defined the other supply options, material compatibility, and the fungibility of specific qualified substitute parts. Because of the BC communication links and processes put in place, the team was able to respond and quickly define and implement their plan. They mitigated the potential loss of production output by 97%, avoiding a potential revenue impact of millions of dollars.

The fire highlighted an area of vulnerability already known to Intel and validated the need to further develop the BC program. After-event-analyses were conducted to identify key lessons from the event, find gaps, and further enhance existing BC systems. Working through this crisis helped drive the maturation shift into Phase IV.

Senior management now wanted to make sure the Materials organization was ready for a crisis. We instituted BC reviews for our key materials. The teams took senior management through their risk assessments, their plans to restore supply after a crisis, and the preparedness of the suppliers to respond to a crisis (see Figure 4). At the first of these reviews, senior management asked the teams a lot of questions and reinforced the expectations that they manage the supply line—and that responding to a crisis was not *extra*. Management made it clear that BC was part of their jobs and having BC plans was part of successful supply line management.

With senior management's strong support, the middle management and their teams finally realized: "BC is part of my real job."

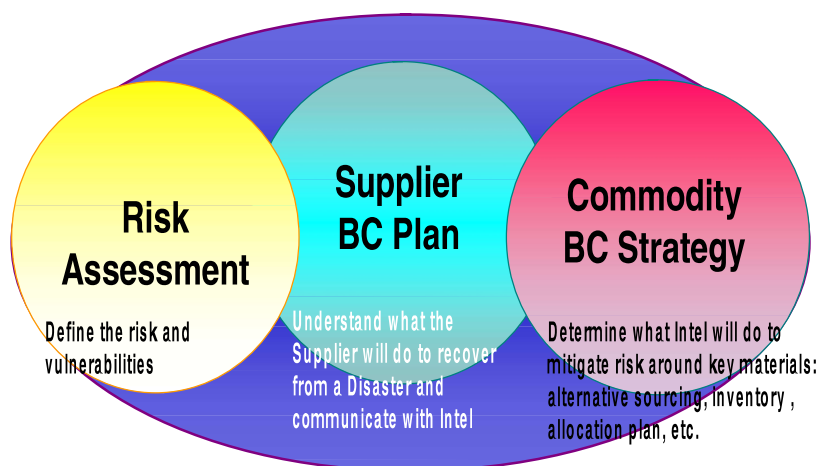


Figure 4: Business continuity

Phase V: “Striking the Balance”

As our BC program has matured, we have put tools and methodologies in place (below) that speed our response and make it easier for the teams to complete their BC planning.

An “auto dialer” tool to contact members of the Crisis Management Team.

A BCP spec, defining the basic steps/approach to BC planning that the Materials teams should apply.

Reference information to speed evaluation of and response to a crisis.

BC information for our suppliers at <http://supplier.intel.com/static/bc/>.

Materials now has a robust BC infrastructure in place. We assess risks, prioritize them, drive risk mitigation where appropriate, etc. Our procurement teams understand the role of BC in their jobs, and they consider it in their work with suppliers. We conduct drills and drive improvements on the lessons learned from drills as well as real-life events. In BC, we must continuously assess, evaluate, and improve.

SUCCESS STORIES

Recent experiences with cyclones further illustrate BC successes and maturation. In August, 2005, the category IV Hurricane Katrina hit the United States. In September, 2006, the Level 4 Typhoon Milengo (Xangsane) hit the Philippines. Both were severe storms, causing significant damage in impacted regions. However, for the purposes of

this paper, they serve to showcase the continued maturation of our Materials BC practice (see Table 1).

Table 1: The continued maturation of our Materials BC practice

	Katrina	Milengo
Year	August 2006	September 2006
Advance notice of storm.	Yes	Yes
Pre-event activation by Materials.	None	Materials site contact notified Materials management and key partners. Began contingency plans. Linked into site emergency plans.
“Trigger” for BC assessment.	Notice that a key supplier’s manufacturing facility was underwater.	Notice that the storm was approaching.
Impact to Intel facilities.	No facility in region.	Damage to Intel factory and buildings. No injuries to personnel.
Activation and response.	Materials Crisis Management Team responded. Chartered taskforce to work issue resolution.	Site emergency management team responded. Local Materials teams worked issue resolution.
Supply line issues.	Restore supply sourced from the underwater plant.	None

Our experience with Katrina highlighted a number of improvements to our BC infrastructure and practice. Between Katrina and Milengo, we put several capabilities in place in Materials:

The ability to identify critical suppliers with manufacturing facilities in the path of a crisis.

Proactive response to major storms and other events with advance notice, evaluating the potential impact and determining what mitigation strategies were appropriate.

Improved crisis communications, enabling us to better inform Materials management and key stakeholders on status of the event, issues, gaps, help needed, and most effectively, focus our response.

Before Milengo hit the Philippines, the local Materials manager had already begun mitigating activities at the site and was part of the site preparations. The Materials BC program manager identified critical suppliers who may be impacted by the storm and notified the teams so they could assess the situation. Once the storm hit, the local Materials manager provided status updates to management and key stakeholders, so they could best focus resources and attention where they were needed. No Materials Crisis Management Team activation was needed, as the response was successfully driven by the local team. This event demonstrated the increased strength and capability of our BC infrastructure to effectively respond to crises.

SUMMARY

Over the past five years, the BC program in the Intel Materials organization has progressed through four phases of maturation. We have a BC infrastructure, tools, and methodology to enable the teams to quickly implement BC plans and flex their BC planning to the appropriate level.

The program now faces the challenge of the next phase: reducing our overall BC investment but getting the Materials organization “prepared enough” within an efficiency-oriented and tightly constrained environment. In Phase III, we addressed our key vulnerabilities and the most critical risks. We then pushed beyond that, asking teams to do more (address the next layer of risk, do BC planning with all suppliers, consider additional scenarios, etc.). In striking the balance, we strive to reach “prepared enough.” We need to understand our vulnerabilities, to drive risk mitigation in critical areas, but also, we need to decide which risks to accept as part of doing business. Since we don’t have the resources to mitigate all risks, we must drive a decision-making process to select the risks we mitigate and the risks we are prepared to take.

The BC infrastructure, methodologies, and tools enable us to more easily drive BC planning and risk mitigation. Our experiences with BCP over the last couple of years helps guide our understanding of where we can accept the risk vs. mitigate it. We are confident that Materials will continue to successfully manage BC risk as we strike the

balance between prepared enough and being over invested.

The maturation of the BC practice in Materials has enabled our organization to be able to quickly restore our supply chain—and to do so efficiently.

CONCLUSION

Maturation of BC planning in the supply chain requires the movement from a corporate-dictated approach to an internalized or embedded BC practice encompassing BC tools, methodologies, and infrastructure. Successful BC planning enables Intel to ensure supply to manufacturing operations and reliably produce quality product.

ACKNOWLEDGMENTS

The authors acknowledge the following people for their contributions to the Materials BC program and to this paper:

Joel Kaspar, for her work as the first Materials BC Manager and documentation of the early phase of the Materials BC Program.

Barry Scott, for his work defining a key infrastructure and BC indicators process.

Cathy Sandstrom and Neeraj Mathur, for their roles in helping to define the chart shown in Figure 4 and to write the BC spec.

Intel BC Program Office, for Figure 2.

AUTHORS' BIOGRAPHIES

Ann Hepenstal is the Risk & Controls Manager for Intel's Materials organization, in the Technology Manufacturing Group (TMG). Her work experience spans risk management, project management and finance positions at Intel and Procter & Gamble. Ann holds an M.S. degree in Engineering-Economic Systems from Stanford University, and a B.S. degree in Systems Engineering from Case Western Reserve University. Her e-mail is Ann.e.Hepenstal at intel.com.

Boon Campbell is a Risk & Controls Manager with the Materials organization in TMG. His work experience spans high-volume yield engineering, materials engineering, supply chain management, and project management positions at Intel and Fairchild Data. Boon holds an M.B.A. degree from Arizona State University, a B.S. degree in Business from the University of Phoenix, and an Electronics Engineering Technology degree from ITT. His e-mail is boon.campbell at intel.com.

BunnyPeople, Celeron, Celeron Inside, Centrino, Centrino logo, Core Inside, FlashFile, i960, InstantIP, Intel, Intel logo, Intel386, Intel486, Intel740, IntelDX2, IntelDX4, IntelSX2, Intel Core, Intel Inside, Intel Inside logo, Intel. Leap ahead., Intel. Leap ahead. logo, Intel NetBurst, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel StrataFlash, Intel Viiv, Intel vPro, Intel XScale, IPLink, Itanium, Itanium Inside, MCS, MMX, Oplus, OverDrive, PDCharm, Pentium, Pentium Inside, skool, Sound Mark, The Journey Inside, VTune, Xeon, and Xeon Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Intel's trademarks may be used publicly with permission only from Intel. Fair use of Intel's trademarks in advertising and promotion of Intel products requires proper acknowledgement.

*Other names and brands may be claimed as the property of others.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Bluetooth is a trademark owned by its proprietor and used by Intel Corporation under license.

Intel Corporation uses the Palm OS® Ready mark under license from Palm, Inc.

Copyright © 2007 Intel Corporation. All rights reserved.

This publication was downloaded from
<http://www.intel.com>.

Additional legal notices at:
<http://www.intel.com/sites/corporate/tradmarx.htm>.

THIS PAGE INTENTIONALLY LEFT BLANK

For further information visit:

developer.intel.com/technology/itj/index.htm