depends on the industry and the economic outlook for RI Furniture's products, current and future competition, sustainable competitive advantage, projected changes in demand, and this borrower's capacity to grow in light of its past financial and operating performance. Risk factors that the firm's bankers will examine carefully include their borrower's financial condition; quality, magnitude, and volatility of cash flows; financial and operating leverage; and management's capacity to sustain operations on a profitable basis. *These primary attributes cannot be ignored when bankers determine distributions associated with assumption variables.*

Simulation and optimization embedded into powerful valuation models provides an intuitive advantage; it is a decidedly efficient and precise way to get deals analyzed, done, and sold.

CASE STUDY: REAL OPTIONS AND KVA IN MILITARY STRATEGY AT THE UNITED STATES NAVY

This case was written by Lieutenant Commander Cesar Rios in collaboration with Dr. Tom Housel and Dr. Johnathan Mun. Lieutenant Commander Rios is an intelligence officer for the U.S. Navy assigned to the Third Expeditionary Strike Group in San Diego, California. Dr. Tom Housel is a professor of Information Sciences at the Naval Postgraduate School in Monterey, California. Please contact Dr. Housel with any questions about the case at tjhousel@nps.edu.

Millions of dollars are spent by the United States military for information technology (IT) investments on Quick Reaction Capability Information Warfare (IW) and intelligence collection systems. To evaluate and select projects yielding maximum benefits to the government, valuation tools are critical to properly define, capture, and measure the total value of those investments. This case study applies Knowledge Value-Added (KVA) and Real Options valuation techniques to the Naval Cryptologic Carry-On Program (CCOP) systems used in the intelligence collection process, with particular focus on human capital and IT processes. The objective is to develop a model and methodology to assist in the budgeting process for IW systems. The methodology had to be capable of producing measurable objectives so existing and future CCOP systems could be evaluated.

The Challenge

The Chief of Naval Operations directed its CCOP Office to focus on three goals for fiscal year 2005: efficiencies, metrics, and return on investment.

Given this mandate, CCOP Program Manager Lieutenant Commander (LCDR) Brian Prevo had the difficult choice of how much funding to allocate among the 12 IW CCOP systems currently in his portfolio. Should he merely allocate an equal amount of continuous funding? Should he ask which ones needed the most funding to continue or upgrade? Should he ask the users which ones they preferred? To make appropriate budget decisions, LCDR Prevo had to analyze the operating performance of each CCOP program by developing metrics, measuring efficiencies, and calculating the return on investment. Moreover, he had to identify which investment options supported the United States Navy's Global Intelligence, Surveillance, and Reconnaissance (ISR) mission. LCDR Prevo teamed with researchers at the Naval Postgraduate School (NPS). He enlisted Professor Thomas Housel and Professor Johnathan Mun at NPS's Graduate School of Operations and Information Sciences to identify valuation techniques to help manage his CCOP portfolio. Prevo also sought the aid of NPS student LCDR Cesar Rios, a Naval Cryptologist and Information Warfare Officer. Rios had operated CCOP systems and other IW systems while conducting ISR missions from various Navy platforms, including ships and aircraft. As the team leader and subject matter expert, LCDR Rios worked with Dr. Housel and Dr. Mun to conduct the analysis required to make the optimal portfolio management decision in his CCOP strategies.

Background

Intelligence is a critical component of U.S. security strategy. It is the first line of defense against threats poised by hostile states and terrorists, according to the National Security Strategy (NSS) of the United States.[2] After the tragic events of September 11, a new world emerged where intelligence techniques from the Cold War era were inadequate to meet the new and complex security threats to the United States. Several initiatives were launched to transform the country's intelligence capabilities to keep pace with emerging threats, including:

- Establishing a new framework for intelligence warning providing seamless and integrated warning across the spectrum of threats facing the nation and its allies.
- Developing new methods for collecting information to sustain intelligence advantage.
- Investing in future capabilities while working to protect them through a more vigorous effort to prevent the compromise of intelligence capabilities.
- Collecting intelligence against the terrorist danger across the government with all-source analysis.[3]

Expenditures on U.S. intelligence activities are estimated at $40 billion annually and a significant amount of that total is spent on ISR activities. The ISR are the systems that gather, process, and disseminate intelligence. The ISR systems cover a multitude of systems and programs for acquiring and processing information needed by national security decision makers and military commanders. The ISR systems range in size from small, handheld cameras to billion dollar satellites. Some ISR programs collect basic information for a wide range of analytical products, whereas others are designed to acquire data for specific weapons systems. Some are "national" systems, collecting information for government agencies, whereas others are "tactical" systems intended to support military commanders on the battlefield. The ISR programs are currently grouped into three major categories: the National Intelligence Program (NIP), the Joint Military Intelligence Program (JMIP), and Tactical Intelligence and Related Activities (TIARA).

Most intelligence used by the military comes from the Defense Intelligence Agency (DIA), which produces some HUMINT, MASINT, and a large portion of the Department of Defense's (DoD) strategic, long-term analysis; the National Security Agency (NSA), which produces most SIGINT; and the National Imagery and Mapping Agency (NIMA), which produces most IMINT.[4] To a lesser extent, the military intelligence community also consists of the Central Intelligence Agency (CIA), State Department, Department of Energy, Department of Justice, and Department of Treasury.

Navy ISR

The Naval Transformation Roadmap of 2003 calls for the reengineering of maritime ISR to align with the DoD's 5000 Series and joint warfighting concepts. Goals are to redefine standards and metrics and ensure interoperability while providing the warfighter-required capabilities in a timely, cost-effective, and efficient manner. Maritime ISR lies at the core of the Naval Operational Doctrine and is an essential element in improving the speed and effectiveness of naval and joint operations. With today's security threats, it is necessary to expand the range of ISR options available to the commander and ensure decision superiority across the range of military operations in accordance with the NSS.

The Intelligence Collection Process (ICP) is the way tactical Navy ISR units of ships, aircraft, and other platforms complete intelligence requests. Once requests are received, human disciplines and IT technologies are used together to search, acquire, process, and report results back to tactical users (i.e., fleet staffs and strike groups), and national-level consumers (i.e., NSA). The generalized process is shown in Figure 14.13.

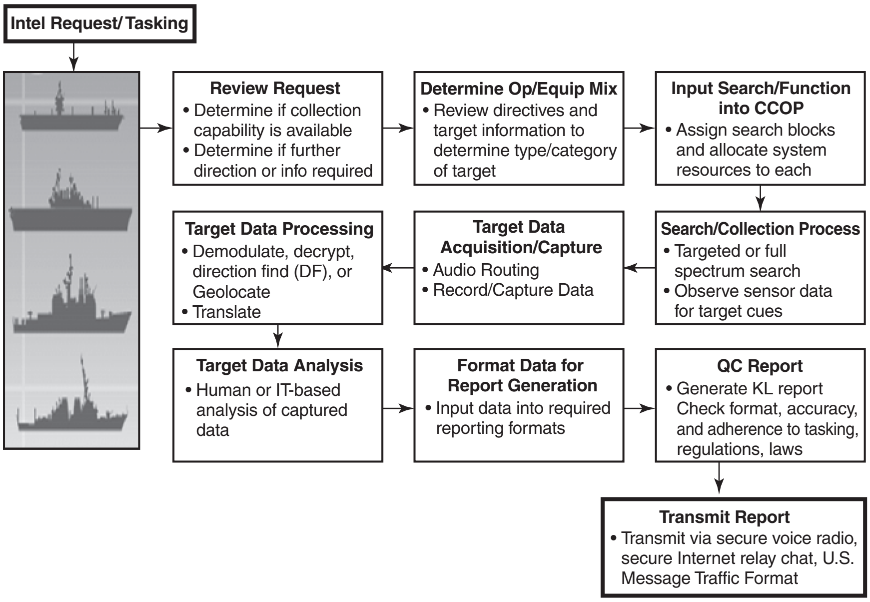

FIGURE 14.13 The intelligence collection process.

Each subprocess is further broken down into individual actions that may be required to perform the subprocess in the ICP. For example, the subprocess Target Data Processing can be broken down into a number of tasks:

1. Human-based (no automation required)
    a. Manual copy directly into report
    b. Human translation and processing
2. IT-based
    a. Direct transfer into report
        (1) Demodulate
            (a) All IT-based
            (b) Human enabled
        (2) Decrypt
            (a) All IT-based
            (b) Human enabled
    b. Direction finding
        (1) Automatic—Local line of bearing (LOB)
        (2) Human-enabled—Local LOB
        (3) Human-enabled—B-rep request
    c. Geolocation
        (1) Special processing

Established in 1994, CCOP developed state-of-the-art ISR capabilities for Combatant Command requirements for a quick-reaction surface, subsurface, and airborne cryptologic carry-on capability. Approximately 100 cryptologic-capable surface ships are currently in the U.S. Navy inventory. Each one is a potential user of carry-on equipment, along with numerous subsurface and air platforms. Although CCOP systems have broad scope and functions, basic capabilities include:

- Tactical surveillance, targeting.
- Passive detection, classification, tracking, enemy intent at extended range.
- Analysis tools allowing interpretation and reporting of the potential or known meaning of intercepted data.
- Correlation and tracking.

As part of the Advanced Cryptologic Systems Engineering program, CCOP utilizes commercial off-the-shelf (COTS) technology, government off-the-self (GOTS) technology, and modular, open systems architectures. COTS and GOTS technologies, when applied to ISR system functionalities, typically require various levels of integration to leverage on-board capabilities to provide system and mission management, product reporting, and data analysis support. COTS and GOTS also require some level of adaptation or modification to meet fleet requirements. Before deployment for operational use, systems must be systematically tested to ensure suitable and reliable operation. They must also be tested for network vulnerabilities (if connected to Navy or joint networks), and tested against joint interoperability requirements.

Valuation Techniques

Assessing information technology investments is a daunting challenge. Although several valuation methods are used to measure and justify IT investments, return on investment (ROI) is the most widely used metric to measure past, present, and potential future performance. Other techniques are used to measure the impact of IT on organizations at the corporate and subcorporate levels. Although approaches differ, the objectives are similar and that is to provide managers with metrics to measure tangible IT investments and intangible knowledge assets. Corporate-level approaches determine the contribution of both IT and knowledge assets on the overall performance of the organization. Subcorporate-level approaches look internally at the subprocesses involved in the production of organizational output and attempt to establish a measure for the benefits of knowledge and IT assets within each subprocess.

ROI in the Public Sector

ROI yields insights for managers and investors making high-level strategic business decisions, yet what if an organization does not produce measurable revenues such as the U.S. DoD? Traditional ROI metrics cannot measure the total value of IT investments made by public sector entities. When conducting an ROI analysis for the public sector, there are several considerations:

- Lack of measurable revenues and profits makes it challenging to determine the overall benefit stream produced by the organization.
- Concrete data is often difficult to collect amid an abundance of seemingly intangible soft data.
- ROI depends on costs and benefits; recipients of benefits or stakeholders are not easily identifiable because potential beneficiaries are program participants, managers of participants, program sponsors, or taxpayers.
- Certain government services are essential for the public good and must be provided, regardless of the accountability or cost.

Budgets of public sector organizations are under increased scrutiny, with stakeholders, managers, and taxpayers demanding higher levels of accountability and transparency of public investment. Compounding the problem further are increased regulations such as the Government Performance Results Act of 1993 (GPRA), requiring the establishment of strategic planning and performance measurement in programs for the accountability of their expenditures. These challenges have forced public sector organizations to adopt quantifiable methods to produce the required metrics for measuring the *total value* of services and products.

ROI in DoD Programs

Funding for many intelligence programs comes from the DoD, which requires all IT programs be managed as investments and not acquisitions. To achieve this goal and meet other government regulations and legislation such as the GPRA and the Information Technology Management and Results Act (ITMRA), the DoD has established performance measures in the IT investment process. Although profitability is not the primary goal of the DoD and other nonprofit organizations, there is pressure to ensure efficient use of taxpayers' money and deliver maximum value to citizens and communities.

Many issues are inherent in determining overall value and risks with ISR systems acquisitions. Technological complexities from the use of COT/GOTS systems, open architectures systems, evolving software standards, shortened acquisitions timelines, and funding instability all contribute to risks in Navy ISR systems. Although the DoD has instituted rigorous types of testing and evaluation (T&E) for all of its programs and projects to mitigate risk, metrics for IT systems have lacked the requisite depth for meaningful valuation. Crucial to successful T&E is the development of measurable key performance parameters (KPPs) and measures of effectiveness (MOEs) to provide accurate projections of system performance in a variety of operational environments.

Another issue in the DoD case is the translation of outputs into monetary benefits. Whereas in the commercial case, a price per unit is assigned to the outputs, there is no equivalent pricing mechanism in the DoD or nonprofit case. This presents a problem when conducting empirical financial analysis and in particular when seeking a baseline from which to formulate sound fiscal decisions. Valuation methodologies used by DoD for acquisitions must include a common framework for understanding, evaluating, and justifying the impact of government IT investments on the overall successful completion of the national security mission of the United States. KVA methodology is a viable valuation technique for that purpose.

Knowledge Value-Added Methodology

Knowledge Value-Added (KVA) was developed by Dr. Thomas Housel and Dr. Valery Kanevsky 15 years ago to estimate the value added by knowledge assets, both human and IT. It is based on the premise that businesses and other organizations produce outputs (e.g., products and services) through a series of processes and subprocesses, which change into raw inputs (i.e., labor into services, information into reports). Changes made on the inputs by organizational processes to produce outputs are the equivalent corresponding changes in entropy. Entropy is defined in the *American Heritage Dictionary* as a "measure of the degree of disorder [or change] in a closed system." In the business context, it can be used as a surrogate for the amount of changes that a process makes to inputs to produce the resulting outputs.[5]

Describing all process outputs in common units allows managers to assign revenues and costs to those units at any given point in time. With the resulting information, traditional accounting and financial performance and profitability metrics can be applied at the suborganizational level. KVA differs from other financial models in two important respects: It provides a method to analyze the metrics at a suborganizational level and allows for the allocation of cost and revenue across subprocesses for accounting purposes.

Knowledge value-added uses knowledge-based metaphor to operationalize the relationship between change in entropy and value added. The units of change induced by a process to produce an output are described in terms of the knowledge required to make the changes. More specifically, the time it takes the average learner "to acquire the procedural knowledge required to produce a process output provides a practical surrogate for the corresponding changes in entropy."[6]

The KVA, Monte Carlo simulation, and real options methodologies are applied to the USS *Readiness* in this case study to demonstrate how program managers can build metrics to conduct a financial analysis of each CCOP system at the process and subprocess levels. Managers and senior decision makers can thereby establish monetary values for traditionally intangible assets such as knowledge.

The USS *Readiness*

The goal of this case study is to assess the effectiveness and efficiency of CCOP systems in the Navy ISR mission. With KVA methodology, metrics are produced and the CCOP portfolio can be compared on existing and future programs. This section reviews how KVA is applied in two of the subprocesses in the CCOP program: Search/Collection Process (P4) and Format Data for Report Generation (P8).

The USS *Readiness* is a fictitious U.S. Navy warship outfitted to conduct ISR missions.[7] Along with the general manning, the ship has a contingent of IW operators performing intelligence collection processes utilizing CCOP systems. The ship is on a typical six-month deployment and receives daily tasking for ISR collection at national and tactical levels. Onboard the USS *Readiness* is an ISR crew of IW Officers: Division Officer, Division Leading Petty Officer, Signals Operators, and Comms Operators. Each IW officer performs certain processes in the ICP. After a request is received, the ISR crew produces a variety of reports that include raw intelligence reports, technical reports, analyst-to-analyst exchanges, and daily collection summaries. USS *Readiness* is outfitted with four CCOP systems (A, B, C, and D).

As shown in Table 14.4, CCOP systems may be used in a single subprocess or across multiple subprocesses along with the existing infrastructure available in each particular platform. Additionally, some systems such as CCOP A are highly complex and comprised multiple subsystems. With the help of KVA, the proxy revenues and costs are obtained and are shown in Table 14.5. Clearly, in the corporate setting, revenues and costs can be obtained quickly and easily, but KVA is required when applied to the public sector.

Table 14.6 lists the preliminary results where ROK is the return on knowledge (a productivity ratio), ROKA is the return on knowledge assets, a profitability ratio, and ROKI is the return on knowledge investment, the value equation.

The KVA provides the structured data required to perform various methods of risk analysis and performance projections such as real options analysis. This combination of KVA historical performance metrics, simulation, and real options analysis will enable the CCOP Program Office and the U.S. Navy to estimate and compare the future value added of different mixes

TABLE 14.4 USS *Readiness* CCOP Systems

	Subprocess Name	CCOP A	CCOP B	CCOP C	CCOP D
P1	Review request/tasking	X			
P2	Determine op/equip mix	X			
P3	Input search function/coverage plan	X			
P4	Search/collection process	X	X		
P5	Target data acquisition/capture	X	X		
P6	Target data processing	X	X	X	X
P7	Target data analysis	X		X	X
P8	Format data for report generation	X			
P9	QC report	X			
P10	Transmit report	X			

of human assets and systems as well as a range of new initiatives for the deployment and employment options of both.

Analyzing Real Options

A real options analysis was performed to determine the prospective value of three basic options over a 3-year period (Figure 14.14). The eight-step real options analysis process with KVA data was used to estimate the value of the options as seen earlier in this book.

The first option (A—Remote to Shore) was to use the various CCOP systems in a way that would allow all the data they generated to be viewed by a geographically remote center, the idea being that if all the intelligence collection processing could be done remotely in a consolidated center, fewer

TABLE 14.5 P4 and P8 Cost Allocation for CCOP C, D, and Fixed IT Infrastructure

Proxy Revenue Assigned to CCOP C Process K ($US)	Cost Assigned to CCOP C Process K ($US)	Proxy Revenue Assigned to CCOP D Process K ($US)	Cost Assigned to CCOP D Process K ($US)	Proxy Revenue Assigned to Fixed Infras Process K ($US)	Cost Assigned to Fixed Infras Process K ($US)
$	$			$28,156	$ 10,250
$	$			$13,868	$ 10,250
$58,253	$12,000	$19,906	$63,462	$241,667	$102,500

TABLE 14.6 P4 and P8 KVA Metrics

KVA Metrics for Total K						
	Subprocess Name	**ROK as Ratio**	**ROK (%)**	**ROKA (%)**	**ROKI (%)**
P4	Search/collection	3.39	339.01	70.50	239.01
P8	Format data for report generation	0.80	79.63	–25.59	–20.37
Metrics for aggregated		14.10	1410.20	157.31	410.20

intelligence personnel would be required on ships. The idea of remoting capabilities to a consolidated center is a popular movement in the military to cut costs and provide more shore-based operations to support warfighting capabilities. This is akin to the consolidation of service operations in businesses—for example in larger, but fewer, call centers.

The second option (B—Direct Support) focused on how the CCOP's equipment and operators could be moved from ship to ship. When a ship came into port for maintenance, repair, or modernization, the idea was to move the CCOP equipment and operators to ships that were about to be deployed. This way, fewer sets of CCOP equipment and operators would be needed to service the intelligence gathering needs of the fleet.

The third option (C—Permanent SSES) basically kept the CCOP systems and operators assigned to given ships at all times. This approach required more operators and CCOP systems raising the potential costs but providing more control of the intelligence capability by the ships and fleet commanders.

The results of the analysis (Figure 14.15) indicated that the highest value was for option C. The result ran contrary to the expected cost savings of options A and B. However, because KVA provided a monetized numerator in the form of surrogate revenue, it was possible to see the effects of greater outputs-revenue for option C. Option C is the preferred option of the commanders of the fleet and ships because it affords greater control of the intelligence assets for their specific operations. So, intuitively, these commanders favored option C, but prior to the real options with KVA data analysis, they had no relatively objective way to support their intuitions.

It is possible that with time and experience, the remoting option would provide greater benefits-revenue per cost than data collection techniques because remoting provides more robust operations from ship platforms. But, the current bandwidth limitations of the naval operating environment mitigate against remoting systems that have high bandwidth requirements.

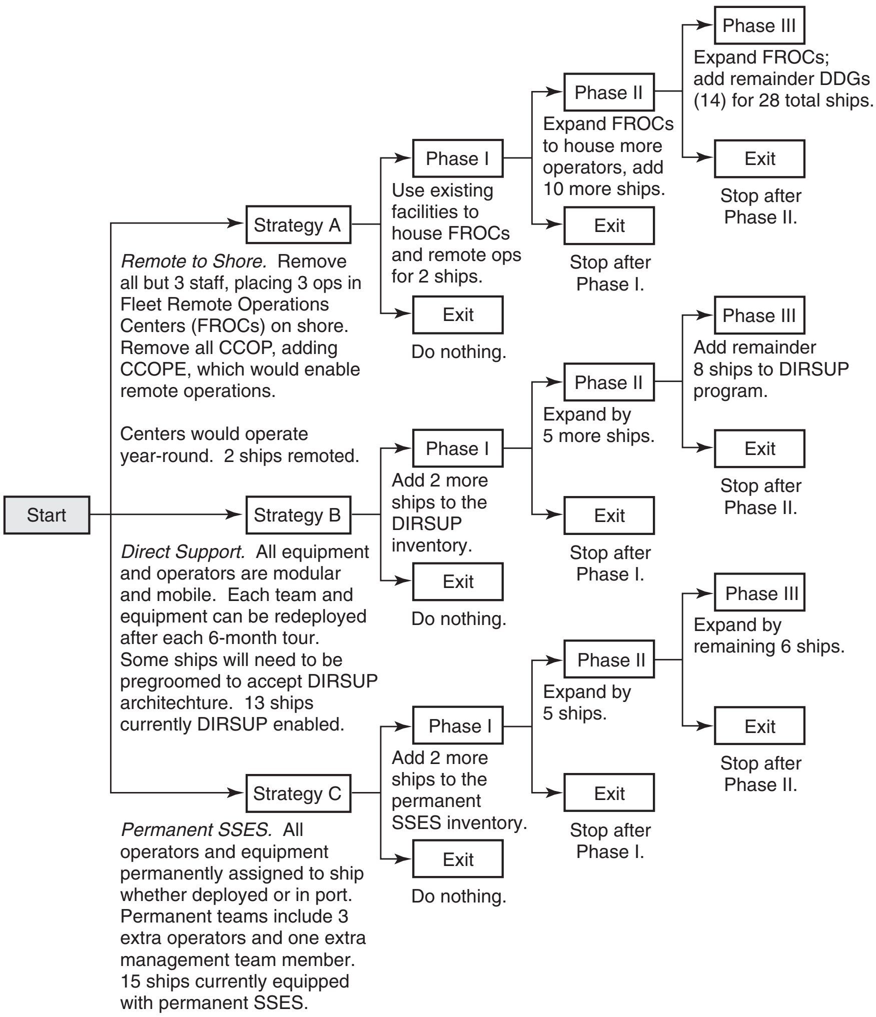

FIGURE 14.14 Staging three path-dependent real options strategies for CCOPs.

The CCOP's program office has asked for further analysis using the KVA and real options methodologies. Software that applies KVA, simulation, and real options analysis are routinely in the process of being deployed with a naval strike group to enable ongoing monitoring of the performance of the data collection process and its supporting CCOP systems. The next step will be to include the use of this software to enable the commanders and program executives to make projections about the best options for

Summary Results	Strategy A	Strategy B	Strategy C
PV Option Cost (Year 1)	$348,533	$1,595,697	$1,613,029
PV Option Cost (Year 2)	$4,224,487	$3,043,358	$4,494,950
PV Option Cost (Year 3)	$3,688,994	$10,105,987	$8,806,643
PV Revenues	$24,416,017	$33,909,554	$48,420,096
PV Operating Costs	$16,220,188	$16,765,513	$9,951,833
PV Net Benefit	$8,195,829	$17,144,041	$28,868,264
PV Cost to Purchase Option	$425,000	$169,426	$72,611
Maturity in Years	3.00	3.00	3.00
Average Risk-Free Rate	3.54%	3.54%	3.54%
Dividend Opportunity Cost	0.00%	0.00%	0.00%
Volatility	26.49%	29.44%	15.04%
Total Strategic Value with Options	$1,386,355	$4,466,540	$15,231,813

FIGURE 14.15 Summary real options analysis results.

deploying the CCOP systems to support the intelligence needs of the naval commanders and other intelligence gathering and analysis agencies in the federal government.

CASE STUDY: MANUFACTURING AND SALES IN THE AUTOMOTIVE AFTERMARKET

This case study was written by Andy Roff and Larry Blair with modeling assistance from the author. Both Andy and Larry are executives from the automotive aftermarket who have owned and managed several businesses. They each have 30 plus years of experience, specifically in the provision of information systems for the shared benefit of both suppliers and distributors. They can be contacted at larblair2@aol.com.

Background and History of the Automotive Aftermarket

The automotive aftermarket (AAM) started soon after the first horseless carriage made its way on to the world's roads more than a century ago. It happened perhaps within a couple of days when the original dog-clutch gave in to the abuse of its erstwhile horse-driving operator! And thus, the AAM was born the moment the first screw needed replacement. Over time, as makes and models of automobiles multiplied, so did the manufacturers of parts to repair and keep them running—some commissioned by the auto