Return on Investment in Nuclear Security: Regulations and Physical Security

by

Jelena Vucicevic

A thesis submitted to the
School of Graduate and Postdoctoral Studies in partial fulfillment of
the requirements for the degree of

Doctor of Philosophy in Nuclear Engineering

Department of Energy and Nuclear Engineering

Faculty of Engineering and Applied Science

University of Ontario Institute of Technology (Ontario Tech University)

Oshawa, Ontario, Canada

December 2025

THESIS EXAMINATION INFORMATION

Submitted by: Jelena Vucicevic

Doctor of Philosophy in Nuclear Engineering

Thesis title: **Return on Investment in Nuclear Security: Regulations and Physical Security**

An oral defense of this thesis took place on December 11, 2025, in front of the following examining committee:

Examining Committee:

Chair of Examining Committee	Dr. Igor Pioro
Research Supervisor	Dr. Ed Waller
Examining Committee Member	Dr. Jennifer McKellar
Examining Committee Member	Dr. Dan Hoornweg
University Examiner	Dr. Khalil El-Khatib
External Examiner	Dr. Akila Frahi-Amroun, University of Sciences and Technology Houari Boumediene of Algiers

The above committee determined that the thesis is acceptable in form and content and that a satisfactory knowledge of the field covered by the thesis was demonstrated by the candidate during an oral examination. A signed copy of the Certificate of Approval is available from the School of Graduate and Postdoctoral Studies.

ABSTRACT

Nuclear security is a crucial part of the nuclear industry, and therefore it is important to observe, research and improve its return on investment (ROI). Investments are made not only in the physical security itself, but also in the regulatory framework, and they should be studied holistically when discussing ROI in nuclear security. This research will analyze the regulatory aspect by analyzing administrative monetary penalties (AMP) in the nuclear industry, and the application of drones in nuclear security, from the side of nuclear facility/licensee security.

An AMP is a penalty imposed by the regulator, the Canadian Nuclear Safety Commission, without court involvement, in the case of a violation of a regulatory requirement. The research includes analysis of AMP, with the focus on the advantages and disadvantages of the AMP system and recommendations for improvements for future implementation. Furthermore, the research focusses on how AMP are implemented in various low probability-high consequence industries, as well as the nuclear industry in Canada and the United States. The emphasis is on the differences in these industries' approaches and how they may be used to improve the implementation in the nuclear industry.

Nuclear facilities invest significantly in security, both for security guards and security tools. Even though drones are relatively new technology, they have been utilized as a tool in emergency situations, fires, floods, search and rescue operations, and surveillance. Due to their characteristics, they show potential for utilization in nuclear security, as they show certain advantages over traditional security systems. The research describes how drones can be effectively utilized in nuclear power plants to complement existing measures and in some cases, replace them.

Finally, through both aspects, it will be shown that ROI in nuclear security can be improved by minor modification of policies or by introducing new tools. Positive ROI is not aways represented by monetary value, but an outcome that meets or exceeds the expectations.

Keywords: nuclear security; AMP; drone; ROI

AUTHOR'S DECLARATION

I hereby declare that this thesis consists of original work of which I have authored. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I authorize the University of Ontario Institute of Technology (Ontario Tech University) to lend this thesis to other institutions or individuals for the purpose of scholarly research. I further authorize University of Ontario Institute of Technology (Ontario Tech University) to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research. I understand that my thesis will be made electronically available to the public.

The research work in this thesis that was performed in compliance with the regulations of Research Ethics Board/Animal Care Committee under **REB 15003**.

Jelena Vucicevic

STATEMENT OF CONTRIBUTIONS

The thesis includes research on both regulation level, and physical security level. The paper "Consideration of Administrative Monetary Penalties in Nuclear Security" was presented at IAEA (International Atomic Energy Agency) conference: International Conference on the Security of Radioactive Material: The Way Forward for Prevention and Detection (December 2018, Vienna), as an oral presentation, and in CRPA (Canadian Radiation Protection Agency), (May 2019, Ottawa) HPS (Health Physic Society), (July 2019, Orlando) and INMM (Institute of Nuclear Material Management) (July 2019, Palm Desert) conferences as posters. At the INMM the poster won the J. D. Williams Student Paper Award. The full paper is published in the International Journal of Nuclear Security as: Vucicevic, Jelena and Waller, Edward (2020) "Consideration of Administrative Monetary Penalties in Nuclear Safety and Security," *International Journal of Nuclear Security*: Vol. 6: No. 1, Article 7. https://doi.org/10.7290/ijns060107 Available at: https://trace.tennessee.edu/ijns/vol6/iss1/7.

Additional research was done after publishing the paper and this work in included in the thesis to provide a complete analysis of the AMPs.

The research related to drones in nuclear security was presented at the INMM conference (July 2019, Palm Desert).

A survey was created and conducted as a part of AMP research. The survey was approved by the Research Ethics Board. The survey involved Department of Energy and Nuclear Engineering (formerly known as Faculty of Engineering

Science and Nuclear Systems (FESNS)) students and experts in the field of nuclear energy and radiation science in academia and industry.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my supervisory committee members, Dr. Jennifer McKellar and Dr. Daniel Hoornweg, for their valuable comments, thoughtful questions, and insightful discussions. Their feedback greatly strengthened this research and was instrumental in bringing it to its final form.

I am deeply thankful to my supervisor, Dr. Ed Waller, for his guidance, encouragement, and unwavering support throughout this journey. Our discussions, exchanges of ideas, and engaging conversations shaped the direction of this research and inspired future work. His mentorship over the years has been truly invaluable.

I would also like to extend my heartfelt thanks to the Vucicevic and Farah families for their patience, understanding, and constant support throughout this process.

Finally, I owe my deepest gratitude to my husband, Dr. Amjad Farah, for his unlimited support, constant encouragement, and inspiration. Our long conversations on nuclear security topics enriched both my research and my perspective. I am profoundly grateful for his presence and support throughout this journey.

TABLE OF CONTENTS

Thesis Examination Information ii

Abstract iii

Author's Declaration v

Statement of Contributions vi

Acknowledgements viii

List of Tables xii

List of Figures xiii

Acronyms xiv

Chapter 1. Introduction 1

Chapter 2. Objective 4

2.1. Rationale of the research 5

2.2. Motivation 6

Chapter 3. Literature Review 9

3.1. Economic aspects of nuclear power 9

3.2. Administrative Monetary Penalties 11

3.2.1. Background 11

3.3. Drones 15

3.3.1. Background 16

3.3.2. Use of drones 22

3.3.3. Regulations 27

3.3.4. Drones as a security threat 29

3.4. Probability of PPS effectiveness 32

Chapter 4. Methodology 44

4.1. AMP 44

4.2. Drones in nuclear security..46

Chapter 5. Analysis of AMPs ROI 47

5.1. Consideration of Administrative Monetary Penalties in Nuclear Security. 47

5.1.2. AMPs in Nuclear Industry in Canada 48

5.1.3. Procedure 50

5.1.4. Optimization of AMPs..54

5.1.5. Survey..63

5.1.6. Conclusions 63

5.2. AMP Application Disparity Across Nuclear and Other Industries in Canada and United States..65

5.2.1. Comparison of nuclear AMPs with other industries in Canada 65

5.2.2. Civil penalties in nuclear industry in the US 74

5.2.3. Comparison of Canadian AMPs and US Civil penalties 85

5.2.4. Suggestions for improvement 86

Chapter 6. Analysis of drone ROI 94
6.1. Drone application in nuclear facilities 94
6.1.1. Potential drones use 94
6.1.2. Equipment/Features 97
6.1.3. The application of drones in nuclear security 105
6.1.4. Drone detection probability 111
6.1.5. Advantages and disadvantages of drones in nuclear facilities 116
6.1.6. Financial consideration 122
6.1.7. Conclusion 125
Chapter 7. Concluding remarks and Future work 127
References 129
Appendix A: AMP Survey 145

LIST OF TABLES

Table 1 Penalty ranges [6] 50

Table 2 Factors and assigned scales 52

Table 3 Modified factors and assigned scales 57

Table 4 Compliance history levels 59

Table 5 Comparison of the original and modified AMP - For the first violation .. 61

Table 6 Comparison of the original and modified AMP - For the second violation 62

Table 7 Base penalties [99] 69

Table 8 Adjustment factors [97] 69

Table 9 Penalties [100] 70

Table 10 Penalties [103] 73

Table 11 Base penalties (Class of licensee) [107] 80

Table 12 Base Penalties (Severity Level) [104] 81

Table 13 Canadian versus US factors (violation significance) 85

Table 14 Comparison of original AMP and modifications 91

Table 14 Characteristics of different drone models 104

Table 15 Average drone prices 123

LIST OF FIGURES

Figure 1 Adversary and PPS Timelines [6] 33

Figure 2 EASI Model (example)........ 36

Figure 3 Adversary Path Example [37] 38

Figure 4 Basic ASD for a facility [37] 39

Figure 5 Neutralization tool (example)........ 42

Figure 6 AMP Calculator........ 45

Figure 7 Comparison of the original and modified AMPs........ 60

Figure 8 Comparison of AMPs issued after 2018 65

Figure 9 Civil penalty calculation process [103]........ 83

Figure 10 Zoom capability example [118] 98

Figure 11 Relative mode of thermal camera [119]........ 99

Figure 12 Spot mode of thermal camera [119] 99

Figure 13 Active Track example [121] 100

Figure 14 Point of Interest example [122] 101

Figure 15 Route for drone and response force 109

Figure 16 Facility area 114

Figure 17 Area covered by stationary camera 114

Figure 18 Area covered by drone camera 115

Figure 19 Average and total pay for Nuclear Security Officer 2012-2021........ 124

ACRONYMS

ADS-B	Automatic Dependent Surveillance- Broadcast
AESA	Active Electronically Scanned Array
AGL	Above Ground Level
AI	Artificial Intelligence
AMP	Administrative Monetary Penalty
APAS	Advanced Pilot Assistance System
ASAP	Aviation Safety Action Program
ASD	Adversary Sequence Diagram
ASRS	Aviation Safety Reporting System
AT	Active Track
AVRS	Airport Voluntary Reporting System
CCPSA	Canada Consumer Product Safety Act
CCW	Counterclockwise (propellers)
CDP	Critical Detection Point
CER	Canada Energy Regulator
CNSC	Canadian Nuclear Safety Commission
COGOA	Canada Oil and Gas Operations Act
CRPA	Canadian Radiation Protection Agency
CTA	Canadian Transportation Agency
CW	Clockwise (propellers)

DHS	Department of Homeland Security
EASI	Estimate of Adversary Sequence Interruption
EO	Electro Optical
ERA	Energy Reorganization Act
ESC	Electronic Speed Controllers
FAA	Federal Aviation Administration
FESNS	Faculty of Engineering Systems and Nuclear Science
FPV	First Person View
GCS	Ground Control Systems
GLONASS	Global Navigation Satellite System
GNSS	Global Navigational Satellite Systems
GPS	Global Positioning System
HPM	High Power Microwave
HPS	Health Physic Society
IAEA	International Atomic Energy Agency
IMU	Inertial Measurement Unit
INMM	Institute of Nuclear Material Management
IP	Ingress Protection
IR	Infrared
KI	Potassium Iodide
MEMS	Micro Electro-Mechanical Systems

NASA	National Aeronautics and Space Administration
NoV	Notice of Violation
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NSCA	Nuclear Safety and Control Act
OCU	Operator Control Unit
PA	Public Announcement
POI	Point of Interest
PPS	Physical Protection System
RF	Radio-frequency
ROA	Remotely Operated Aircraft
RPA	Remotely Piloted Aircraft
RPAS	Remotely Piloted Aircraft System
SASC	Site Access Security Clearance
SDP	Significance Determination Process
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
VDRP	Voluntary Disclosure Reporting Program
VPN	Virtual Private Network
VTOL	Vertical Take-Off and Landing

CHAPTER 1. INTRODUCTION

The importance of energy in today’s world cannot be understated. The importance of nuclear energy is more pronounced knowing that the world needs more energy due not only to population growth, but also the development of technology for which this energy is consumed, and the environmental impacts of other energy production methods. According to the IAEA’s report on energy, electricity and nuclear power, by 2050 electricity consumption is expected to double from the 2023 level [1]. The nuclear industry provides a crucial role in supplying reliable energy to support a sustainable and resilient energy future.

The nuclear industry has always intrigued the public and caused opposing opinions. Some might think it is a necessary and near-perfect energy source for a clean future, while others may see it as dangerous and frightening. There are many reasons behind these opinions, prime amongst which is the lack of understanding of the physics, as well as the safety and security aspects. The science behind nuclear energy is complex, as science writer Christian Parenti summarizes:

> “Nuclear fission is a mind-bogglingly complex process, a sublime, truly Promethean technology. Let’s recall: it involves smashing a subatomic particle, a neutron, into an atom of uranium-235 to release energy and more neutrons, which then smash other atoms that release more energy and so on infinitely, except the whole process is controlled and used to boil water, which spins a turbine that generates electricity… In this nether realm, where industry and science seek to reproduce a process akin to that which occurs inside the sun, even basic tasks – like moving the fuel rods, changing spare parts – become

> complicated, mechanized and expensive. Atom-smashing is to coal power, or a windmill, as a Formula One race-car engine is to the mechanics of a bicycle. [2]"

Similarly, the safety and security of a nuclear facility should be quite complex to support the complexity of the facility itself, and to reduce any potential risk that may be associated with nuclear or radioactive materials.

As William O. Douglas, U.S. Supreme Court Justice stated: security cannot be static. It can only be achieved through constant change and adoption of new ideas and technologies [3]. This is especially true in high consequence industries. Having in mind the specific nature of nuclear materials, it is very significant to see that the security of nuclear facilities and therefore, the safety of people who work or live nearby is organized in such a way to ensure minimal risk of any unwanted events. Due to security events in the past (such as the attacks of 9/11 [4] and A.Q. Khan illicit nuclear technology [5]), nuclear security is becoming of paramount interest for many countries.

Nuclear security is a complex concept which consists of many layers to achieve a common goal: to prevent the misuse of nuclear or radiological material and facilities by adversaries. One of the important pillars of nuclear security is physical protection. It can be defined as ensuring the detection, delay and response to malicious acts against nuclear materials and nuclear facilities through an integrated system of people, technology and procedures [6].

Because of the high consequences which may arise from a security breach in a nuclear facility, very often the security measures include seemingly unnecessary and expansive technologies and protection layers. The significance of return on investment analyses in nuclear security is apparent in the fact that without careful assessment, resources would be wasted on unnecessary protection, or worse, underspending on crucial protection layers could lead to failure of the protection systems of critical assets in a nuclear facility.

CHAPTER 2.OBJECTIVE

Return on investment in nuclear industry is significant due to the high capital cost associated with it, but also because of the specifics of the industry such as the use of nuclear and radioactive materials, which could potentially lead to events of high safety and security significance. If any investments do not give expected results the returns will not be positive. The return does not always have to be immediately monetary, but it could be represented by the level of security (and safety) in a facility after certain investments were made, or after certain regulations were implemented. For example, these are measured using metrics which are audited by national and international bodies, and the results, if positive, aid in granting continued operational licenses and building new nuclear projects.

The objective of the research is to explore the yield of investments in different areas of the nuclear security, including regulations (by example of AMP), and physical security (by example of drones), to find areas that can be improved to give better return on investment, and to propose a different solution for areas in which previous investment does not give expected results.

The research will cover an investigation of specific layers of physical security as well as regulations to analyze their return on investment. Based on the results, improvements will be suggested in specific areas in order to obtain better cost-benefit ratios. This will include:

- Analyzing Administrative Monetary Penalty (AMP) policy, investigating deficiencies in its implementation and explore areas for improvement;
- Examine new technologies (drones) and explore their utilization;

- Compare current implementations with proposed new technologies and analyze the return on investment.

2.1. Rationale of the research

The reason for researching AMPs together with drones as a part of ROI is to look into two very different perspectives of nuclear security, that have a common goal: to ensure that nuclear materials and facilities are adequately protected. Regulations are an essential part in maintaining the security of nuclear facilities, as they are set to prevent any incidents by setting up the regulations and ensuring that the licensees are compliant with the regulations, and if not, the regulator can take actions (such as AMPs) as a response to non-compliance. When observed through the ROI, AMPs are important as there is an initial investment in this policy, as well as investment in maintenance and implementation, but the expected outcome is not only monetary. Outcome of the AMPs should be ensuring that the licensee complies with the regulations, while at the same time, encouraging self-identification of violations, in order for a regulator to build a body of knowledge or a database of potential violations, and to prevent these or similar violations in the future. If these aspects are not satisfied, AMP ROI can be considered to be negative, as the policy does not completely fulfill its purpose.

The second element of the ROI research is drone technology. Drones could be used in nuclear security for surveillance and response to a security event, as a stand-alone tool, or as a support to an existing system. ROI in the case of drones is more straightforward: the investment in purchasing drones, compared to the potentially improved security of the facility, as well as savings in different areas due to the multipurpose use of drones. The cost of physical security in a nuclear facility has many elements: security forces, equipment, surveillance systems, deterrence systems, physical barriers, cyber security, etc. By introducing a new technology a few of these aspects may be addressed and costs could be reduced significantly by substituting or supporting multiple systems at the same time.

If a protection measure falls below a certain level of effectiveness, it leaves facilities unprotected. However, if it goes too far above this level, it wastes resources. Achieving the right balance for nuclear security is a challenge [7].

2.2. Motivation

Nuclear power plant designs have evolved over the years, however, significant changes in design did not shift the interest of potential adversaries. Their targets largely remain the same: nuclear fuel, cooling water, and pumps or power to drive the coolant [8], but what did change is the nature of the threat. Security systems are still relying on the basic systems of “guns, gates and guards” which now, with evolved threats, are no longer adequate. Trying to cover the gap and update the systems just by layering new systems upon the old ones is not sustainable nor economical. Enough layers will provide protection, however the cost of the system may increase enough to be prohibitively impractical.

The motivation behind the research is to improve these layers of security so that they address specific threats in adequate way and to minimize unnecessary spendings. The research should show if new technologies applied in nuclear security can achieve this goal, as well as the effect of improving regulations may have on this goal.

The drone analysis is motivated by the enormous technical development in recent years and the availability of the technology to the public. This causes drones to be seen as a threat to nuclear facilities, but also as an opportunity for significant improvement and modernization of nuclear security. Drones have the potential to positively affect the cost of security in a nuclear facility, and while all power plants could benefit from these improvements, it would be crucial for small modular reactors (SMRs) where power-production income relative to their staffing is greatly reduced compared to large reactors. Reducing staffing requirements for SMRs yields significant improvement in ROI as a result.

The reason behind the AMP analysis is linked to the aviation industry, as one of the low probability – high consequence industries, besides nuclear. The aviation industry has some specific regulation such as Aviation Safety Reporting System (ASRS), Airport Voluntary Reporting System (AVRS), Aviation Safety Action Program (ASAP), and Voluntary Disclosure Reporting Program (VDRP) [9]. All these programs are based on voluntary reporting of violations regarding safety and security, which have significantly contributed to the commercial aviation safety record [9]. The value of confidential reporting is in the contribution to aviation safety, and the ability to gather information often not reported through other tools [10]. The main goal of the voluntary reporting is to prevent any potential accidents by ensuring the flow of information [11]. This method could be applied in the nuclear industry in addition to or in combination with current regulation to obtain better results. In the nuclear industry, safety is the fundamental regulatory objective. Compliance with the requirements plays an important role in giving the regulators confidence that safety is being maintained. Requirements, including technical specifications, other license conditions, orders, and regulations, have been designed to ensure adequate protection. In the context of risk-informed regulation, compliance plays a very important role in ensuring that key assumptions used in underlying risk and engineering analyses remain valid. While adequate protection is presumptively assured by compliance with the requirements, circumstances may arise where new information reveals that an unforeseen hazard exists or that there is a substantially greater potential for a known hazard to occur [12]. Therefore, timely information would be of great significance for the prevention of any accidents.

These improvements, both in regulations and physical security, could have a significant impact on costs generated in nuclear security and on return on the investment.

CHAPTER 3. LITERATURE REVIEW

When it comes to economic benefits in nuclear security investment, there is a significant gap in the knowledge. Other than practical uses in industry, there is very little published research in this area.

3.1. Economic aspects of nuclear power

The economics of nuclear power, as with the process of nuclear power generation itself, can become quite complex, as each nuclear generating station has a unique number of factors when it comes to economic calculations, and comparing costs, benefits, and return on investment. According to the World Nuclear Association, nuclear power is cost-competitive with other electricity generating industries, apart from those which have direct access to low-cost fossil fuels [13]. The main economic factors in nuclear power include capital costs, plant operational costs and external costs. Each of these factors have several elements that affect the total cost of nuclear generated electricity: capital costs include cost of site preparation, construction, manufacturing, commissioning, and overall financing the power plant. Plant operating costs include the cost of fuel, operation and maintenance, treating and disposing of used fuels and wastes, etc. [13]. However, the cost of nuclear power production does not end here. In addition to the nuclear power plant costs there are further costs in the nuclear industry – costs of regulating it. Regulatory bodies in each country where nuclear power generation exists play a crucial role in regulating “the use of nuclear energy and materials in order to protect health safety, security and the environment”, as the CNSC describe in their mandate [14].

A significant portion of power plant operating costs falls under nuclear security. Nuclear security costs can be divided into two groups: regulatory compliance costs, and direct security costs. Direct security costs include security forces staffing, physical security measures, security screening, cyber security, information protection, emergency preparedness, etc. Regulator costs include time and financial means invested in initial policy creation and implementation, maintenance, and compliance monitoring. This research will not focus on all aspects of nuclear security, but it will focus on areas where relatively small changes may yield a significant return. These changes should help by enhancing, supporting and, in some instances, replacing the outdated elements, and therefore reducing costs and/or improving security of the facility.

Economic benefits in the nuclear industry through nuclear security can be achieved by maximizing the performance of nuclear security in the facility while minimizing its cost. This can be done in two ways: by ensuring the current systems are functioning properly (including regulations), therefore ensuring that investments made in these systems yield expected results; and by introducing new technologies with low cost but high outcome.

Economic impact of nuclear energy is another significant aspect for countries which have nuclear facilities, as it supports local economies. Historically, local communities have had many benefits from the nuclear industry, including providing reliable employment, increasing local tax revenues, and decreasing consumer vulnerability to electricity price volatility [15].

3.2. Administrative Monetary Penalties

AMPs are mainly used by the government for deterring the violation of a regulatory requirement. Even though the goal of AMPs is to reduce time and costs for the regulator and industry by issuing AMPs without court involvement [16], there is no firm proof that this goal is met. There is not enough research of this topic in the literature to show the efficiency of this policy.

3.2.1. Background

According to the Canadian Nuclear Safety Commission (CNSC), the legal framework in Canada consists of acts and regulations, licences and documents. In Canada, acts are made by Parliament. Regulations may be perceived as a part of a law; therefore, they have to be in compliance with the act. Acts and regulations are legally binding documents [17]. Since this research is related to nuclear security, only legal framework related to nuclear security will be described here.

Acts

Nuclear Safety and Control Act (S.C. 1997, c. 9) [18] :

The Nuclear Safety and Control Act (NSCA) is the basis to control activities, substances or information related to nuclear power in Canada. It is the highest-level legal document specific to Nuclear Energy Control in Canada. NSCA came into force on May 31, 2000. This created the CNSC, and set out its mandate, responsibilities and powers. The purpose of this Act is to provide the limitation of the risks to national security, the health and safety of persons and the environment, production and use of nuclear energy and the production, possession and use of nuclear substances, prescribed equipment and prescribed information. Moreover, it implements measures to which Canada has agreed, respecting international control of the development, production and use of nuclear energy, including the non-proliferation of nuclear weapons and nuclear explosive devices.

Security of Canada Information Disclosure Act (S.C. 2015, c. 20, s. 2) [19]:

This Act should ensure that information is shared among the institutions of the Government. This is in order to protect Canada against activities that undermine the security of the nation. This would include proliferation of nuclear, chemical, radiological or biological weapons.

Transportation of Dangerous Goods Act, 1992 [20]:

This act classifies nuclear material as Category 7 dangerous goods. It also establishes security requirements for equipment, systems and processes used in importing, offering for transport, handling or transporting dangerous goods, including means of transport tracking and identification protocols.

Regulations

Regulations establish requirements for all types of licence applications and obligations and provide for exemptions from licensing. By-laws are in place to govern the management and conduct of the Commission's affairs [21]. The following regulations include those related to nuclear security:

- Administrative Monetary Penalties Regulations

AMPs are one of the tools available to the CNSC to ensure compliance with NSCA. These penalties are imposed by the CNSC, as a response to a violation of a regulation, without court involvement. According to the CNSC, not all violations are subject to AMP. The list of violations that are subject to AMPs was created and is part of this regulation. Part 9 of this list is related to nuclear security [22]. CNSC also created the method and criteria by which the penalty amounts will be determined, and the manner in which notices of violations must be served. More on AMP regulation can be found in Chapter 5.

- Packaging and Transport of Nuclear Substances Regulations, 2015

Provide requirements for transport of nuclear substances. This includes requirements for record keeping, design and certification of packages, special form radioactive material and other prescribed equipment.

- Nuclear Security Regulations

Define all information regarding nuclear security. This includes nuclear security requirements and general obligations for its application. This document regulates both high-security sites and lower-risk facilities.

- Nuclear Non-proliferation Import and Export Control Regulations

Provide requirements for import or export of controlled nuclear substances, controlled nuclear equipment, or controlled nuclear information.

Regulatory documents [23]

Regulatory documents include both requirements and guidance. The difference between them is in the use of mandatory and non-mandatory language.

Certain documents regarding nuclear security contain information which are not available to the public. Information in the document is made available only to stakeholders with appropriate security clearance with a valid reason. These documents are:

- REGDOC-2.12.1, *High Security Facilities, Volume I: Nuclear Response Force*, Version 2

- REGDOC-2.12.1, *High-Security Facilities, Volume II: Criteria for Nuclear Security Systems and Devices*

Other documents are available for public on the CNSC website:

- REGDOC-2.12.2, Site Access Security Clearance, 2013

Provides guidance regarding the site access security clearance (SASC) for authorized unescorted entry to a protected area. This document should help prevent risk to high-security sites.

- REGDOC-2.12.3, Security of Nuclear Substances: Sealed Sources *and Category I, II and III Nuclear Material*, Version 2.1, 2020

Regulates security measures for licensees in order to prevent the loss, sabotage, illegal use, illegal possession, or illegal removal of sealed sources during their entire lifecycle.

- REGDOC-2.13.1, *Safeguards and Nuclear Material Accountancy, 2018*

CNSC keeps account of all nuclear material in Canada. The licensees must report any nuclear material in possession or any inventory changes to the CNSC. Through this document Canada complies with bilateral Nuclear Cooperation Agreements with nuclear trading partners worldwide under the terms and conditions of the non-proliferation treaties.

- REGDOC-2.13.2, Import and Export, Version 2, 2018

This document represents the guidance of the CNSC for current and prospective licensees. It is related to import or export nuclear and nuclear-related items, also known as controlled nuclear substances, equipment and information.

3.3. Drones

The amount of research done on application of drones in security systems has been very limited because they are a relatively new technology. Recently, drones have been evolving rapidly and have developed a multitude of capabilities.

Unmanned Aerial Vehicle or UAV is the most common term used to describe what the world has come to know as drones. There are other terms such as Unmanned Aircraft System (UAS), Remotely Piloted Aircraft (RPA), Remotely Operated Aircraft (ROA), Unmanned Aircraft (UA), but for simplicity and consistency throughout the thesis, the term drone will be used [24].

3.3.1. Background

In the past decades drone technology has gone through a significant development. This development of the drone technology has affected other industries. Many people know drones as recreational model aircrafts, but they can be more than that. Used for aerial photography, film industry, recreation, delivery, etc. drones are part of everyday life. In the recent years some industries started to recognize the opportunities that drones offer and started to utilize their capabilities, however still not reaching their maximal potential. This low-cost and high-efficiency tool can be used for surveillance, fast delivery of small parts across facilities or inspection in industrial settings. Similarly, all these properties could be used by adversaries, so this technology could be not only a significant improvement, but also a security threat.

Drone technology is in constant state of development. This adjustability makes drones ideal for widespread use.

Drones come in a wide variety of sizes, with fixed or rotary wings. The largest are mostly used for military purposes such as the Predator drone, measuring over 14 meters in wingspan and over 8 meters in length [25]. The next in size are unmanned aircrafts, which have fixed wings and require short runways. These are generally used to cover large areas, such as geographical surveying or to combat wildlife poaching. Next are what is known as VTOL (Vertical Take-Off and Landing) drones. Many, but not all, of these are quadcopters. Quadcopters, also called a quad rotor helicopters, use two pairs of identical fixed pitched propellers, and use independent variation of the speed of each rotor to achieve control. The main characteristic of VTOL drones is that they can take off, fly, hover and land vertically. Due to their design and mechanical properties quadcopters are often cheaper and more durable than conventional helicopters [26, 27].

Drones are usually made of light composite materials. This composite material strength allows military drones to cruise at extremely high altitudes, while it reduces weight and increases maneuverability. An unmanned aerial vehicle system consists of two parts, the drone and the control system. Drones are equipped with different technology such as infrared cameras, global positioning system (GPS) and laser. They are controlled by remote ground control systems (GCS) also referred to as a ground cockpit. Drones are built from materials designed to absorb vibrations, which decrease the noise produced. This is very important when it comes to drone precision. All the sensors and navigational systems are located in the nose of the drone, while the rest of the body is full of drone technology systems since there is no need for space to accommodate pilots [26].

Highly accurate navigation is important for flying a drone. Many of the latest drones have dual Global Navigational Satellite Systems (GNSS) such as GPS and GLONASS (Global Navigation System). Drones can fly in both GNSS and non-satellite modes. When in use, it searches and detects GNSS satellites. Some of the GNSS systems use groups of satellites working together known as Satellite Constellation technology for higher precision and better coverage [26]. When the drone is on, the radar technology can signal the following on the remote controller display:

- signal that enough GNSS satellites have been detected and the drone is ready to fly
- display the current position and location of the drone in relation to the pilot
- record the home point for “Return to Home” safety feature [26]

Most of the latest drones have 3 types of Return to Home drone technology:

- Pilot initiated return to home by pressing button on Remote Controller or in an app.
- Low battery level where the drone will fly back automatically back to home point.
- Loss of transmission between the drone and Remote Controller with the drone flying back automatically to its home point [28].

Some of the latest drones can sense and actively attempt to avoid obstacles during automatic return to home:

- The drone slows down when an obstacle is sensed
- It stops and hovers, then flies backward and ascends upwards until no obstacle is sensed.
- Next the Return to Home process resumes and the drone will return to home point at the new altitude [26, 29].

These systems fuse one or more of the following sensors to sense and avoid obstacles: Vision Sensor, Ultrasonic, Infrared, Lidar, Time of Flight (sensors emit a very short infrared light pulse and each pixel of the camera sensor measures the return time.), and Monocular Vision [26, 30, 31].

Using these sensors, a drone can fly around obstacles, or, if it is unable to work out a flight path around the object, hover in front of the obstacle. This is known as APAS (Advanced Pilot Assistance System) [26].

For a drone to fly perfectly, the Inertial Measurement Unit (IMU), gyro stabilization and flight controller technologies are essential. To provide information for navigation, drones use three and six gyro stabilization technology. This makes them safer and easier to fly. Gyro stabilization is one of the most important components, allowing the drone to fly smoothly even in strong winds and gusts. Gyro stabilization is a part of integrated gimbals, which are in use in the latest drones. During the flight a number of forces affect drones constantly. These forces, such as wind, affect the drone's movement making the drone difficult to control. Integrated gyroscopes can detect changes in the position of a drone and compensate for it in such a way, that it basically seems unaffected, as it re-adjusts its position hundreds of times every second. This technology gives the on-board camera or sensor a vibration free movement; a characteristic that can be very significant if drones are used in security [26, 32, 33].

An IMU detects the current rate of acceleration, and changes in rotation (pitch, roll and yaw) using one or more gyroscopes. The processors then calculate the drone's position repeatedly. First, it integrates the sensed acceleration, together with an estimate of gravity, to calculate the current velocity. It then integrates the velocity to calculate the position. The flight controller gathers the IMU data and sends new data to the motor electronic speed controllers (ESC), in order to fly in different directions. The ESCs send signals to the motors about the level of thrust and speed required for the quadcopter to fly or hover. Another important component of the IMU is 3D accelerometers, used to measure the orientation of a drone relative to earth's surface. It works by sensing the acceleration of gravity using MEMS (Micro Electro-Mechanical Systems) [32, 33].

The motors and propellers are the drone components which move the drone into the air and to fly in any direction or hover. On a quadcopter, the motors and propellers work in pairs with 2 motors and propellers rotating clockwise (CW Propellers) and 2 motors and propellers rotating counterclockwise (CCW Propellers). They receive data from the flight controller and the ESC on the drone motor direction to either hover or fly [26].

Nearly all drones have a GCS, or a smartphone app allowing the pilot to keep track of the current flight and see what the drone sees on a mobile device. The main tasks of the GCS are to work as an ergonomic user interface and a data integration hub between multiple sensors mounted on drones and a control centre. It has the function to integrate the data streams coming from a range of sensors. Like computers, drones send commands to the physical components in the aircraft or remote controller through software. Most unmanned aircrafts use Linux and a few use MS Windows. In 2014 a project was launched called the Dronecode project.

This is an open source, collaborative project that aims to connect existing and future open source unmanned aerial vehicle projects. The result is a common, shared open source platform for drones [26, 34].

Methods of controlling drones are divided into internal piloting and external piloting. Internal piloting is the method of controlling the aircraft through a first-person view (FPV), from a perspective of a pilot sitting in the cockpit on board. Military drones are controlled from a pilot's perspective in a control simulator (internal piloting), the same as controlling an actual aircraft. In this case, the ground pilot flies the aircraft as if they were on-board the aircraft instead of looking at the aircraft from the pilot's actual ground position. External piloting, on the other hand, indicates remotely controlling the drone from a third-person view on the ground by a remote controller. This way of piloting might create control and safety problems, since pilots would have difficulty guessing the drone orientation and may not be able to keep eye contact with them even at short distances (>100 m). Therefore, the ground control gets more challenging the further the drone gets from the operator. It can be extremely challenging for pilot to estimate drone's position relative to nearby objects to avoid obstacles [35, 36].

For the use in nuclear power plants the internal piloting or the FPV feature would be essential. A video camera is mounted on the unmanned aerial vehicle and this camera broadcasts the live video to the pilot on the ground. FPV allows for the following:

- The unmanned aircraft to fly much higher and further than otherwise possible by looking at the aircraft from the ground.
- More precise piloting especially around obstacles.
- Easier control while flying indoors, or through forests and around buildings.

This FPV technology uses radio signals to transmit and receive live video. The receiver of the live video signals can be either the remote-control unit, a computer, tablet or smartphone device. Depending on the strength of the signal between the ground control on the drone this video feed can have higher or lower quality. Some drones have an FPV live video range of 8 km (5 miles) with a 1080p quality video transmission [26].

3.3.2. Use of drones

Drones are a relatively new topic in the nuclear field, and there are not many papers dealing with the question of drones in nuclear power plants from a security perspective. Due to this, and the fact that they have gained the attention of the public, many sources for further research are not in peer reviewed publications but rather in blogs, news and technological magazines. Most of the journal papers in this area are focused on prevention of drone flights over high risk facilities, but it is rare that authors suggest the utilization of drones in nuclear security. One of the most respected authors in the field Mary Lynn Garcia, in one of her books "*Design and Evaluation of Physical Protection Systems*" describes security systems in nuclear facilities as a traditional system composed of cameras, sensors, and alarms, but does not mention drones neither as a security threat nor as a tool [37].

This shows that modern technologies such as drones are not researched enough for the use in nuclear facilities. In most cases the study of drones with respect to nuclear security have only considered the threat of drones. Even though Solodov et al. [38] recognize that drones have many beneficial applications, they focus on the potential security concerns drones present for nuclear facilities. They analyze the threat without giving opportunity for this technology to be used for the purpose of protection or defense. Other authors such as Islam et al. [39] have similar approach. They analyze the threat and suggest protection strategies against drones. One author who sees the opportunity in the utilization of drones for nuclear security is Baylon [40], who advocates that the use of drones can help enhance nuclear security. This could be accomplished by using drones for surveillance, radiation monitoring, or in disaster response and clean-up operations at nuclear facilities. Some of the suggested methods of drone application are already in use: drones are used as aerial radiation monitoring systems. These systems are very useful to search and locate radioactive sources in places like scrap yards, cargo storage or in case of an emergency [41] [42]. Another author who believes that the use of drones could significantly improve nuclear security is Rosano [8], who claims that drones, smart cameras and even robotic systems can be used in surveillance and monitoring, assessment of threat, and interdiction and response in nuclear security event. According to a World Institute of Nuclear Security Report, it is expected that remotely operated and autonomous technologies provide significant improvement in the performance of security systems. This could affect security costs, which could be decreased by replacing some personnel with semi or fully autonomous systems [7].

The use of drones is widely spread, in everyday recreational or entertainment purposes, but even more in professional settings, where precision, speed and low cost are important. The purpose is still mainly monitoring, video recording or high-quality photography, but with expanding technological capabilities, there are new ways of implementation every day such as surveillance, assisting in emergencies and rescue missions, or deliveries [43, 44, 45, 46].

The capability of drones in emergency situations is very high. They are capable of flying at night and over dense smoke. Additional advantage is that drones can cover large areas to provide situational awareness, even in remote and hard to access areas, with higher efficiency in regard to personnel and overall resources. [47]. These capabilities are being extensively used for firefighting and disaster recovery [47, 48, 49, 50, 51, 52, 53, 54]. Drones can be equipped with infrared cameras that peer through smoke, as well as sensors for wind direction and other weather variables that affect how wildfires spread [55, 56] . This was widely used by the emergency response teams throughout fire seasons in US and Canada since 2017 and more in the recent years (Oregon 2017/2018, Colorado 2024, California 2017/2018, 2021, 2025, British Columbia 2021, Quebec 2024 [57] [58] [59] [60] etc.) helping with wildfire suppression using drones which include Infrared and Electro-optical cameras and sensors.

Drones are proven tools for disaster recovery in other natural disasters as well. For example, in 2017, the drone technology assisted with disaster recovery during the aftermath of Hurricane Harvey [61]. In 2022 United Nations Development Programme recognized drones as an efficient and accurate tool for assessment of disaster damage [54].

Furthermore, drones can be used in search and rescue missions. In some countries drones equipped with infrared cameras are used for locating people faster and safer that they would be able to otherwise [56].

This technology can easily be applied in nuclear security, helping both security and safety.

The commercial use of drones is increasing daily. Drones are being tested for new ways of use by delivery companies, which started testing drones for delivery of small packages in US, India and Russia [62] [56]. In 2016 a drone manufacturer partnered with the Federal Aviation Administration (FAA) and National Aeronautics and Space Administration (NASA) for the first successful US drone delivery in July 2015 and again from ship-to-shore in New Jersey in June 2016, as a potential disaster-relief delivery method [62]. In 2017 the FAA started a program of testing and issuing certificates for packages delivery by drones [63].

One of the advantages of drone technology is the speed of deployment and flight speed compared to other commonly used technologies. A study conducted to show if drones would be more useful in delivering a defibrillator, which could be used by a member of the public, showed a drone arrived 16 minutes faster than the emergency services on average. The study found that the median time from call to dispatch of the emergency services was 3 min 0 sec compared with 3 sec for the drone. The median time from dispatch to arrival of the drone was 5 min 21 sec, compared with 22 min 0 sec for the emergency services. The drone arrived faster than the emergency services in all cases with a median reduction in response time of 16 min 39 seconds over a median flight distance of about two miles [64].

The Department of Homeland Security (DHS) United States Secret Service relies on drones for identifying threats, mitigating vulnerabilities, and creating secure environments for statutorily protected peoples, places, and events. In the past DHS used manned aerial vehicles but they found them insufficient because the manned aircraft usually used are limited in scope, unable to provide a persistent and dedicated overhead coverage for the Secret Service fixed sites secured over a longer period of time, and too loud for certain Secret Service protected outdoor sites or venues [65]. Therefore, they turned to drones.

Nuclear facilities already use drones in different ways. Environmental monitoring and safety related issues such as radiation monitoring, or structural inspections are dealt with by drones. They have many advantages over conventional ways of monitoring, in that capital and operational costs are substantially lower and the drone can survey small areas at low airspeeds (< 2 meters/sec) and low altitudes (< 5 meters). A suitable drone for remote monitoring must also have adequate payload, stability in flight, and have reasonable flight time between refueling/recharging [66]. After the Fukushima accident in 2011 the use of drones was an obvious choice. Drones are highly convenient because of their ability to fly into airborne radioactive plumes without exposing human crew to radiation. They can also be pre-programmed to undertake some missions without direct human control. These capabilities can all be extremely useful after a nuclear accident [67].

Finally, the recent events in Ukraine and Russia, during the armed conflict, confirm that drones can be used as a weapon, as they have become one of the most used weapons of the war. Drones have transformed the battlefield in Ukraine by providing accessible and affordable capabilities. They are being used for surveillance, intelligence gathering and strike operations, as well as support for other military systems, decoys, or transporting equipment, and laying mines. It is assessed that models of drones in use are ranging from toy-sized systems to larger models with wingspans of almost 20 meters, but majority of the drone fleet consists of low cost quadcopters available to civilians [68] [69]. FPV drones are favoured because they are far more accurate than most artillery, as pilots can guide them to the target. As a form of defence against the drone attacks both sides use jamming of frequencies. Successfully jammed signal will disable the pilot's control of the craft or disrupt the video signal, depending on which frequency has been affected [69].

3.3.3. Regulations

Drones in Canada are regulated by Transport Canada. The Canadian Aviation Regulations enabled by Aeronautics Act regulates Canadian airspace, and defines remotely piloted aircraft system (RPAS), a set of configurable elements consisting of a remotely piloted aircraft, its control station, the command and control links and any other system elements required during flight operation. Remotely piloted aircraft is defined as a "navigable aircraft, other than a balloon, rocket or kite, that is operated by a pilot who is not on board" [70]. The Regulations consist of ten parts, where Part IX provides regulations for registration, pilot certification, general operating procedures for both basic and advanced operations, requirements for manufacturer, as well as prohibitions for operations. Small remotely piloted aircraft in Canadian Aviation Regulations is defined as a remotely piloted aircraft that has a maximum take-off weight of at least 250 g but not more than 25 kg [70].

According to these regulations a drone, amongst other aircrafts, should not be operated within a controlled airspace or within restricted airspace. Every drone must be registered and must have certification number which would help identifying the owner if needed. Drone pilots must be at least 14 years of age and must carry a valid drone pilot certificate for small remotely piloted aircraft. This certificate implies that a candidate has successfully completed the examination “Remotely Piloted Aircraft Systems — Basic Operations” for drones which weigh between 250 grams and 25 kilograms [71]. If a drone weighs over 25 kg or is needed to fly outside the rules for a special purpose a pilot must obtain special flight operations certificate. This applies to those:

- who are residents of countries other than Canada,
- who want to fly more than 5 drones at the time,
- flying a drone which carries dangerous or hazardous payloads,
- or if they want to fly at a special aviation event [72].

According to Government of Canada, the main reason for these changes is because the commercial and recreational drone industry continues to grow at an unprecedented rate. The rapid surge in popularity and accessibility of drones has led to an increase in the number of reported incidents, as the majority of new and inexperienced users are flying their drones without a clear understanding of the potential safety risks associated with their use. In Canada, between 2014 and 2016, the number of reported aviation-related drone incidents rose from 41 to 148, an increase of 260% [73], including cases of near misses with aircrafts (Porter flight was forced to take action to avoid a drone near Toronto in November 2016 that injured two flight attendants) and drones flying too close to flight paths, airports and commercial aircrafts, and in a dangerous manner over people on the ground [73]. In Canada, these incidents can be resolved by issuing a number of rules according to which a drone pilot should behave while operating a drone.

If drones are to be used in nuclear facilities as an addition to security and safety measures, they would have to be regulated. This use does not fall under any existing regulation. The World Institute for Nuclear Security in one of their reports claim that drones are legitimate security concerns and as such, a supportive legislation framework needs to be developed [7].

3.3.4. Drones as a security threat

Drones can have a high impact on the security of nuclear power plants, because of the non-traditional threats they pose. They may represent threats for a nuclear facility in two ways: when used by the facility employees for safety and security purposes they may be hacked, and taken over, or when used by an adversary they could be brought to the facility to attack or sabotage the facility.

With an operating system, flight controllers and main boards with programmable code, drones can be hacked into similarly to hacking a computer. There are drones that have been developed with a capability to fly around searching for other drones and hacking into their wireless network, disconnecting the pilot and taking over that drone, however, there are some ways to prevent this. [26]. To hack a drone, a connection must be made to either the remote controller (cellphone, tablet, laptop) or to the drone by intercepting the signal. This can be prevented by installing antivirus and Virtual Private Network (VPN) on the ground controller. Additionally, a new operating system is being developed to isolate the varying functions of the device it is installed on. This could prevent the entire system from being compromised, even if a hacker manages to get part of the way in [74].

In case of drones used by adversaries to conduct an attack on a nuclear facility, protection must include detection and interception or neutralization of adversary drones. The most common detection techniques are radar, radio-frequency (RF) detection, EO, and IR, while jamming is commonly used for interception. Other than these techniques, methods for detection and tracing include acoustic, where the specific sound of drone motors is recognized by a special software and combined sensors, to provide a more robust detection capability. Methods for interdiction include RF jamming where radio frequency link between the drone and its operator is disrupted; GNSS jamming which disrupts the drone’s satellite link, which is used for navigation; spoofing where drone’s communications link is hijacked and one can take control over the drone; laser, that can destroy vital elements of the drone’s airframe using directed energy; nets which are designed to entangle drone and its rotors; and projectile which is ammunition designed to destroy targeted drone. Many of these elements could be combined to increase the probability for intercepting the drone. All these elements could be ground based, hand-held or UAV based [75]. One example of the combined elements on a drone is an “intercept drone” designed to hunt down nearby drones, hover overhead and drop a tangle-line into their rotors, forcing them to crash [76]. The problem with this technology would be that it could be effective only in certain cases, since the technology would be ineffective against ‘fixed wing’ drones that lack rotor blades [40]. The intercept drone could have cameras, and scan for nearby drones, and therefore could potentially be used by the nuclear industry to prevent drone flyovers. Newer research by Yang and Quan proposes use of autonomous drones for intercepting unwanted drones in specific area such as airports or nuclear power plants [77].

One specific example for a versatile detection element is the electronic scanning radar, also known as AESA (Active Electronically Scanned Array), which is currently used in fighter jets. AESA has the advantage of being extremely versatile, both in terms of host platforms and detection capabilities, but even though they are very advanced, they cannot accurately identify hostile drones [38].

There are some other radar technologies developed which can detect, track and identify flying objects, discriminating between possibly dangerous drones and other objects such as birds or balloons. Once the object is identified as a drone the device can attempt to jam the drone’s control or navigation signals, or to attack drones using nets. This radar is the size of a paperback book and can accurately detect and follow drones in three dimensions, up to a kilometer (0.6 miles) away [78].

Previous experiences from many airports around the world show that even though airports are restricted areas for drones, the flyovers may happen. As many airports were not equipped with counter-drone systems, military equipment had to be involved, which in many cases is too expensive and it is involved when the event has already happened. In many cases in the past few years, drones were found flying around airports in Canada, US, UK, and other countries causing disturbance and flight delays, resulting in significant economic losses [79] [80] [81]. The recent high-profile case was the Gatwick airport incident that was solved by introducing military anti-drone equipment. The system, which is said to have a range of several miles, uses four radars to give 360-degree detection in order to identify and track targets [82] [83]. There were other cases of drones disrupting airports, including Ottawa, New York, Florida, Dubai, Warsaw, Beijing, Kabul [84, 85]. The exception of the Gatwick incident is that no airport has ever been closed for so long. In many of these cases, the military was involved in trying to protect the airports from the drones by sending fighter jets, which was neither effective (due to speed of drones and time from spotting a drone to sending a fighter jet) nor economical solution [82].

3.4. Probability of PPS effectiveness

Drones can be used to enhance physical protection, therefore in this chapter, an explanation of the effectiveness of physical protection systems will be described. The significance of the modeling of physical protection system (PPS) is to set up a timeline of adversary activities and the timeline of PPS which would respond to these activities. These can be seen as competing timelines: adversary timeline, which is the time to cross areas, penetrate or bypass barriers, and remove or sabotage a target; the PPS timeline covers the detection, delay, and response processes. The combination of these timelines illustrates the requirement for PPS effectiveness (Figure 1) [6].

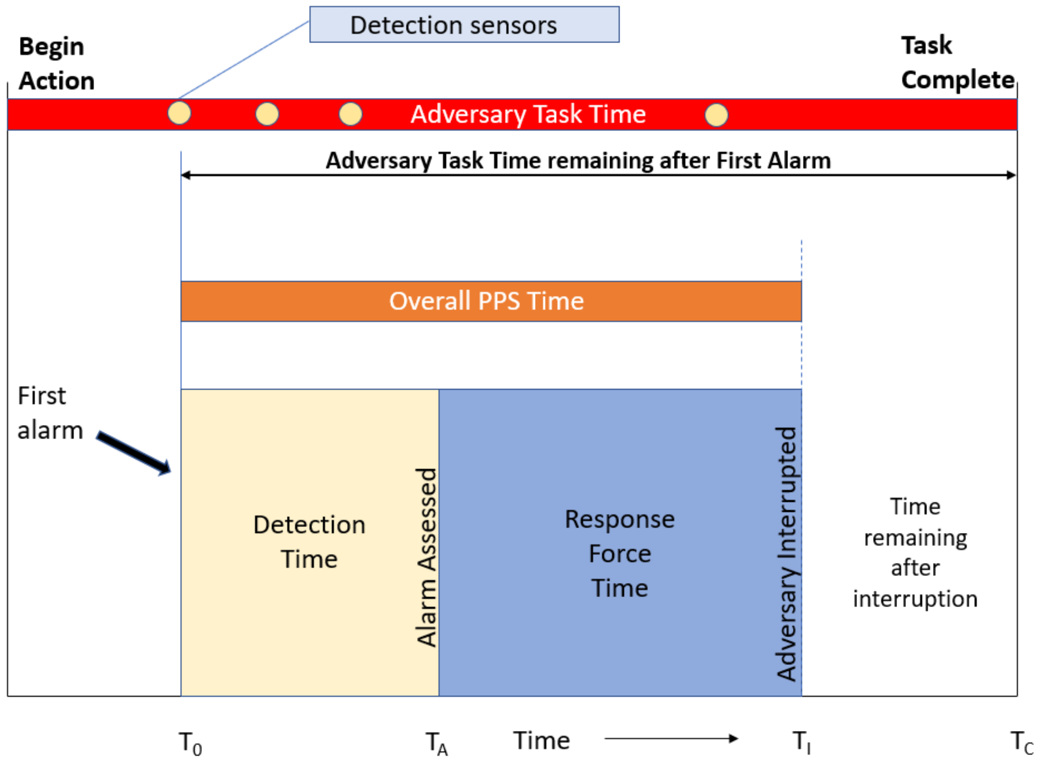

Figure 1 Adversary and PPS Timelines [6]

The goal of PPS is to interrupt and neutralize adversaries before they complete their theft or sabotage task. In order to achieve this, the PPS response time must be less than the adversary task time remaining after detection [6]. The PPS is based on principle of timely detection, where detection must occur early enough that a response force has enough time to interrupt the adversary before their task is completed. Another important term is critical detection point (CDP), defined as the last detection point along the adversary path after which the system response time is less than remaining adversary task time. An effective PPS reduces the risk of a successful adversary attack to an acceptable level. Risk is defined as the product of probability of an event occurring and the consequence of that event:

$$R = P * C \tag{1}$$

In this case we may assume that the probability of an attack is 1, but the concern is the probability of a successful attack, therefore [86]:

$$R = \left[P_A * P_{S|A}\right] * C \tag{2}$$

Where: P_A – Probability of adversary attack

$P_{S|A}$ – Probability of adversary success if attack occurs

C – Consequences of successful attack

The probability of adversary success if attack occurs is:

$$P_{S|A} = 1 - P_E \tag{3}$$

Where P_E represents the probability of the effectiveness of PPS.

Finally:

$$R = [P_A * (1 - P_E)] * C \tag{4}$$

The main question regarding PPS is then: what is the probability of the system effectiveness?

Probability of the system effectiveness is the probability that PPS will defeat the adversary:

$$P_E = P_I * P_N \tag{5}$$

Where P_I is probability of interruption and it is the estimate of likelihood of response force arriving before adversary completes attack.

$$P_I = (1 - \prod_{i=1}^{n}(1 - P_{D_i})) * P_C \qquad (6)$$

Where: P_{D_i} is probability of adversary detection at each detection element;

P_C is probability of communication to the response force.

Evaluation and analysis of many systems developed by Sandia National Laboratories shows that most communication systems work with probability of 0.95. Factors that may affect this probability include: lack of training of personnel for the use of communication tools, poor maintenance, dead spots in radio communication, battery life (depending on the communication equipment), or the stress experienced during an attack [37].

Probability of interruption

Probability of interruption (P_I) can be analyzed by using a simple software named EASI (Estimate of Adversary Sequence Interruption) (Figure 2). This model can analyze and calculate probability of interruption on different paths or scenarios adversaries could use during the attack, but it can only calculate one path at the time. The main idea behind the software is that the probability of interruption is based on interactions of detection, delay, response and communication in the PPS. The inputs necessary for this model are the probabilities that detection and communication functions will be successful, and delay and response as mean times for each element. The output is the probability that adversaries will be interrupted before any theft or sabotage occurs. In order to defeat an adversary attack attempt, the response force must be notified of the attempt while sufficient time remains to respond and interrupt the adversary. The detection element in

EASI model is a function of each sensor encountered by an adversary and it represents three different probabilities: probability that the detector will sense abnormal or unauthorized activities by the adversary (P_S), the probability that an alarm indication will be transmitted to an evaluation or assessment point (P_T), and the probability of accurate assessment of the alarm (P_A). Therefore, the final probability of detection is the product of these probabilities [37]:

$$P_D = P_S * P_T * P_A \tag{7}$$

Estimate of Adversary Sequence Interruption

Probability of Guard Communication		Response Force Time (in Seconds)	
		Mean	Standard Deviation
0.95		90	9.486832981

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	GAT N	0.3	e	50	0.547722558
2	GAT	0.7	e	20	0.836660027
3	GAT	0.7	e	20	0.836660027
4	DOR	0.8	e	30	0.894427191
5	DOR	0.8	e	30	0.894427191
6	OPN	0.5	e	30	0.707106781
7					
8					
9					
10					
11					
12					
				180	

Probability of Interruption:	0.811543601

Figure 2 EASI Model (example)

Delay time in the model represents the sum of times needed for an adversary to perform a certain task and to travel a given path segment. These times are usually obtained through practical exercises. Since it is not possible to predict the exact times for which adversaries will complete certain task, these times are given as an average or mean value, calculated over several attempts. Due to variations in delay values, standard deviations are included in the model [37].

Standard deviation is included in EASI model to ensure that the model is as accurate as possible. It is a measure of dispersion in a set of data or a measure of the amount that a given data point is likely to deviate from the mean [37]:

$$S_n = \sqrt{\frac{\sum_{i=1}^{n} \left(x_i - x_{avg}\right)^2}{n-1}} \tag{8}$$

For higher accuracy in the EASI model, it is necessary to have as many data points as possible for calculating standard deviation. As an alternative, in cases where there have not been enough tests to obtain a statistically significant standard deviation, tests at Sandia National Laboratory have shown that the standard deviation of a time event can be conservatively estimated at 30% of the mean [37].

The response time in the model is the time between the first alarm triggered by the adversaries and the confrontation of the adversaries and response force. This time includes: alarm communication time, time required for alarm assessment, guard communication time, time required for the guards to prepare for the response, and guard travel time.

Another input in the EASI model is the location, used to describe the point at which detection occurred during the mean time for that element: beginning, middle, or end (Figure 2). If the detection happens before the delay time starts, then the input in the location column will be (*B).* The delay time is calculated using the mean delay time for that element ± the standard deviation. If the detection happens in the middle of the delay (*M*), the calculation will take the half delay time ± the standard deviation. If it happens at the end of delay time (E), EASI uses 0 as the time delay for this task. This calculation allows the analyst to have a better and more accurate understanding of probability of interruption, because it is based on the relationship of detection and delay time at each protection element [37].

As mentioned before, the EASI model analyzes the path of adversaries to calculate probability of effectiveness of PPS. Therefore, the first step in using this model would be a selection of a specific path which would be used by the adversaries during the attack (Figure 3). This selection should be based on knowledge of the facility and reasonable assumptions about the adversaries.

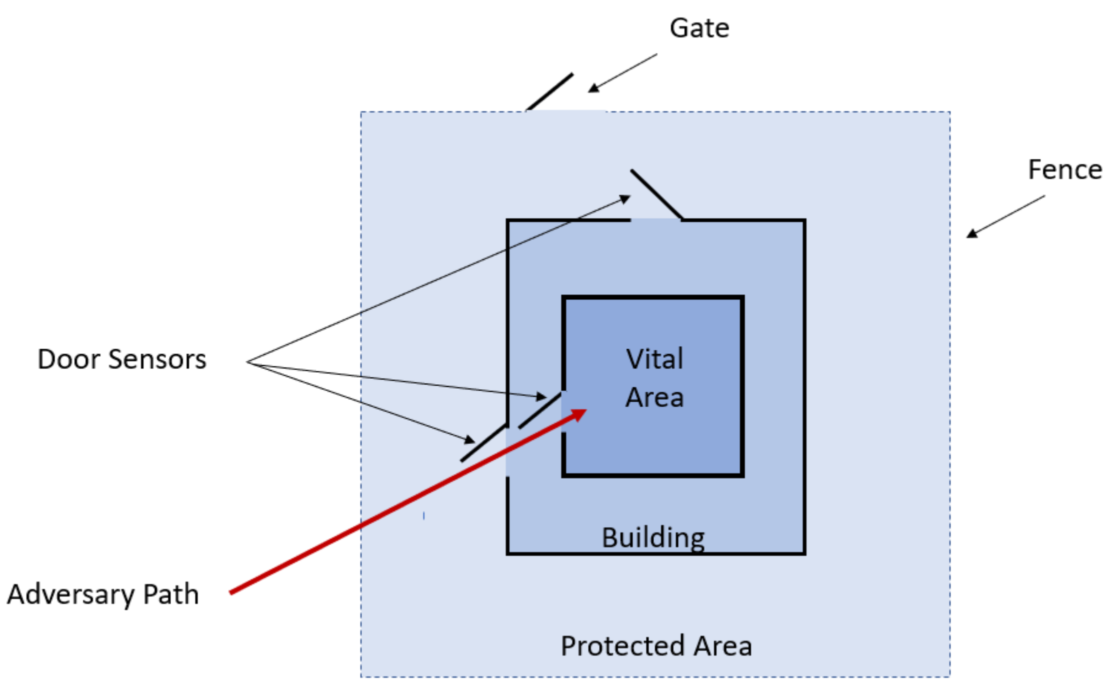

Figure 3 Adversary Path Example [37]

Paths are created using ASD (Adversary Sequence Diagram) method. This method is a graphic representation of the facility with all elements of the PPS and it shows the paths which adversaries can take during the attack. Basic steps for developing an ASD are:

1. Modeling the facility by separating physical areas;
2. Defining protection layers and path elements between the adjacent areas;
3. Finding detection and delay values for each element.

In this representation, every physical area is separated from another physical area by a protection layer, which contains the protection elements (Figure 4) [37].

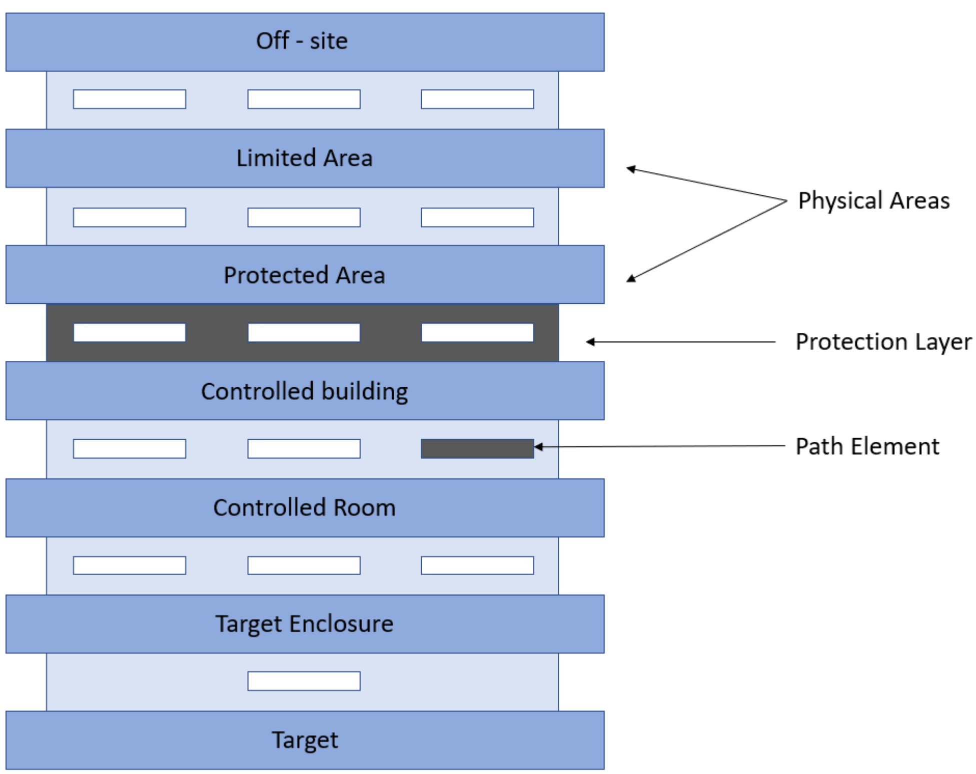

Figure 4 Basic ASD for a facility [37]

The significance of EASI model is in the adjustability of the factors. If the P_I is not high enough or acceptable with P_D and delay times, the EASI model allows to change probability of detection on certain elements or delay times and acquire acceptable P_I, while making the best economic decision and finding the least expensive way to obtain this probability.

Probability of neutralization

P_N is probability of neutralization, and it estimates the likelihood of response force preventing adversary from completing the task. It provides the information on how effective the response will be under different attack scenarios. P_N can be seen as a measure of response force capability, proficiency, training and tactics [3]. It is the probability, given interruption of the adversary by the response force, that the response force will gain complete physical control of the adversary force [87]. Response force must neutralize adversary following interruption for PPS to be effective.

$$P_N = \frac{N_{wins}}{N_{engagements}} \quad (9)$$

and

$$P_N = 1 - \left(1 - P'_{N_{i,j}}\right)^k \quad (10)$$

where $P'_{N_{i,j}}$ is the probability of winning an engagement if the weapons on both sides are the same while "i" would represent guards and "j" adversaries, and *k* is force multiplication coefficient [86].

This coefficient is used to estimate outcomes for engagements between unlike forces. The rule of two states that every level of armament difference, such as batons to pistols, or pistols to rifles is worth twice as many participants as the previous level. This gives k a value of 2 when the opponent is armed with the lesser equipment and 0.5 when the response force is underequipped [88].

Probability of neutralization is an important factor in facilities where armed conflict between response force and adversaries is expected. In order to estimate P_N, several characteristics of the adversaries and response force should be known. These characteristics include data on: weapons, number of adversaries and response officers, strategies, communication, transportation, response times, etc. for every target.

P_N can be estimated by using the neutralization tool. This estimation tool is Visual basic menu-driven tool based in Microsoft excel (Figure 5).

Figure 5 Neutralization tool (example)

For estimation of P_N using this tool, the user must input the number of security guards, number of adversaries, their weapons, and delay times. All other parameters are equal. This means that there is no difference if the adversaries are terrorists or activists, the probability for their success will be the same. Adversaries and response force officers with the same weapon category (batons, handguns, and automatic rifles) are all assumed to have the same exposure, firing rate, suppression, etc. Force multiplication coefficients are used to account for differences in weapons. The neutralization tool is based on assumptions that [87]:

- Superior weapons increase P_N for equal numbers of personnel
- Superior numbers increase P_N for equal weapons

- Response forces are counted in the battle only if they can arrive in time to interrupt, given detection at the CDP
- P_N increases when response groups arrive earlier in time versus later.

Due to its lack of precision, this tool is used only as a guidance. It is often used in combination with other tools or tabletop exercises, used before or after force on force exercises [6]. It is very helpful for training and it can help improve the probability of effectiveness of the PPS. By estimating P_N, opportunities for upgrades in the security system can be explored.

CHAPTER 4. METHODOLOGY

In order to achieve the objectives set out for this work, a methodology was created to describe the needed tasks and how they relate to their corresponding objectives. Since the research consists of several different elements, the methodology for each element is described in this chapter.

4.1. AMP

The AMP study introduces the question of regulatory efficiency and resolves whether the regulatory framework and its proposed modification justify the investment of creating, maintaining, and applying the policy. Analysis of the regulations and documents has been conducted and based on the results, suggestions for improvement were introduced. The analysis includes an investigation of every case of AMP issued in Canada since 2013 until the end of 2018, (with later adjustment for more recent cases) along with a statistical analysis of these cases. A sensitivity analysis is carried out for each factor in the calculation of the AMP penalties. The calculation formula created and used by the CNSC is examined and modified to improve the overall system, and particularly the response of the stakeholders to the AMP scheme. Furthermore, the two calculation methods are compared to show the differences in outcomes. A survey was created and approved by the Research Ethics Committee at Ontario Tech, on the possible behaviour of nuclear workers in different situations where AMP could be issued. The survey involved Department of Energy and Nuclear Engineering (formerly known as Faculty of Engineering Systems and Nuclear Science (FESNS)) students and experts in the field of nuclear energy and radiation science in academia and industry. Please see Appendix A for the survey questions. An AMP calculator was created using Visual Basic with all changes included that can be used for easy calculation of the future penalties as shown in Figure 6

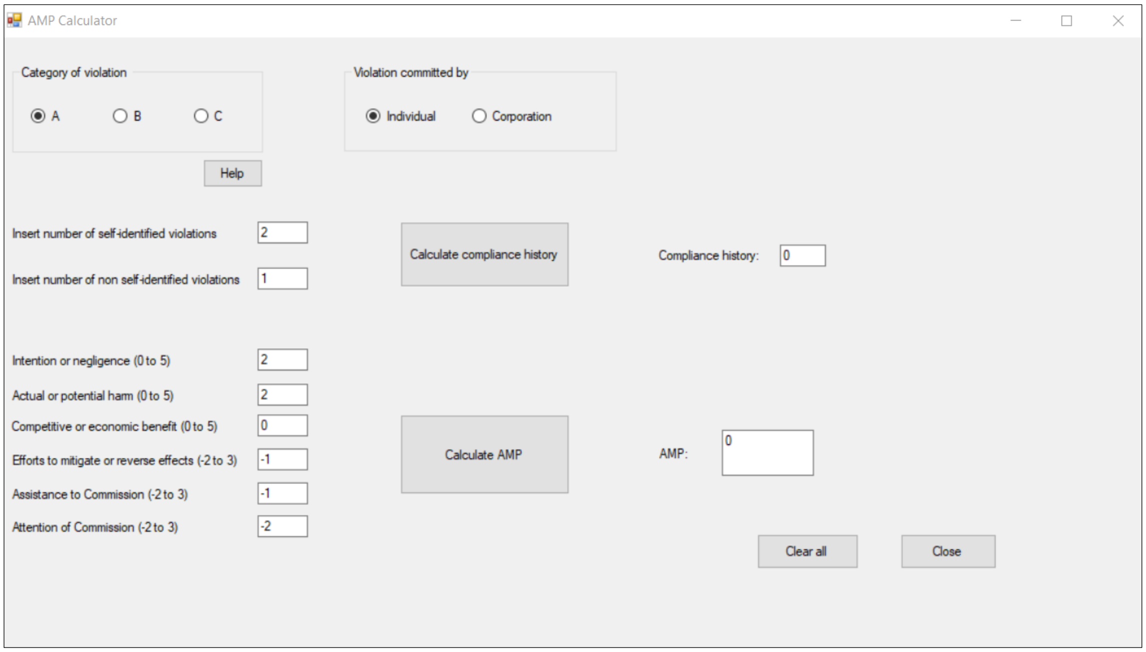

Figure 6 AMP Calculator

Additionally, comparison of AMPs in Canadian nuclear regulations and in other industries in Canada is conducted, as well as comparison of Canadian nuclear AMPs and civil penalties in nuclear industry in the US. Through this comparison best practises from other industries and countries are recommended for implementation in the Canadian AMP framework. Moreover, additional adjustments for the AMP calculations are suggested with aim to create an environment where licensees would self-report any violation and therefore provide insight for the regulator on how, when, and why violations happen with minimal changes in the AMP but significant changes in the expected outcome.

4.2. Drones in nuclear security

The research on drones describes the utilization of technologies currently available and proposes possible improvements which could be implemented to decrease costs while improving nuclear security. The idea behind this work is to assess the return on investment and give suggestions for improvement of the economic benefits in nuclear security. Comparison of costs of drones and current elements of the security systems, as well as efficiency before and after introducing drones to the security systems are modeled and analyzed, for detection, delay and response. The analysis compares response times for drones versus a team of armed security officers to an alarm, intrusion or any other security event. The main goal of the study is to see if drones can reduce alarm assessment time and therefore increase response force time and increase the probability of interrupting the adversary.

CHAPTER 5.ANALYSIS OF AMPS ROI

The following chapter will provide in-depth analysis of AMP process, calculation, and outcomes, as well as comparison with other similar industries, and comparison with similar policy in the US. Furthermore, suggestions for improvement are proposed, and analyzed for their effectiveness.

5.1. Consideration of Administrative Monetary Penalties in Nuclear Security

5.1.1. Introduction

The AMP is a tool used for discouraging non-compliance with rules and regulations in a certain area. An AMP is an administrative penalty imposed by the CNSC, without court involvement. It is used in the case of a violation of a regulatory requirement. An AMP can be applied against any individual or corporation subject to the NSCA, which regulates the development, production and use of nuclear energy and the production, possession and use of nuclear and radioactive material. However, AMPs are not the same as criminal offences. They are civil sanctions which try to secure compliance through the application of monetary penalties for non-compliance with regulatory requirements, and have been in use in the nuclear industry in Canada since 2013. AMPs are not exclusive to the CNSC and are used by several other federal and provincial government agencies, including Canadian Food Inspection Agency, Transport Canada, Canada Border Service Agency, Canadian Radio-television and Telecommunications Commission and The Financial Transactions and Reports Analysis Centre of Canada. Organizations in other countries, such as the United States, have also incorporated AMPs as a part of their regulatory regimes [16]. One of the characteristics of this system is that it can cause significant financial loss to the organization through reoccurring non-compliance and subsequent penalization [89].

AMPs are not the only tool used to ensure compliance with the NSCA. Other enforcement options include [90]:

- regular interaction (discussions/meetings/letters)
- written notice or warning
- increased regulatory scrutiny (more frequent inspections)
- an order by an inspector or designated officer
- formal request under subsection 12 (2) of the *General Nuclear Safety and Control Regulations*
- licensing action (licence hold points, suspension, revocation)
- decertification of persons or equipment
- investigation and prosecution

Enforcement options may be chosen in any order or combined with others, which creates a wide range of enforcement options.

5.1.2. AMPs in Nuclear Industry in Canada

In June 2012, as part of the Government of Canada's Responsible Resource Development initiative, amendments were made to the NSCA to authorize the CNSC to implement the AMP system to strengthen the environmental protection and to increase compliance with the NSCA and its associated regulations [91].

The CNSC has a robust compliance and enforcement program, which includes several tools to enforce compliance when requirements are not met. Some of these tools are orders, revocation of a licence, and prosecution. An AMP system should provide the CNSC with additional means for enforcement. The selection of the appropriate enforcement tool depends on factors such as the severity and risk posed by the act of non-compliance [91].

AMPs came into force in 2013, and since then over 30 AMPs have been issued [16]. These penalties do not require or create any new regulations. AMPs are only a tool for enforcing existing regulations. Also, the AMP will not be the only tool for enforcing regulations or responding to non-compliance, but only the non-compliance listed as violations in the AMPs regulations may be subject to monetary penalties.[1] Other than written orders, warnings or licensing actions the CNSC as well use prosecution for actions that are considered offences under the NSCA [92]. The reasons for the implementation of AMPs are that it is faster, and the fact that judicial proceedings often result in considerable costs to the federal government and to the individual and/or corporation involved. Unlike prosecution, an AMP is a monetary penalty that is imposed for violations of regulatory requirements. The introduction of the AMP Regulations benefits the Canadian public by allowing the CNSC to enforce requirements using an administrative process rather than resorting to prosecution in the courts. Judicial proceedings often result in considerable costs to the Government of Canada and to the individual and/or corporation involved, and may be too strict of a tool to utilize except in extreme circumstances. Prosecution is also often lengthy for all parties. An AMP system is

---

[1] A non-compliance is a regulatory requirement that has not been met. A non-compliance becomes a violation if it is listed in the schedule to the AMP Regulations and the CNSC selects AMPs as the appropriate enforcement option. [92]

relatively inexpensive to administer, and it normally results in more timely and effective enforcement than prosecution. As a result, the individual or corporation may present a case without needing a lawyer. The maximum monetary penalties under the AMP system (Table 1) are significantly less than the maximum allowed amount under the NSCA. An AMP system simply provides the CNSC with an additional tool to address non-compliance. Penalty ranges are different for individuals and corporations and are divided in three categories depending on the severity of the violation. Violations are listed under these categories in the Schedule of violations [22].

Table 1 Penalty ranges in CAD [6]

	Category A	Category B	Category C
Individual	$300 - $3,000	$300 - $10,000	$300 - $25,000
Corporation	$1,000 - $12,000	$1,000 - $40,000	$1,000 - $100,000

5.1.3. Procedure

An AMP can be applied against any individual or corporation subject to the NSCA. The CNSC may consider issuing an AMP for any of the following reasons [16]:

- Compliance is not obtained using either regular interaction or written notices.
- The non-compliance is likely to reoccur.
- There is a history of repeated non-compliance.

- The non-compliance was intentional or a result of negligence.
- Harm resulted or could have resulted from the non-compliance.
- The non-compliance was motivated by competitive or economic benefit.
- There was unreasonable risk to health, safety, the environment, security or Canada’s international obligations.
- There is a need to correct behaviour that violates requirements.

The NCSA allows both CNSC Inspectors and Designated Officers to issue AMPs. However, under the CNSC program, AMPs will be issued only by Designated Officers, on the recommendation of Inspectors, Licensing Officers, Specialists or other trained staff. Every AMP is issued in the form of a Notice of Violation (NoV) along with instructions on payment and request for review. According to the CNSC, AMPs will rarely be the first response to the non-compliance. Licensees will be given several opportunities to correct a non-compliance prior to AMPs being considered. In rare circumstances will AMPs be the first response to a non-compliance [92].

Once an AMP is chosen as an appropriate tool for the certain violation, the amount is determined using the following determining factors [92]:

- the compliance history of the person who has committed the violation
- the degree of intent or negligence on the part of the person
- the harm that resulted or could have resulted from the violation
- whether the person derived any competitive or economic benefit from the violation

– whether the person made reasonable efforts to mitigate or reverse the violation's effects

– whether the person provided all reasonable assistance to the Commission

– whether the person brought the violation to the attention of the Commission

Each of these factors is assigned a weight based on regulatory significance in order to ensure a consistent approach to determining penalty amounts. The scale of factors has six different levels officers can choose from, depending on the severity of the violation of each factor. These factors will be summed up to one final score which will be used in further calculation.

Table 2 Factors and assigned scales

	Factor	Description	Scale
1	Compliance history	Compliance history of the person who has committed the violation	0 to +5
2	Intention or negligence	Degree of intent or negligence on the part of the person	0 to +5
3	Actual or potential harm	Harm that resulted or could have resulted from the violation	0 to +5
4	Competitive or economic benefit	Whether the person derived any competitive	0 to +5

		or economic benefit from the violation	
5	Efforts to mitigate or reverse effects	Whether the person made reasonable efforts to mitigate or reverse the violation's effects	-2 to +3
6	Assistance to Commission	Whether the person provided all reasonable assistance to the Commission	-2 to +3
7	Attention to Commission	Whether the person brought the violation to the attention of the Commission	-2 to +3

Currently, the AMP calculation process consists of 5 steps:

(1) Subtract the minimum penalty amount from the maximum penalty amount of the applicable penalty range (Table 1).

(2) Assess the score for each factor and add the scores up to one final number (Table 2).

(3) Divide the total of the assessed scores by 29, which is the maximum score of the determining factors.

(4) Multiply the result from step 1 by the result from step 3.

(5) Add the minimum penalty amount for the applicable category to the result from step 4.

This formula takes into consideration all factors mentioned in the procedure, calculates total assessed score and then this total score is divided by maximal number of points from scale of regulatory significance, which is in this case 29, and this result (rounded to 2 decimal points) is multiplied by the difference between maximum and minimum amounts for that category. Finally, the minimal amount for the category is added to this amount. In this way, even if the score is zero, the minimal amount will have to be paid. This is why currently self-identification is not used very often. Moreover, even if the individual or company admit violation of the Act and have some relief as they proactively informed the Commission, they will be in a worse situation for any future violation, where even if they self-identify, they will have a bad history of compliance, and therefore pay a higher penalty. This way of penalization does not motivate self-identification of violation of the Act.

If requested, an AMP can be reviewed, by submitting a request for review to the Commission within 30 days of receiving the NoV. The Commission Members then form the Review Panel and make the decision. Once the case is reviewed, the decision is final and binding and, except for judicial review under the *Federal Courts Act*, is not subject to appeal or to review by any court [92].

5.1.4. Optimization of AMPs

As mentioned, AMPs are an important regulatory tool, with the purpose of promoting compliance. The question is if the current AMP system does that satisfactorily. It appears, currently, that there is an opportunity for improvement. So far, the practise of AMPs does not motivate operators or corporations significantly on self-identification of violations. This can be seen in previously issued penalties where only 12% of all penalties were self - identified. [93] The reason for this might be that they will be penalized with a minimal amount in the best case or have a "non-compliance" on their record. Another reason might be in the nature of violation.

In order to promote compliance and prevent violations, it is very important that all possible ways of non-compliance are recognized. This means that AMPs should help in providing insights into the different ways in which one could commit a violation listed in the schedule of violations. These insights will generate a body of knowledge, which is crucial in further development and optimization of AMPs. Concurrently, creating a body of knowledge on possible violations would also improve prevention and this can be built only if we motivate self-identification of violations.

For the purpose of this paper, violations will be classified into two categories: first – violation committed by accident, and second – violations committed on purpose. The first group represents violations that were committed without being previously planned, and without intent for achieving economic benefit. The second group of violations includes those committed in order to obtain certain benefits and previously planned. These violations will rarely or never be self – identified, therefore the aim of the research is to increase the probability of the first group self-identification, and therefore increase the body of knowledge.

Creating a body of knowledge is not easy in this situation. It requires identification of all violations, from which many tend to stay hidden for a long time. The individuals or companies do not have any interest in self-identifying the violation, as the minimum penalty is $300 for individuals or $1000 for companies.

One possible solution would be to use AMPs with some modifications so that self-identification of non-compliance would be treated with positive effect to a certain extent. This could be done by changing minimum penalties to $0. Moreover, companies and individuals would have the self-identification in the record, so if the next time a discovery of a violation is made, this would come as a redeeming feature. This would be calculated as a negative score in the determining factor, and the final score would be lower, meaning a lower final penalty. This would reduce the AMP amount for any future non-compliance.

The current AMP system takes into consideration self-identification, but in every next violation after self-identified, the first violation will be taken as “bad compliance history” which means that previous violation will increase every next penalty, regardless of self-identification. The new, revised and modified calculation process takes special notice if the previous violation was self-reported, and if it was, the points will be reduced, i.e. the amount will be reduced. This would be significant because it would motivate individuals and companies to self-report in case of violation, and in case of any other future violation they will receive benefits.

Table 3 Modified factors and assigned scales

	Factor	Description	Scale
1	Compliance history	Compliance history of the person who has committed the violation	-2 to +3
2	Intention or negligence	Degree of intent or negligence on the part of the person	0 to +5
3	Actual or potential harm	Harm that resulted or could have resulted from the violation	0 to +5
4	Competitive or economic benefit	Whether the person derived any competitive or economic benefit from the violation	0 to +5
5	Efforts to mitigate or reverse effects	Whether the person made reasonable efforts to mitigate or reverse the violation's effects	-2 to +3
6	Assistance to Commission	Whether the person provided all reasonable assistance to the Commission	-2 to +3
7	Attention to Commission	Whether the person brought the violation to the attention of the Commission	-2 to +3

The adjustment of the calculation could be done by introducing changes in two important parts of the already existing formula:

1. No minimal penalties *or* remove Step 1 from the previous calculation, and instead multiply the total score by the maximum amount for the category; remove Step 5
2. Change compliance history from 0 to +5 to -2 to +3.

After introducing these changes calculation of the penalty amount should consist of the following steps:

1. Assess the score for each factor and add the scores up to one final number (Table 3)
2. Divide the total of the assessed scores by 27, which is the maximum score of the determining factors
3. Multiply the result from step 2 by the maximal penalty for the category (Table 1)

These modifications would improve the current system because there will be no minimum penalties required in every case. Moreover, the change in factor scale from 0 to +5 to -2 to +3 there would still be 6 levels of compliance history, but it would offer negative points or "positive history" for violators in case they self-identified previous violation. This modification would reduce future penalty amounts and motivate individuals and corporations to report every non-compliance with the Act.

In addition to these modification it would be crucial to define the use of factor 1 – Compliance history. Considering all cases of AMPs issued in the previous period, this factor could be one of the reasons for subjectivity in the AMP calculations. In order to further improve this policy some changes are suggested regarding this factor. Compliance history modifications could be defined further by describing each level of the scale and determining when they will be used. This will not only help in motivation of self – identification of violations, but also prevent subjectivity in score assessment. The suggested changes in compliance history would include change factor scale from 0 to +5 to -2 to +3 and including one new level “Not applicable” (NA). This level would be used for those who did not have previous violations. In case violator has NA for compliance history the total score will be divided by 29 instead of 27. This is to make distinction between score of NA and 0. For those who had previous violations scale -2 to +3 would be used in a precisely defined way (Table 4).

Table 4 Compliance history levels

Score	Definition
NA	$si = 0 \; and \; nsi = 0$
-2	$si = 1 \; and \; nsi = 0$
-1	$si = 2 \; and \; nsi = 0$
0	$si > nsi \; and \; 2 < si + nsi \leq 4$
$+1$	$si = 1 \; and \; nsi = 1 \; or$ $si < nsi \; and \; si \leq 1 \; and \; nsi \leq 2$
$+2$	$si = 2 \; and \; nsi = 2 \; or$ $si < nsi \; and \; 2 < nsi \leq 4 \; and \; si + nsi \leq 6 \; or$ $si > nsi \; and \; 4 < si + nsi \leq 6$

$+3$	$si = nsi = 3\ or$ $si < nsi\ and\ nsi > 4\ or$ $si + nsi > 6$

**si: self – identified; nsi: not self – identified*

While the proposed modifications do not alter the structure of the current system fundamentally, they do introduce significant improvement to the outcome. The change of the outcome is shown in the graph (Figure 7) where issued penalties are recalculated according to the new formula and compared.

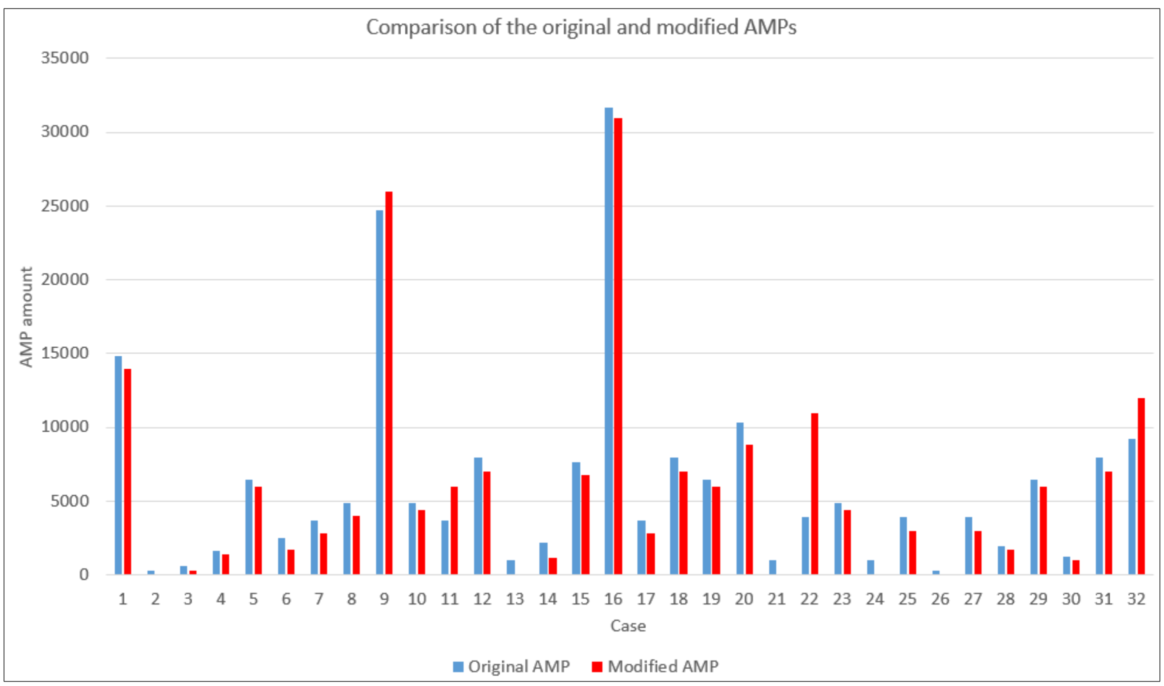

Figure 7 Comparison of the original and modified AMPs

In this modified AMP system if a person commits a violation listed in the schedule, self – identifies and reports, the amount will be significantly lower for the first violation. If the same person commits additional violations after the first self – reported, every subsequent violation will be penalized, but the amount would be lower than if the violations were discovered by inspection due to good non-compliance history. The example is shown in Table 5, which shows the case of the violation a person committed for the first time if this violation was self – identified and reported.

Table 5 Comparison of the original and modified AMP - For the first violation

Factor	Original AMP	Modified AMP
1. Compliance history	0	NA
2. Intention or negligence	+2	+2
3. Actual or potential harm	+2	+2
4. Competitive or economic benefit	0	0
5. Efforts to mitigate or reverse effects	-1	-1
6. Assistance to Commission	-1	-1
7. Attention to Commission	-2	-2
Final penalty	$300	$0

The second case shown in Table 6, represents a case of a repeated violation, where the same person from the first case committed second violation which was also self – identified and reported.

Table 6 Comparison of the original and modified AMP - For the second violation

Factor	Original AMP	Modified AMP
1. Compliance history	+1	-2
2. Intention or negligence	+2	+2
3. Actual or potential harm	+2	+2
4. Competitive or economic benefit	0	0
5. Efforts to mitigate or reverse effects	1	1
6. Assistance to Commission	-1	-1
7. Attention to Commission	-1	-1
Final penalty	$1658	$400

In both cases, the difference in the amount between the original and modified AMP is significant, which should motivate individuals and corporations to report any non – compliance with the Act. Moreover, it is important that in cases where violations are not self – reported but discovered through inspection or in any other way, the amounts between the original and modified AMPs will not differ significantly, which shows that impact of these modifications will mainly be on the self – identification. While the factor 7 acknowledges the self-identification for the current violation, it does not take into consideration previous cases, which is the role of the factor 1. Introducing changes to factor 1 would significantly improve the system and take all the previous violation into account.

5.1.5. Survey

A survey was conducted at the University of Ontario Institute of Technology (UOIT) to discover if the proposed changes would make the anticipated difference. The survey was sent to all undergraduate and graduate students of the nuclear engineering program of this university, as they would be, the future workers in the nuclear industry, the most relevant subject of the survey. The survey was voluntary, anonymous, and was approved by the UOIT Research Ethics Board - REB 15003 - on October 26, 2018. 32 individuals have participated in this survey.

The results of the study have shown that the baseline is 65.6% who would self-report under the current system. Removing the negative effect on the compliance history could increase self-identification by 18.8% (84.4%). This would increase a further 2.7% (87.1%) if there was no monetary penalty or a negative compliance history. Having a positive compliance history (good behaviour) would increase the self-identification by a further 6.4% (93.5%).

The most effective way of ensuring higher self-reporting appears to be reducing the impact on the compliance history, followed by a positive (rewarding) compliance history. The monetary penalty in comparison seems to be of a lesser importance, accounting for a mere 2.7% incremental change to the total self-reporting percentage, compared to a more substantial 25.2% increase due to the compliance history effect.

5.1.6. Conclusions

AMPs are not a substitution for any existing tool. They are, however, highly significant as they represent the only tool which could provide a body of knowledge on potential violations of the Act since they could motivate self-identification and reporting of a non-compliance. This is important for the nuclear industry, but it could be important for other low-probability high-consequence industries. The modifications presented in this paper, show significant improvements to current systems can be made with minimal interference with the existing implementation. This outcome is significant to ROI, as with minimal investment in modification there is a significant change in the desired outcome of the policy.

Addendum

Since the paper was published in 2018, there were additional AMPs given to licensees in Canada. The summary of the post 2018 AMPs are given in Figure 8 Comparison of AMPs issued after 2018 The review of the latest penalties and their comparison to their modified versions shows that those with no previous history (case 1) or more importantly - with (previously) self identified violations (case 4) would receive $0 penalty, however those with multiple violations that were not self reported but discovered during an inspection would receive somewhat higher penalties (e.g. cases 3, 5, and 9). The modified AMP would create revenue that is approximately 6% lower than the original (overall since 2013, with original AMP generating $334,778, and if modified formula is used the amount generated would be $313,680), which should not be considered significant, as it would promote and motivate self reporting of violations and reduce the amount of time (and cost) inspectors would have to spend on each specific case.

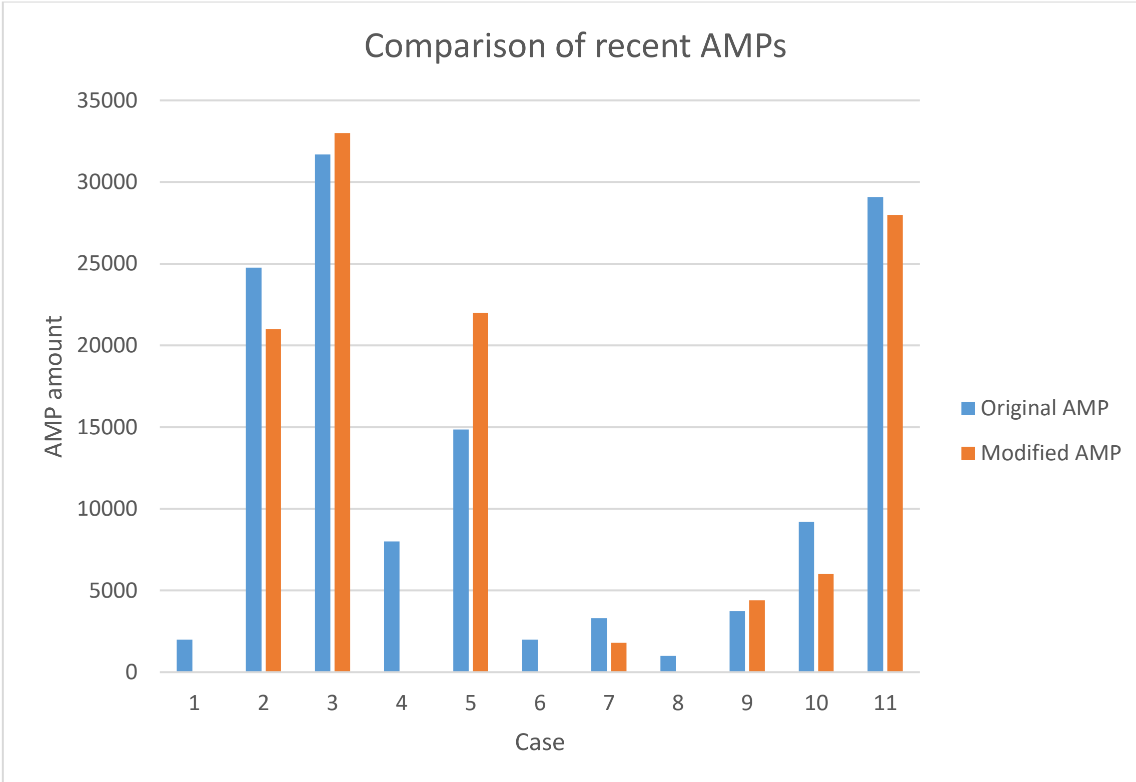

Figure 8 Comparison of AMPs issued after 2018

5.2. AMP Application Disparity Across Nuclear and Other Industries in Canada and United States

5.2.1. Comparison of nuclear AMPs with other industries in Canada

Canadian Transportation Agency (Aviation and Railway)

The aviation industry is presumably the most comparable to nuclear when it comes to the probability and consequences of an accident. Safety and security in these industries are more similar than initially perceived: insider threats, cyber security, human reliability, regulations, and the implementation of efficient and effective security systems [94] are some of the safety and security aspects that these industries have in common.

Canada Transportation Act regulates AMPs issued for air transportation and railway. The similarity between AMPs in transportation and nuclear industry is that the notice of violation is served to a person or a corporation who may then pay the indicated amount, or request a review of the penalty [95].

AMPs in transportation are created under the Canada Transportation Act and regulated by the Canadian Transportation Agency (CTA). Penalties according to this policy are fixed and prescribed for each violation [96]. In contrast to the CNSC's AMP, there is no precise calculation. Under the Canada Transportation Act the penalty amounts are determined by the severity of the violation (administrative, minor, serious, and very serious) and they are in range from $50 to $1,000 for individuals (or $500 to $5,000 for corporations) for the first violation, while every next violation is doubled, up to the maximum amount of $25,000 [95]. One deviation from the rules is under certain provisions of the Air Transportation Regulations (Part VII), Personnel Training for the Assistance of Persons with Disabilities Regulations, Accessible Transportation for Persons with Disabilities Regulations, and Accessible Transportation Planning and Reporting Regulations, where these penalties can go from $2,500 to $50,000 for the first violation, and up to $250,000 for repeated violations [95] [97].

Unlike the nuclear industry, where the notice of violation or the amount of penalty is only decided upon by CNSC's designated officers and inspectors, in the Canadian Transportation Act AMP, the Minister of Transport has an important role. In addition to the CTA, the minister may also prescribe a maximum amount payable for each violation, but as is the case with the CTA, the amount shall not exceed

$5,000, in the case of an individual, and $25,000, in the case of a corporation. The minister may also dictate contraventions other than those mentioned in the Act, to be considered as violations of the law [96]. The CTA or the minister may designate persons as enforcement officers who are authorized to issue notices of violation. They may also establish the form and content of notices of violation [96].

Once a NoV has been issued, the CTA may, upon request by a regulated entity, enter into a compliance agreement subject to terms that CTA considers appropriate for the purpose of ensuring the entity's compliance with its legal obligations. The terms may include a provision for the deposit of reasonable security as guarantee that the person will comply with the agreement and may provide for the reduction, in whole or in part, of the amount of the penalty [95]. If the CTA is of the opinion that a person/corporation who has entered into a compliance agreement has not complied with it, then they will be liable to pay an amount that is twice the original amount in the notice of violation. This is called the Notice of Default. The CTA may publish information about any violation for the purpose of encouraging compliance with the Canadian Transportation Act [96].

National Energy Board

In Canada, the Canada Energy Regulator (CER) is an independent federal agency responsible for regulating pipelines, energy development and trade in the Canadian public interest. AMP regulations were introduced in 2013 under the previously enacted National Energy Board Act (in 2019 replaced with the Canadian Energy Regulator (CER) Act), allowing the Regulator to impose financial penalties on companies or individuals for non-compliance with the Act, regulations, decisions, permits, orders, licenses or certificate conditions intended to promote safety or environmental protection. The CER Act continued to have the same provisions for AMPs. In 2016, changes to the Canada Oil and Gas Operations Act (COGOA) came into effect to also allow the CER to issue AMPs for designated violations under this Act [98].

Under the CER Act, the Chief Executive Officer of the CER has the power to designate persons authorized to issue notices of violation (AMP Officers). AMPs will be issued in the form of NoV from the CER's head office [98].

The AMP sections in the Acts set out the maximum daily penalties for both individuals and corporations. For individuals the maximum daily penalty is $25,000 for each violation, and for corporations the maximum daily penalty is $100,000 per violation. The Acts states that each day that a violation continues is considered to be a separate violation. Therefore, one incident could result in more than one violation, with no maximum total financial penalty [99].

The process of AMP is:

1. Notice of violation (NoV) is served to the person/corporation
2. Basic info of the violator is published on the external website
3. Review (if requested)
4. Payment
5. NoV is published on the external website [98].

According to the AMP Regulations the violations could be classified under two categories. Type A violations, which may involve a failure to submit, report, notify, or record information; and type B violations which may involve the contravention of an order or a decision made under the CER Act or the failure to comply with a term or condition of any certificate, license, permit, leave or exemption that is granted under the CER Act [98].

The calculation of the penalty starts with determination of a baseline penalty that can be increased or decreased using a number of adjustment factors that are listed in the AMP Regulations. The base penalties are:

Table 7 Base penalties in CAD [100]

Category	Individual	Corporation
Type A	$1,365	$5,025
Type B	$10,000	$40,000

There are nine adjustment factors that affect the baseline penalty. These factors are designed to promote certain behaviors such as prompt voluntary reporting, undertaking mitigation actions quickly, and taking steps to prevent the recurrence of a violation. The factors are also intended to deter behaviors such as negligence, repeat violations, and financial gain from a violation [98].

Table 8 Adjustment factors [98]

	Factor	Effect on gravity value
1.	Whether the person who committed the violation has other violations in the previous 7 years	0 to +2
2.	Whether the person derived any competitive or economic benefit from the violation	0 to +2
3.	Whether the person made reasonable efforts to mitigate or reverse the violation's effects	-2 to +2
4.	Whether there was negligence on the part of the person who committed the violation	0 to +2

5.	Whether the person provided all reasonable assistance to the Board with respect to the violation	-2 to +2
6.	Whether the person, after becoming aware of the violation, promptly reported the violation to the Board	-2 to +2
7.	Whether the person has taken any steps to recurrence of the violation	-2 to +2
8.	For type B violations, whether the violation was primarily a reporting or record-keeping requirement failure	-2 to 0
9.	Whether there are any other aggravating factors in relation to the risk of harm to people or the environment	0 to +3

The National Energy Board prescribes exact penalty amounts for each gravity level (from -3 or less to +5 or more) as shown in Table 9 [101]. The increase is approximately 30% of the base penalty for each additional level.

Table 9 Penalties in CAD [101]

Gravity Level	Type A Violation		Type B Violation	
	Individual	Any Other Person	Individual	Any Other Person
–3 or less	$250	$1,000	$1,000	$4,000
–2	$595	$2,375	$4,000	$16,000
–1	$990	$3,750	$7,000	$28,000
0	$1,365	$5,025	$10,000	$40,000
1	$1,740	$6,300	$13,000	$52,000
2	$2,115	$7,575	$16,000	$64,000
3	$2,490	$8,850	$19,000	$76,000
4	$2,865	$10,125	$22,000	$88,000

5 or more	$3,000	$12,000	$25,000	$100,000

In the interest of greater public transparency, the CER posts issued AMPs on its Compliance and Enforcement webpage. This information includes the name of the company believed to have committed the violation, the issue date, the region and facility, the nature of the violation, and the amount of the penalty. Unlike the AMPs used in the nuclear industry, for most violations, the name of an individual, if applicable, will not be published [98].

Canada Consumer Product Safety Act

The Canada Consumer Product Safety Act (CCPSA) is not similar to the Nuclear Safety Act as it does not belong to a similar industry branch, but it is significant since the violation of this Act may affect health of many Canadians. Therefore, for completeness, the analysis of AMPs under CCPSA will be compared to CNSC AMPs.

The regulating body under CCPSA is Health Canada, which uses a number of compliance and enforcement tools to ensure compliance with the Act. Failure to comply with some of these tools may result in Health Canada issuing a NoV. As well as Health Canada, the Minister of Health may issue a NoV. If the Minister believes on reasonable grounds that a consumer product is a danger to human health or safety, they (or a designated officer) may order a person who manufactures, imports or sells the product for commercial purposes to recall it [102]. As a part of a NoV, a person or a company may be required to pay a financial penalty (AMP). The AMP is a compliance and enforcement tool that assigns a penalty to those that do not comply with an order made under the CCPSA. The penalty is based on the compliance history, the type of order violated and the classification of the alleged violation [103].

Under the CCPSA's AMP violations are classified as [104]:

- minor, if the total gravity factor for the violation is two;
- serious, if the total gravity factor for the violation is three or four; and
- very serious, if the total gravity factor for the violation is five.

The gravity factor is calculated based on history of violations and type of violation. History gravity factors are [104]:

> 0 - No previous violation in respect of which a notice of violation was issued was committed by the person within the five years before the day on which the violation is committed;
>
> 1 - One violation in respect of which a notice of violation was issued was committed by the person within the five years before the day on which the violation is committed;
>
> 2 - More than one violation in respect of which a notice of violation was issued was committed by the person within the five years before the day on which the violation is committed.

According to the type of the violation the gravity factor may be [104]:

> 2 - Failure to comply with an order by the Minister to take measures — person did not comply with an order made under section 12 of the Act

2 - Failure to comply with an order by the Minister to take measures — Minister believes on reasonable grounds that a product is the subject of a voluntary measure or recall

2 - Failure to comply with an order by the Minister to take measures — Minister believes on reasonable grounds that there is a contravention of the Act or its regulations

3 - Failure to comply with an order by the Minister to recall a product

3 - Failure to comply with an order by the Minister to take measures — Minister has already made an order under section 31 of the Act

AMP amounts differ based on total gravity factor and if the violation was committed by a non-profit organization, or any other organization. The amounts in each specific case are given in Table 10.

Table 10 Penalties in CAD [104]

	Total Gravity Factor (Classification of Violation)	Penalty for Violation Committed by a Non-profit Organization or by any Other Person for Non-commercial Purposes	Penalty for Violation Committed in any Other Case
1	2 (minor)	\$1,000	\$10,000
2	3 (serious)	\$2,000	\$15,000
3	4 (serious)	\$3,500	\$20,000
4	5 (very serious)	\$5,000	\$25,000

There are alternatives to payment: the AMP may be adjusted (reduced) if a person named in the NoV requests to enter into a compliance agreement with the Minister that ensures the person's compliance with the order to which the violation relates (at the discretion of the Minster or delegated authority). Alternatively, the person may request a review of the AMP, however, the penalty may still be payable, depending on the results of the review [102]. The penalty for a violation may be reduced if the payment is provided no later than 15 days from the day of NoV. The full penalty has to be paid within 30 days of the NoV [104]. A violation that is continued on more than one day constitutes a separate violation for each day on which it is continued [102]. This is similar to the National Energy Board AMPs, showing a wider industry adoption.

The Governor in Council may make regulations, and introduce changes in respect to each violation. He or she may also introduce regulations to increase or reduce penalty amount in respect of circumstances under which the violation was committed [102]. This does not improve the objectivity of the AMP.

5.2.2. Civil penalties in nuclear industry in the US

Similar to Canadian regulations, the US has its own version of the AMP in the form of the civil penalty. The purpose of the civil penalty is to [105]:

1. Deter noncompliance by emphasizing the importance of compliance with Nuclear Regulatory Commission (NRC) requirements,
2. Encourage prompt identification and comprehensive correction of violations of NRC requirements

Like AMP, civil penalties may be imposed in cases of regulatory violations, and they consist of Notice of Violation (NoV) and, in some cases, a financial penalty.

The importance of reporting of any changes or issues, and more importantly violations, is recognized by the NRC: “Even inadvertent reporting failures are important because many of the surveillance, quality control, and auditing systems on which both the NRC and its licensees rely in order to monitor compliance with safety standards are based primarily on complete, accurate, and timely recordkeeping and reporting.” [12].

The regulatory body in the US is the NRC. All regulations are made under the Atomic Energy Act of 1954 and the Energy Reorganization Act (ERA) of 1974. The Atomic Energy Act is the fundamental US law on both the civilian and the military uses of nuclear materials. It authorizes the NRC to impose civil penalties for the violation of certain provisions of the Act [106]. Under the Atomic Energy Act, the US Government has issued a General Statement of Policy and Procedure for NRC Enforcement Actions (NUREG-1600). It is important to note that NUREG-1600 is a policy statement and not a regulation. It describes the enforcement policy and procedures that the NRC intends to follow in initiating and reviewing enforcement actions in response to violations of NRC requirements, however, the NRC may deviate from it as appropriate under the circumstances of a particular case [12].

The NRC’s goal is to protect health and safety of people, promote security, and protect the environment through regulation of nuclear materials. This is achieved through specific activities [105]:

- Regulation and guidance: rulemaking, guidance development, generic communications, standards development
- Licensing, decommissioning, and certification
- Oversight: inspection, performance assessment, enforcement, allegations, investigations

- Operational experience: events assessment, generic issues
- Support for decisions: research activities, advisory activities, adjudication.

Based on the NRC's evaluation of noncompliance, the appropriate action in case of regulatory violations could include refraining from taking any action, taking specific enforcement action, issuing orders, or providing input to other regulatory actions or assessments, such as increased oversight (e.g., increased inspection). Each enforcement action is dependent on the circumstances of the case. However, the licensees who are not able to achieve and maintain adequate levels of safety will not be allowed to continue licensed activities [12].

Civil Penalty Process and calculation

The NRC's enforcement process has the following basic steps [105].

1. Identification of violations.
2. Assessment of the severity and significance of the violation.
3. Disposition the violation.

After identification of the violation, a notice of violation is issued to the person charged. When receiving the notice, the person is informed that the civil penalty may be fully paid, or the proposed penalty may be protested in its entirety or in part, within 20 days, by a written answer, either denying the violation or showing special circumstances which would justify the violation. The outcome of this answer could be an order dismissing the proceeding or imposing, mitigating, or remitting the civil penalty. After this order the person can request a hearing. Following the hearing the order is issued to announce the outcome of the hearing [107].

The next step is to determine the significance of the violation. There are four specific factors to consider [105]:

a. actual safety or security consequences;

b. potential safety or security consequences;

c. potential for impacting the NRC's ability to perform its regulatory oversight function; and

d. any willful aspects of the violation.

The NRC factors are defined in regulatory guidance documents for the purpose of clarity of the regulations [12]:

- **Actual safety consequences** are actual onsite or offsite releases of radiation, onsite or offsite radiation exposures, accidental criticalities, core damage, loss of significant safety barriers, loss of control of radioactive material or radiological emergencies.
- **Potential safety consequences** are considered those which according to the NRC, have realistic likelihood of affecting safety.
- **Potential for impacting the NRC's ability to perform its regulatory function** is an interesting issue for our comparison. These would include: failure to provide complete and accurate information, failure to notify the NRC about any changes in licensed activities, reporting failures [12]. This

could be compared to “Assistance to Commission” (factor 6) and “Attention to Commission” (factor 7), in the Canadian AMP policy. The main difference here when the NRC and CNSC factors are compared is that in the NRC factor there is no positive outcome, this factor can only increase the penalty. However, in the CNSC penalties, factors 6 and 7 may bring relief to the violator, by reducing the penalty in case the violator provided assistance to the Commission and brought the violation to their attention.

- **Willfulness** is another interesting point to compare US and Canadian regulations. Both the CNSC and the NRC see the willful violation as a particular problem, and violations which have the element of willfulness are considered more significant. This is due to the fact that the “regulatory program is based on licensees and their contractors, employees, and agents acting with integrity and communicating with candor”. In case of a willful violation, the NRC retains the right to determine a civil penalty which might be up to three times base penalty, in spite of civil penalty process, where maximum amount would be 2 times base penalty. Also, this penalty could be mitigated or escalated, based on a merit of a specific case [105]. According to the NRC, the term "willfulness" embraces a spectrum of violations ranging from deliberate intent to violate or falsify to and including careless disregard for requirements. The economic or other advantage, gained as a result of the violation is also included under this factor [12]. While the NRC sees this as one factor, the CNSC separates intention or negligence (factor 2) from violations which are committed intentionally and have economic gain as the final goal (factor 4).

Not every regulatory violation has the same safety significance. Some violations have more safety implications than others and this is important in determining civil penalty. A process called Significance Determination Process (SDP) is used to determine the safety significance of most inspection findings at commercial nuclear power plants. Depending on their significance, inspection findings are assigned colors of green, white, yellow, or red. For those violations which are considered to be minor ("green") notice of violation may be issued, licensee must correct the violation, and they will be noted as violations of minor significance that are not subject to further enforcement action. For other violations which are assessed to have moderate ("white"), substantial ("yellow"), or high safety significance ("red") the NoV will be issued, and the civil penalty will be enforced. The NRC reserves the use of discretion for particular cases, in accordance with the Atomic Energy Act of 1954 [12].

Apart from safety significance, the NRC categorizes violations according to severity. There are five severity categories (SL I-IV, and minor violations). Severity level I is assigned to violations that are the most severe and Severity level IV violations are the least severe. Minor violations are less then SL IV. There is usually no enforcement action or documentation required for minor violations, but they have to be corrected [105].

Civil penalties are considered only for certain categories of safety significance and severity levels: Only violations associated with inspection findings evaluated through an SDP that involve actual consequences may receive civil penalties as well as, and violations that have SL I - III.

Before the enforcement action, the NRC may call for a pre-decisional enforcement conference. This is the opportunity for the NRC and licensee to meet and discuss what were the causes of the violation, what corrective measures could be taken, and how significant the violation is. The NRC uses this information in determining the appropriate enforcement action [12].

A NoV starts the enforcement process for violation of regulation. After issuing a NoV, the NRC can ask the licensee to provide a written statement in which they describe the details of the violation and corrective measures, if any. Some of these statements may be given under oath (for severity levels I-III, or greater safety significance). For minor violations (low safety significance) there may be no further enforcement actions, but for more serious violations a civil penalty will be calculated and charged.

The next step is determining the base penalty for the violation. The NRC divides violations into different levels based on the severity level, and class of licensee. For this purpose, the NRC created base penalty tables [108]. Base penalties are adjusted on annual basis to account for inflation. Table 11 shows base penalty depending on the class of licensee in 2024, and Table 12 shows what percent of the base penalty will be applied, depending on severity level of the violation.

Table 11 Base penalties in USD (Class of licensee) [108]

	Class of licensee	Base penalty
a.	Power reactors and gaseous diffusion uranium enrichment plants, and high-level waste repository	$360,000
b.	Fuel fabricators authorized to possess Category I or II quantities of SNM and uranium conversion facilities	$180,000

c.	All other fuel fabricators, including facilities under construction, authorized to possess Category III quantities of SNM, industrial processors, independent spent fuel and monitored retrievable storage installations, mills, gas centrifuge and laser uranium enrichment facilities	$90,000
d.	Test reactors, contractors, waste disposal licensees, industrial radiographers, and other large material users	$36,000
e.	Research reactors, academic, medical, or other small material users	$18,000
f.	Loss, abandonment, or improper transfer or disposal of regulated material, regardless of the use or type of licensee: 1. Sources or devices with a total activity greater than 3.7×10^4 MBq (1 Curie), excluding hydrogen-3 (tritium) 2. Other sources or devices containing the materials and quantities listed in 10 CFR 31.5(c)(13)(i) 3. Sources and devices not otherwise described above	$54,000 $17,000 $7,000
g.	Individuals who release safeguards information	$9,000

For SL I – III the licensee will receive a penalty that is 100%, 80% or 50% of base penalty respectively for their class Table 12, while SL IV or minor violations may result in corrective actions only.

Table 12 Base Penalties (Severity Level) [105]

Severity Level	Base Civil Penalty Amount (Percent of amount listed in Table 11)
I	100%
II	80%
III	50%

After deciding on the base penalty, every violation is measured against four decisional points. These are [12]:

1. whether the licensee has had any previous escalated enforcement action (regardless of the activity area) during the past 2 years or past 2 inspections, whichever is longer;
2. whether the licensee should be given credit for actions related to identification;
3. whether the licensee's corrective actions are prompt and comprehensive; and
4. whether, in view of all the circumstances, the matter in question requires the exercise of discretion.

The outcome of this assessment could be [12]:

- no civil penalty,
- a base civil penalty, or
- a base civil penalty escalated by 100 percent.

The decision process is shown in Figure 9 Civil penalty calculation process:

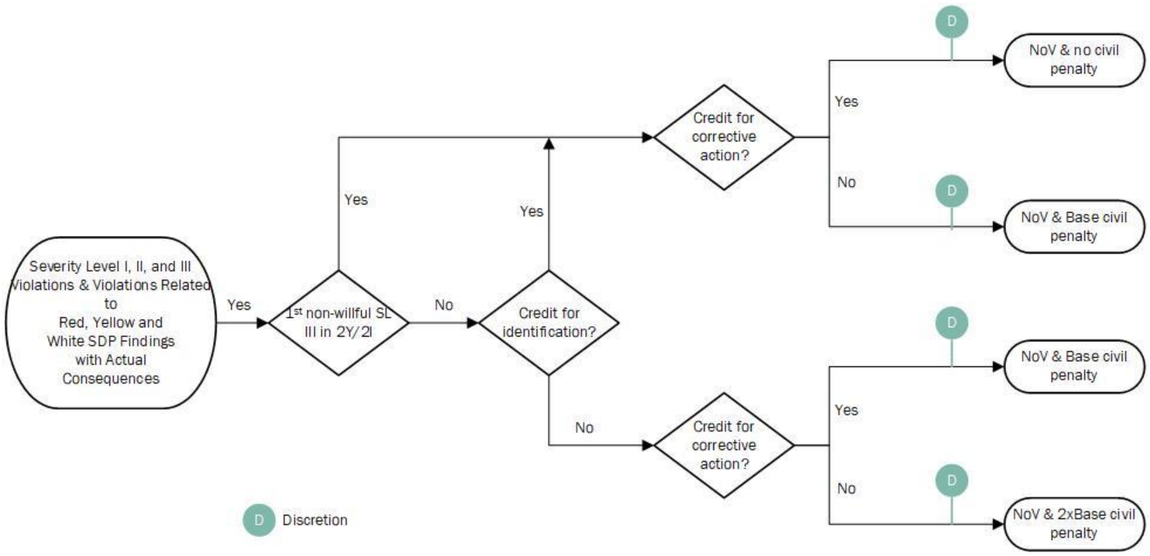

Figure 9 Civil penalty calculation process [105]

After establishing that a violation has occurred the NRC should decide if this violation is non-willful, happening for the first time in a 2-year period, or for the first time in 2 inspection periods. This means that the violation is not repetitive [105]. If this is the case, the NRC shall determine if credit for corrective action should be given, which means that the licensee took prompt and comprehensive action to correct, or reverse the effects of the violation. If so, the NoV will be issued without a civil penalty. Otherwise, the NoV will be issued with a base penalty for the specific class of licensee and severity level of violation (Table 11, Table 12). In case of a repetitive violation, the NRC shall determine if the licensee should receive a credit for identification. This step implies that the licensee who identifies the violation recognizes the existence of a problem and understands that corrective action is needed. When the violation is identified by the licensee, the next step is to define if the credit for corrective action should be assigned. This will (just as in the previous case) lead to NoV without a civil penalty, or NoV with the base penalty, if corrective measures were not implemented. In case the licensee did not identify the violation, it is necessary to determine if corrective actions were taken, but in this case the outcome will be different: if corrective actions are taken the licensee will receive a NoV and the base penalty, and if not, they will receive NoV and civil penalty in the amount of 2 base penalties for the specific class of licensee and severity of violation (Table 11, Table 12). In all the cases above the NRC may exercise discretion by either escalating or mitigating the amount of the civil penalty determined after applying the adjustment factors to ensure that the proposed civil penalty reflects all relevant circumstances of the particular case. However, a civil penalty for any violation will never exceed the statutory daily limit [105].

When calculating the penalty amount, the NRC also considers the ability to pay. This is done in order to protect the licensee's business, because NRC's intention is not that the economic impact of a civil penalty be so severe that it puts a licensee out of business or affects their ability to safely conduct their activities. The NRC finds that the civil penalties have the best effect if the ability to pay is considered, therefore the tables are not the final amount, but the recommended amounts which may be decreased or increased to reflect the licensee's ability to pay [12].

In some cases, the enforcement actions will involve individuals. This may happen if the individual deliberately causes or would have caused, if not detected, a licensee to be in violation of any regulation, or if they deliberately submit materially inaccurate or incomplete information to any relevant party. NoVs and Orders are examples of enforcement actions that may be issued to individuals, while the civil penalties are issued only in specific situations. According to the Act, the NRC may issue a civil penalty to any individual who deliberately releases Safeguards Information [105].

The NRC recognizes the importance of the civil penalty for prevention of future violations: “Civil penalties are designed to deter future violations both by the involved licensee and other licensees conducting similar activities. Civil penalties also emphasize the need for licensees to identify violations and take prompt comprehensive corrective action. […] Civil penalties are used to encourage prompt identification and prompt and comprehensive correction of violations, to emphasize compliance in a manner that deters future violations, and to serve to focus licensees' attention on significant violations.” [12].

5.2.3. Comparison of Canadian AMPs and US Civil penalties

In nuclear industry in Canada AMPs are calculated based on 7 factors during a single stage process, however in the US there are two stages with different factors against which the violation is compared. These factors are shown in Table 13. In order to compare Canadian and US monetary penalty policy, it would be beneficial to find common areas to compare. Table 13 contains the summary of factors in Canada and US, aligned in a way to show similarity and common factors.

Table 13 Canadian versus US factors (violation significance)

Canada (CNSC)	**US (NRC)**	
	Determine the significance of the violation (Stage 1)	***Determine final penalty (Stage 2)***
1. Compliance history		1st non-willful violation
2. Intention or negligence	Any willful aspects of the violation	

3. Actual or potential harm	Actual safety consequences	
	Potential safety consequences, including the consideration of risk information	
4. Competitive or economic benefit	Any willful aspects of the violation	
5. Efforts to mitigate or reverse effects		Corrective actions
6. Assistance to Commission	Potential for impacting the NRC's ability to perform its regulatory function	
7. Attention to Commission		Identification of violation

From Table 13 it could be concluded that factors for violation assessment are very similar, however, the CNSC and the NRC have different approaches to this assessment. The CNSC will assess the violation comparing it to all seven factors at the same stage and assign the value to each factor in order to calculate final penalty. NRC will cover these factors through different stages of assessment, as necessary. For the NRC these factors are descriptive, without any numeric value, but their value is binary: Yes and No, and it leads to the final penalty through a path based on these answers.

5.2.4. Suggestions for improvement

Keeping in mind the severities of consequences that may rise from violations of regulations in the nuclear industry, the CNSC's AMP regulations should be adjusted in order to incorporate best practices from other industries with potentially high consequences. One of the underlying problems, apart from hidden violations [109], is late reporting [110]. As per Vucicevic and Waller, around 12% of all AMP cases in Canada between 2013 and 2018 were self-identified and reported late, weeks or months after the violation was committed, meanwhile 19% were self-identified and reported, and the rest of the cases (69%) were not self-identified but discovered through other means [109] [111]. With the recent data included, total perspective doesn't shift significantly. For all cases between 2013 - 2024 the percentage of self-reported cases is approximately 25% which includes late self-identification, and cases that were discovered by inspection or means other than self-reporting reached approximately 75% [112].

Knowing the nature of nuclear and radiological materials, it is important to prevent any delay in reporting violations, in order to minimize or prevent any negative outcomes. This could be accomplished by adopting the approaches of the National Energy Board or Consumer Product Safety Act, where each day of violation is treated as a new violation.[2] With some modification this rule may be applied in CNSC's AMP regulations. If this is applied, it would allow CNSC to issue a new AMP for each day a violation is not reported. The CNSC could issue AMPs for each day of the violation retroactively, once the violation is reported or discovered by a CNSC inspector. This could encourage violators to self-report immediately after the violation is committed in order to avoid increasing number of violations, which would cause not only monetary loss to the violator, but would also affect compliance history factor in the future penalty calculations [109]. Other, less aggressive options, would be:

[2] This practise is currently inconsistent and it is based on designated officer discretion.

- introduce a short grace period for reporting (e.g 24-48 hours following the incident), after which an AMP is issued for each day or non-reporting, or
- introduce a late penalty, which would have to be paid for each day a violation is not reported, but without resulting in a separate AMP for each day and therefore would not affect compliance history.

Compliance agreements, which are in use in the Canada Transportation Act and Canada Consumer Product Safety Act, could also be considered for CNSC AMPs. If the regulations stipulated that only self-identified cases may be considered for this agreement, this would further promote self-identification.

The difference between nuclear and other industries, such as aviation and railway, is that in nuclear industry in Canada an AMP is calculated for each specific case, using factors to assess each violation. This may provide a higher level of objectivity and fairness, since violations will rarely have the exact same circumstances, and calculating a penalty based on the conditions and circumstances of each case is important.

As previously mentioned, the NRC has a different approach to civil penalties. The NRC adjusts base penalties each year to account for inflation and that is something Canadian AMPs do not take into consideration. Bearing in mind the economic changes that occur, and inflation rates, it is safe to say that AMPs should be adjusted on a yearly basis as well, as the penalties which were created in 2013 cannot have the same impact 10 years later.

Another good practice of the US NRC Civil penalties is taking into consideration the size of the company, or their income. This is introduced in order to protect a licensee's business, and the safety of their activities. This practice could be easily applied in Canada. The CNSC's AMPs could be calculated as a percentage of a licensee's yearly net income. As it currently stands, the same penalty would not have the same impact on a licensee with a high income and those with much lower income. To achieve fairness and accountability, the penalty must be in some way proportional to the profitability of the licensee. A proposed scheme for including profits into the AMP calculation, is to divide licensees into levels based on their net income/profits, for example:

- Level 1: Licensees with yearly net income up to $100,000
- Level 2: Licensees with yearly net income between $100,000 - $1,000,000
- Level 3: Licensees with yearly net income between $1,000,000 - $10,000,000
- Level 4: Licensees with yearly net income between $10,000,000 – $100,000,000
- Level 5: Licensees with yearly net income between $100,000,000 - $1,000,000,000
- Level 6: Licensees with yearly net income greater than $1,000,000,000

The penalty would depend on the specific level each licensee would fall under. Depending on the level, the penalty coefficient would be calculated, and the original

AMP would be multiplied by this coefficient to get the final penalty. Proposed coefficients are:

Level 1: $c_P = 1$

Level 2: $c_P = 1 + \frac{P}{P_{max}}$

Level 3: $c_P = 2 + \frac{P}{P_{max}}$

Level 4: $c_P = 3 + \frac{P}{P_{max}}$

Level 5: $c_P = 4 + \frac{P}{P_{max}}$

Level 6: $c_P = 5 + \frac{P}{P_{max}}$

Where: C_P represents the profit coefficient, P is the licensee profit for the previous year, and P_{max} is the upper limit for their specific level.

The final calculation of the penalty in that case would be the original amount multiplied by the coefficient:

$$AMP_f = AMP_o * c_P$$

Where AMP_f represents the final penalty for the specific company level, and AMP_o represents the original AMP calculated according to CNSC regulations and adjusted according to Vucicevic and Waller [109]. All companies could be considered as Level 1 during their first year of business, as there would be no available information on their revenue and profits.

To depict the effect these changes could have on the Canadian AMP policy examples are given in Table 14. These examples represent cases which are adjusted to better reflect proposed changes.

Table 14 Comparison of original AMP and modifications (CAD)

	Original AMP	AMP with modified factors [109]	AMP with modified factors and adjusted for net income
Level 1	$1658	$400	$400
Level 2	$1658	$400	$620
Level 3	$1658	$400	$1020
Level 4	$1658	$400	$1420
Level 5	$1658	$400	$1820
Level 6	$1658	$400	$2220

Table 14 shows what the penalty would be for a fictional violation. The example was based on scenario given by Vucicevic and Waller [109]: the violation is repeated, self-identified and voluntarily reported (Table 6). It shows what the amount would be if the penalty is calculated according to the current AMP policy (Original AMP), what the amount would be based on the modification proposed previously by Vucicevic and Waller in "C*onsideration of Administrative Monetary Penalties in Nuclear Safety and Security"* (Modification of factors) shown in Table 6 [109], and finally what the penalty amounts would be if the net income was accounted for in addition to the previous modifications.

The profit coefficient for this example was calculated according to the proposed formula, assuming that the licensee has a midrange profit for each level, e.g. for level 2 it is assumed that the licensee's profit is approximately $550,000 therefore

$c_P = 1 + \frac{550,000}{1,000,000} = 1.55$. For level 3, it is assumed that the licensee's profit is $5,500,000, therefore $c_P = 2 + \frac{5,500,000}{10,000,000} = 2.55$.

This should have a significant effect on licensees' AMPs, as the penalty will be proportional to the licensee's profit, increasing fairness and driving accountability.

The AMP (or similar) policies in industries throughout Canada and in US vary in principle and application of policy. The analysis in this work was aimed at studying the similarities and differences in AMPs across different industries and countries, and to assess if there is room for improvement in the Canadian nuclear security implementation of the policy. In order to improve the Canadian AMP, and to reach the desired outcome (increased number of self-identified and reported cases) the current policy should be adjusted. The proposed adjustments are relatively small but could yield a significant change in outcome. They include: factors adjustment, consideration of the size of the licensee (net income), yearly base penalties adjustments, and late-reporting penalties. The changes increase fairness and drive accountability by removing the disproportional aspect of the penalty applied to licensees regardless of the economic impact on their business.

The goal is to motivate license holders to communicate with the CNSC and promote self-identification and reporting, which would lead to a better understanding of the different types of violations which might occur. By building a comprehensive body of knowledge, the regulator could work on preventing these and similar violations in the future, thus increasing nuclear safety and security. Importantly, these adjustments do not require additional investments, but only a change in the application of the current policy, so the economic aspect of enforcing the policy would not be affected.

CHAPTER 6. ANALYSIS OF DRONE ROI

This chapter will provide insight into drone technology, potential application in nuclear security, cost of the new technology and other financial considerations. Additionally, analysis and examples provided show how drones would improve security systems.

6.1. Drone application in nuclear facilities

6.1.1. Potential drones use

Drones technology have been in use for a few decades, however, their application was not widespread until the size and price allowed an average person to own one for personal use [113]. It can be defined as a flying robot that can be remotely controlled or fly autonomously using software-controlled flight plans in its embedded systems, that work in conjunction with onboard sensors and GPS [114]. Large drones have been in use for military purposes for a significantly longer time. In the recent times drones have become more than video equipment: they are used for search and rescue missions, emergency situations, military operations, geo-surveillance, and even being considered (and tested) for package and medical supply delivery [115] due to their versatility, adaptability, quick deployment and charge, and relatively low cost and maintenance. Drones have been used in aerial surveillance by military and law enforcement in different situations due to the fact they can cover significantly more terrain than ground base vehicles and provide a better perspective [116]. Another reason for their increased use is that they are cheaper to operate than manned aerial assets for previously mentioned reasons. From fixed wings drones which can cover vast areas in a short time, to small quadcopters which have ability to hover over area of interest, drones can be utilized as a very important, modern tool which would help security in nuclear facilities improve the probability of intercepting and/or neutralizing adversary activities. The practicality and fast-growing industry, as well as rapidly improving technology means that drones should be an important point of interest for security and emergency experts.

The use of drones in nuclear facilities can be expanded beyond their current use. Even though they are not specifically regulated for the nuclear security use, their technical characteristics make drones highly convenient for utilization in physical security, safety and emergencies. In most nuclear power plants surveillance is done by cameras, sensors, and security officers. Due to rotary winged drones' ability to hover over certain areas or fly steadily they can be used in many ways in a nuclear facility. Drones could be utilized in this case as camera carriers which would be very good due to their mobility, so there would be no "blind spots" [40]. Moreover, they would be able to reach different height and fly in different speed which is a winning point compared to stationary cameras. The data from the drones would be transmitted in real time to the security personnel, and they could respond as necessary [55].

The speed of deploying drones and their flying speed makes them very convenient for response to alarms. If the alarms indicate intrusion of the security perimeter drones would be able to fly and reach the potential breach point faster than security officers and assess the alarm. This would reduce time to respond and reduce the probability that adversaries reach their goal. These drones can be preprogramed to fly on certain routes and monitor the security perimeter, but also outside of the security perimeter, by using cameras and sensors. This could be a significant security improvement because the adversaries could be stopped before they even reach the facility.

On the safety side, drones are already in use for radiation detection and measurements. There are some examples of drones being used for environmental monitoring [66] or in post-disaster and clean up operations after the earthquake and tsunami in Fukushima Daiichi. An improvement to speed and efficiency in completing different tasks can be achieved by combining some safety and security tasks using the same drones. For example they can be utilized for inspections in high radiation-dose areas in addition to surveillance [40].

In case of an accident, drones could emit siren-like sounds, which would help in alerting people to the incident [67]. But the role of drones in emergencies could be further enhanced by sending iodine pills by drones to different areas, in cases iodine pills were not distributed earlier or in cases where people are stranded in traffic jams, or any public area at the time of accident.

The use of drones in NPPs would significantly increase the safety of workers, because in many tasks they would be replaced by drones. Drones could reduce the requirement to work at heights. It would also decrease costs, because there would be no need for expensive equipment, and certain tasks such as inspections would be shorter.

In order to be used in a nuclear facility, drones should be relatively light and easy to use, but at the same time reliable. They need to be able to fly in different weather conditions and to be launched from a small area. Accurate positioning, precise control and battery life are important technical characteristics, which are being improved constantly. This allows users to expand the use of drones as their technical capabilities become more advanced.

6.1.2. Equipment/Features

Drones have highly adjustable features and optional equipment. Depending on its purpose, equipment can be added to the drone or could be removed to allow for lighter weight and longer battery life. The following characteristics could be considered very important when considering a drone as a security tool.

<u>Cameras:</u> One of the most important features for surveillance drones are cameras. Since 2017, drones have had integrated onboard cameras with motion tracking, obstacle avoidance that can communicate with the flight controller and adjust flight paths when under autonomous operation to avoid trees/houses. Cameras typically use a separate wireless signal from that of the onboard receiver [117]. All high-end drones available on the market have high quality video and imaging equipment. An example of zoom capabilities is shown in Figure 10. Some of the main characteristics of these cameras are [118]:

- Multiple camera modules, including a wide-angle camera, thermal camera, telephoto camera
- High video and image quality
- High angular resolution, (e.g., allows the user to discern 10 cm details at a distance of 1.5 km)

- Latest optical zoom capabilities (e.g., allows to observe people from over 2 km away)
- Optical unit with a large temperature range (operational from -43°C to 45°C)
- Active alignment of the optical unit, provides clear and sharp image during flight

Most of drones nowadays have high quality image transmission technology, delivering smooth, clear and reliable image feed [119].

Figure 10 Zoom capability example [120]

<u>Thermal Camera:</u> Detects centimetric hot spots from an altitude of up to 40 meters, with sensitivity of 0.05°C. Measurable temperature range is between -40°C to 180°C [121]. Usually these cameras have multiple modes, so images (and videos) can be seen as a general view of the thermographic of a scene, on a colored scale,

graduated from 0 (dark blue) to 100 (bright yellow) as seen in Figure 11, or it can provide an image where only coldest or hottest spots of the image are colorized as seen in Figure 12, depending on the user's needs [121].

Figure 11 Relative mode of thermal camera [121]

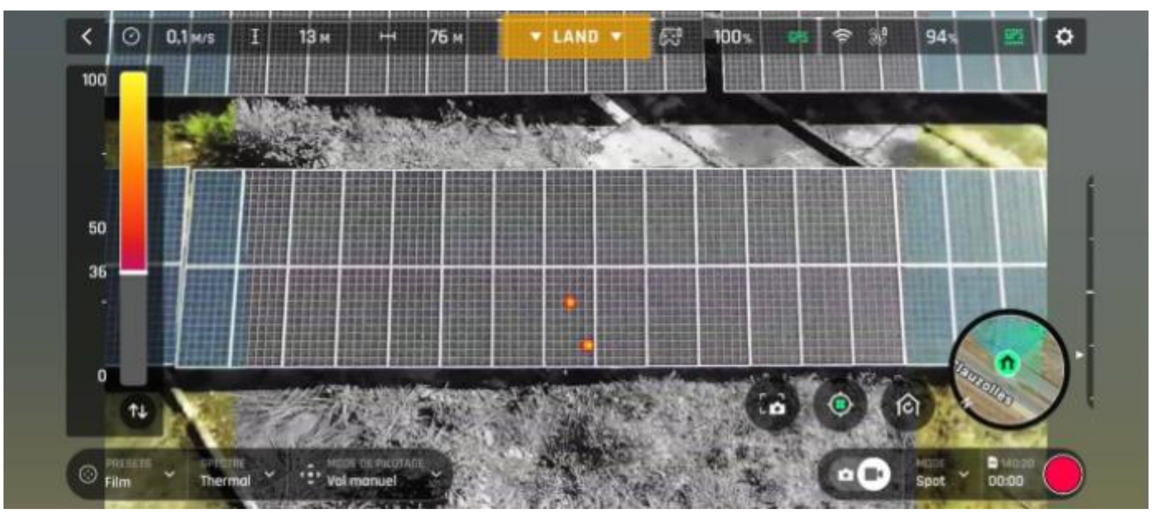

Figure 12 Spot mode of thermal camera [121]

<u>Active Track (AT):</u> AT allows the drone to track an object autonomously, using visual recognition, GPS, obstacle detection, and collision avoidance. This feature allows the pilot to draw a box around the object of interest and the drone will keep

following this object autonomously, as long as the object is in the visual or sensing range of the drone. Even if the object is moving fast with sharp turns, the drone can quickly readjust its position and camera's position to keep following it. Active Track uses GPS to control for navigation and altitude, and visioning systems which enables it to identify the object of interest. GPS also allows the drone to "return to home" in case it loses connection or if battery is low [122]. Figure 13 shows the user's view of the AT feature.

Figure 13 Active Track example [123]

<u>Point of Interest (POI):</u> POI allows the user to select a target and the drone will orbit around it, while focusing on it. The desired altitude of the drone and radius from the target can be controlled by the user. POI uses GPS to keep the drone pointing in the correct position, which contributes to a more stable flight compared to when a drone is controlled by a pilot [124]. Figure 14 shows an example of POI

feature, while the red arrow shows possible adjustments to radius, altitude, and speed.

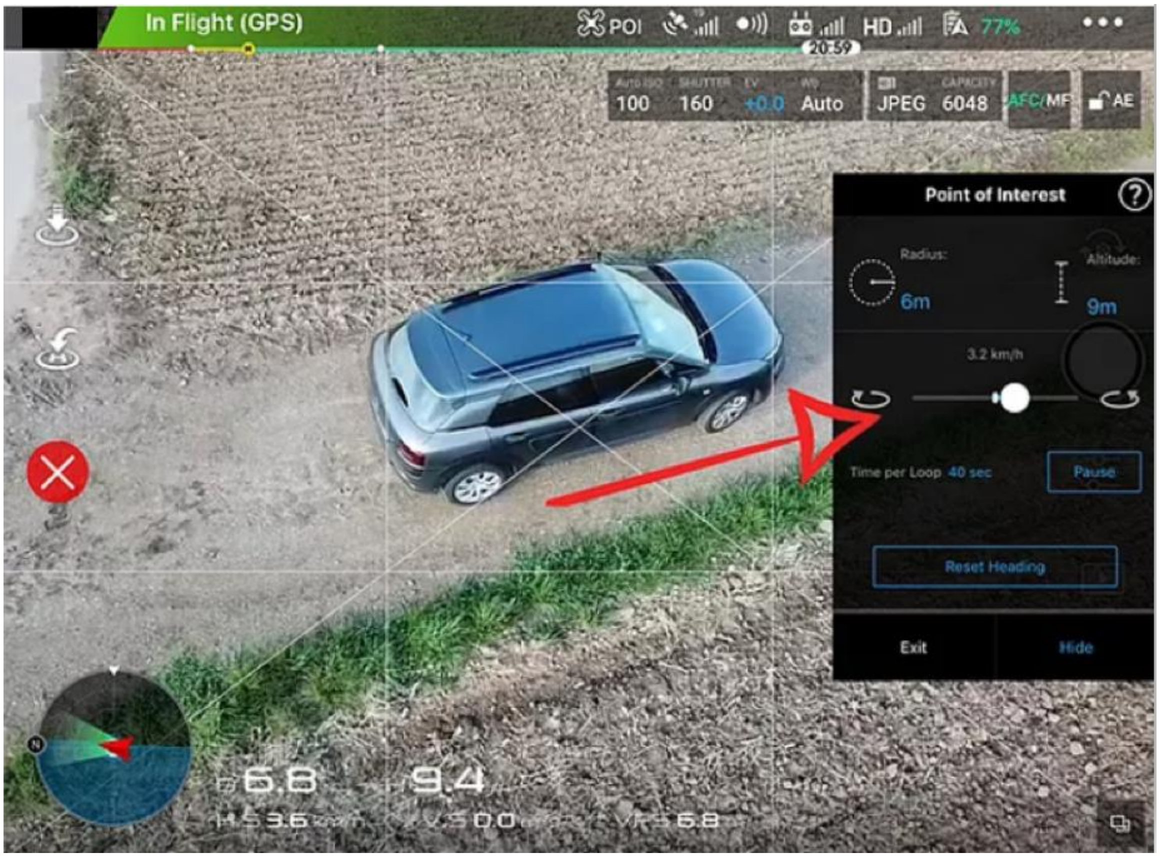

Figure 14 Point of Interest example [124]

AI Spot-Check: Some drones have the ability of using Artificial Intelligence (AI) to recognize the subject of interest, and if necessary, identify it in subsequent automated missions [125].

Waypoint: this feature can allow user to plan the flight in advance using two or more points. With this feature the path can be pre-planned, and the user does not have to interfere with the path during the flight, but only when needed to control the camera. Apart from the path, the user may set the speed, and the altitude of the drone. These can also be adjusted during the flight [125] [126].

Obstacle avoidance: This technology uses sensors to find obstacles along the path and map out a path for the drone to follow by avoiding these obstacles. This happens in real time and often when AT or POI modes are on [122].

ADS-B – when it comes to safety, drones of newer generation have an added safety system which allows them to know flight location information from airplanes and helicopters in the area. This is done by using Automatic Dependent Surveillance-Broadcast (ADS-B), that transmits signals, which are received by the drone. ADS-B Out works by broadcasting information about an aircraft's GPS location, altitude, ground speed and other data to ground stations and other aircraft, once per second [127]. It can display those aircrafts on a map and provide audio and visual alerts through the app to help the user keep the drone safe [119].

These are only some examples of drone capabilities which are available on the market at the time of conducting this research, but equipment packages can be customized for specific needs by adding, removing, or replacing equipment such as cameras or sensors.

Battery: There are options which allow wireless battery charging, which can be beneficial for security purposes, as drones would be able to charge faster, without human assistance since the charging platforms allow charging even if drone isn't aligned with perfect accuracy. These platforms (as they are created to be used outdoors) are suited for highly volatile outdoor environments such as water, dust, dirt, and chemicals [128].

In order to be used as a security tool, drones should have combination of characteristics such as flight speed and distance, battery life, ability to avoid obstacles, operate in extreme weather conditions. Based on these characteristics, 9 drones were selected for further study. The average weight of the drones in this study is between 0.5 and 1.4 kg, and they are relatively small in size, made to be compact and easy to carry around when needed [129] [130] [131]. The drones were chosen by speed, amongst other characteristics. The slowest has a maximum speed of 50 km/h, and the fastest is at 140 km/h, while average speed across reviewed drones is around 70 km/h. Most of these drones have omnidirectional or multidirectional obstacle sensing [118] [121] [129] [130] [131].

Drones are extensively tested to confirm their functionality in different conditions and some models are proven to work in high temperatures (over 50°C in dry heat), low temperatures (-35°C), resistant to temperature shock (-35°C to +43 in one hour), functional after falls on concrete (after 18 drops from 1 m height) [129]. Another important characteristic is ability to fly in varied severe weather conditions. The majority of modern drones are able to sustain heavy winds (up to 21 m/s or 75 km/h), dust, and in rain (10 liters/min) [129]. This is characterized by the ingress protection (IP) ratings, which grade the resistance of an enclosure against the intrusion of dust or liquids, where the first numeral refers to the protection against solid objects and is rated on a scale from 0 (no protection) to 6 (no ingress of dust), and the second numeral rates the enclosure’s protection against liquids and uses a scale from 0 (no protection) to 9 (high-pressure hot water from different angles) [132]. A summary of these characteristics can be found in Table 15.

Table 15 Characteristics of different drone models

UAV[3]	Operating temperature	Wind/rain-dust resistance	Flight speed	Flight time	Flight distance	Obstacle sensing
1	-30 to +50°C	18 m/s IP54	50 km/h	40 mins	8 km	yes
2	-35 to +50°C	15 m/s IP 53	54 km/h	32 mins	5 km	no
3	-20 to +50°C	15 m/s IP 55	82.8 km/h	41 mins	15 km	yes
4	-20 to +50°C	15 m/s IP 54	50 km/h	60 mins	8 km	yes
5	-20 to +50°C	16 m/s IP 45	82.8 km/h	55 mins	15 km	yes
6	-10 to +40°C	20 m/s IP 67	79.2 km/h	30 mins	5 km	no data available
7	-10 to +40°C	21 m/s IP 67	79.2 km/h	31 mins	1.6 km	no data available
8	-10 to +40°C	14 m/s IP 53	61 km/h	32 mins	22.5 km	yes
9	-10 to +40°C	14 m/s no IP rating	140 km/h	20 min	16.8 km	yes

Most of the drones reviewed have all or most of the characteristics described previously, including high quality cameras and smart features such as object detection and classification; find and track moving objects; precise and smart return to home; automated take-off and landing; route planning and management; AI tools and image analytics; possibility to develop software as needed, as well as many fail-safe systems.

Drones were included in the research based on their characteristics. Drones with low flight speed (under 40 mph), or short battery life (under 30 minutes) were not included in the comparison, as they would not be efficient enough compared to comparable actions of security officers. The exception to this is a drone that was included in the study with a slightly shorter battery life, but very high speed (140

[3] UAVs are represented by numbers, as this research should not to promote any brands. Additionally, the specifications will change with technological development. This study is aiming to show that UAVs can be a significant tool, and not to recommend a specific brand.

km/h). It can be assumed that slightly shorter battery life could be compensated by very high speed. The data on these drones were found on manufacturers' websites, as well as on retailers' websites where price history was available for some models. It should be noted that the review of given drones was done in the past few months with drones available on the market at the time. As the companies develop new models it is expected that enhanced features will be available.

6.1.3. The application of drones in nuclear security

The areas in which drones may be utilized at a nuclear facility include:

- Enhanced surveillance and risk assessment: drones can fly to the facility perimeter and observe even beyond the facility borders. This allows for security officers to notice any irregularities further away and prevent a potential security breach before it happens. Another advantage is that drones could carry different cameras and image further during both day and night by using thermal and infrared imaging cameras. Keeping in mind that nuclear facilities are adjacent to usually a large body of water, drones can fly and survey the area which would otherwise require the use of boats. They would be able to inspect security barriers such as fences or roadblocks for any hidden damages or anomalies. This perimeter inspection method is more efficient as the officers would be able to have a bird's eye view including rooftops, parking lots, and water surfaces, in a shorter time than with conventional tools. This is crucial since time is very important in security operations and the aim is to find intruders as early as possible and maximize the time for security officers to respond.

Drones can be utilized in nuclear security as a tool which could support or even replace some of the current tools or procedures, for example drones can be used as a surveillance support, where they could have cameras and be preprogrammed to fly different routes. The advantage in this case is that, in addition to existing stationary cameras, drones would be able to cover any area which (as a “blind spot”) could be used by adversaries to obtain access to the facility. Drones could spot the adversaries faster than the conventional surveillance tools because they could be mobile, patrolling different areas.

Drones in the NPP could be tethered or untethered. For the purpose of surveillance in NPP, tethered drones could be a viable solution. The tethered drone is controlled from the Operator Control Unit (OCU), which is a laptop that provides user interface software to operate the system. The tethered drone can be programmed to autonomously fly 300-400 feet (90-120 meters) Above Ground Level (AGL), allowing the operator to control and operate an Electro Optical/Infrared (EO/IR) camera from the OCU. The camera transmits video images through the tether back to the OCU using an encrypted feed; images are not stored onboard the drone [65]. The tethered drone camera operator can focus on any area of the secure zones of protection in and around the nuclear facility.

The other option is the use of untethered drones which would be remotely piloted or that would have previously programed paths and they could fly automatically along the selected path [42]. Cameras used on these drones should be capable of providing high quality images which could be used for facial recognition programs. The untethered drone needs a power supply in the form of a battery. These batteries in average would provide 20 – 40 minutes flight time [133]. These drones can be convenient for alarm assessment, patrol, and in situations where it’s not feasible to have a physical tether to the drone.

- Alarm assessment: Unlike the stationary cameras, drones could help security officers in alarm assessment. If the camera carried by the drone registers some irregularity the drone could assess if the threat is real or not. This could be done simply by flying drone closer to the targeted area and seeing it from different angles, which would not be possible otherwise. This would significantly reduce time for alarm assessment. Moreover, drones could be sent to assess alarms which cannot be assessed using other cameras but would have to be assessed by a security officers. This could significantly reduce the time needed to assess alarm and respond if necessary.
- Response: since drones would allow early detection of intruders it would be possible to send drones close to the intruders and communicate with them without putting security officers at risk by exposing them to potentially armed adversaries. Communication could be possible by simply adding speakers and microphones to drones.
- Secure transport of radioactive or nuclear materials: Drones could be an added layer for transportation security, where they could fly before the

vehicle and provide a visual input to security officers making sure there are no adversaries on the route. They could also provide live feed of the vehicle transporting the material.

An example of drone used for response in a nuclear facility is given in Figure 15. Possible breach point is chosen to be the point which is the furthest from the security building, where response forces are most likely to be dispatched from. This point is chosen, as adversaries could assume they would be least likely to be interrupted or detected early as security officers may not always be located in the vicinity, and the distance to their target (if we assume it is a reactor building) is the shortest, allowing them to achieve their goal with the shortest adversary task time and potentially longest response time. The distance from the security building to the breach point for drone is 694.3 m (purple line), and for response forces the fastest route would be 1,017 m (dark blue), or 1,026.6 m for response force to reach breach point (light blue). Distances were measured using Google Earth tools. Drones can fly at different speeds varying significantly based on type of drone. Beginner drones fly at relatively low speed of 12 mph (~ 19 km/h), trick drones (most popular) fly at speed 40 - 70 mph (~ 64 - 112 km/h), and racing drones which have speed between 60 - 120 mph (~ 96 - 193 km/h) [134]. For the drones selected in this study (according to the previously given characteristics) the speed goes up to 140 km/h. Considering this range of speed of proposed drones, the average maximum speed is around 75 km/h, resulting in flight time of around 33.1 seconds to the breach site.

However, if a high-speed drone would be used for the response in this case, with maximum speed of 140 km/h, the time needed for the same distance would be significantly shorter, around 17.8 seconds, therefore increasing the probability of interruption of adversaries before they complete their task. Canada does not have regulation on drone speed, but in the United States, the maximum allowed speed for a drone is 100 mph [135] (160 km/h), which shows that higher speed than assumed in the calculation is possible. The average speed considered in this case is relatively low in order to disregard the difference in height it may have to overcome. It is also recommended to have the drones' starting point at a significant heights (roofs for example) to minimize climbing time and therefore minimize flying time. The speed depends on many factors including, weight, size, payload, weather conditions, etc.

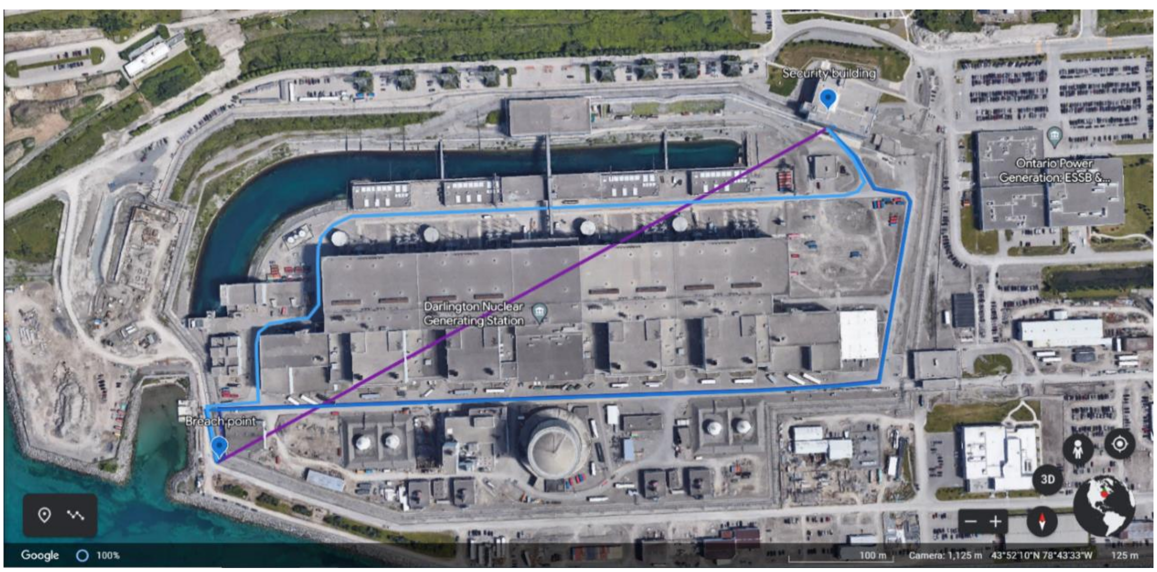

Figure 15 Route for drone and response force

For the same task of alarm assessment, security officers would have a different route and therefore a different response time. In Figure 15 the blue line shows possible route for security officers. Depending on the route the distance varies from 938 m to 1027 m. If responders would use a vehicle which would have average velocity of 70 km/h the time they would need to reach the point of breach would be between 48 and 53 seconds. The speed is based on the maximum speed of the light armoured vehicles (130 km/h) [136] and conditions of the road which include sharp turns on the route, braking distances, and considering the longest straight part of the road is only 680 m, in which the vehicle would not be able to develop maximal speed and brake in time for the next sharp turn. This assumption takes into consideration the weight of the vehicle which is around 7 000 kg without human crew or equipment [136]. This is conservative approach, as it is highly unlikely that any vehicle reaches average speed of 70 km/h, due to often cluttered and narrow roads. More realistic approach would be that average speed is 50 to 60 km/h, in which case time to reach the breach point would be approximately 72 seconds.

This example is purely descriptive as it is based on assumptions that, while very likely, cannot be confirmed, however it serves to illustrate why drones should be considered in nuclear security, based on their feature set and low cost which can provide very significant results.

It is important to note that these times show only travel times, and do not include time necessary to communicate and dispatch drones or security officers. Time to dispatch a drone is significantly shorter compared to times necessary to send a team of responders. The advantage the drones have is in the technology that constantly develops. Thanks to advanced technology, drones can be stationed in “nests” and dispatched in very short time. “Nests” are a protective home or base station where drones can stay charged and ready to be deployed [137]. This would allow drones to be airborne only seconds after the communication with the security officer (pilot), while for the team this time would be longer, due to the fact they may not necessarily be in the vicinity of the response vehicle.

Communications should be considered additionally since times for drone dispatch could be shortened by preprogramming a drone to takeoff when an alarm goes off. No additional communication here would be necessary, while in case of response forces (security guards) they would have to be informed about the alarm location, communicate back, and go to a vehicle, before travelling to the alarm assessment.

As previously described drones come with different characteristics, including different airspeeds, payloads, and weather resistance. Because of the varying needs in the security use cases, it would be a good approach to create a fleet of different drones for different purposes. For example, high-speed drone(s) for response, a tethering drone(s) and drones with good AT or POI for surveillance, a long battery-life drone for surveillance and communication. This variety of types and features will affect the total cost. It is expected that new and improve models with even better features and multiple options are available in the future. It is also possible that if nuclear facilities decide to include drones in security, drone manufacturers would be able to create custom drones which would have security focused characteristics.

6.1.4. Drone detection probability

The probability for detection of adversaries by using drones depends on following factors:

- Probability of the camera (working correctly) attached to the drone: P_{cd}. They can be assumed to be the same as the stationary camera used in security systems. Probability of this element is given by manufacturer or is calculated during exercises.
- Probability of drone failure: P_{df}. This probability is given by the manufacturer, but for the system (fleet) can be considered very low, since there would be multiple drones. Drones within the fleet can be programmed to fly back to charging stations when battery is on a certain level (e.g. when battery is < 20%), which should reduce the probability of failure while on duty.
- Probability of communication between the drone and security monitoring room: P_c. The communication could be wireless (for free flying drones) or wired (for tethering drones). This incudes data transfer. Drone height, the area visually covered by the drone camera will affect significantly the probability of detection, since the probability of detecting an adversary somewhere in the facility perimeter would be higher when the drone is high enough to cover larger spatial area (compared to stationary cameras which are always on predefined heights), but still low enough to give a clear image, which can be interpreted correctly.

In order to compare the probability of detection between a stationary camera and a camera on a drone, a factor of area should be introduced - F_a. This factor would provide dependency of probability on the area covered by drone camera at any given moment. The value of this factor would be assigned based on the area covered, compared to a stationary camera and it could be between 0 and 1, where 1 would be assigned if the whole area of the facility is covered and 0 if the area is so small it may be considered irrelevant.

Introducing this multiplicative factor, the probability could be calculated using the following formula:

$$P_{dd} = P_{cd} * \left(1 - P_{df}\right) * P_c * F_a \qquad (11)$$

Using the proposed equation, a comparison between stationary camera and a drone camera detection probability can be made. Fa in both cases can be calculated based on the following assumptions:

- Fa for the whole facility area is 1 (0.89 km^2 Figure 16).
- An area that can be reasonably assumed to be seen from a stationary camera is approximately 2800 m^2 (Figure 17), which represents 0.3% of the total area, therefore the Fa for stationary camera would be 0.003.
- An area that can be reasonably assumed to be seen from a drone camera is approximately 30000 m^2 (Figure 18), which is approximately 3.4% of the total area, therefore Fa for the drone would be 0.034. It is important to note that this is a conservative approach, as the drone could fly higher, covering a larger area.

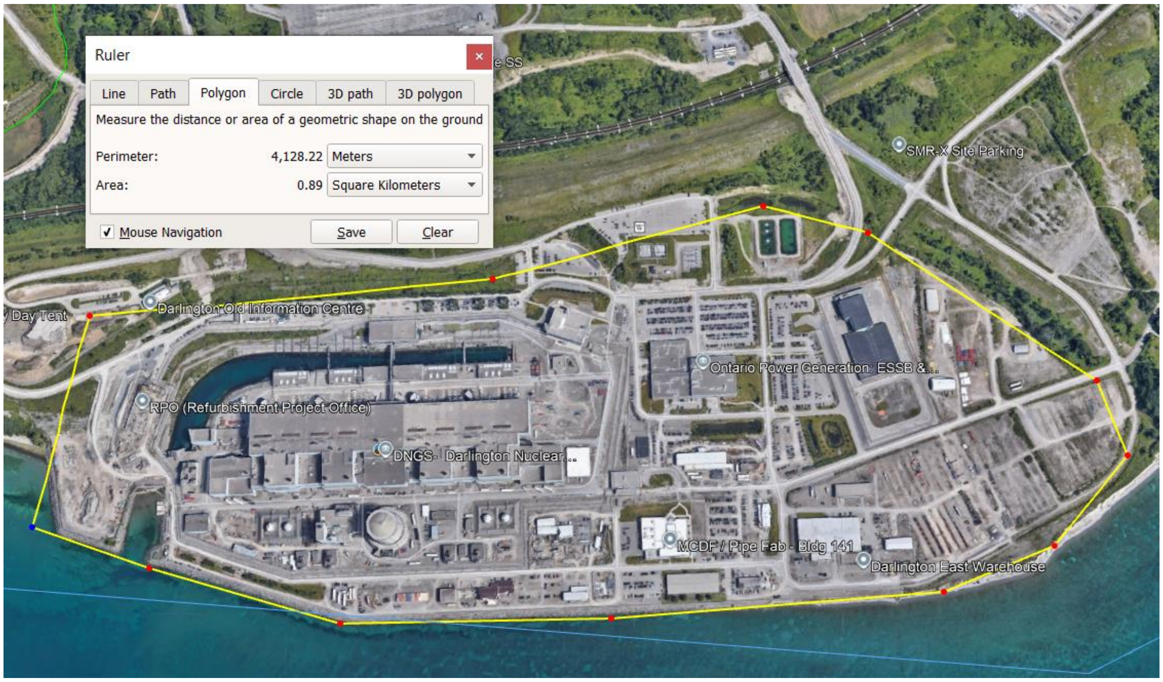

Figure 16 Facility area

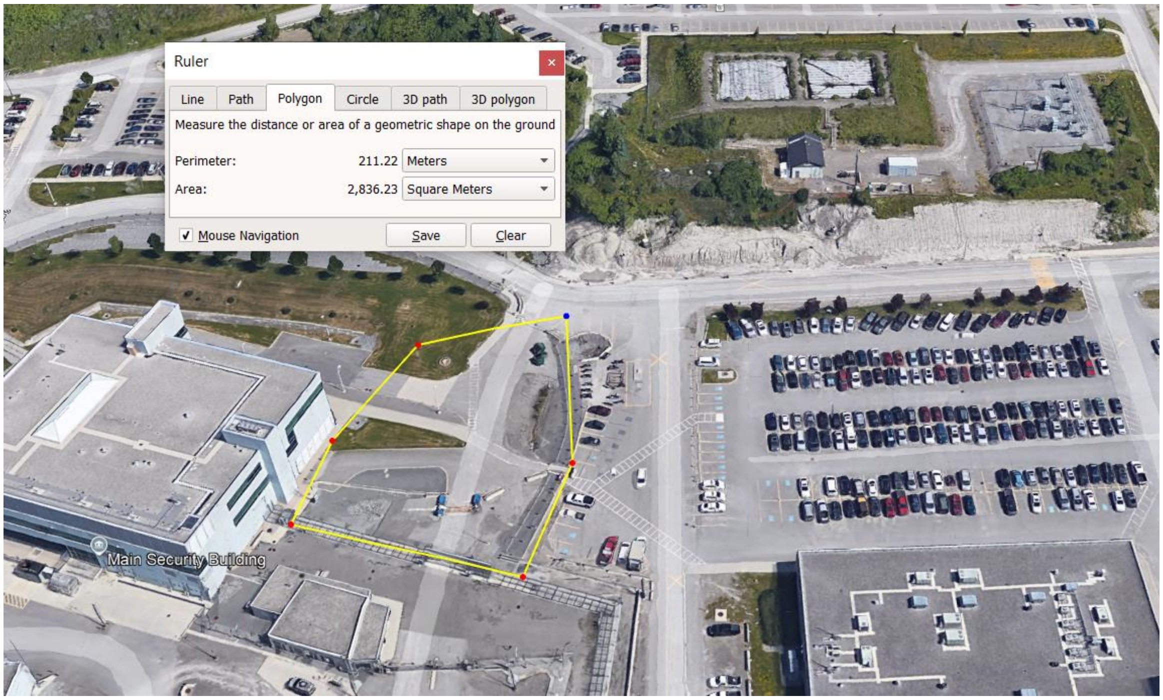

Figure 17 Area covered by stationary camera

Figure 18 Area covered by drone camera

Using equation 11, we can compare the probability of detection from drone with probability of a stationary camera, based on the area covered:

$$\frac{P_{dd}}{P_{dc}} = \frac{P_{cd} * \left(1 - P_{df}\right) * P_c * F_{ad}}{P_{cs} * \left(1 - P_{df}\right) * P_c * F_{ac}}$$

If we assume that the probability of a stationary camera working successfully P_{cs} is the same as a drone camera (P_{cd}), and the probability of communication (P_c) is the same in both cases, then:

$$\frac{P_{dd}}{P_{dc}} = \frac{\left(1 - P_{df}\right) * F_{ad}}{\left(1 - P_{df}\right) * F_{ac}}$$

Since probability of drone failure in case of stationary camera is 0, then:

$$\frac{P_{dd}}{P_{dc}} = \frac{\left(1 - P_{df}\right) * F_{ad}}{F_{ac}}$$

By incorporating previously assumed factor F_a, the result is:

$$\frac{P_{dd}}{P_{dc}} = \left(1 - P_{df}\right) * 11.33$$

As $\left(1-P_{df}\right)$ actually represents drone operating successfully (P_{dos}), the final expression is:

$$\frac{P_{dd}}{P_{dc}} = P_{dos} * 11.33$$

In a security system the probability of drone failure would be very low due to before mentioned characteristics and redundancy, which would increase P_{dos}, and also increase F_a.

The increase in F_a and the corresponding P_{dd} are proportional to the flight height while maintaining adequate visibility of the facility and the various objects in the field of view. However, in all cases, it represents an improvement over an equivalent stationary camera.

It should be noted that this formula only calculates ratio of probability of detection, however, drones would be able to participate in response as well, as they would be able to communicate with adversaries once they are detected much faster than response forces and without exposing them to risk. Additional, drones could follow adversaries on their path, which would be beneficial for response forces.

6.1.5. Advantages and disadvantages of drones in nuclear facilities

As with any other tool, while drones have significant advantages in the area of safety and security, they are not perfect. It is important to understand that even though disadvantages exist they could be overcome if the use is well balanced with the drone fleet, and other existing security tools and personnel.

Some of the most prominent advantages include:

- Fewer cameras needed (lower initial cost and maintenance cost), wider coverage, and mobility

As drones would be mobile cameras with the possibility to cover larger areas than stationary cameras would, it is clear that the same area would need fewer stationary cameras in the future. It is a good idea to combine stationary cameras and drones, to maximize return on investment, as it would be possible to combine a certain number of cameras and drones to achieve the best coverage for the lowest price. Additionally, this configuration would allow wider coverage as drones would be able to provide continuous surveillance of area which could not be covered by stationary cameras, such as areas outside of security perimeter, areas on the water, etc.

- Video quality

Even entry-level, low-cost drones come with high quality cameras (as photography and videography is their primary purpose). These would ensure high quality of video and images. Additionally, these cameras are usually equipped with high optical zoom function which allows users to spot any adversary activity clearly from further away, giving them significant advantage in longer response time (compared with current systems of sensors and cameras [37]).

- Reduced risk for security officers

Using drones as security tools would decrease risk of injuries for security officers and increase probability of successful response to adversary activities. Since any activity would be spotted from further away the time for response would be longer and therefore probability for successful interruption of the adversary would be higher. Additionally, communication between security officers and adversaries would be possible without direct contact while security officers are safe from adversary attack. This would potentially decrease insurance premiums for security staff which would additionally reduce costs of security personnel.

- Automation of security represents less risk of insider threat

Automated patrol by drones, especially if assisted by smart/AI recognition systems, around the facility means fewer security personnel are required for that role. With fewer people involved in the process, the probability of insider threat is lower.

- Holistic approach (safety, security, emergency response)

Drones do not have to be used solely in security of nuclear facilities. They could be a valuable asset for communication, delivery, and inspection. They can be considered for almost any type of emergency, for example, if an emergency happens which requires distribution of potassium iodide (KI) pills to people on and off site. Even though in Ontario KI pills are pre-distributed (upon a request) to the population in the vicinity of nuclear facilities, there is a high probability that the additional distribution would be needed for those who do not have pills (or have expired pills) or for those who are outside of their homes. It is expected that in a case of emergency some of the roads might be blocked and traffic would be higher in some areas, therefore those people would need KI pills delivered and the safest way would be to deploy drones and drop off pills to those in need. Additionally, they could be used as a communication support in addition to public alert/announcement (PA) system in case of emergency.

Disadvantages include:

- Drones are more expensive than stand-alone cameras

  The price of a high-end drone is likely higher than a stationary camera, however one drone could potentially replace more that one stationary camera which justifies the price. On average, drone prices are in the range of $1,400 – $17,000 CAD (according to manufacturers and retailers) as shown in Table 16, while security cameras for industrial sites could cost somewhere between $150 and $13,000 CAD [138]. Considering that drones could significantly decrease time for response forces to interrupt adversaries compared to stationary cameras, as they could be used in the response as well. This would provide a better security system, the price difference could become negligible.
- Battery life

  As drone batteries have limited capacity this could be considered a significant downside. It can be overcome by using multiple drones in shifts so that some are in use while others charge their batteries. In addition, battery technology is improving rapidly, and longer battery life can be expected with newer versions of drones. As mentioned previously, tethered drones can be use whenever possible, to solve the problem of short battery life. Tethered drones do not need to carry their primary power source since they can receive power from a power bank connected through tether, and thus can could fly as long as required. [139]

- Weather conditions effects

  Drones can be affected by severe weather such as strong winds and rain, and extreme temperatures. Manufacturers specify wind and rain resistances according to IP ratings and according to those specifications the highest wind speed a drone can sustain is 21 m/s. Many drones are water resistant, and some of them are manufactured for aquatic environment, and have ability to take off, land or float on water, or to be fully immersed/submerged for up to 30 minutes [140].

- Regulations

  Drones in Canada are regulated under Canada transport regulations and there are no specific regulations for their use as security tools. In order to be used in such way it would be beneficial to have a specific set of regulations developed for the use of drones in nuclear security.

- Potential security threat

  Other than being a potential security tool for nuclear facilities, drones are often perceived as a threat to the security of nuclear material since they are easily available as a tool and relatively easy to fly. As such, drones can be used to make videos of a targeted nuclear facility, or even carry a payload which can be used to attack, sabotage, or disrupt facility operation. Soon after the 9/11 attacks the fundamentals of security planning in facilities which could be potential targets for similar attacks were questioned, and as a result, security measures were improved to protect from, until then, an unconsidered method of attack: aerial attack. Nuclear power plants developed strategies to address aircraft impacts. According to Mogavero [141], nuclear plants are among the most robust structures in the U.S. Containment buildings are usually constructed with high strength reinforced concrete with 4 - 6 feet thick shell and steel liner. Fuel building usually also has high strength reinforced concrete floors, walls, and roofs, supported by a steel truss system. A potential risk that comes with drones is cyber security: hacking and data theft. The risk is present, and it should be compared to the benefits. It should be also compared to the existing risk of having a cyber security breach via another carrier: cellphone, tablets, personal laptops which may be used on site daily. Mogavero also claims that since power plants are "data islands" it would be more complicated to use drone to perform a cyberattack [141].

Nevertheless, countermeasures are developed to prevent misuse of drones. These countermeasures exist in order to prevent any malicious use of drones against nuclear facility, e.g., for attack (physical or cyber), sabotage, or in any way disruption of normal function. In general, countermeasure systems could be divided in two groups: monitoring and deterrence, and both are currently implemented into commercially available solutions. Monitoring technologies include i) detection, ii) classification or identification, iii) locating and tracking, iv) alerting. There are four types of monitoring equipment: radio frequency analyzers, Radar, electro-optical/Infrared (EO/IR), and acoustic sensors (microphones). Deterrence can be grouped as either: physically destroying the drone, neutralizing the drone, or taking control of the drone. For these activities currently available methods include i) radio frequency jammers, ii) GPS spoofers, iii) high power microwave (HPM) devices, iv) nets and guns, v) high-energy lasers, and vi) trained birds of prey. Depending on the UAV that is affected by one (or more) of these methods the results may vary from controlled landing, return to home, falling on the ground uncontrollably, flying uncontrollably, or gaining control over UAV [142].

6.1.6. Financial consideration

As the technology develops drones become relatively affordable. The price of a drone with some of the advanced surveillance technologies is in range of $1,400 to $17,000 CAD, depending on the brand, model, availability, and retailer. Average prices for models from Table 15 are given in Table 16 [143] [144] [145] [146] [147] [148] [149].

Table 16 Average drone prices

Drone model	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
Year of price	2022	2022	2022	2022	2022	2022	2022	2022	2022
Price[4] (CAD)[5]	Not available	$9113	$12120	Not available	$16274	$3250	$1880	$5200	$1400

Considering the prices of different drones and knowing that they could be used to supplement the activities of security officers, a cost comparison of nuclear security officers and drones could be conducted. Since the cost of security equipment and security officers is not publicly available from nuclear power plants (confidential information), data was collected from the publicly available "Ontario Sunshine List" [150]. The data includes only salaries with benefits which are over $100,000. It can be assumed there are additional personnel whose salary is under $100,000, but this data allows us to see the trend in the past 10 years of increasing investment in nuclear security officers. It should be noted that even though not all security officers are included, the investments are recurring (yearly), and if the NPP was to invest in drones the recurrence would not be yearly, nor would the investments be so drastic. The security staffing issue is of great importance, since in a typical reactor, the security force is roughly 20% of the total workforce in the power plant [151].

[4] Prices last updated February 2023.

[5] For prices given in US Dollars the exchange rate for the specific year was used to calculate price in CAD

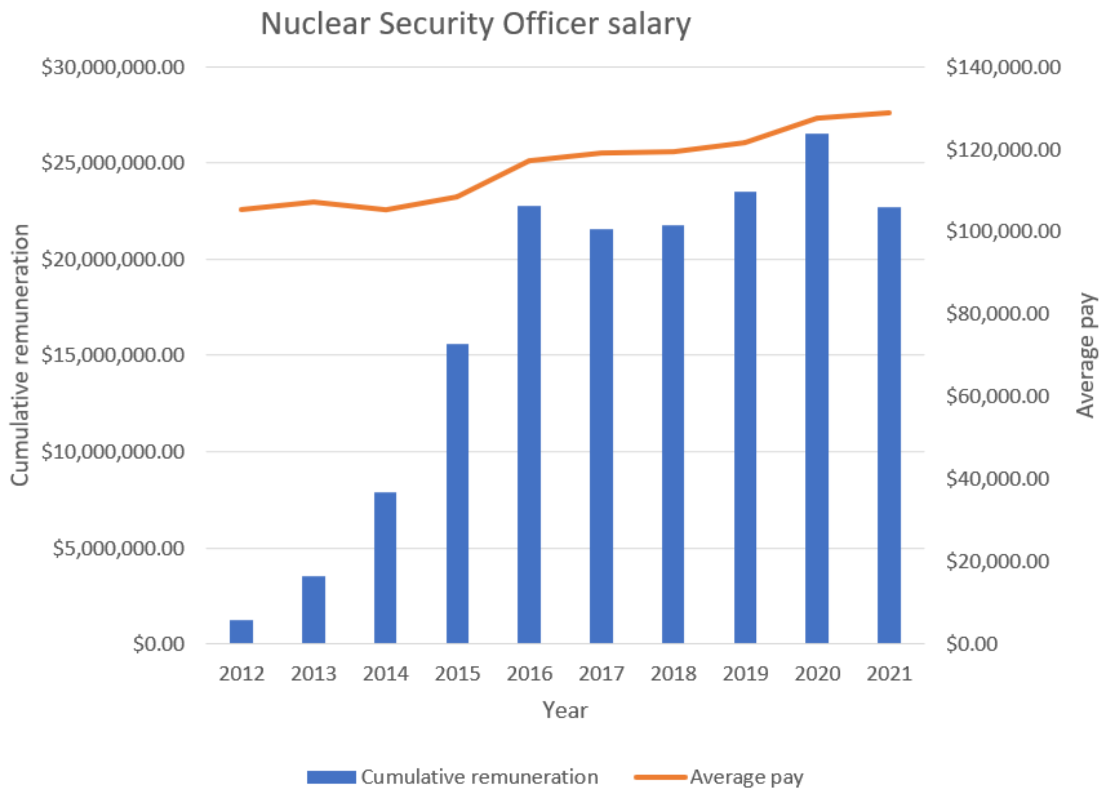

Figure 19 Average and total pay for Nuclear Security Officer 2012-2021

Figure 19 shows the trend of investment in nuclear security officers. The left side shows cumulative remuneration, which is the total amount paid to security staff making over $100,000. This means that the total amount per year is higher, as we may assume that some security staff will have salaries under that threshold. These amounts do not include benefits (health coverage, pension, insurance), investing in new equipment, regular maintenance of existing equipment, trainings for the security officers, nor any other security position. Therefore, we may assume that these amounts are minimal investment for nuclear security officers. Average pay in Figure 19 represents average investment per person. Here we can observe the trend over time, and we can assume that due to inflation and increasing costs, this trend will continue to go up.

6.1.7. Conclusion

As new technologies develop, it is obvious that they bring advantages for society, but at the same time they provide numerous ways for misuse and pose potential threats to critical infrastructure. Drone technology is rapidly developing and becoming one of the most important tools, where the low price and high technology content made it useful in all areas of industry. From military to everyday use drones have become a significant new technology, with applications in many areas. Their use has been increasing in security and emergency response, and due to their characteristics, it has become clear that drones can be successfully utilized in nuclear security as well. Apart from representing modernization and technological development in security, drones can save resources by performing tasks in the area of nuclear security and emergency response. Their high potential is also in flexibility and adjustability of the technology.

Even though drones are often perceived as a security threat that could be used by adversaries, they should also be seen as a new security tool, and utilizing drones for these purposes could represent an important step toward implementing new technologies in nuclear security.

Considering investments that are made yearly for security personnel, it becomes obvious that investing in a fleet of drones would be equivalent (or less) to investment in one security officer, but the achievements of a fleet of drones could be much higher providing a more secure environment in a nuclear facility.

Unfortunately, many still see this technology more as a threat than the opportunity that it is. It is important to realize what advantages drone technology might give us in the nuclear security field, and the ways of improving the current state of security in nuclear facilities by using drones. While at the same time keeping in mind that they can be misused and can be a serious threat. Improving protection and reducing risk by promoting regulations and utilizing drones effectively for nuclear security should be the industry's goal for the future.

CHAPTER 7. CONCLUDING REMARKS AND FUTURE WORK

In the nuclear industry, a monetary investment can have a return as an immediate economic benefit, but also as an improvement in the technology or regulations and therefore in the efficiency of a system, leading reputational benefits which aid in future returns in the form of continued operation and opportunities for new facility developments.

The nuclear industry is highly regulated, and as such, it is important to maximize the effect of the regulations in order to maintain nuclear safety and security, and in order to receive a positive return on investment. This research shows that certain changes in regulations could have higher impact and yield better outcomes, therefore maximize the return on investment. In case of AMPs, it's minimal incremental investment of modified policy resulting in potentially outsized impact form licensees engagement, resulting in a database of potential violations of the policy. This would allow regulator to predict how violations could happen and prevent them before they happen. Additionally, comparatively inexpensive new technology (such as drones) introduction in the nuclear security could have a great impact as it would support multiple systems, making them more robust and reliable, providing opportunity for cost reduction through other systems and creating a positive ROI.

Future work should include analysis of other regulations in order to analyze their effect on return on investment in the nuclear industry in Canada.

Knowing that drones could be very reliable, future work should further focus on utilizing drones in nuclear security and analyzing the costs and benefits of a smart security system which would include both drones and artificial intelligence. This can include:

- Monte Carlo simulation for the neutralization of adversaries
- Analysis of drone regulations and proposal of changes to accommodate drones in nuclear facilities
- Analysis and possible application of artificial intelligence in nuclear security.
- Analysis and possible application of Remotely operated weapon systems

The results would be compared with conventional security systems used in many nuclear facilities and show the return on investment with these systems.

The return on investment is to be based on the current investment in security systems in the nuclear industry. The current investment would then be compared to the investments that would be made if drone systems are implemented, which could possibly reduce the number of personnel needed in the security forces. This can be especially significant for Small Modular Reactors due to their economic need to reduce personnel numbers in order to be profitable, as automatic and autonomous systems are needed to make these plants feasible.

REFERENCES

[1] International Atomic Energy Agency, "Energy, Electricity and Nuclear Power Estimates for the Period up to 2050," IAEA, Vienna, 2024.

[2] B. K. Sovacool and S. V. Valentine, The National Politics of Nuclear Power, Abingdon: Routledge, 2012.

[3] M. L. Garcia, Vulnerability Assessment of Physical Protection Systems, Burlington: Elsevier Butterworth-Heinemann, 2006.

[4] D. S. McDonough, Canada's national security in the post-9/11 world: strategy, interests, and threats, Toronto: University of Toronto Press, 2012.

[5] D. Frantz and C. Collins, The Nuclear Jihadist: The True Story of the Man Who Sold the World's Most Dangerous Secrets...And How We Could Have Stopped Him, New York: Twelve, 2007.

[6] E. Waller, *Module 8.1: Physical Protection Systems,* Oshawa, 2018.

[7] World Institute for Nuclear Security, "Autonomous and Remotely Systems: Benefits and Challenges for Nuclear Security," WINS, Vienna, 2019.

[8] R. P. Rosano, "The Future of Nuclear Security," in *International Conference on Nuclear Security: Commitments and Actions*, Vienna, 2016.

[9] FAA, "Fact Sheet – Aviation Voluntary Reporting Programs," FAA, 22 05 2019. [Online]. Available: https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=23034. [Accessed 21 08 2019].

[10] L. J. Connell, "Cross-Industry Applications of a Confidential Reporting Model," NASA ASRS, Moffett Field, 2004.

[11] W. D. Reynard, C. E. Billings, E. S. Cheaney and R. Hardy, "The Development of the NASA Aviation Safety Reporting System," NASA, Moffet Field, 1986.

[12] U.S. Nuclear Regulatory Commission Office of Enforcement , "NUREG 1600 - General Statement of Policy and Procedure for NRC Enforcement Actions," May 2000. [Online]. Available:

https://www.nrc.gov/docs/ML0037/ML003715971.pdf. [Accessed November 2020].

[13] "Economics of Nuclear Power," World Nuclear Association, 2023. [Online]. Available: https://world-nuclear.org/information-library/economic-aspects/economics-of-nuclear-power#assessing-the-costs-of-nuclear-power. [Accessed 2024].

[14] "Our Mission," Goverment of Canada, 2024. [Online]. Available: https://www.cnsc-ccsn.gc.ca/eng/about-us/our-mission/. [Accessed 2024].

[15] National Renewable Energy Laboratory, "Nuclear Energy - Providing Power, Building Economies," 2022.

[16] CNSC, "CNSC's Administrative monetary penalties program," CNSC, 6 10 2017. [Online]. Available: http://nuclearsafety.gc.ca/eng/resources/educational-resources/feature-articles/administrative-monetary-penalties.cfm. [Accessed 14 3 2018].

[17] CNSC, "Regulatory framework overview," CNSC, 2014. [Online]. Available: http://nuclearsafety.gc.ca/eng/acts-and-regulations/regulatory-framework/index.cfm. [Accessed 2018].

[18] Minister of Justice, "Nuclear Safety and Control Act," 2000. [Online]. Available: http://laws-lois.justice.gc.ca/eng/acts/N-28.3/page-1.html. [Accessed 06 February 2018].

[19] Minister of Justice, "Security of Canada Information Disclosure Act," 1 August 2015. [Online]. Available: http://laws-lois.justice.gc.ca/eng/acts/S-6.9/index.html. [Accessed 06 December 2024].

[20] Minister of Justice, "Transportation of Dangerous Goods," 1992. [Online]. Available: http://laws-lois.justice.gc.ca/eng/acts/T-19.01/index.html. [Accessed 06 February 2018].

[21] CNSC, "List of Regulations," CNSC, 2016. [Online]. Available: http://nuclearsafety.gc.ca/eng/acts-and-regulations/regulations/index.cfm. [Accessed 06 February 2018].

[22] "Administrative Monetary Penalties Regulations (Canadian Nuclear Safety Commission)," Government of Canada, 2013. [Online]. Available: http://canadagazette.gc.ca/rp-pr/p2/2013/2013-07-03/html/sor-dors139-eng.html. [Accessed March 2018].

[23] CNSC, "Regulatory Documents," CNSC, 2018. [Online]. Available: http://nuclearsafety.gc.ca/eng/acts-and-regulations/regulatory-documents/index.cfm. [Accessed 06 February 2018].

[24] Altigator, "Altigator Unmanned Solutions," Altigator, [Online]. Available: https://altigator.com/drone-uav-uas-rpa-or-rpas/. [Accessed 17 May 2019].

[25] "MQ-1 Predator Unmanned Aerial Vehicle UAV Drone," Army Recognition, 27 September 2018. [Online]. Available: https://www.armyrecognition.com/us_american_unmanned_aerial_ground_vehicle_uk/mq-1_predator_unmanned_aerial_vehicle_uav_data_sheet_specifications_information_description_uk.html. [Accessed 28 June 2019].

[26] F. Corrigan, "How Do Drones Work And What Is Drone Technology," DroneZon, 26 June 2019. [Online]. Available: https://www.dronezon.com/learn-about-drones-quadcopters/what-is-drone-technology-or-how-does-drone-technology-work/. [Accessed 28 June 2019].

[27] Z. Blackwood and G. S. King, "Vertical Take-off Unmanned Aerial Vehicle with Forward Flight Transition," *The West Indian Journal of Engineering,* vol. 40, no. 2, pp. 62-71, 2018.

[28] S.-C. Choi, N.-M. Sung, J.-H. Park, I.-Y. Ahn and J. Kim, "Enabling drone as a service: OneM2M-based UAV/drone management system," in *Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*, Milan, 2017.

[29] Y.-T. Huang, H.-h. Chu, Y.-H. Ho and L.-J. Chen, "Adaptive Drone Sensing with Always Return-To-Home Guaranteed," in *1st International Workshop on Experiences with the Design and Implementation of Smart Objects*, Paris, 2015.

[30] N. Gageik, T. Müller and S. Montenegro, "Obstacle detection and collision avoidance using ultrasonic distance sensors for an autonomous quadrocopter," University of Würzburg, Aerospace Information Technology, Würzburg, 2012.

[31] N. Gageik, P. Benz and S. Montenegro, "Obstacle Detection and Collision Avoidance for a UAV With Complementary Low-Cost Sensors," *IEEE Access,* vol. 3, pp. 599 - 609, 2015.

[32] M. Gasparovic and L. Jurjevic, "Gimbal Influence on the Stability of Exterior Orientation Parameters of UAV Acquired Images," *Sensors,* vol. 17, no. 2, p. 401, 2017.

[33] F. Corrigan, "Drone Gyro Stabilization, IMU And Flight Controllers Explained," DroneZon, 27 August 2018. [Online]. Available: https://www.dronezon.com/learn-about-drones-quadcopters/three-and-six-axis-gyro-stabilized-drones/. [Accessed 29 June 2019].

[34] A. Bürkle, "Collaborating Miniature Drones for Surveillance and Reconnaissance," in *SPIE Security + Defence*, Berlin, 2009.

[35] K. Cho, M. Cho and J. Jeon, "Fly a Drone Safely: Evaluation of an Embodied Egocentric Drone Controller Interface," *Interacting with Computers,* vol. 29, no. 3, p. 345–354, 2017.

[36] N. Smolyanskiy and F. M. Gonzalez, "Stereoscopic First Person View System for Drone Navigation," *Frontiers in Robotics and AI,* vol. 4, p. 11, 2017.

[37] M. L. Garcia, The Design and Evaluation of Physical Protection Systems, Burlington: Elsevier Butterworth-Heinemann, 2007.

[38] A. Solodov, A. Williams, S. Al Hanaei and B. Goddard, "Analyzing the threat of unmanned aerial vehicles," *Security Journal,* vol. 31, no. 1, p. 305, 2018.

[39] S. Islam, M. Ahmed and S. Islam, "A conceptual system architecture for countering the civilian unmanned aerial vehicles threat to nuclear facilities," *International Journal of Critical Infrastructure Protection,* vol. 23, pp. 139-149, 2018.

[40] C. Baylon, "How to use drones to improve nuclear security," World Economic Forum, 22 January 2015. [Online]. Available: https://www.weforum.org/agenda/2015/01/how-to-use-drones-to-improve-nuclear-security. [Accessed 10 April 2019].

[41] P. a. K. P. Chaudhury, "Aerial Radiation Monitoring Systems, Methodology and Exercises to Demonstrate Capability for Search of Orphan Sources and Assessment of Large Area Radioactive Contamination," in *International Conference on Nuclear Security: Commitments and Actions*, Vienna, 2016.

[42] K. Boudergui, F. Carrel, T. Domenech, N. Guénard, J.-P. Poli, A. Ravet, V. Schoepff and R. Woo, "Development of a drone equipped with optimized sensors for nuclear and radiological risk characterization," in

2nd International Conference on Advancements in Nuclear Instrumentation, Measurement Methods and their Applications, Ghent, Belgium, 2011.

[43] Electronic Privacy Information Center, "Drones and Aerial Surveillance," Electronic Privacy Information Center, [Online]. Available: https://epic.org/issues/surveillance-oversight/aerial-surveillance/. [Accessed 05 2023].

[44] B. Rao, A. G. Gopi and R. Maione, "The societal impact of commercial drones," *Technology in Society,* vol. 45, pp. 83-90, 2016.

[45] T. Mesar, A. Lessig and D. R. King, "Use of Drone Technology for Delivery of Medical Supplies During Prolonged Field Care," *Journal of Special Operations Medicine,* vol. 18, no. 4, pp. 34-35, 2018.

[46] "Drones for Search and Rescue Operations," Flytnow, 04 2023. [Online]. Available: https://www.flytnow.com/blog/drones-for-search-rescue#:~:text=%E2%80%8D-,Q%3A%20What%20are%20the%20benefits%20of%20drones%20in%20search%20and,the%20missing%20person%20in%20time.. [Accessed 05 2023].

[47] G. Hilson, "The expanding roles of emergency drones for disaster management," Verizon, [Online]. Available: https://www.verizon.com/business/resources/articles/s/the-role-of-emergency-drones-in-disaster-management/. [Accessed 05 2023].

[48] Schnee, Brian, "Oregon used drones the most in 2018 on federal wildfires," KATU, 05 2019. [Online]. Available: https://katu.com/news/local/oregon-used-drones-the-most-in-2018-on-federal-wildfires. [Accessed 05 2023].

[49] "2018 Pacific Northwest Wildland Fire Season Summary of key events and issues," Bureau of Land Management Oregon and Washington, USDA Forest Service - Region 6 Oregon, Washington, Alaska, 2019.

[50] B. Bull, "Drones with incendiary ‘ping pong balls’ help crews fight fires in Oregon," OPB, 09 2022. [Online]. Available: https://www.opb.org/article/2022/09/12/drones-incendiary-ping-pong-balls-help-fight-oregon-fires/. [Accessed 05 2023].

[51] A. Tabor, "At California Blazes, NASA Team Observes How Drones Fight Wildfire," NASA, 10 2021. [Online]. Available:

https://www.nasa.gov/feature/at-california-blazes-nasa-team-observes-how-drones-fight-wildfire. [Accessed 05 2023].

[52] "L3HARRIS DRONE TECHNOLOGY HELPING FIREFIGHTERS COMBAT CALIFORNIA WILDFIRES," L3Harris Technologies, 10 2020. [Online]. Available: https://www.l3harris.com/newsroom/editorial/2020/10/l3harris-drone-technology-helping-firefighters-combat-california. [Accessed 05 2023].

[53] A. Marshall, "Above Devastated Houston, Armies of Drones Prove Their Worth," Wired, 09 2017. [Online]. Available: https://www.wired.com/story/houston-recovery-drones/. [Accessed 05 2023].

[54] D. Van Hung, "Drones for Assessment of Disaster Damage and Impact - Revolutionizing Disaster Response," United Nations Development Programme, 2023. [Online]. Available: https://www.undp.org/vietnam/blog/drones-assessment-disaster-damage-and-impact-revolutionizing-disaster-response. [Accessed 2025].

[55] D. Ritchey, "Security, Robots And Drones, Oh My!," BNP Media, March 2019. [Online]. Available: http://digital.bnpmedia.com/publication/?i=570971&ver=html5&p=18#%22{\%22page\%22:18,\%22issue_id\%22:570971%22. [Accessed 14 March 2019].

[56] A. R. Jha, Theory, Design, and Applications of Unmanned Aerial Vehicles, Boca Raton: CRC Press, 2016.

[57] USDA, "Drones help make fighting fires safer, cheaper, better throughout Rocky Mountain Region," Forest Service Department of Agriculture, 11 2024. [Online]. Available: https://www.fs.usda.gov/inside-fs/delivering-mission/deliver/drones-help-make-fighting-fires-safer-cheaper-better#:~:text=The%20Oak%20Ridge%20Fire%20was,and%20within%20the%20fire's%20perimeter.. [Accessed 2025].

[58] S. Howe, "Los Angeles Fires Highlight the Promise (and Problems) of Using Drones for Firefighting," 2025. [Online]. Available: https://www.commercialuavnews.com/los-angeles-fires-highlight-the-promise-and-problems-of-using-drones-for-firefighting#:~:text=The%20current%20crisis%20in%20LA,awareness%20in%20real%2Dtime.%E2%80%9D. [Accessed 2025].

[59] "Drones For Good: wildfires," Transport Canada, 2022. [Online]. Available: https://tc.canada.ca/en/aviation/drone-safety/drone-innovation-

collaboration/video-series-drones-good/drones-good-wildfires. [Accessed 2025].

[60] M. McNabb, "Australian Drone Technology Assists in Combating Canadian Wildfires: Zombie Fires," Drone Life, 2024. [Online]. Available: https://dronelife.com/2024/08/26/australian-drone-technology-assists-in-combating-canadian-wildfires-zombie-fires/#:~:text=Advanced%20Drones%20Deployed%20to%20Detect,in%20remote%20and%20challenging%20terrains.. [Accessed 2025].

[61] "Case Study – Drones, the Law and Hurricane Harvey," 911 Security, 05 2021. [Online]. Available: https://www.911security.com/blog/case-study-drones-the-law-and-hurricane-harvey/. [Accessed 05 2023].

[62] N. Woolf and S. Gibbs, "Amazon to test drone delivery in partnership with UK government," The Guardian, 26 July 2016. [Online]. Available: https://www.theguardian.com/technology/2016/jul/25/amazon-to-test-drone-delivery-uk-government. [Accessed 01 April 2019].

[63] "Package Delivery by Drone (Part 135)," Federal Aviation Administration, 03 2023. [Online]. Available: https://www.faa.gov/uas/advanced_operations/package_delivery_drone. [Accessed 05 2023].

[64] A. Claesson, A. Bäckman, M. Ringh and e. al, "Time to Delivery of an Automated External Defibrillator Using a Drone for Simulated Out-of-Hospital Cardiac Arrests vs Emergency Medical Services," *Journal of the American Medical Association ,* vol. 317, no. 22, p. 2332–2334, 2017.

[65] U.S. Department of Homeland Security, "Privacy Impact Assessment for the United States Secret Service Counter Surveillance Division Unmanned Aircraft Systems Program Test," 2 August 2017. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/privacy-pia-usss-csduas-august2017.pdf. [Accessed 17 April 2019].

[66] P. M. M. and K. J. Hofstetter, "Application of UAVs at the Savannah River Site," in *Association for Unmanned Vehicle Systems Symposium*, Orlando, 1996.

[67] D. Lochbaum, "Drones at nuclear power plants: enemies or helpers?," Bulletin of the Atomic Scientists, 23 March 2015. [Online]. Available: https://thebulletin.org/2015/03/drones-at-nuclear-power-plants-enemies-or-helpers/. [Accessed 10 April 2019].

[68] U. Franke, "Drones in Ukraine: Four lessons for the West," European Council on Foreign Relations, 2025. [Online]. Available: https://ecfr.eu/article/drones-in-ukraine-four-lessons-for-the-west/. [Accessed 2025].

[69] M. Zafra, M. Hunder, A. Rao and S. Kiyada, "How drone combat in Ukraine is changing warfare," Reuters, 2024. [Online]. Available: https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/. [Accessed 2025].

[70] Government of Canada, "Canadian Aviation Regulations," [Online]. Available: https://laws-lois.justice.gc.ca/eng/regulations/SOR-96-433/PITIndex.html. [Accessed 2025].

[71] Transport Canada, "Canadian Aviation Regulations (SOR/96-433)," 14 May 2019. [Online]. Available: https://laws-lois.justice.gc.ca/eng/regulations/SOR-96-433/index.html. [Accessed 17 May 2019].

[72] Government of Canada, "Get permission to fly your drone outside the rules (new rules)," Government of Canada, 02 May 2019. [Online]. Available: https://www.tc.gc.ca/en/services/aviation/drone-safety/get-permission-fly-drone-outside-rules.html. [Accessed 08 May 2019].

[73] Government of Canada, "Canada Gazette, Part I, Volume 152, Number 24: GOVERNMENT NOTICES," 31 May 2018. [Online]. Available: http://www.gazette.gc.ca/rp-pr/p1/2018/2018-06-16/html/notice-avis-eng.html#ne6. [Accessed 18 April 2019].

[74] F. Corrigan, "How to Secure your drone from hackers permanently," DroneZon, 14 November 2015. [Online]. Available: https://www.dronezon.com/learn-about-drones-quadcopters/how-to-protect-your-drone-from-hackers-permanently/. [Accessed 13 July 2019].

[75] A. Holland Michel, "Counter-drone Systems," Center for the Study of the Drone at Bard College , 20 February 2018. [Online]. Available: https://dronecenter.bard.edu/files/2018/02/CSD-Counter-Drone-Systems-Report.pdf. [Accessed 13 May 2019].

[76] S. Dredge, "Developers plan interceptor drone to hunt and crash other drones," The Guardian, 15 January 2015. [Online]. Available: https://www.theguardian.com/technology/2015/jan/15/drone-hunt-crash-rapere. [Accessed 12 April 2019].

[77] K. Yang and Q. Quan, "An Autonomous Intercept Drone with Image-based Visual Servo," in *IEEE International Conference on Robotics and Automation (ICRA)*, Paris, 2020.

[78] M. Harris, "Super Bowl: experimental radar aims to stop drone drama at game," The Guardian, 28 January 2019. [Online]. Available: https://www.theguardian.com/technology/2019/jan/28/super-bowl-drones-radar-start-up-experiment. [Accessed 12 April 2019].

[79] D. Burke, "Drones flying into restricted airspace 'going to kill somebody,' says pilot," CBC, 2018. [Online]. Available: https://www.cbc.ca/news/canada/nova-scotia/drones-illegal-airports-aircraft-flying-safety-1.4842502. [Accessed 2024].

[80] V. Dodd and M. Weaver, "Heathrow drone: police investigating whether it is linked to Gatwick chaos," The Guardian, 9 January 2019. [Online]. Available: https://www.theguardian.com/uk-news/2019/jan/09/heathrow-drone-police-investigating-whether-it-is-linked-to-gatwick-chaos. [Accessed 03 April 2019].

[81] A. Davies, "Two arrested after 'hazardous drone operation' near Boston airport," BBC, 2024. [Online]. Available: https://www.bbc.com/news/articles/clyvnnj8g34o. [Accessed 2025].

[82] Press Association , "MoD removes anti-drone military hardware from Gatwick," The Guardian, 02 January 2019. [Online]. Available: https://www.theguardian.com/uk-news/2019/jan/02/mod-removes-anti-drone-military-hardware-from-gatwick. [Accessed 03 April 2019].

[83] K. Rawlinson, "Heathrow and Gatwick invest millions in anti-drone technology," The Guardian, 03 January 2019. [Online]. Available: https://www.theguardian.com/world/2019/jan/03/heathrow-and-gatwick-millions-anti-drone-technology. [Accessed 03 April 2019].

[84] M. J. Boyle, "The Race for Drones," *Orbis,* vol. 59, no. 1, pp. 76-94, 2015.

[85] J. Chong and N. Sweeney, "Civilian Drone Use in Canada," Economics, Resources, and International Affairs Division Parliamentary Information and Research Service, Ottawa, 2017.

[86] E. J. Waller, "Combined Adversary-Responder Approach to Physical Protection System Effectiveness Estimation with Stochastic Uncertainty Analysis," TUDelft, Delft, 2014.

[87] M. K. Snell, "Report on Project Action Sheet PP05 Task 3 between the U.S. Department of Energy and the Republic of Korea Ministry of

Education, Science, and Technology (MEST)," Sandia National Laboratories, Albuquerque, 2013.

[88] N. J. Chornoboy, "Determining the Effectiveness of Nuclear Security Through Computer Simulation," UOIT, Oshawa, 2015.

[89] M. G. Williams, "Canadian Maritime Law Association: Admnistrative Monetary Penalties: Practise considerations and a review of experience to date," 03 June 2010. [Online]. Available: http://www.cmla.org/papers/3%20-%20Administrative%20Monetary%20Penalties%20-%20Williams.pdf. [Accessed March 2018].

[90] "REGDOC-3.5.2, Compliance and Enforcement: Administrative Monetary Penalties," CNSC, 02 2014. [Online]. Available: http://nuclearsafety.gc.ca/eng/acts-and-regulations/regulatory-documents/published/html/regdoc3-5-2/index.cfm. [Accessed April 2018].

[91] "What We Heard Report – DIS-12-05," CNSC, 03 02 2014. [Online]. Available: http://nuclearsafety.gc.ca/eng/acts-and-regulations/consultation/completed/dis-12-05.cfm. [Accessed 03 2018].

[92] "CNSC Administrative Monetary Penalty (AMP) System Frequently Asked Questions," CNSC, 25 08 2015. [Online]. Available: http://nuclearsafety.gc.ca/eng/resources/frequently-asked-questions/administrative-monetary-penalties/index.cfm#sec1-1. [Accessed 15 03 2018].

[93] CNSC, "Regulatory actions," CNSC, 02 2018. [Online]. Available: http://nuclearsafety.gc.ca/eng/acts-and-regulations/regulatory-action/index.cfm. [Accessed 11 2018].

[94] R. Howsley, "Nuclear and Avation Security - A Comparative Analysis," in *IAEA International Conference on Physical Protection of Nuclear Material and Nuclear Facilities*, Vienna, 2017.

[95] Canadian Transportaton Agency, "Monetary Penalty Framework," [Online]. Available: https://otc-cta.gc.ca/eng/monetary-penalty-framework. [Accessed November 2024].

[96] Government of Canada, "Canada Transportation Act," 1996. [Online]. Available: http://laws-lois.justice.gc.ca/. [Accessed October 2024].

[97] Canadian Transportation Agency, "Enforcing Compliance – enforcement actions and types of violations," 01 2022. [Online]. Available: https://otc-

cta.gc.ca/eng/enforcing-compliance-enforcement-actions-and-types-violations. [Accessed 07 2023].

[98] Canada Energy Regulator, "Administrative Monetary Penalties Process Guide," Government of Canada, 16 December 2019. [Online]. Available: https://www.cer-rec.gc.ca/bts/ctrg/gnnb/dmnstrtvmntrypnlts/dmnstrtvmntrypnltsprcssgd/index-eng.html. [Accessed 30 March 2020].

[99] Canada Energy Regulator, "Administrative Monetary Penalties," Government of Canada, 16 December 2019. [Online]. Available: https://www.cer-rec.gc.ca/bts/ctrg/gnnb/dmnstrtvmntrypnlts/index-eng.html. [Accessed 30 March 2020].

[100] Canada Energy Regulator, "Administrative Monetary Penalty – Plains Midstream Canada ULC (PMC) – AMP-001-2019," Canada Energy Regulator, 28 August 2019. [Online]. Available: https://www.cer-rec.gc.ca/sftnvrnmnt/cmplnc/rprts/dmnmntrypnlty/2019/AMP-001/nv2019-01-30-eng.html. [Accessed 14 May 2020].

[101] Government of Canada, "Administrative Monetary Penalties Regulations (National Energy Board) (SOR/2013-138)," Government of Canada, 09 June 2016. [Online]. Available: https://laws-lois.justice.gc.ca/eng/regulations/SOR-2013-138/page-3.html#docCont. [Accessed 14 May 2020].

[102] Government of Canada, "Canada Consumer Product Safety Act," Government of Canada, 17 October 2018. [Online]. Available: https://laws-lois.justice.gc.ca/eng/acts/C-1.68/page-4.html#docCont. [Accessed 20 May 2020].

[103] Government of Canada, "Notices of Violation under the Canada Consumer Product Safety Act," Government of Canada, 22 Deceber 2017. [Online]. Available: https://www.canada.ca/en/health-canada/services/consumer-product-safety/legislation-guidelines/guidelines-policies/administrative-monetary-penalties-under-canada-consumer-product-safety-act.html. [Accessed 19 May 2020].

[104] Government of Canada, "Administrative Monetary Penalties (Consumer Products) Regulations," Government of Canada, 04 April 2018. [Online]. Available: https://laws-lois.justice.gc.ca/eng/regulations/SOR-2013-101/page-1.html#docCont. [Accessed 19 May 2020].

[105] U.S. Nuclear Regulatory Commission, Office of Enforcement, "NRC Enforcement Policy Revision 2020," NRC, January 2020. [Online].

Available: https://www.nrc.gov/docs/ML1935/ML19352E921.pdf. [Accessed February 2021].

[106] Nuclear Regulatory Commission, "Governing Legislation," September 2013. [Online]. Available: https://www.nrc.gov/docs/ML1327/ML13274A489.pdf#page=23. [Accessed October 2020].

[107] US NRC, "2.205 Civil penalties," February 2020. [Online]. Available: https://www.nrc.gov/reading-rm/doc-collections/cfr/part002/part002-0205.html#:~:text=%C2%A7%202.205%20Civil%20penalties.,violation%20upon%20the%20person%20charged.. [Accessed December 2020].

[108] USNRC, "NRC Enforcement Policy," 2024. [Online]. Available: https://www.nrc.gov/docs/ML2420/ML24205A249.pdf. [Accessed 2025].

[109] J. Vucicevic and E. Waller, "Consideration of Administrative Monetary Penalties in Nuclear Safety and Security," *International Journal of Nuclear Security,* 2020.

[110] J. Vucicevic and E. Waller, "Consideration of Administrative Monetary Penalties in Nuclear Security Regulation," in *INMM Annual Meeting*, Palm Desert, 2019.

[111] CNSC, "Regulatory actions," CNSC, 27 02 2020. [Online]. Available: http://nuclearsafety.gc.ca/eng/acts-and-regulations/regulatory-action/index.cfm. [Accessed 28 04 2020].

[112] CNSC, "Regulatory actions," 18 December 2024. [Online]. Available: https://www.cnsc-ccsn.gc.ca/eng/acts-and-regulations/regulatory-action/. [Accessed 2025].

[113] K. Vyas, "A Brief History of Drones: The Remote Controlled Inmanned Aerial Vehicles (UAVs)," Interesting Engineering, 29 06 2020. [Online]. Available: https://interestingengineering.com/innovation/a-brief-history-of-drones-the-remote-controlled-unmanned-aerial-vehicles-uavs. [Accessed 05 04 2023].

[114] B. Lutkevich, "Drone definition," TechTarget, 12 2021. [Online]. Available: https://www.techtarget.com/iotagenda/definition/drone. [Accessed 04 2023].

[115] I. Singh, "An inside look at Amazon's drone delivery system, flight-testing facilities," Drone DJ, 11 August 2022. [Online]. Available: https://dronedj.com/2022/08/11/amazon-drone-delivery/.

[116] Electronic Frontier Foundation, "Surveillance Drones," Electronic Frontier Foundation, [Online]. Available: https://www.eff.org/issues/surveillance-drones. [Accessed 05 2023].

[117] S. Ahrens, "The Status of Drone Technology in Security," Security Infowatch, 1 September 2021. [Online]. [Accessed January 2022].

[118] Parrot, "Anafi USA 32x zoom camera," Parrot, [Online]. Available: https://www.parrot.com/en/drones/anafi-usa/32x-zoom.

[119] DJI, "Mavic Air 2," DJI, [Online]. Available: https://www.dji.com/ca/mavic-air-2?site=brandsite&from=nav..

[120] Parrot, "Anafi USA White Paper," Parrot Drones, 2021.

[121] Parrot, "Thermal Camera," Parrot, [Online]. Available: https://www.parrot.com/en/drones/anafi-usa/thermal-camera.

[122] P. Karanja, "Follow Me and ActiveTrack on DJI Drones," DroneBlog, 2022. [Online]. Available: https://www.droneblog.com/dji-follow-me-and-activetrack/.

[123] Dronemade, "All about DJI's Active Track intelligent drone flight mode," 2021. [Online]. Available: https://www.drone-made.com/post/dji-active-track-mode. [Accessed 2022].

[124] Dronemade, "All about DJI's Point of Interest intelligent drone flight mode," 2021. [Online]. Available: https://www.drone-made.com/post/dji-point-of-interest-mode#:~:text=DJI%20uses%20the%20GPS%20built,the%20camera%20pointed%20straight%20down.. [Accessed 2022].

[125] DJI, "Matrice 300 RTK," DJI, 2022. [Online]. Available: https://www.dji.com/ca/matrice-300..

[126] DJI, "DJI Waypoints," DJI, [Online]. Available: https://www.droneblog.com/dji-waypoints/.

[127] Federal Aviation Administration, "Automatic Dependent Surveillance - Broadcast (ADS-B)," [Online]. Available: https://www.faa.gov/about/office_org/headquarters_offices/avs/offices/afx/afs/afs400/afs410/ads-b#:~:text=ADS%2DB%20Out%20works%20by,other%20aircraft%2C%20once%20per%20second.. [Accessed 06 2023].

[128] "Wireless charging for drones," Powermat, 2022. [Online]. Available: https://powermat.com/wireless-charging-technology-for-drones/. [Accessed 2022].

[129] Parrot, "Flight ready in 55 sec," Parrot, [Online]. Available: https://www.parrot.com/en/drones/anafi-usa/rugged-easily-deployable.

[130] DJI, "DJI Specs," 2022. [Online]. Available: https://www.dji.com/ca/phantom-4-pro-v2/specs.

[131] DJI, "Specs," DJI, 2022. [Online]. Available: https://www.dji.com/ca/dji-fpv/specs.

[132] International Electrotechnical Commission, "IP Ratings," International Electrotechnical Commission, [Online]. Available: https://www.iec.ch/ip-ratings. [Accessed 05 2023].

[133] J. Carter, "Drones With the Longest Flight Times," RC Hobby Review, [Online]. Available: https://rchobbyreview.com/drones-longest-flight-times/. [Accessed 29 April 2019].

[134] Drone Omega, "How Fast do Drones Fly," 2020. [Online]. Available: https://www.droneomega.com/how-fast-do-drones-fly/.

[135] Federal Aviation Administration, "Fact Sheet – Small Unmanned Aircraft Systems (UAS) Regulations (Part 107)," Federal Aviation Administration, 06 10 2020. [Online]. Available: https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=22615. [Accessed 01 07 2021].

[136] Terradyne, "Terradyne Specs," Terradyne, 2017. [Online]. Available: http://www.terradyneinc.com/specs.html. [Accessed 01 07 2021].

[137] C. Fleming, "Remote Drone Dispatch: Law Enforcement's Future?," California Commission on Peace Officer Standards and Training, 2019. [Online]. Available: https://www.policechiefmagazine.org/remote-drone-dispatch/. [Accessed 24 09 2021].

[138] Axis, "Amazon," [Online]. Available: https://www.amazon.ca/s?i=electronics&bbn=677230011&rh=n%3A677230011%2Cp_4%3AAxis&dc&qid=1675956665&ref=sr_ex_p_36_0&ds=v1%3ALYR3E9RyLdMiq9Oix2MojcBPZ6DqOR1N35GrkHcZ%2BLk. [Accessed 2023].

[139] M. Patrick, "Design guide to powering tethered UAVs," Mouser Electronics, 2020. [Online]. Available:

https://www.electronicspecifier.com/industries/robotics/design-guide-to-powering-tethered-uavs. [Accessed 2025].

[140] "IP Waterproof Ratings," SwellProUK, 2024. [Online]. Available: https://swellpro-uk.co.uk/blogs/news/ip-waterproof-ratings#:~:text=Fly%20confidently%2C%20capture%20breathtaking%20moments,take%20off%20from%20the%20water.. [Accessed 2024].

[141] R. Mogavero, "4 Reasons Why U.S. Nuclear Power Plants are Safe from Drones," *Nuclear Enegry Institute,* 6 August 2018.

[142] "10 Counter-Drone Technologies To Detect And Stop Drones Today," Robin Radar Systems, 18 June 2022. [Online]. Available: https://www.robinradar.com/press/blog/10-counter-drone-technologies-to-detect-and-stop-drones-today.

[143] "DJI Air 2S - Drone Quadcopter UAV with 3-Axis Gimbal Camera, 5.4K Video, 1-Inch CMOS Sensor, 4 Directions of Obstacle Sensing, 31-Min Flight Time, Max 7.5-Mile Video Transmission, MasterShots, Gray," Amazon, 2022. [Online]. Available: https://www.amazon.ca/dp/B08Z3DYBMC?asc_campaign=&asc_refurl=https%3A%2F%2Fwww.wired.com%2Fgallery%2Fbest-drones&asc_source=&ascsubtag=5dea76ae7907ac0008b8aff8&linkCode=gs2&tag=wiredcanada-20&th=1. [Accessed 2022].

[144] "DJI Grey Mavic 2 Pro Drone Quadcopter with 4K Hasselblad Camera HDR Video UAV Adjustable Aperture 20MP 1" CMOS Sensor," Amazon, 2022. [Online]. Available: https://www.amazon.ca/dp/B07GSVXHCC?ref=emc_p_m_5_i&th=1. [Accessed 2022].

[145] "DJI Mavic Air 2 - Drone Quadcopter UAV with 48MP Camera 4K Video 8K Hyperlapse 1/2" CMOS Sensor 3-Axis Gimbal 34min Flight Time ActiveTrack 3.0 Ocusync 2.0, Gray," Amazon, 2022. [Online]. Available: https://www.amazon.ca/dp/B086X7QKHD?ref=emc_p_m_5_i&th=1. [Accessed 2022].

[146] "DJI Mavic 2 Zoom - Drone Quadcopter UAV with Optical Zoom Camera 3-Axis Gimbal 4K Video 12MP 1/2.3" CMOS Sensor, up to 48mph, Gray," Amazon, 2022. [Online]. Available: https://www.amazon.ca/dp/B07GD9XY6J/ref=emc_b_5_t?th=1. [Accessed 2022].

[147] "ANAFI Ai Available in January: First 4G-Connected UAV," Drone life, 2021. [Online]. Available: https://dronelife.com/2021/12/11/anafi-ai-

available-in-january-first-4g-connected-uav/#:~:text=Leading%20European%20drone%20company%20Parrot,available%20from%20Parrot's%20leading%20resellers.. [Accessed 2022].

[148] "Parrot Launches $7,000 Anafi USA Drone for Industry Customers," PCMag, 2020. [Online]. Available: https://www.pcmag.com/news/parrot-launches-7000-anafi-usa-drone-for-industry-customers#:~:text=It's%20built%20to%20fly%20in,priced%20at%20a%20staggering%20%247%2C000. [Accessed 2022].

[149] DJI, "DJI Shop Canada," DJI, 2023. [Online]. Available: https://store.djishopcanada.com/collections/dji-fpv.

[150] "Public sector salary disclosure," Government of Ontario, 2021. [Online]. Available: https://www.ontario.ca/page/public-sector-salary-disclosure#section-1. [Accessed 2022].

[151] C. Hatch, "Modeling physical security can help lower costs for nuclear power plants," Nuclear Newswire, 2024. [Online]. Available: https://www.ans.org/news/article-6302/modeling-physical-security-can-help-lower-costs-for-nuclear-power-plants/#:~:text=The%20Nuclear%20Regulatory%20Commission%20requires,workforce%20at%20many%20power%20plants..

APPENDIX A: AMP SURVEY

TITLE OF THE RESEARCH STUDY: ADMINISTRATIVE MONETARY PENALTIES IN NUCLEAR SECURITY

CONSENT FORM:

You are invited to participate in a research study entitled Administrative Monetary Penalties in Nuclear Security. This study has been reviewed the University of Ontario Institute of Technology Research Ethics Board 15003 and originally approved on October 26th, 2018.
Please read this consent form carefully, and feel free to ask the Researcher any questions that you might have about the study. If you have any questions about your rights as a participant in this study, please contact the Research Ethics Coordinator at 905 721 8668 ext. 3693 or researchethics@uoit.ca.

Researcher: Jelena Vucicevic
Principal Investigator and Faculty Supervisor: Ed Waller
Departmental and institutional affiliation: Faculty of Energy Systems and Nuclear Science, University of Ontario Institute of Technology
Contact email: jelena.vucicevic@uoit.ca, ed.waller@uoit.ca

PURPOSE
This is a research project being conducted by Jelena Vucicevic, a student at The University of Ontario Institute of Technology (UOIT). It should take approximately 10 – 15 minutes to complete. The purpose of this study is to increase the understanding of AMP imposed by Canadian Nuclear Safety Commission, and to inspect the effects of potential changes in the policy on human behavior.
Your participation in this questionnaire is voluntary. You may refuse to take part in the research at any time without consequence. The data will not be saved. You are free to decline to answer any particular question you do not wish to answer for any reason.

POTENTIAL BENEFITS
You will receive no direct benefits from participating in this research study. However, this study might help you to understand AMPs which are part of rules and regulations imposed by CNSC. Your responses may help us learn more about AMPs and their effects on behavior.

POTENTIAL RISKS OR DISCOMFORT
There are no foreseeable risks involved in participating in this study other than those encountered in day-to-day life.

STORAGE OF DATA

The survey and the answers will be stored in a locked cabinet. Only researchers will have access to this cabinet. After the conclusion of the study (2021/09/01) all the data will be destroyed.

CONFIDENTIALITY

The survey does not require identifying information such as your name or email address. Therefore, your responses will remain anonymous. No one will be able to identify you or your answers, and no one will know whether or not you participated in the study. Your privacy shall be respected. No information about your identity will be shared or published without your permission, unless required by law. Confidentiality will be provided to the fullest extent possible by law, professional practice, and ethical codes of conduct. Please note that confidentiality cannot be guaranteed while data are in transit over the Internet.

RIGHT TO WITHDRAW:

Your participation is voluntary, and you can answer only those questions that you are comfortable with answering. The information that is shared will be held in strict confidence and discussed only with the research team. You can withdraw from the survey at any moment without consequences. You will be given information that is relevant to your decision to continue or withdraw from participation. If you withdraw from the research project at any time, any data or human biological materials that you have contributed will be removed from the study and you need not offer any reason for doing making this request. However it may not be feasible to remove your data after the survey is added to a data pool since the survey is anonymous.

CONFLICT OF INTEREST

There are no real or perceived conflicts of interest in this study.

COMPENSATION

Participants will not receive any compensation for their participation.

DEBRIEFING AND DISSEMINATION OF RESULTS

The results of the study will be published in a paper. If you wish to receive these results and to be informed about the paper publication please contact the researcher at jelena.vucicevic@uoit.ca

PARTICIPANT CONCERNS AND REPORTING

If you have any questions concerning the research study or experience any discomfort related to the study, please contact the researcher Jelena Vucicevic at jelena.vucicevic@uoit.ca or Ed Waller at ed.waller@uoit.ca. Any questions regarding your rights as a participant, complaints or adverse events may be addressed to Research Ethics Board through the Research Ethics Coordinator – researchethics@uoit.ca or 905.721.8668 x. 3693.

By consenting, you do not waive any rights to legal recourse in the event of research-related harm.

CONSENT TO PARTICIPATE

1. I have read the consent form to the participant they have indicated that he/she understands the study being described.
2. The participant has had an opportunity to ask questions and these questions have been answered. The participant is free to ask questions about the study in the future.
3. The participant freely consents to participate in the research study, understanding that he/she may discontinue participation at any time without penalty. A physical/digital Consent Form has been made available to him/her.

____

____

(Name or identifier of Participant) (Date)

____

(Signature of Researcher)

AMP SURVEY

Please check the appropriate box:

I am from: Industry ☐ Academia ☐

Explanation:

The current policy of the Canadian Nuclear Safety Commission (CNSC) is to penalize any non-compliance with licences defined by the Nuclear Safety and Control Act (NSCA). Administrative Monetary Penalties (AMP) are imposed by the regulator, without court involvement for the violation of a regulatory requirement. AMP prescribes a minimal penalty of $300 for individuals or $1000 for corporations and up to $25000 for individuals or $100000 for corporations for severe misconducts. In addition to the monetary penalty the incident is noted on the individual's or corporation's compliance history, which will affect them negatively in future violations.

In some questions instruction will be given that the regulations are changed and there is no minimal penalty ($0 minimal penalty for individuals and corporations). Have this in mind when answering the questions. In every question it will be emphasised if you should answer according to the existing regulations or changed where minimal penalty is $0. The goal of the survey is to discover if the changes in regulation will change the decision made in similar situations.

Questions:

1. You are working in a nuclear facility, your task includes handling radioactive sources. One day you finished work and left the facility without properly securing these sources (did not lock them). Knowing that you might face a penalty **(current regulation)** will you:
    a. Come back and secure the sources without telling anyone, as to avoid the fine
    b. Come back, secure the sources and call the CNSC to report the non-compliance with the licence knowing you will be fined
    c. No one is in that area in the facility at this time, so you will leave it as is and come back tomorrow morning to lock it
2. In the same scenario as in question #1, if the regulation **were changed** so that you might face lower or no penalty, your answer will be:
    a. Come back and secure the sources without telling anyone, as to avoid the fine
    b. Come back, secure the sources and call the CNSC to report the non-compliance with the licence knowing you will be fined
    c. No one is in that area in the facility at this time, so you will leave it as is and come back tomorrow morning to lock it

3. Under the current law, you are required to report any non-compliance with the licence. There will be a monetary penalty and the incident will be noted on your compliance history, which will affect you negatively in future violations.
   Would you report your non-compliance (misconduct) under the current law? If you do not report your non-compliance it might be discovered by inspection, or it might stay undiscovered, and you avoid the penalty and the bad record.
   a. Yes
   b. No
4. What would your answer to the question #3 be if by self-reporting you would risk receiving monetary penalty, but no negative points on your compliance history?
   a. Yes
   b. No
5. What would your answer to question #3 be if by self-reporting you would not receive a monetary penalty and there will be no negative effect on your compliance history, but if the misconduct was discovered by inspection you will receive both monetary penalty and a negative compliance history?
   a. Yes
   b. No
6. What would your answer to question #3 be if by self-reporting you would risk receiving a monetary penalty, and you would have “good behaviour” noted on your compliance history, which might exempt you from monetary penalties in the future?
   a. Yes
   b. No
7. Current AMP policy prescribes minimal penalties for every misconduct even if the offender self-identified the mistake. Do you think that the change of this policy (removing the minimal penalty so that if the misconduct is not severe there might be no monetary penalty) would encourage offenders to self-report a misconduct?
   a. Yes
   b. No